COMPUTATIONAL ASPECTS OF THE COMBINATORIAL NULLSTELLENSATZ METHOD VIA A POLYNOMIAL APPROACH TO MATRIX AND HYPERMATRIX ALGEBRA

BY EDINAH K. GNANG

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Computer Science

Written under the direction of

Ahmed Elgammal, Vladimir Retakh

and approved by

_____

_____

_____

_____

New Brunswick, New Jersey

October, 2013

ABSTRACT OF THE DISSERTATION

COMPUTATIONAL ASPECTS OF THE COMBINATORIAL NULLSTELLENSATZ METHOD VIA A POLYNOMIAL APPROACH TO MATRIX AND HYPERMATRIX ALGEBRA

by EDINAH K. GNANG

Dissertation Director: Ahmed Elgammal, Vladimir Retakh

We discuss a polynomial encoding which provides a unified framework for discussing the algebra and the spectral analysis of matrices and hypermatrices. In addition to describing some algorithms for performing orthogonalization and spectral analysis of hypermatrices, we discuss some computational aspects, more specifically the important role of symmetries in Alon's Combinatorial Nullstellensatz method for solving combinatorial problems.

Acknowledgements

I am incredibly grateful to my advisors Ahmed Elgammal, Vladimir Retakh, for their guidance and encouragement. Their influence on me has been tremendous, and I could not ask for better dissertation mentors. I am indebted to Doron Zeilberger and Mario Szegedy for numerous insightful comments and suggestions which have improved this work significantly. I am also grateful to Michael Saks, Henry Cohn, Eileen Kowler, William Massey, Lek-Heng Lim, Neil Sloane and Avi Wigderson for their valuable time and assistance. I very much appreciate each of their contributions to this work. I owe many thanks to fellow graduate students Eric Rowland, Vidit Nanda, Abdul Basit and Jules Lambert for their careful reading, comments, and patience during the writing process. Research conducted in this thesis was supported in part by the NSF grant NSF-DGE-0549115

Dedication

To my wife Jeanine Sedjro and two children Joy and Raphael Sedjro-Gnang.

Table of Contents

List of Figures

Chapter 1
Introduction

It is well-known that systems of polynomial equations over algebraically-closed fields provide a concise encoding for classical NP-hard problems such as subgraph isomorphism. In [1], Alon presents a general unified algebraic framework for establishing the existence of solutions to numerous problems in combinatorics and combinatorial number theory. In the concluding remarks of [1] Alon points out that the proofs presented in [1] are based on algebraic non-constructive arguments and hence supply no efficient algorithm for solving the corresponding algorithmic problems. Alon then proceeds to raise the fundamental question of whether or not it is possible to modify such arguments so as to deduce from them efficient algorithms for solving the corresponding algorithmic problems. Following up on the problem raised by Alon, we remark that it is well-known that combinatorial problems, formulated as systems of polynomial constraints, can be solved using standard tools in computational algebra such as Grobner basis [4, 12]. Nevertheless, it has been experimentally demonstrated that current Grobner bases implementations often cannot directly solve polynomial systems with large a number of equations. Furthermore the precise analysis of the performance of Grobner bases algorithms in relation to special instances of combinatorial problems has not yet been established. In the subsequent work [47, 45, 46, 50] the authors follow up on the problem raised by Alon in [1] and propose the Nullstellensatz Linear Algebra

algorithm (NulLA), which relies on the experimentally-observed low degrees of Hilbert's Nullstellensatz certificates for polynomial encodings of combinatorial problems.

The research program developed in [47, 45, 46, 50] follows up on connections between Hilbert's Nullstellensatz [31] and complexity theory as first observed by Lovasz in [48]. Margulies establishes in [50] that given a graph G, where $\alpha(G)$ denotes the size of the largest independent set in G. The minimum-degree Nullstellensatz certificate (associated with the Lovasz encoding) for the non-existence of an independent set of size greater than $\alpha(G)$ must have degree equal to $\alpha(G)$, and contains at least one monomial per independent set in G. In [47, 45, 46, 50] the authors, investigate how algebraic formulations enable us to crucially exploit sparsity of typical algebraic encoding of NP-hard combinatorial problems. The authors also point out that the typical combinatorial problems have many non-trivial symmetries, which might be exploited to improve the performance of algebraic solvers. The important role of symmetries for solving combinatorial problems is well established in the literature [64, 34]. We show here that the order of magnitudes of the symmetries of the algebraic constraints crucially determines the performance of algorithms naturally suggested by Alon's Combinatorial Nullstellensatz arguments. We further show how the Combinatorial Nullstellensatz method provides a natural framework for attenuating the hardness of combinatorial problems by exploiting tradeoffs between the size of the algebraic certificates and the success probability for randomized algorithms.

Having used polynomials to both encode combinatorial problems and design combinatorial algorithms, we proceed to show that polynomials also yield

a unified framework for discussing the algebra and the spectral analysis of matrices and hypermatrices. The spectral theory of hypermatrices is an important part of numerical multi-linear algebra [36, 63, 68]. While it is likely that ideas of eigenvalues of hypermatrices had been raised earlier, it was in 2005 that Lim in [42] and Qi in [57] initiated a tremendous expansion and intensification of mathematical research on the topic of hypermatrix spectral analysis. In these papers, Lim and Qi independently defined eigenvalues and eigenvectors of real symmetric tensors and explored their usefulness in determining positive definiteness of even-degree multivariate forms. These works extend the classical concept of eigenvalues and eigenvectors of square matrices originally formulated by Joseph Louis Lagrange in 1762. Spectral methods also constitute an important part of numerical multi-linear algebra and have found applications in the field of automatic control, statistical data analysis, optimization, magnetic resonance imaging, solid mechanics, quantum physics, higher order Markov chains, spectral hypergraph theory, Finsler geometry, etc. We further note that generalizations of concepts arising from linear algebra have been investigated quite extensively in the literature. Cayley in [9] instigated investigations on hyperdeterminants generalizing the matrix determinants. Gelfand, Kapranov, and Zelevinsky followed up on Cayley's work on hyperdeterminants by relating hyperdeterminants to X-discriminants in their classical book [18]. Their work has stimulated many research directions including recent approaches for generalizing the concept of eigenvalue and eigenvectors discussed by Qi in[56, 54] , Lim in[41], Cartwright and Sturmfels [13].

An alternative generalization of matrix algebra was also proposed by Mesner and Bhattacharya in [51, 52]. The authors proposed a generalization of the classical association scheme to higher dimensions called association schemes

on n-tuples. In particular for triples they describe the corresponding ternary, non-associative algebra, which naturally generalizes the Bose-Mesner algebra [5]. They further deduce from the generalization a ternary third order hypermatrix algebra in addition to natural definitions for identity pairs and inverse pairs. In [3] P. Bhattacharya develops a new 3-D transform generalizing the Fourier transform using their proposed ternary third order hypermatrix algebra and the concept of inverse pairs. In the same work Bhattacharya raises the fundamental problem of formulating a mathematical theory for the spectral analysis of third order hypermatrices which is consistent with their proposed ternary algebra. We follow up on this line of research and propose here a spectral framework by generalizing to hypermatrices the notion of unitarity. We also formulate a weak version of the spectral theorem and describe algorithms performing weak spectral decomposition of hypermatrices. Finally, we show how the strong version of the spectral theorem for matrices and hypermatrices can be reduced to the classical Brower fixed point theorem.

1.1 Thesis organization.

The thesis is organized as follows. Chapter 2 describes the basic mathematical background used throughout the work. Chapter 3 reviews the third order hypermatrix algebra proposed as a generalization of matrix algebra, and introduces new orthogonalization procedures for matrices and hypermatrices. Chapter 4 provides a detail account of the polynomial algebra framework, which simultaneously encompasses the algebra of matrices and hypermatrices. Chapter 5 investigates the weak and strong formulation of the spectral theorem as well as describing algorithmic frameworks for spectrally analyzing hypermatrices. Finally, chapter 6 discusses computational aspect of Alon's

Combinatorial Nullstellensatz method and discusses the role of symmetries in the analysis of performance of algorithms deduced from Alon's Combinatorial Nullstellensatz argument. In addition chapter 6 also discusses the combinatorial hardness attenuation framework.

Chapter 2
Background

2.1 Fields and rings

A subset of the complex numbers is called a *field* if it is closed under the four arithmetic operations, that is, if the addition, difference, product, and quotient (aside from division by zero) of any two elements (not necessarily distinct) of the field is again in the field.[1]

Roughly speaking, a *ring* is an algebraic structure that has most but not necessarily all, of the properties of a field. In particular the requirements for the product operation are less strict. The most important relaxation is that nonzero elements of a ring are not required to have multiplicative inverses.

Let us use the conventional notation and write $\mathbb{Q}[x]$ for the set of polynomials in the variable x with rational coefficients. More generally we will sometimes consider $\mathbb{C}[x_0, \cdots, x_{n-1}]$ (also more conveniently noted as $\mathbb{C}[\mathbf{x}]$) to denote the set of polynomials in the variables $\{x_k\}_{0 \leq k < n}$ with coefficients from the field of complex numbers $\mathbb{C}$. Clearly the set $\mathbb{C}[x]$ is closed under addition, substraction and multiplication of its elements, consequently $\mathbb{C}[x]$ forms a ring, but not a field.

---

[1] The notion of a field is usually defined in greater generality to include sets that are not subsets of the complex numbers. However, for our purposes the definition given here will suffice.

2.2 Quotient rings

Let R be an arbitrary commutative ring and let f, g denote two polynomials in $R[x]$ with $f \neq 0$. Let us further assume that the leading coefficient of f is a unit in R. Then by the polynomial division theorem, there is a unique pair of polynomials $(p, q) \in (R[x])^2$ where q corresponds to the quotient and r to the remainder such that $deg(r) < deg(f)$ and most importantly

$$g = f\,q + r\,. \tag{2.1}$$

We say that g is congruent to r modulo f and more succinctly written

$$g \equiv r \mod f. \tag{2.2}$$

Furthermore, the *quotient ring* $R[x]/f$ corresponds to the set of remainders resulting from dividing elements of $R[x]$ by f. In particular we have that

$$\forall g(x) \in \mathbb{C}[x]\,, \text{ and } a \in \mathbb{C}, \quad g(x) \equiv g(a) \mod (x-a)\,, \tag{2.3}$$

so that the set of evaluations of elements in $\mathbb{C}[x]$ at an arbitrary $a \in \mathbb{C}$ corresponds to the quotient ring $\mathbb{C}[x]/(x-a)$.

2.3 Reviewing the Lagrange interpolation

Consider the sets $\{(x_k, y_k)\}_{0 \leq k < n} \subset \mathbb{C} \times \mathbb{C}$ such that $x_i \neq x_j$ for $i \neq j$, and consider the corresponding map prescribed by

$$\forall\ 0 \leq k < n, \quad x_k \to y_k. \tag{2.4}$$

Such maps can be described by the following minimal degree polynomial f using the well known Lagrange interpolation formula

$$f(z) = \sum_{0 \leq k < n} y_k \prod_{0 \leq t \neq k < n} \left(\frac{z - x_t}{x_k - x_t} \right) \tag{2.5}$$

and hence by construction we have

$$\forall\, 0 \leq k < n, \quad f\left(x_k\right) = y_k, \tag{2.6}$$

or alternatively

$$\forall\, 0 \leq k < n, \quad f\left(z\right) \equiv y_k \mod \left(z - x_k\right). \tag{2.7}$$

In particular, a single-dimensional array can be encoded as a map of the form

$$\forall\, 0 \leq k < n, \quad k \to y_k,$$

where y_k corresponds to the k-th entry of the array, and the pre-image set in the map corresponds to the indexing set. For algebraic convenience, we shall often prefer roots of unity, as our default indexing set and we consider maps of the form

$$\forall\, 0 \leq k < n, \quad \left(e^{\frac{2\pi i}{n}}\right)^k \to y_k.$$

2.4 The Hadamard product

The Hadamard product of two given column vectors $\mathbf{a}, \mathbf{b} \in \mathbb{C}^{n\times 1}$ noted $\mathbf{a} \star \mathbf{b}$, corresponds to a column vector of the same dimensions whose entries correspond to the product of the corresponding entries of $\mathbf{a}$, and $\mathbf{b}$; we write

$$k - \text{th entry of } \mathbf{a} \star \mathbf{b} \text{ is } a_k b_k. \tag{2.8}$$

Let us recall here the familiar notation used for the vector product of $\mathbf{a}, \mathbf{b} \in \mathbb{C}^{n\times 1}$ with background matrix the $n \times n$ matrix $\mathbf{M}$. We write

$$\left\langle \mathbf{a}, \mathbf{b} \right\rangle_{\mathbf{M}} := \sum_{0 \leq k_0, k_1 < n} a_{k_0} m_{k_0,k_1} b_{k_1}, \tag{2.9}$$

in particular it follows that

$$\left\langle \mathbf{a}, \mathbf{b} \right\rangle := \left\langle \mathbf{a}, \mathbf{b} \right\rangle_{\mathbf{I}} = \sum_{0 \leq k < n} a_k b_k \tag{2.10}$$

and hence the inner-product of $\mathbf{a}$ and $\mathbf{b}$ can be expressed as

$$\left\langle \mathbf{a},\, \overline{\mathbf{b}} \right\rangle. \tag{2.11}$$

Furthermore we have

$$\mathbf{a} \star \left(\sum_{0 \leq t < m} \mathbf{b}_t \right) = \sum_{0 \leq t < m} \mathbf{a} \star \mathbf{b}_t, \tag{2.12}$$

and

$$\langle \mathbf{1}_{n\times 1},\, \mathbf{a} \star \mathbf{b} \rangle = \langle \mathbf{a},\, \mathbf{b} \rangle = \langle \mathbf{a} \star \mathbf{b},\, \mathbf{1}_{n\times 1} \rangle \tag{2.13}$$

finally it shall be convenient to adopt the notation convention

$$\mathbf{a}^{\star^{\alpha}} := \left((a_k)^{\alpha} \right)_{0 \leq k < n} \tag{2.14}$$

and for a set of vectors $\left\{ \mathbf{v}_j \right\}_{0 \leq j < n} \subset \mathbb{C}^{n\times 1}$ we have

$$\left(\bigstar_{0 \leq j < n} \mathbf{v}_j \right) := \mathbf{v}_0 \star \cdots \star \mathbf{v}_{n-1} \tag{2.15}$$

2.5 Quick review of basic properties of roots of unity

We recall that the n-th roots of unity are solutions to the equations

$$x^n - 1 = 0 \tag{2.16}$$

its solutions are easily obtained by rewriting the equation above as

$$\begin{aligned} &\forall\, k \in \mathbb{Z}, \quad x^n = e^{2\pi i\, k}, \\ &\Rightarrow x \in \left\{ \left(e^{\frac{2\pi i}{n}} \right)^k \right\}_{k \in \mathbb{Z}/n\mathbb{Z}}. \end{aligned} \tag{2.17}$$

Let ω_n the denote the primitive n-th root of unity expressed by

$$\omega_n = e^{\frac{2\pi i}{n}} \tag{2.18}$$

and

$$\Omega_n := \left\{ (\omega_n)^k \right\}_{k \in \mathbb{Z}/n\mathbb{Z}}. \tag{2.19}$$

Some of the basic properties of Ω_n include the following two facts

$$\forall\, r \in \Omega_n,\ \bar{r} = r^{-1} \tag{2.20}$$

$$\forall\, \alpha \in \mathbb{R} \text{ and } r \in \Omega_n,\ |r^{\alpha}| = 1 \tag{2.21}$$

The Discrete Fourier Transform (DFT) matrix $\mathbf{W}$ whose entries are specified as follows

$$\mathbf{W} := \left(w_{uv} = (\omega_n)^{u \cdot v} \right)_{0 \leq u,v < n} \tag{2.22}$$

is such that

$$\mathbf{W} \cdot \mathbf{W}^{\dagger} = n\, \mathbf{I} = \mathbf{W}^{\dagger} \cdot \mathbf{W}. \tag{2.23}$$

We shall often denote the set of column vectors of the DFT matrix $\mathbf{W}$ by the set $\left\{ \mathbf{w}^{\star^k} \right\}_{0 \leq k < n}$, where

$$\mathbf{w} := \left(w_k = (\omega_n)^k \right)_{0 \leq k < n}. \tag{2.24}$$

Furthermore the column vectors of $\mathbf{W}$ can be used to parametrize arbitrary hyperplanes. Given an arbitrary hyperplane $\mathcal{H}$ specified by

$$\mathcal{H} := \{ \mathbf{x} \in \mathbb{C}^n \text{ such that } \langle \mathbf{a},\, \mathbf{x} \rangle = \alpha \} \tag{2.25}$$

for some given $\mathbf{a} \in (\mathbb{C} \setminus \{0\})^{n \times 1}$. Points lying on the hyperplane $\mathcal{H}$ are parametrized by

$$\mathbf{x} = \left\{ \gamma_1, \cdots, \gamma_{n-1} \in \mathbb{C}, \quad \left(\frac{\alpha}{n}\, \mathbf{w}^{\star^0} + \sum_{0 < k < n} \gamma_k\, \mathbf{w}^{\star^k} \right) \star\, \mathbf{a}^{\star^{-1}} \right\} \tag{2.26}$$

since

$$\left\langle \mathbf{a},\, \left(\frac{\alpha}{n}\, \mathbf{w}^{\star^0} + \sum_{0 < k < n} \gamma_k\, \mathbf{w}^{\star^k} \right) \star\, \mathbf{a}^{\star^{-1}} \right\rangle = \left\langle \mathbf{w}^{\star^0},\, \left(\frac{\alpha}{n}\, \mathbf{w}^{\star^0} + \sum_{0 < k < n} \gamma_k\, \mathbf{w}^{\star^k} \right) \right\rangle$$

$$= \left(\frac{\alpha \left\| \mathbf{w}^{\star^0} \right\|_{\ell_2}^2}{n} + \sum_{0<k<n} \gamma_k \left\langle \mathbf{w}^{\star^0}, \mathbf{w}^{\star^k} \right\rangle \right) = \alpha$$

$$\Rightarrow \mathbf{x} = \left(\frac{\alpha}{n} \mathbf{w}^{\star^0} + \sum_{0<k<n} \gamma_k \mathbf{w}^{\star^k} \right) \star \mathbf{a}^{\star^{-1}} \tag{2.27}$$

consequently if for an arbitrary $f \in \mathbb{C}[\mathbf{x}]$ we have that

$$f(\mathbf{x}) = (\langle \mathbf{a}, \mathbf{x} \rangle - \alpha)\ h(\mathbf{x}) \tag{2.28}$$

then it follows that

$$\forall\, \gamma_1, \cdots, \gamma_{n-1} \in \mathbb{C}, \quad f(\mathbf{x}) \equiv 0$$

$$\mod \left\{ \mathbf{x} - \begin{pmatrix} \frac{1}{a_0} \\ \frac{1}{a_1} \\ \vdots \\ \frac{1}{a_{n-1}} \end{pmatrix} \star \left(\frac{\alpha}{n} \mathbf{w}^{\star^0} + \sum_{0<k<n} \gamma_k \mathbf{w}^{\star^k} \right) \right\} \tag{2.29}$$

in other words the restriction of the polynomial f to the hyperplane $\mathcal{H}$ is zero if the polynomial $(\langle \mathbf{a}, \mathbf{x} \rangle - \alpha)$ divides f. More succintly we write

$$(\langle \mathbf{a}, \mathbf{x} \rangle - \alpha) \mid f(x_0, \cdots, x_{n-1}). \tag{2.30}$$

Finally we note that given $f \in \mathbb{C}[\mathbf{x}]$ expressed by

$$f(\mathbf{x}) = \sum_{\left\{0 \le \langle \boldsymbol{\alpha}, \mathbf{e}_j \rangle \le d_j\right\}_{0 \le j < n}} a_{\left\{\alpha_j\right\}_{0 \le j < n}} \prod_{0 \le j < n} (x_j)^{\alpha_j} \tag{2.31}$$

we have

$$f(\mathbf{x}) \equiv$$

$$\sum_{\left\{0 \le \langle \boldsymbol{\alpha}, \mathbf{e}_j \rangle \le d_j\right\}_{0 \le j < n}} a_{\left\{\alpha_j\right\}_{0 \le j < n}} \prod_{0 \le j < n} (x_j)^{\alpha_j \mod n} \mod \left(\mathbf{x}^{\star^n} - \mathbf{w}^{\star^0} \right) \tag{2.32}$$

we shall often refer to the remainder polynomial

$$\sum_{\left\{0 \leq \left\langle \boldsymbol{\alpha}, \mathbf{e}_j \right\rangle \leq d_j\right\}_{0 \leq j < n}} a_{\left\{\alpha_j\right\}_{0 \leq j < n}} \prod_{0 \leq j < n} \left(x_j\right)^{\alpha_j} \bmod n$$

as the reduced polynomial associated with f modulo $\left(\mathbf{x}^{\star^n} - \mathbf{w}^{\star^0}\right)$ where $\mathbf{w}^{\star^0}$ denotes the first column of the DFT matrix, and hence, has all of it's entries equal to 1.

Chapter 3
Third order hypermatrix algebra

3.1 Overview of the third order hypermatrix algebra

At the center of the algebraic framework lies the definition of a ternary product operation for third order hypermatrices, which generalizes matrix multiplication. The definition was first proposed by Mesner, Battacharya in [51, 52] as a generalization of matrix multiplication. Let $\mathbf{A} = (a_{uvw})$ be a hypermatrix of dimensions $(m \times l \times p)$, $\mathbf{B} = (b_{uvw})$ a hypermatrix of dimensions $(m \times n \times l)$, and $\mathbf{C} = (c_{uvw})$ a hypermatrix of dimensions $(l \times n \times p)$. The ternary product of $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ results in a hypermatrix $\mathbf{D} = (d_{uvw})$ of dimensions $(m \times n \times p)$ which is expressed by :

$$d_{uvw} = \sum_{0 \leq k < l} a_{ukw} \cdot b_{uvk} \cdot c_{kvw} \tag{3.1}$$

There are potentially several ways of generalizing matrix multiplication and an alternative generalization is discussed in [8]. We favor the Mesner-Battacharya definition for three reasons: First, every entry of the hypermatrix $\mathbf{D} = \circ(\mathbf{A}, \mathbf{B}, \mathbf{C})$ can be thought of as correlating a row vector, a depth vector, and a column vector taken from $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ respectively. This fact is compellingly analogous to matrix multiplication as illustrated in Figure 3.1. Second, matrix multiplication becomes a special case of third order hypermatrix multiplication. Finally, the definition of hypermatrix multiplication

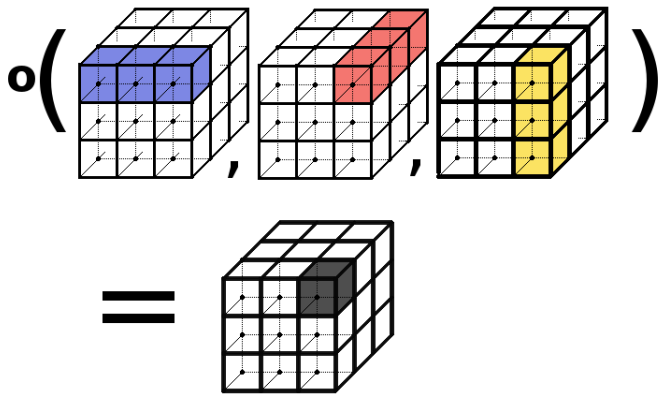

Figure 3.1: Third order hypermatrix ternary Product $\circ(\mathbf{A}, \mathbf{B}, \mathbf{C}) = \mathbf{D}$.

also suggests a generalization to the vector outer-product operation; that is, given hypermatrices **A**, **B**, and **C** of dimensions $(m \times 1 \times p)$, $(m \times n \times 1)$, and $(1 \times n \times p)$ respectively, the ternary outer-product **D**, noted $\mathbf{D} = \otimes(\mathbf{A}, \mathbf{B}, \mathbf{C})$ is an $(m \times n \times p)$ hypermatrix defined by the entry relations expressed as

$$d_{ijk} = a_{i1k} \cdot b_{ij1} \cdot c_{1jk}, \tag{3.2}$$

and depicted in Figure 3.2. Note that **A**, **B** and **C** are matrices with distinct orientations in the same way that column and row vectors have distinct orientations. Furthermore, matrix and hypermatrix multiplication can both be viewed as summations of outer-products as depicted for hypermatrices in the equation below

$$d_{uvw} = \sum_{0 \le k < l} a_{ukw} \cdot b_{uvk} \cdot c_{kvw} \Leftrightarrow \mathbf{D} = \left(\sum_{0 \le k < l} \otimes (\mathbf{A}_{\bullet,k,\bullet}, \mathbf{B}_{\bullet,\bullet,k}, \mathbf{C}_{k,\bullet,\bullet}) \right). \tag{3.3}$$

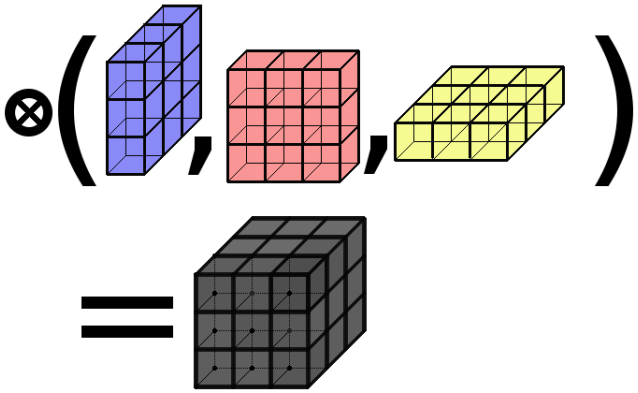

Figure 3.2: Matrix outer-product operation $\otimes(\mathbf{A},\mathbf{B},\mathbf{C}) = \mathbf{D}$.

3.2 Generalizing other fundamental matrix notions and matrix operations

Transpose of a third order hypermatrix : Given a hypermatrix $\mathbf{A} = (a_{u,v,w})$ we define its *transpose* $\mathbf{A}^T$ and its *double transpose* $\mathbf{A}^{T^2}$as follows:

$$\mathbf{A}^T = (a_{vwu})\,,\ \mathbf{A}^{T^2} \equiv \left(\mathbf{A}^T\right)^T = (a_{wuv})\,. \tag{3.4}$$

It immediately follows, from the definition of the transpose, that for all hypermatrix $\mathbf{A}$, $\left(\mathbf{A}^{T^2}\right)^T = \mathbf{A}$. Consequently, the transpose operator corresponds to a cyclic permutation of the indices of $\mathbf{A}$'s entries . Furthermore, a hypermatrix $\mathbf{A}$ is said to be symmetrical if $\mathbf{A} = \mathbf{A}^T = \mathbf{A}^{T^2}$. It follows from the definitions of the transpose and the product that by complete analogy with matrices we have :

$$[\circ(\mathbf{A},\mathbf{B},\mathbf{C})]^T = \circ\left(\mathbf{B}^T,\mathbf{C}^T,\mathbf{A}^T\right). \tag{3.5}$$

Identity pair for third order hypermatrices : Let $\mathbf{1}_{(m\times n\times p)}$ denote the hypermatrix having all of it's entries equal to one and of dimensions $(m \times n \times p)$. Recalling that $\mathbf{\Delta} = \left(\delta_{ijk}\right)$ denotes the Kronecker third order hypermatrix defined by having it's entry assigned the value one, when the corresponding three indices equal each other or zero otherwise. We define the *identity third order hypermatrix* $\mathbf{I}$ to be :

$$\mathbf{I} = \circ\left(\mathbf{1}_{(l\times l\times l)}, \mathbf{1}_{(l\times l\times l)}, \mathbf{\Delta}\right) = \circ\left(\mathbf{1}_{(l\times l\times l)}, \mathbf{1}_{(l\times l\times l)}, \left(\sum_{1\leq k\leq l} \mathbf{e}_k \otimes \mathbf{e}_k \otimes \mathbf{e}_k\right)\right) \tag{3.6}$$

The identity *hypermatrix* plays a role quite analogous to that of the identity matrix, as pointed out by Battacharya and Mesner in [3, 51, 52] that is to say that $\forall\, \mathbf{A} \in \mathbf{C}^{l\times l\times l},\ \circ\left(\mathbf{I}, \mathbf{A}, \mathbf{I}^{T^2}\right) = \mathbf{A}$.

Inverse hypermatrix pairs: By analogy to matrix inverse $\mathbf{A}^{-1}$ where for a matrix $\mathbf{A}$, $\mathbf{A}^{-1}$, is its inverse if $(\mathbf{MA})\,\mathbf{A}^{-1} = \mathbf{M}$, for any non zero matrix $\mathbf{M}$, the ordered pairs $(\mathbf{A}_1, \mathbf{A}_2)$ and $(\mathbf{B}_1, \mathbf{B}_2)$ are related by inverse relationship if for any non-zero third order hypermatrix $\mathbf{M}$ with appropriate dimensions the following identity holds

$$\mathbf{M} = \circ\left(\mathbf{B}_1 \circ \left(\mathbf{A}_1, \mathbf{M}, \mathbf{A}_2\right), \mathbf{B}_2\right). \tag{3.7}$$

Transposition of third order hypermatrices: Incidentally one may also define *transposition hypermatrices* associated with an arbitrary transposition σ of the permutation group S_n expressed by

$$\forall\, \sigma \in S_n,\ \mathbf{P}_\sigma \equiv \circ\left(\mathbf{1}_{(n\times n\times n)}, \mathbf{1}_{(n\times n\times n)}, \left(\sum_{1\leq k\leq l} \mathbf{e}_k \otimes \mathbf{e}_k \otimes \mathbf{e}_{\sigma(k)}\right)\right) \tag{3.8}$$

$$= \sum_{1 \le k \le l} \circ \left(\mathbf{1}_{(n \times n \times n)}, \mathbf{1}_{(n \times n \times n)}, \left(\mathbf{e}_k \otimes \mathbf{e}_k \otimes \mathbf{e}_{\sigma(k)} \right) \right) \tag{3.9}$$

Incidentally any permutation of the depth slices of $\mathbf{A}$ can be obtained by a finite composition of transpositions of the form

$$\circ \left(\mathbf{P}_{\sigma_n}, \cdots, \circ \left(\mathbf{P}_{\sigma_k}, \cdots, \circ \left(\mathbf{P}_{\sigma_1}, \mathbf{A}, \mathbf{P}_{\sigma_1}^{T^2} \right) \cdots, \mathbf{P}_{\sigma_k}^{T^2} \right), \cdots, \mathbf{P}_{\sigma_n}^{T^2} \right). \tag{3.10}$$

3.3 Hypermatrix orthogonality

Orthogonality plays an important role in linear algebra, however for third order hypermatrices, the notion of orthogonality induces a symmetry breaking between two equivalent matrix definitions of orthogonality. The generalization to hypermatrices of the notion of orthogonality was first proposed by Gnang, Elgammal and Retakh in [19]. The first interpretation of matrix orthogonality is associated with correlation constraints and is motivated by expressing for some $l \times l$ matrix $\mathbf{Q}$ the constraints

$$\mathbf{\Delta} = \mathbf{Q} \cdot \mathbf{Q}^T \Leftrightarrow \langle \mathbf{q}_m, \mathbf{q}_n \rangle = \left(\sum_{1 \le k \le l} q_{mk} \, q_{nk} \right) = \delta_{mn}. \tag{3.11}$$

Consequently, the corresponding correlation constraints for an $l \times l \times l$ hypermatrix $\mathbf{Q}$ is expressed by

$$\mathbf{\Delta} = \circ \left(\mathbf{Q}, \mathbf{Q}^{T^2}, \mathbf{Q}^T \right) \Leftrightarrow \langle \mathbf{q}_{mp}, \mathbf{q}_{nm}, \mathbf{q}_{pn} \rangle = \delta_{mnp}. \tag{3.12}$$

More generally we shall consider the ordered triplet of third order hypermatrices $(\mathbf{Q}, \mathbf{R}, \mathbf{S})$ to form an uncorrelated triplet if

$$\mathbf{\Delta} = \circ \left(\mathbf{Q}, \mathbf{R}, \mathbf{S} \right). \tag{3.13}$$

The second interpretation of matrix orthogonality is motivated by the *Kronecker invariance* identity, expressed for some square matrix $\mathbf{Q}$ by

$$\mathbf{\Delta} = \mathbf{Q} \cdot \mathbf{\Delta} \cdot \mathbf{Q}^T. \tag{3.14}$$

Incidentally, the corresponding Kronecker hypermatrix invariance identity is expressed by

$$\mathbf{\Delta} = \circ \left(\circ \left(\mathbf{Q}, \circ \left(\mathbf{Q}^T, \mathbf{Q}^{T^2}, \mathbf{\Delta} \right), \mathbf{Q}^{T^2} \right), \mathbf{Q}, \mathbf{Q}^T \right). \tag{3.15}$$

The Kronencker invariance identity above corresponds to the conjugation operation for some third-order transposition hypermatrix $\mathbf{Q}$. Finally, we note that while for matrices these two definitions of orthogonality are equivalent, and furthermore while transposition hypermatrices simultaneously satisfy both of these interpretations of orthogonality, in general these two definitions of orthogonality are not equivalent for third order hypermatrices, i.e.

$$\mathbf{\Delta} = \circ \left(\mathbf{Q}, \mathbf{Q}^{T^2}, \mathbf{Q}^T \right) \not\Rightarrow \circ \left(\circ \left(\mathbf{Q}, \circ \left(\mathbf{Q}^T, \mathbf{Q}^{T^2}, \mathbf{\Delta} \right), \mathbf{Q}^{T^2} \right), \mathbf{Q}, \mathbf{Q}^T \right) = \mathbf{\Delta}. \tag{3.16}$$

3.3.1 Hypermatrix orthogonalization procedures

We describe here a new matrix orthogonalization procedure which naturally extends to hypermatrices, thereby establishing the existence of $n \times n \times n$ orthogonal hypermatrices for arbitrary integer $n \geq 2$. Consider a $n \times n$ matrix $\mathbf{M}$, we seek to deduce from $\mathbf{M}$ a square matrix $\mathbf{Q}$ such that

$$0 \leq i < j < n, \quad \langle \mathbf{q}_i, \mathbf{q}_j \rangle = 0 \tag{3.17}$$

Assuming an appropriately chosen matrix $\mathbf{M}$ (i.e. whose columns $\{\mathbf{m}_i\}_{0\leq i<n}$ are linearly independent). The procedure begins by initializing the $\binom{n}{2}$ Hadamard product $\mathbf{q}_i \star \mathbf{q}_j$ as follows

$$\forall\, 0 \leq i < j < n, \quad \mathbf{q}_i \star \mathbf{q}_j = \mathbf{m}_i \star \mathbf{m}_j - \left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\, \mathbf{m}_i \star \mathbf{m}_j \right\rangle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}} \tag{3.18}$$

and entry-wise , for some particular entry k we have

$$\forall\, 0 \leq i < j < n, \quad q_i(k)\, q_j(k) = m_i(k)\, m_j(k) - n^{-\frac{1}{2}} \left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\, \mathbf{m}_i \star \mathbf{m}_j \right\rangle \tag{3.19}$$

because the entries do not interact, they can be treated independently. For entry k, consider the linear constraints:

$$\begin{aligned} &\forall,\, 0 < j < n, \quad \ln\{q_0(k)\} + \ln\{q_j(k)\} = \\ &\ln\left\{ m_0(k)\, m_j(k) - n^{-\frac{1}{2}} \left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\, \mathbf{m}_0 \star \mathbf{m}_j \right\rangle \right\} \end{aligned} \tag{3.20}$$

in addition to the constraint

$$\begin{aligned} &\sum_{0<i<j<n} c_{i,j} \left(\ln\{q_i(k)\} + \ln\{q_j(k)\} \right) = \\ &\sum_{0<i<j<n} c_{i,j} \ln\left\{ m_i(k)\, m_j(k) - \frac{\left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\, \mathbf{m}_i \star \mathbf{m}_j \right\rangle}{\sqrt{n}} \right\}. \end{aligned} \tag{3.21}$$

So that inverting the resulting symbolic matrix yields a parametrization of orthogonal matrices deduced from $\mathbf{M}$. It is furthermore relatively easy to modify the procedure described above so as deduce from $\mathbf{M}$ the nearest orthogonal matrix $\mathbf{Q}$ in the ℓ_2 norm sense. While the orthogonalization procedure described above is a variant of the well known Gram–Schmidt orthogonalization process, the main advantage of our proposed variation is the fact that the resulting set of orthogonalized column vectors is independent of the ordering of the column vectors in the original matrix.

Let us now describe the third order hypermatrix formulation of the orthogonalization procedure. We consider the indexing set

$$\mathcal{I}dx_n := \left\{ \underbrace{\binom{n}{2}}_{(i,j,j)} \cup \underbrace{\binom{n}{2}}_{(i,i,j)} \cup \underbrace{\binom{n}{3}}_{(i,j,k)} \cup \underbrace{\binom{n}{3}}_{(j,i,k)} \right\}, \left|\mathcal{I}dx_n\right| = \frac{(n-1)\,n\,(n+1)}{3}. \quad (3.22)$$

Similarly to the matrix case we start from some appropriately chosen $n \times n \times n$ third order hypermatrix $\mathbf{M}$ ($n \geq 3$), and deduce from it an orthogonal hypermatrix $\mathbf{Q}$ that is to say

$$\forall\,(i,j,k) \in \mathcal{I}dx_n, \quad \left\langle \mathbf{q}_{ik},\, \mathbf{q}_{ji},\, \mathbf{q}_{kj} \right\rangle = 0 \quad (3.23)$$

where $\mathbf{m}_{ij}$ denotes the depth vectors located at the intersection of row i and column j of the third order hypermatrix $\mathbf{M}$. We start by initializing Hadamard products as follows

$$\forall\,(i,j,k) \in \mathcal{I}dx_n, \quad \mathbf{q}_{ik} \star \mathbf{q}_{ji} \star \mathbf{q}_{kj} =$$

$$\mathbf{m}_{ik} \star \mathbf{m}_{ji} \star \mathbf{m}_{kj} - \left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\, \mathbf{m}_{ik} \star \mathbf{m}_{ji} \star \mathbf{m}_{kj} \right\rangle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}} \quad (3.24)$$

because different entry locations do not interact, they can be treated independently. Hence for an arbitrary entry t, consider the linear constraints:

$$\forall\,(i,j,k) \in \mathcal{I}dx_n, \quad \ln\left\{q_{ik}\,(t)\right\} + \ln\left\{q_{ji}\,(t)\right\} + \ln\left\{q_{kj}\,(t)\right\} =$$

$$\ln\left\{ m_{ik}\,(t)\; m_{ji}\,(t)\; m_{kj}\,(t) - n^{-\frac{1}{2}} \left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\, \mathbf{m}_{ik} \star \mathbf{m}_{ji} \star \mathbf{m}_{kj} \right\rangle \right\}, \quad (3.25)$$

we may consider a partition of the index set into two disjoint sets

$$\mathcal{I}dx_n = \mathcal{J}_n \cup \mathcal{H}_n \quad (3.26)$$

such that

$$\left|\mathcal{J}_n\right| = n^2 - 1, \quad \left|\mathcal{H}_n\right| = 3^{-1}\,(n-1)\,n\,(n+1) - n^2 + 1 \quad (3.27)$$

in addition to the linear constraints

$$\forall (i,j,k) \in \mathcal{J}_n, \quad \ln\left\{q_{ik}(t)\right\} + \ln\left\{q_{ji}(t)\right\} + \ln\left\{q_{kj}(t)\right\} =$$

$$\ln\left\{m_{ik}(t)\ m_{ji}(t)\ m_{kj}(t) - n^{-\frac{1}{2}}\left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\ \mathbf{m}_{ik} \star \mathbf{m}_{ji} \star \mathbf{m}_{kj}\right\rangle\right\}. \tag{3.28}$$

The partition should be made so as to ensure that the constraints are linearly independent and taken in conjunction with the symbolic constraint

$$\sum_{(i,j,k)\in\mathcal{H}_n} c_{ijk}\left(\ln\left\{q_{ik}(t)\right\} + \ln\left\{q_{ji}(t)\right\} + \ln\left\{q_{kj}(t)\right\}\right) =$$

$$\sum_{(i,j,k)\in\mathcal{H}_n} c_{i,j,k} \ln\left\{m_{ik}(t)\, m_{ji}(t)\, m_{kj}(t) - \left\langle \frac{\mathbf{1}_{n\times 1}}{\sqrt{n}},\ \mathbf{m}_{ik} \star \mathbf{m}_{ji} \star \mathbf{m}_{kj}\right\rangle n^{-\frac{1}{2}}\right\}. \tag{3.29}$$

So that inverting the resulting symbolic matrix yields a parametrization of orthogonal hypermatrices deduced from $\mathbf{M}$. Finally just as we suggested for matrices one can easily modify the derivation to deduces from the procedure the nearest orthogonal hypermatrix to $\mathbf{M}$.

Chapter 4

A polynomial and probabilistic approach to matrix and hypermatrix algebra

4.1 Vectors as polynomials

To the uninitiated, it is at first helpful to equate vectors with arrays, and typically the access to elements of an array is symbolized by specifying the name of the array followed by the corresponding index in brackets or in parenthesis. For instance, $a(i)$ indicates the access to the i-th element of the array a. Fortunately this convention is also used in mathematics to symbolize the evaluation of a function. Incidentally, we may think of arrays as functions defined over discrete Cartesian product sets. For algebraic convenience we will use roots of unity as default indexing set. The convenience of this choice stems from the fact that the absolute value of arbitrary powers of any roots of unity is always 1. Furthermore, the complex conjugation operation of arbitrary powers of roots of unity is an algebraic operation.

For an arbitrary field $\mathbb{F}$ and an arbitrary integer $n > 0$, $\mathbb{F}_n^x$ will denote the parametric family of polynomial rings defined by

$$\mathbb{F}_n^x := {}^{\mathbb{F}[x]}/_{(x^n-1)}. \tag{4.1}$$

In other words, $\mathbb{F}_n^x$ corresponds to the set of polynomials with coefficients from the field $\mathbb{F}$ with degree bounded above by n. Let ω_n (or simply ω when no confusion arises about the corresponding value of n) denote the primitive n-th

root of unity $e^{\frac{2\pi i}{n}}$, and Ω_n denote the multiplicative group of n-th roots of unity, hence $\Omega_n := \left\{\omega^k\right\}_{0\leq k<n}$. The fact that polynomials can be used to encode arrays indexed by roots of unity, follows from the *fundamental Lagrange invariance identity* : $\forall\, f(x) \in \mathbb{C}[x]$,

$$f(x) \equiv \sum_{r\in\Omega_n} f(r) \prod_{s\in\Omega_n\setminus\{r\}} \left(\frac{x-s}{r-s}\right) \mod (x^n-1), \tag{4.2}$$

we recall that

$$\forall\, r \in \Omega_n, \quad f(r) := f(x) \mod (x-r) \tag{4.3}$$

and the polynomial $\sum_{r\in\Omega_n} f(r) \prod_{s\in\Omega_n\setminus\{r\}} \left(\frac{x-s}{r-s}\right)$ is the unique minimal degree polynomial in $\mathbb{C}[x]$ which is congruent to $f(x)$ modulo (x^n-1).

4.1.1 Application to sorting

The *sorting problem* arises frequently in practice and will constitute the first example of a family of combinatorial problems whose resolution implicitly requires a search over permutations of n elements. Given a polynomial

$$f : \Omega_n \to \mathbb{Q}[\omega]$$

such that

$$\forall\, r \in \Omega_n, \quad f(r) = y_r \in \mathbb{Q}^+,$$

f encodes an array of positive rational numbers. By *the fundamental Lagrange invariance identity* we have

$$f(x) = \sum_{r\in\Omega_n} y_r \prod_{s\in\Omega_n\setminus\{r\}} \left(\frac{x-s}{r-s}\right). \tag{4.4}$$

The sorting problem therefore amounts to solve for a permutation p of the elements of Ω_n such that

$$\forall\, 0 \leq u < v < n,$$

$$f\left(p\left(\omega^{u}\right)\right)\,\overline{f\left(p\left(\omega^{u}\right)\right)}-f\left(p\left(\omega^{v}\right)\right)\,\overline{f\left(p\left(\omega^{v}\right)\right)}\geq 0. \tag{4.5}$$

Let us describe the algebraic constraints on the polynomial p, which ensure that p corresponds to an automorphism of Ω_n. As a further consequence of *the fundamental Lagrange invariance identity,* an automorphism of Ω_n is described by a multivariate polynomial p (in the main variable z and the auxiliary vector variable $\mathbf{r}=\left(r_k\right)_{0\leq k<n}$) expressed by

$$p\left(z;\,\mathbf{r}\right)\equiv$$

$$\sum_{0\leq k<n} r_k \prod_{0\leq t\neq k<n}\left(\frac{z-\omega^{t}}{\omega^{k}-\omega^{t}}\right) \mod \left\{r_k-\omega^{\sigma(k)}\right\}_{\sigma\in S_n,0\leq k<n}. \tag{4.6}$$

The constraints in the equation 4.6 expresses the fact that $p\left(z;\,\mathbf{r}\right)$ is associated with a bijective map of Ω_n to itself. Therefore the sorting constraints corresponds to semi-algebraic constraints specified by:

$$\forall\, 0\leq u<v<n,\ \left|f\left(p\left(\omega^{v}\right)\right)\right|^2-\left|f\left(p\left(\omega^{u}\right)\right)\right|^2\geq 0$$

$$\mod \left\{r_k-\omega^{\sigma(k)}\right\}_{\sigma\in S_n,0\leq k<n}. \tag{4.7}$$

We remark that although the sorting constraints in 4.7 are semi-algebraic unfortunately they are not equality constraints. We can turn the inequality constraints into equality constraints by introducing slack variables as follows

$$\forall\, 0\leq u<v<n,\quad \left|f\left(p\left(\omega^{v};\,\mathbf{r}\right)\right)\right|^2-\left|f\left(p\left(\omega^{u};\,\mathbf{r}\right)\right)\right|^2\equiv$$

$$\left(\sum_{0\leq s<m}\left(\frac{1+y_{u,v,s}}{2}\right)2^{s}\right)\left(1+\sum_{0\leq t<m}\left(\frac{1+z_{u,v,t}}{2}\right)2^{1+t}\right)^{-1}$$

$$\mod \left\{\begin{array}{l}\left(y_{u,v,s}\right)^2-1\\ \left(z_{u,v,s}\right)^2-1\end{array},\ r_k-\omega^{\sigma(k)}\right\}_{\sigma\in S_n,0\leq s<m,0\leq k<n}, \tag{4.8}$$

where m denotes the minimum number of bits required to encode in binary form both integers in the numerators and in the denominators of the slack variables. We may assume that m is given as part of the input. Having algebraically

specified sorting instances, we briefly sketch the steps for determining their solution. We could for instance solve sorting instances via Hilbert Nullstellensatz certificates using such methods as the NullLA [47, 45, 46, 50]. Unfortunately such algorithms could possibly yield exponential worst case run time performance. This in turn suggests that the combinatorial underpinning of sorting problems plays a crucial role in the design of efficient algorithms. In fact one easily obtains an efficient algebraic solver for sorting by exploiting well known divide and conquer schemes describe in [11].

4.2 Matrix algebra from the algebra of bivariate polynomials

Having described how single-dimensional arrays indexed by roots of unity can be encoded as polynomials in a single variable, we now proceed to discuss how the algebra of bivariate polynomials naturally embeds matrix algebra. Consequently, throughout the discussion, we will de-emphasize the distinction between matrices and polynomials (and subsequently de-emphasize the distinction between hypermatrices and polynomials). Consider the following parametric family of polynomial rings, subset of $\mathbb{C}[x, y]$, defined for an arbitrary field $\mathbb{F}$ and arbitrary integers $m, n > 0$ by

$$\mathbb{F}^{x,y}_{(m,n)} := {}^{(\mathbb{F}[x]/(x^m-1))[y]}/_{(y^n-1)} = {}^{(\mathbb{F}[y]/(y^n-1))[x]}/_{(x^m-1)}, \tag{4.9}$$

(since polynomials in $R[x, y]$ can be re-expressed as $(R[x])[y]$ or equivalently as $(R[y])[x]$). It also follows as a consequence of the *fundamental Lagrange invariance identity* that $\forall f \in \mathbb{C}[x, y]$ the unique minimal degree polynomial

in $\mathbb{C}^{x,y}_{(m,n)}$ which is congruent to f is expressed by

$$\sum_{(r_0,r_1)\in\Omega_m\times\Omega_n} f\left(r_0,\, r_1\right)\left(\prod_{s_0\in\Omega_m\setminus\{r_0\}}\left(\frac{x-s_0}{r_0-s_0}\right)\right)\left(\prod_{s_1\in\Omega_n\setminus\{r_1\}}\left(\frac{y-s_1}{r_1-s_1}\right)\right) \tag{4.10}$$

where

$$(r_0,r_1)\in\Omega_m\times\Omega_n,\quad f\left(r_0,\, r_1\right):=f\left(t_0,t_1\right)\mod\left\{\begin{array}{c} t_0-r_0 \\ t_1-r_1 \end{array}\right\}. \tag{4.11}$$

We remark that the degrees of freedom in the polynomial encoding described above correspond precisely to the degrees of freedom of an $m\times n$ complex entry matrices.

4.2.1 Matrix multiplication as uncentered covariance.

Given two arbitrary polynomials $f\left(x,\, y\right), g\left(x,\, y\right)\in\mathbb{C}\left[x,y\right]$, and a discrete joint probability distribution $\mathcal{P}$, defined over the pair of random variables $\left(R_0,R_1\right)$ whose support is over the Cartesian product set $\Omega_k\times\Omega_k$, the uncentered covariance associated with the new random variables $\left(f\left(x,R_0\right),\, g\left(R_1,y\right)\right)$, is defined to be the element of $\mathbb{C}^{x,y}_{(m,n)}$ expressed by

$$\mathbb{E}_{\mathcal{P}}\left[f\left(x,\, R_0\right)\, g\left(R_1,\, y\right)\right]=\sum_{(r_0,r_1)\in\Omega_k^2} f\left(x,r_0\right) g\left(r_1,y\right)\,\mathcal{P}\left(r_0,r_1\right). \tag{4.12}$$

Following the usual linear algebra convention, our default choice for the joint probability distribution $\mathcal{P}$ will be the polynomial encoding of the normalized identity matrix i.e.

$$\mathcal{P}\left(r_0,r_1\right)=n^{-1}\mathcal{I}_{n\times n}\left(r_0,r_1\right)\equiv\frac{\left(-1\right)^{\binom{n}{2}}}{n}\times$$

$$\prod_{0\leq s<t<n}\left(\frac{\left(r_1-r_0\right)^2-\left(\omega^s-\omega^t\right)^2}{\left(\omega^s-\omega^t\right)^2}\right)\mod\left\{\begin{array}{c}\left(r_0\right)^n-1\\ \left(r_1\right)^n-1\end{array}\right\} \tag{4.13}$$

hence

$$\mathcal{P}\left(r_0, r_1\right) = n^{-1}\mathcal{I}_{n\times n}\left(r_0, r_1\right) \equiv$$

$$\sum_{\substack{0 \leq k_0, k_1 < n \\ \left(k_0 + k_1\right) \mid n}} \frac{\left(r_0\right)^{k_0}\left(r_1\right)^{k_1}}{n^2} \mod \left\{ \begin{array}{l} \left(r_0\right)^n - 1 \\ \left(r_1\right)^n - 1 \end{array} \right\} \tag{4.14}$$

Subsequently, for convenience we adopt the following convention

$$\mathbb{E}\left[f\left(x,\, R_0\right)\, g\left(R_1,\, y\right)\right] := \mathbb{E}_{n^{-1}\mathcal{I}_n}\left[f\left(x,\, R_0\right)\, g\left(R_1,\, y\right)\right] =$$

$$n^{-1}\sum_{r\in\Omega_n} f\left(x, r\right) g\left(r, y\right). \tag{4.15}$$

We remark that, except for the normalizing factor n^{-1}, $\mathbb{E}\left[f\left(x,\, R_0\right)\, g\left(R_1,\, y\right)\right]$ corresponds to the usual definition of matrix multiplication, and hence the matrices respectively associated with the polynomials f, $\mathrm{Inv}_f \in \mathbb{C}\left[x, y\right]$ are said to be inverses to one another if $\forall g \in \mathbb{C}_{(n,n)}^{x,y}$

$$\mathbb{E}\left[\mathbb{E}\left[f\left(x,\, R_0\right)\, \mathrm{Inv}_f\left(R_1,\, S_0\right)\right] g\left(S_1, y\right)\right] =$$

$$\mathbb{E}\left[\mathbb{E}\left[\mathrm{Inv}_f\left(x,\, R_0\right)\, f\left(R_1,\, S_0\right)\right] g\left(S_1, y\right)\right] = n^{-2} g\left(x, y\right). \tag{4.16}$$

In particular a bivariate polynomial $q \in \mathbb{C}\left[x, y\right]$ will be said to be unitary over the ring $\mathbb{C}_{(n,n)}^{x,y}$ if

$$\mathbb{E}\left[\left|q\left(x,\, R_0\right)\right| \left(\frac{q\left(x,\, R_0\right)}{\left|q\left(x,\, R_0\right)\right|}\right)^{\left(\omega_2\right)^0} \left|q\left(y,\, R_1\right)\right| \left(\frac{q\left(y,\, R_1\right)}{\left|q\left(y,\, R_1\right)\right|}\right)^{\left(\omega_2\right)^1}\right] \equiv$$

$$n^{-1}\mathcal{I}_{n\times n}\left(x, y\right) \mod \left\{ \begin{array}{l} x^n - 1 \\ y^n - 1 \end{array} \right\} \tag{4.17}$$

we remark that the complex conjugation operation may be defined as

$$\bar{z} = \left|z\right| \left(\frac{z}{\left|z\right|}\right)^{\left(\omega_2\right)^1} \tag{4.18}$$

where

$$\forall\, \theta \in \mathbb{R}, \quad \left| e^{i\theta} \right| = 1. \tag{4.19}$$

The definition above suggests a natural generalization of the complex conjugation operation that we shall further discuss in the next chapter.

4.2.2 Matrix Kronecker product as a product of polynomials.

Let us recall that given an $m \times n$ matrix $\mathbf{A}$ and a $p \times q$ matrix $\mathbf{B}$ their Kronecker product $\mathbf{A} \otimes \mathbf{B}$ is the $m\,p \times n\,q$ matrix $\mathbf{C}$ with entries given by

$$c_{p\,u+k,\,q\,v+l} = a_{u,v}\, b_{k,l}. \tag{4.20}$$

The Kronecker product in the polynomial encoding framework is encoded as follows

$$h\left(e^{i2\pi\left(\frac{p\,u+k}{mp}\right)}, e^{i2\pi\left(\frac{q\,v+l}{nq}\right)}\right) = f\left(e^{i\frac{2\pi}{m}u}, e^{i\frac{2\pi}{n}v}\right) g\left(e^{i\frac{2\pi}{p}k}, e^{i\frac{2\pi}{q}l}\right)$$

$$\Rightarrow h\left((\omega_m)^u \sqrt[m]{(\omega_p)^k},\, (\omega_n)^v \sqrt[n]{(\omega_q)^l}\right) = f\left((\omega_m)^u, (\omega_n)^v\right)\, g\left((\omega_p)^k, (\omega_q)^l\right), \tag{4.21}$$

In summary we say that given $f \in \mathbb{C}^{x_0,y_0}_{(m,n)}$ and $g \in \mathbb{C}^{x_1,y_1}_{(p,q)}$ the polynomial corresponding to their Kronecker product, $h \in \mathbb{C}^{x_0\,\sqrt[m]{x_1},\, y_0\,\sqrt[n]{y_1}}_{(m\cdot p,\, n\cdot q)}$ is expressed by

$$h\left(x_0\,\sqrt[m]{x_1},\, y_0\,\sqrt[n]{y_1}\right) := f \otimes g := f\left(x_0, y_0\right)\, g\left(x_1, y_1\right). \tag{4.22}$$

Incidentally for unitary polynomials f and g over $\mathbb{C}^{x_0,y_0}_{(m,m)}$ and $\mathbb{C}^{x_1,y_1}_{(n,n)}$ respectively it follows that $f \otimes g$ is also unitary over $\mathbb{C}^{x_0\,\sqrt[m]{x_1},\, y_0\,\sqrt[n]{y_1}}_{(mp,\, nq)}$.

4.3 Hypermatrix algebra from the algebra of polynomials.

We now discuss how polynomial algebra also encompasses the algebra of hypermatrices. The discussion here will focus on third order hypermatrices, since

further generalization to k-th order hypermatrices, though notationally more complicated, is not essentially different. Consider the parametric family of polynomial rings defined for some arbitrary field $\mathbb{F}$ and integers $m, n, p > 0$ by

$$\mathbb{F}^{x,y,z}_{(m,n,p)} := \left(\left(\mathbb{F}[x]/\langle x^m - 1\rangle\right)[y]/\langle y^n - 1\rangle\right)[z]/\langle z^p - 1\rangle. \tag{4.23}$$

As a consequence of the *fundamental Lagrange identity* it follows that $\forall\, f \in \mathbb{C}[x, y, z]$, the unique minimal degree polynomial element of $\mathbb{C}^{x,y,z}_{(m,n,p)}$, which is congruent to f is expressed by

$$\sum_{(r_0,r_1,r_2)\in\Omega_m\times\Omega_n\times\Omega_p} f(r_0, r_1, r_2) \left(\prod_{s_0\in\Omega_m\setminus\{r_0\}} \left(\frac{x - s_0}{r_0 - s_0}\right)\right) \times$$

$$\left(\prod_{s_1\in\Omega_n\setminus\{r_1\}} \left(\frac{y - s_1}{r_1 - s_1}\right)\right) \left(\prod_{s_1\in\Omega_p\setminus\{r_2\}} \left(\frac{z - s_2}{r_2 - s_2}\right)\right) \tag{4.24}$$

where

$$f(r_0, r_1, r_2) := f(t_0, t_1, t_2) \mod \left\{ \begin{array}{c} t_0 - r_0 \\ t_1 - r_1 \\ t_2 - r_2 \end{array} \right\}. \tag{4.25}$$

We note that the degrees of freedom in this encoding corresponds precisely to that of an $m \times n \times p$ hypermatrix. Furthermore, given three arbitrary polynomial $f, g, h \in \mathbb{C}[x, y, z]$ and a discrete joint probability distribution $\mathcal{P}$ over the random variables (R_0, R_1, R_2) whose support is over the Cartesian product $\Omega_k \times \Omega_k \times \Omega_k$, we define their uncentered correlation measure to be

$$\mathbb{E}_{\mathcal{P}}\left[f(x, R_0, z)\; g(x, y, R_1)\; h(R_2, y, z)\right] =$$

$$\sum_{(r_0,r_1,r_2)\in\Omega_k^3} f(x, r_0, z)\, g(x, y, r_1)\, h(r_2, y, z)\; \mathcal{P}(r_0, r_1, r_2). \tag{4.26}$$

By analogy to the linear algebra convention, our default choice for the joint distribution $\mathcal{P}$ will be the Kronecker delta third order hypermatrix whose corresponding polynomial is expressed by

$$\mathcal{P}\left(r_0,\, r_1,\, r_2\right) = n^{-1}\, \mathcal{I}_{n\times n\times n}\left(r_0,\, r_1,\, r_2\right) \equiv n^{-1} \prod_{m_0+m_1\,\omega_3+m_2(\omega_3)^2\neq 0}$$

$$\left(\frac{\left(r_0+\omega_3\, r_1+(\omega_3)^2\, r_2\right)-\left((\omega_n)^{m_0}+\omega_3\,(\omega_n)^{m_1}+(\omega_3)^2\,(\omega_n)^{m_2}\right)}{(\omega_n)^{m_0}+\omega_3\,(\omega_n)^{m_1}+(\omega_3)^2\,(\omega_n)^{m_2}}\right)$$

$$\mod \left\{(r_0)^n-1,\,(r_1)^n-1,\,(r_2)^n-1\right\} \tag{4.27}$$

and hence

$$n^{-1}\, \mathcal{I}_{n\times n\times n}\left(r_0,\, r_1,\, r_2\right) \equiv$$

$$\sum_{\substack{0\leq k_0,k_1,k_2<n\\ k_0+k_1+k_2\equiv 0 \mod n}} \frac{(r_0)^{k_0}\,(r_1)^{k_1}\,(r_2)^{k_2}}{n^{-3}} \mod \left\{\begin{array}{l}(r_0)^n-1\\(r_1)^n-1\\(r_2)^n-1\end{array}\right\} \tag{4.28}$$

and similarly to the matrix case we adopt the convention

$$\mathbb{E}\left[f\left(x,\, R_0,\, z\right)\, g\left(x,\, y,\, R_1\right)\, h\left(R_2,\, y,\, z\right)\right] :=$$

$$\mathbb{E}_{n^{-1}\mathcal{I}_{n\times n\times n}}\left[f\left(x,\, R_0,\, z\right)\, g\left(x,\, y,\, R_1\right)\, h\left(R_2,\, y,\, z\right)\right] =$$

$$n^{-1}\sum_{r\in\Omega_k} f\left(x,\, r,\, z\right)\, g\left(x,\, y,\, r\right)\, h\left(r,\, y,\, z\right). \tag{4.29}$$

Remark that except for the normalizing factor n^{-1} we have that

$$\mathbb{E}\left[f\left(x,\, R_0,\, z\right)\, g\left(x,\, y,\, R_1\right)\, h\left(R_2,\, y,\, z\right)\right]$$

corresponds to a ternary third order hypermatrix product operation as proposed by Mesner and Bhattacharya [51, 52] and further discussed in [3, 19]. Furthermore, given two ordered pairs of polynomials $\left(a\left(x,\, y,\, z\right),\, b\left(x,\, y,\, z\right)\right) \in$

$\mathbb{C}^{x,y,z}_{(n,n,n)} \times \mathbb{C}^{x,y,z}_{(n,n,n)}$ and $(\alpha(x,\,y,\,z)\,,\,\beta(x,\,y,\,z)) \in \mathbb{C}^{x,y,z}_{(n,n,n)} \times \mathbb{C}^{x,y,z}_{(n,n,n)}$ we say that such pairs are inverse pairs if $\forall f \in \mathbb{C}^{x,y,z}_{(n,n,n)}$

$$\mathbb{E}\left[\mathbb{E}\left[f(x,\,R_0,\,z)\;a(x,\,S_0,\,R_1)\;b(R_2,\,S_0,\,z)\right]\;\alpha(x,\,y,\,S_1)\;\beta(S_2,\,y,\,z)\right] \equiv$$

$$n^{-2} f(x,\,y,\,z) \mod \left\{ \begin{array}{c} x^n - 1 \\ y^n - 1 \\ z^n - 1 \end{array} \right\}. \tag{4.30}$$

furthermore a polynomial $q \in \mathbb{C}^{x,y,z}_{(n,n,n)}$ is said to be unitary over $\mathbb{C}^{x,y,z}_{(n,n,n)}$ if

$$\mathbb{E}\left[q(x,R_0,z)\,|q(y,R_1,x)|\left(\frac{q(y,R_1,x)}{|q(y,R_1,x)|}\right)^{(\omega_3)^2} |q(z,R_2,y)|\left(\frac{q(z,R_2,y)}{|q(z,R_2,y)|}\right)^{(\omega_3)^1}\right]$$

$$\equiv n^{-1}\,\mathcal{I}_{n\times n\times n}(x,\,y,\,z) \mod \left\{ \begin{array}{c} x^n - 1 \\ y^n - 1 \\ z^n - 1 \end{array} \right\}. \tag{4.31}$$

4.4 Lagrange interpolation for solving linear constraints.

Solving linear systems of equations is a classical topic in linear algebra. It is well known that polynomial interpolation indeed reduces to solving a special system of linear equations, we proceed to show here that the converse also holds. We show that solving a general linear system of equation naturally reduces to a special multivariate polynomial interpolation problem. We recall that the Lagrange interpolation formula associated with the map

$$\forall\; 0 \leq k < n, \quad x_k \to f(x_k)\,,$$

expressed by

$$f(x) = \sum_{0\leq k<n} f(x_k) \left(\prod_{0\leq t\neq k<n} (x - x_t)\right)\left(\prod_{0\leq t\neq k<n} (x_k - x_t)\right)^{-1}. \tag{4.32}$$

Using the DFT hyperplane parametrization presented in Eq 2.26 we formulate a vector version of the Lagrange interpolation formula above as follows

$$f_{\mathbf{\Gamma}}\left(\mathbf{x}\right) = \sum_{0\leq k<n} f\left(\mathbf{x}_k\right) \times$$

$$\left\langle \left(\bigstar_{0\leq t\neq k<n}\left(\mathbf{x}-\mathbf{x}_t\right)\right),\ \left(\bigstar_{0\leq t\neq k<n}\left(\mathbf{x}_k-\mathbf{x}_t\right)\right)^{\star^{-1}} \star \left(\frac{\mathbf{w}_0}{n} + \sum_{0<j<n}\gamma_j\left(\mathbf{x}_k\right)\ \mathbf{w}_j\right)\right\rangle \tag{4.33}$$

where $\left\{\gamma_j\left(\mathbf{x}_k\right)\right\}_{0\leq i,j\neq 0<n}$ are parameters to be determined. It is clear from the expression above that the entries of the vectors $\left\{\mathbf{x}_k\right\}_{0\leq k<n} \subset \mathbb{C}^{n\times 1}$ must be chosen such that no two pair of distinct vectors $\left(\mathbf{x}_i,\ \mathbf{x}_j\right)$ have equal entries. Fortunately, this restriction is not particularly limiting. We further remark that, while in the single variable Lagrange interpolation case the formula resulted in only one polynomial, the vector formulation in 4.33 describes a family of interpolating multivariate polynomials of degree at most $n-1$ in each of the variables. Since our goal is to solve systems of linear equations, we make the *linear form "Ansatz"* that is to say we pre-suppose the existence among the interpolating polynomials of a linear form with no constant term expressed by

$$f\left(\mathbf{x}\right) = \left\langle \mathbf{s},\ \mathbf{x}\right\rangle. \tag{4.34}$$

Note that given such an interpolating polynomial the solutions to our constraints are determined by

$$\left\{s_k = f\left(\mathbf{e}_k\right)\right\}_{0\leq k<n} \tag{4.35}$$

where $\left\{\mathbf{e}_k\right\}_{0\leq k<n}$ denotes the canonical Euclidean basis vectors, or in other words the columns vectors of the identity matrix.

Let us illustrate this with 2×2 system of linear equations. Consider the

system of equation

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} s_0 \\ s_1 \end{pmatrix} = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}. \tag{4.36}$$

Solving for $\begin{pmatrix} s_0 \\ s_1 \end{pmatrix}$ in the equation above, amounts to determining a linear interpolating polynomial

$$f : \mathbb{C}^2 \to \mathbb{C}$$

such that for $\mathbf{a}_0^T = \begin{pmatrix} a_{00} & a_{01} \end{pmatrix}$ and $\mathbf{a}_1^T = \begin{pmatrix} a_{10} & a_{11} \end{pmatrix}$ we have

$$\begin{cases} f(\mathbf{a}_0) &= b_0 \\ f(\mathbf{a}_1) &= b_1 \end{cases} \tag{4.37}$$

using the proposed vector formulation of the Lagrange interpolation formula we obtain that

$$\begin{aligned} f(\mathbf{x}) = b_0 \left\langle (\mathbf{x} - \mathbf{a}_0), \begin{pmatrix} \frac{1}{a_{00}-a_{10}} \\ \frac{1}{a_{01}-a_{11}} \end{pmatrix} \star \left[\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] \right\rangle - \\ b_1 \left\langle (\mathbf{x} - \mathbf{a}_1), \begin{pmatrix} \frac{1}{a_{00}-a_{10}} \\ \frac{1}{a_{01}-a_{11}} \end{pmatrix} \star \left[\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] \right\rangle \end{aligned} \tag{4.38}$$

so that

$$\begin{aligned} f(\mathbf{x}) = b_0 \begin{pmatrix} (x_0 - a_{00}) & (x_1 - a_{01}) \end{pmatrix} \begin{pmatrix} \frac{1/2+\gamma}{a_{00}-a_{10}} \\ \frac{1/2-\gamma}{a_{01}-a_{11}} \end{pmatrix} - \\ b_1 \begin{pmatrix} (x_0 - a_{10}) & (x_1 - a_{11}) \end{pmatrix} \begin{pmatrix} \frac{1/2+\gamma}{a_{00}-a_{10}} \\ \frac{1/2-\gamma}{a_{01}-a_{11}} \end{pmatrix}. \end{aligned} \tag{4.39}$$

By the *ansatz* we have

$$f(\mathbf{0}) = -b_0 \begin{pmatrix} a_{00} & a_{01} \end{pmatrix} \begin{pmatrix} \frac{1/2+\gamma}{a_{00}-a_{10}} \\ \frac{1/2-\gamma}{a_{01}-a_{11}} \end{pmatrix} + b_1 \begin{pmatrix} a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} \frac{1/2+\gamma}{a_{00}-a_{10}} \\ \frac{1/2-\gamma}{a_{01}-a_{11}} \end{pmatrix} = 0. \tag{4.40}$$

Hence the solution to the linear system of equation is given by

$$\mathbf{s} := \begin{pmatrix} f(\mathbf{e}_0) \\ f(\mathbf{e}_1) \end{pmatrix} \mod f(\mathbf{0}) \Leftrightarrow \mathbf{s} := (a_{00}a_{11} - a_{01}a_{10})^{-1} \begin{pmatrix} -a_{01}b_0 + a_{11}b_1 \\ a_{00}b_0 - a_{10}b_1 \end{pmatrix} \tag{4.41}$$

The 2×2 example is rather misleadingly simple, since the general $n \times n$ case is much more intricate. Indeed the vector version of the Lagrange interpolation formula parametrizes a family of interpolating polynomials of the form

$$f_{\mathbf{\Gamma}}(\mathbf{x}) = \sum_{0 \leq k < n} \left\langle \mathbf{x}^{\star^k}, \mathbf{a}_k(\boldsymbol{\gamma}(\mathbf{x}_0), \cdots, \boldsymbol{\gamma}(\mathbf{x}_{n-1})) \right\rangle \tag{4.42}$$

where the vectors $\mathbf{\Gamma} = \{\boldsymbol{\gamma}(\mathbf{x}_j)\}_{0 \leq j < n}$ are parameters to be determined, however without lost of generality we can set the vector $\boldsymbol{\gamma}(\mathbf{x}_{n-1})$ to

$$\begin{pmatrix} n^{-1} \\ \gamma_1(\mathbf{x}_{n-1}) \\ \vdots \\ \gamma_{n-1}(\mathbf{x}_{n-1}) \end{pmatrix} = \begin{pmatrix} n^{-1} \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{4.43}$$

and by linear form "Ansatz" the solution to the linear system of equation is determined by the constraints

$$\begin{gathered} \forall \mathbf{x} \in \mathbb{C}^n, \quad f(\mathbf{x}) := \langle \mathbf{s}, \mathbf{x} \rangle \equiv f_{\mathbf{\Gamma}}(\mathbf{x}) \\ \mod \left\{ \left\langle \mathbf{x}^{\star^k}, \mathbf{a}_k(\boldsymbol{\gamma}(\mathbf{x}_0), \cdots, \boldsymbol{\gamma}(\mathbf{x}_{n-1})) \right\rangle \right\}_{0 \leq k \neq 1 < n} \end{gathered} \tag{4.44}$$

which induces a linear system having $(n-1)^2$ unknowns in $n(n-2)+1$ equations. Fortunately, the resulting constraints can be split into $n+1$ independent linear systems of equations each of which have only $n-1$ unknowns in $n-1$ equations, thereby allowing us to recursively determine the solution.

4.5 Higher order Lagrange invariance identities as higher order Fourier expansions.

In recent years many applications have arisen in which it has been necessary to go beyond the linear phases in the usual Fourier expansion, replacing them with higher order functions such as polynomials. Such expression had appeared earlier in the Physics community associated with path integral computations introduced by Feynman in [16]. They have also appeared in combinatorics as discussed by Tao in [66]. We show here that higher order Fourier expansion can viewed as natural generalizations to the *fundamental Lagrange invariance identity.* We therefore refer to such generalizations as *higher order Lagrange invariance identi*ties.

It is clear that polynomial interpolation over roots of unity induce a Fourier expansions over some finite Abelian groups, as suggested by the following rewriting of the *fundamental Lagrange invariance identity* for f

$$f\left(\omega_{n_0}^{x_0}\right) = \sum_{t_0 \in \mathbb{Z}/n_0\mathbb{Z}} f\left(\omega_{n_0}^{t_0}\right) \prod_{s_0 \neq t_0} \frac{e^{2\pi i\left(\frac{x_0}{n_0}+\frac{0}{2}\right)} + e^{2\pi i\left(\frac{s_0}{n_0}+\frac{1}{2}\right)}}{e^{2\pi i\left(\frac{t_0}{n_0}+\frac{0}{2}\right)} + e^{2\pi i\left(\frac{s_0}{n_0}+\frac{1}{2}\right)}}. \tag{4.45}$$

We further recall that the bivariate version of the *fundamental Lagrange identity* yields the the following Fourier expansion for g

$$g\left(\omega_{n_0}^{x_0}, \omega_{n_1}^{x_1}\right) = \sum_{(t_0,t_1) \in \mathbb{Z}/n_0\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}} g\left(\omega_{n_0}^{t_0}, \omega_{n_1}^{t_1}\right) \times$$

$$\prod_{s_0 \neq t_0} \frac{e^{2\pi i\left(\frac{x_0}{n_0}+\frac{0}{2}\right)} + e^{2\pi i\left(\frac{s_0}{n_0}+\frac{1}{2}\right)}}{e^{2\pi i\left(\frac{t_0}{n_0}+\frac{0}{2}\right)} + e^{2\pi i\left(\frac{s_0}{n_0}+\frac{1}{2}\right)}} \prod_{s_1 \neq t_1} \frac{e^{2\pi i\left(\frac{x_1}{n_1}+\frac{0}{2}\right)} + e^{2\pi i\left(\frac{s_1}{n_1}+\frac{1}{2}\right)}}{e^{2\pi i\left(\frac{t_1}{n_1}+\frac{0}{2}\right)} + e^{2\pi i\left(\frac{s_1}{n_1}+\frac{1}{2}\right)}}. \tag{4.46}$$

Finally, we recall that the *fundamental Lagrange identity* yields the the following Fourier expansion for h an exponential polynomial in three variables

$$h\left(\omega_{n_0}^{x_0}, \omega_{n_1}^{x_1}, \omega_{n_2}^{x_2}\right) =$$

$$\sum_{(t_0,t_1,t_2)\in\mathbb{Z}/n_0\mathbb{Z}\times\mathbb{Z}/n_1\mathbb{Z}\times\mathbb{Z}/n_2\mathbb{Z}} h\left(\omega_{n_0}^{t_0},\,\omega_{n_1}^{t_1},\,\omega_{n_2}^{t_2}\right)\prod_{s_0\neq t_0}\frac{e^{2\pi i\left(\frac{x_0}{n_0}+\frac{0}{2}\right)}+e^{2\pi i\left(\frac{s_0}{n_0}+\frac{1}{2}\right)}}{e^{2\pi i\left(\frac{t_0}{n_0}+\frac{0}{2}\right)}+e^{2\pi i\left(\frac{s_0}{n_0}+\frac{1}{2}\right)}}\times$$
$$\prod_{s_1\neq t_1}\frac{e^{2\pi i\left(\frac{x_1}{n_1}+\frac{0}{2}\right)}+e^{2\pi i\left(\frac{s_1}{n_1}+\frac{1}{2}\right)}}{e^{2\pi i\left(\frac{t_1}{n_1}+\frac{0}{2}\right)}+e^{2\pi i\left(\frac{s_1}{n_1}+\frac{1}{2}\right)}}\prod_{s_2\neq t_2}\frac{e^{2\pi i\left(\frac{x_2}{n_2}+\frac{0}{2}\right)}+e^{2\pi i\left(\frac{s_2}{n_2}+\frac{1}{2}\right)}}{e^{2\pi i\left(\frac{t_1}{n_2}+\frac{0}{2}\right)}+e^{2\pi i\left(\frac{s_2}{n_2}+\frac{1}{2}\right)}} \tag{4.47}$$

we may introduce here a *higher order version of the fundamental Lagrange invariance identity* and associated with the same function h as follows

$$h\left(\omega_{n_0}^{x_0},\,\omega_{n_1}^{x_1},\,\omega_{n_2}^{x_2}\right)=$$

$$\sum_{\{0\leq u_k<n_k\}_{0\leq k<3}} h\left(\omega_{n_0}^{u_0},\,\omega_{n_1}^{u_1},\,\omega_{n_2}^{u_2}\right)\prod_{\substack{\{0\leq\mu_k<n_k\}_{0\leq k<3}\\(\mu_0\neq u_0)\text{ or }(\mu_1\neq u_1)\text{ or }(\mu_2\neq u_2)}}$$
$$\left(\frac{e^{2\pi i\left(\left(\frac{x_0}{n_0}\right)^3+\left(\frac{\mu_1}{n_1}\right)^2+\left(\frac{\mu_2}{n_2}\right)+\frac{0}{4}\right)}+e^{2\pi i\left(\left(\frac{\mu_0}{n_0}\right)^3+\left(\frac{x_1}{n_1}\right)^2+\left(\frac{\mu_2}{n_2}\right)+\frac{1}{4}\right)}+}{e^{2\pi i\left(\left(\frac{u_0}{n_0}\right)^3+\left(\frac{\mu_1}{n_1}\right)^2+\left(\frac{\mu_2}{n_2}\right)+\frac{0}{4}\right)}+e^{2\pi i\left(\left(\frac{\mu_0}{n_0}\right)^3+\left(\frac{u_1}{n_1}\right)^2+\left(\frac{\mu_2}{n_2}\right)+\frac{1}{4}\right)}+}\to\right.$$
$$\left.\to\frac{e^{2\pi i\left(\left(\frac{\mu_0}{n_0}\right)^3+\left(\frac{\mu_1}{n_1}\right)^2+\left(\frac{x_2}{n_2}\right)+\frac{2}{4}\right)}+e^{2\pi i\left(\left(\frac{\mu_0}{n_0}\right)^3+\left(\frac{\mu_1}{n_1}\right)^2+\left(\frac{\mu_2}{n_2}\right)+\frac{3}{4}\right)}}{e^{2\pi i\left(\left(\frac{u_0}{n_0}\right)^3+\left(\frac{\mu_1}{n_1}\right)^2+\left(\frac{u_2}{n_2}\right)+\frac{2}{4}\right)}+e^{2\pi i\left(\left(\frac{u_0}{n_0}\right)^3+\left(\frac{\mu_1}{n_1}\right)^2+\left(\frac{\mu_2}{n_2}\right)+\frac{3}{4}\right)}}\right). \tag{4.48}$$

It is immediately apparent that uniqueness fails to hold for higher order Fourier expansions. We shall refer to the expression above as the canonical cubic order Fourier expansion of f more generally, the *n-th order* Fourier expansion expressed by

$$f\left(\omega_{m_0}^{x_0},\cdots,\omega_{m_{n-1}}^{x_{m_{n-1}}}\right)=\sum_{\{0\leq u_t<m_t\}_{0\leq t<n}} f\left(\omega_{m_0}^{u_0},\cdots,\omega_{m_{n-1}}^{u_{m_{n-1}}}\right)\prod_{\substack{\{0\leq\mu_t<m_t\}_{0\leq t<n}\\\bigvee\{\mu_t\neq u_t\}_{0\leq t<n}}}$$
$$\left(\sum_{0\leq k<n}\exp\left\{2\pi i\left(\sum_{0\leq t<k}\left(\frac{\mu_t}{m_t}\right)^{n-t}+\left(\frac{x_k}{m_k}\right)^{n-k}+\sum_{k<t<n}\left(\frac{\mu_t}{m_t}\right)^{n-t}+\frac{k}{n}\right)\right\}\right)$$

$$\left(\sum_{0\leq k<n}\exp\left\{2\pi i\left(\sum_{0\leq t<k}\left(\frac{\mu_t}{m_t}\right)^{n-t}+\left(\frac{u_k}{m_k}\right)^{n-k}+\sum_{k<t<n}\left(\frac{\mu_t}{m_t}\right)^{n-t}+\frac{k}{n}\right)\right\}\right)^{-1}$$

We therefore think of the higher order Fourier expansion described above as providing a natural way of extending the polynomial framework described here to non polynomial kernel approaches.

Chapter 5
Matrix and hypermatrix spectral analysis

5.1 Generalization of the complex conjugation operation.

We start by first discussing a slight generalization to the complex conjugation operation. We recall that the usual complex conjugation operation is defined as follows

$$\forall\, z \in \mathbb{C}^*, \quad z = z^{\mathfrak{c}_2^0} := |z| \left(\frac{z}{|z|}\right)^{(\omega_2)^0} \text{ and } \overline{z} = z^{\mathfrak{c}_2^1} := |z| \left(\frac{z}{|z|}\right)^{(\omega_2)^1} \tag{5.1}$$

where ω_k denotes the primitive k-the root of unity and

$$\forall\, \theta \in \mathbb{R}, \left|e^{i\,\theta}\right| = 1.$$

Incidentally, we think of the usual complex conjugation operation as a second order operation. More generally we define the k-th complex conjugate of order p for an arbitrary non-zero complex number z to be

$$z^{\mathfrak{c}_p^k} := |z| \left(\frac{z}{|z|}\right)^{\left(\omega_p\right)^k}, \tag{5.2}$$

it follows from the definition that

$$\forall\, z \in \mathbb{C}, \quad \left(\prod_{0 \leq k < p} z^{\mathfrak{c}_p^k}\right) = |z|^p. \tag{5.3}$$

Hence, for an arbitrary $f \in \mathbb{C}\left[x, y, z\right]$ its ℓ_p norm over $\mathbb{C}^{x,y,z}_{(n_0,n_1,n_2)}$ noted $\|f\|_{\ell_p}$ is implicitly defined by the equality

$$\left(\|f\|_{\ell_p}\right)^p := \sum_{(r_0,r_1,r_2) \in \Omega_{n_0} \times \Omega_{n_1} \times \Omega_{n_2}} \prod_{0 \leq k < p} \left(f\left(r_0, r_1, r_2\right)\right)^{\mathfrak{c}_p^k}. \tag{5.4}$$

In particular the k-th complex conjugate of order p of an arbitrary $f \in \mathbb{C}[x,y,z]$ over $\mathbb{C}^{x,y,z}_{(n_0,n_1,n_2)}$ corresponds to the polynomial

$$f^{\mathfrak{c}_p^k}(x_0,x_1,x_2) = \sum_{(r_0,r_1,r_2)\in\Omega_{n_0}\times\Omega_{n_1}\times\Omega_{n_2}} (f(r_0,r_1,r_2))^{\mathfrak{c}_p^k} \left(\prod_{s_0\in\Omega_{n_0}\setminus\{r_0\}} \left(\frac{x-s_0}{r_0-s_0}\right)\right) \times \left(\prod_{s_1\in\Omega_{n_1}\setminus\{r_1\}} \left(\frac{y-s_1}{r_1-s_1}\right)\right)\left(\prod_{s_2\in\Omega_{n_2}\setminus\{r_2\}} \left(\frac{z-s_2}{r_2-s_2}\right)\right) \tag{5.5}$$

5.2 The weak form of the matrix and hypermatrix spectral theorem.

We recall that the matrix spectral theorem is formulated for an arbitrary $n \times n$ hermitian matrix $\mathbf{A}$ as follows

$$\begin{cases} \mathbf{A} &= (\mathbf{Q}\cdot\mathbf{D}_0)\cdot(\mathbf{Q}\cdot\mathbf{D}_1)^{\dagger_2} \\ \mathbf{\Delta} &= \mathbf{Q}\cdot\mathbf{Q}^{\dagger_2} \\ \mathbf{D}_j^{\star^2} &= \mathbf{D}_j^T\cdot\mathbf{D}_j, \quad 0\le j<3 \end{cases}$$

where the $\dagger_2$ operation corresponds to a second order conjugation applied to the entries of a matrix followed by a transpose. The spectral constraints are equivalently written as

$$\begin{cases} a_{i,j} &= \left\langle (\boldsymbol{\mu}\star\mathbf{q}_i),\ (\boldsymbol{\nu}\star\mathbf{q}_j)^{\mathfrak{c}_2^1}\right\rangle \\ \delta_{i,j} &= \left\langle \mathbf{q}_i,\ \mathbf{q}_j^{\mathfrak{c}_2^1}\right\rangle \end{cases} ,\forall\ 0\le i\le j<n\ . \tag{5.6}$$

Theorem (weak form of the matrix spectral theorem): The entries of an arbitrary hermitian matrix $\mathbf{A}$, admit an expansion of the form

$$\forall\ 0\le i\le j<n,\quad \begin{cases} a_{ij} &= \langle \boldsymbol{\lambda}_{ij},\ \mathbf{q}_{ij}\rangle \\ \delta_{ij} &= \langle \mathbf{1},\ \mathbf{q}_{ij}\rangle \end{cases} \tag{5.7}$$

for $\binom{n+1}{2}$ vectors $\left\{\boldsymbol{\lambda}_{ij}\right\}_{0\leq i\leq j<n}$ and $\binom{n+1}{2}$ vectors $\left\{\mathbf{q}_{ij}\right\}_{0\leq i\leq j<n}$.

Proof : It is immediate that the weak form of the spectral theorem trivially follows from the usual formulation of the spectral theorem, which we refer to as the strong form of the spectral theorem. We shall instead offer here an alternative proof of the weak form of the spectral theorem. Our proof has the advantage of naturally extending to hermitian hypermatrices of arbitrary finite order. In addition, the proof suggests a natural recursive algorithm for performing the weak spectral analysis of matrices and hypermatrices.

Our proposed proof is inductive, and starts by establishing that the theorem holds for 2×2 hermitian matrices as the base case. Let

$$\mathbf{A} = \begin{pmatrix} a_{00} & a_{01} \\ a_{01}^{\mathfrak{c}_2^1} & a_{11} \end{pmatrix} \in \mathbb{C}^{2\times 2}, \tag{5.8}$$

we note that the constraints

$$\forall\ 0 \leq i \leq j < 2, \quad a_{ij} = \left\langle \boldsymbol{\lambda}_{ij},\, \mathbf{q}_{ij} \right\rangle \text{ and } \delta_{ij} = \left\langle \mathbf{1},\, \mathbf{q}_{ij} \right\rangle \tag{5.9}$$

can be rewritten as

$$\mathbf{M} \cdot \begin{bmatrix} q_{000} \\ q_{001} \\ q_{010} \\ q_{011} \\ q_{110} \\ q_{111} \end{bmatrix} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{11} \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{5.10}$$

where

$$\mathbf{M} = \begin{bmatrix} \lambda_0 & \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_0 & \lambda_1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \tag{5.11}$$

from which we deduce that

$$\begin{pmatrix} \frac{1}{\lambda_0} - \frac{\lambda_1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0^2} & 0 & 0 & \frac{\lambda_1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0} & 0 & 0 \\ \frac{1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0} & 0 & 0 & -\frac{1}{\frac{\lambda_1}{\lambda_0}-1} & 0 & 0 \\ 0 & \frac{1}{\lambda_0} - \frac{\lambda_1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0^2} & 0 & 0 & \frac{\lambda_1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0} & 0 \\ 0 & \frac{1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0} & 0 & 0 & -\frac{1}{\frac{\lambda_1}{\lambda_0}-1} & 0 \\ 0 & 0 & \frac{1}{\lambda_0} - \frac{\lambda_1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0^2} & 0 & 0 & \frac{\lambda_1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0} \\ 0 & 0 & \frac{1}{\left(\frac{\lambda_1}{\lambda_0}-1\right)\lambda_0} & 0 & 0 & -\frac{1}{\frac{\lambda_1}{\lambda_0}-1} \end{pmatrix}.$$

$$\begin{bmatrix} a_{00} \\ a_{01} \\ a_{11} \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} q_{000} \\ q_{001} \\ q_{010} \\ q_{011} \\ q_{110} \\ q_{111} \end{bmatrix}. \tag{5.12}$$

Where for convenience we shall define

$$\mathbf{q} = \begin{bmatrix} q_{000} \\ q_{001} \\ q_{010} \\ q_{011} \\ q_{110} \\ q_{111} \end{bmatrix}, \mathbf{a} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{11} \\ 1 \\ 0 \\ 1 \end{bmatrix}.$$

We have

$$\mathbf{M} \cdot \mathbf{q} = \mathbf{a} \tag{5.13}$$

$$\Rightarrow \left(\mathbf{M} - \operatorname{diag}\left\{\mathbf{q}^{\star^{-1}} \star \mathbf{a}\right\}\right) \cdot \mathbf{q} = \mathbf{0}_{n\times 1}. \tag{5.14}$$

Consequently entries of $\boldsymbol{\lambda}$ and $\mathbf{q}$ must be roots of the multivariate rational function

$$\det\left\{\mathbf{M} - \operatorname{diag}\left\{\mathbf{q}^{\star^{-1}} \star \mathbf{a}\right\}\right\}, \tag{5.15}$$

which we think of as a variant of the characteristic equation. It is implicit in the expressions above that we assume that $\mathbf{q}$ has no non-zero entries. Fortunately, this assumption incurs very little loss of generality because, if $\mathbf{q}$ had zero entries, a small additive perturbation will turn such entries into non-zero entries, while only slightly perturbing the spectral decomposition. Working over the algebraic closed field $\mathbb{C}$, we have therefore reduced the existence of a weak spectral decomposition for a hermitian 2×2 matrices to the fundamental theorem of algebra. Having established the base case of the induction, we work out the remaining part of the argument by deriving the weak spectral decomposition of $(n+1) \times (n+1)$ matrices from the weak spectral decomposition of $n \times n$ matrices. For some given $(n+1) \times (n+1)$ matrix $\mathbf{A}$ we consider the

$n+1$ minors defined as follows

$$\forall\, 0 \leq t \leq n, \quad \mathbf{A}^{[t]} = \left(a_{ij}^{[t]} = \begin{cases} a_{ij} & \text{if } 0 \leq i \neq t, j \neq t \leq n \\ 0 & \text{otherwise} \end{cases} \right), \tag{5.16}$$

for each one of these minors, according to the induction hypothesis, we assume that we have at our disposal the corresponding weak spectral decomposition expressed by

$$\forall\, 0 \leq i \neq t \leq j \neq t \leq n, \quad a_{ij}^{[t]} = \left(\sum_{0 \leq k \neq t \leq n} \lambda_{ijk}^{[t]}\, q_{ijk}^{[t]} \right) = \left\langle \boldsymbol{\lambda}_{ij}^{[t]},\, \mathbf{q}_{ij}^{[t]} \right\rangle \tag{5.17}$$

$$\forall\, 0 \leq i \neq t \leq j \neq t \leq n, \quad \delta_{ij} = \left(\sum_{0 \leq k \neq t \leq n} q_{ijk}^{[t]} \right) = \left\langle \mathbf{1},\, \mathbf{q}_{ij}^{[t]} \right\rangle \tag{5.18}$$

and

$$q_{ijk}^{[t]} = \begin{cases} q_{ijk}^{[t]} & \text{if } 0 \leq k \neq t \leq n \\ 0 & \text{otherwise} \end{cases}. \tag{5.19}$$

We think of the vectors $\mathbf{q}_{ij}^{[t]}$ as being $(n+1)$ dimensional. By adding up the expression associated with the weak spectral decomposition of the $(n+1)$ minors we obtain that

$$\forall\, 0 \leq i \leq j \leq n, \quad a_{ij} = \sum_{0 \leq k \leq n} \left\langle \boldsymbol{\lambda}_{ij}^{[k]},\, \frac{\mathbf{q}_{ij}^{[k]}}{n} \right\rangle = \sum_{0 \leq k \leq n} \left\langle \mathbf{1}_{n \times 1},\, \boldsymbol{\lambda}_{ij}^{[k]} \star \frac{\mathbf{q}_{ij}^{[k]}}{n} \right\rangle \tag{5.20}$$

and

$$\forall\, 0 \leq i \leq j \leq n, \quad \delta_{ij} = \sum_{0 \leq k \leq n} \left\langle \mathbf{1},\, \frac{\mathbf{q}_{ij}^{[k]}}{n} \right\rangle \tag{5.21}$$

we may rewrite the constraints above as

$$\forall\, 0 \leq i \leq j \leq n, \quad a_{ij} = \left\langle \mathbf{1},\, \sum_{0 \leq k \leq n} \boldsymbol{\lambda}_{ij}^{[k]} \star \frac{\mathbf{q}_{ij}^{[k]}}{n} \right\rangle \tag{5.22}$$

and

$$\forall\, 0 \leq i \leq j \leq n, \quad \delta_{ij} = \left\langle \mathbf{1},\, \sum_{0 \leq k \leq n} \frac{\mathbf{q}_{ij}^{[k]}}{n} \right\rangle. \tag{5.23}$$

Furthermore, we have

$$a_{ij} = \left\langle \left(\sum_{0 \leq k \leq n} \boldsymbol{\lambda}_{ij}^{[k]} \star \frac{\mathbf{q}_{ij}^{[k]}}{n} \right) \star \left(\sum_{0 \leq k \leq n} \frac{\mathbf{q}_{ij}^{[k]}}{n} \right)^{\star^{-1}}, \sum_{0 \leq k \leq n} \frac{\mathbf{q}_{ij}^{[k]}}{n} \right\rangle, \tag{5.24}$$

from which we conclude that

$$\boldsymbol{\lambda}_{ij} = \left(\sum_{0 \leq k \leq n} \boldsymbol{\lambda}_{ij}^{[k]} \star \frac{\mathbf{q}_{ij}^{[k]}}{n} \right) \star \left(\sum_{0 \leq k \leq n} \frac{\mathbf{q}_{ij}^{[k]}}{n} \right)^{\star^{-1}} \tag{5.25}$$

and we set

$$\mathbf{q}_{ij} = \sum_{0 \leq k \leq n} \frac{\mathbf{q}_{ij}^{[k]}}{n} \tag{5.26}$$

in the weak form of the spectral decomposition of the $(n+1) \times (n+1)$ matrix $\mathbf{A}$ is expressed by

$$\forall\, 0 \leq i \leq j \leq n, \quad \begin{cases} a_{ij} &= \left\langle \boldsymbol{\lambda}_{ij},\, \mathbf{q}_{ij} \right\rangle \\ \delta_{ij} &= \left\langle \mathbf{1}_{(n+1)\times 1},\, \mathbf{q}_{ij} \right\rangle \end{cases} \quad \square. \tag{5.27}$$

It is clear from the discussion above that the weak spectral decomposition of a symmetric $n \times n$ matrix $\mathbf{A}$ is determined by it's $\binom{n}{2}$ 2×2 Hermitian matrix minors. We may obtain a canonical weak spectral decomposition, by using the following explicit parametrization of 2×2 unitary matrices derived here. Recall that 2×2 unitary matrices are expressed by

$$\begin{cases} \|\mathbf{q}_0\|_{\ell_2}^2 &= 1 \\ \left\langle \mathbf{q}_0,\, \mathbf{q}_1^{\mathfrak{c}_2^1} \right\rangle &= 0 \\ \|\mathbf{q}_1\|_{\ell_2}^2 &= 1 \end{cases}. \tag{5.28}$$

By expanding out the constraints above we have

$$\begin{cases} \left(|q_{00}|\, e^{i\,(\omega_2)^2 \theta_{00}} \right) \left(|q_{00}|\, e^{i\,(\omega_2)^1 \theta_{00}} \right) + \left(|q_{01}|\, e^{i\,(\omega_2)^2 \theta_{01}} \right) \left(|q_{01}|\, e^{i\,(\omega_2)^1 \theta_{01}} \right) = 1 \\ \left(|q_{00}|\, e^{i\,(\omega_2)^2 \theta_{00}} \right) \left(|q_{10}|\, e^{i\,(\omega_2)^1 \theta_{10}} \right) = e^{i\pi} \left(|q_{01}|\, e^{i\,(\omega_2)^2 \theta_{01}} \right) \left(|q_{11}|\, e^{i\,(\omega_2)^1 \theta_{11}} \right) \\ \left(|q_{10}|\, e^{i\,(\omega_2)^2 \theta_{10}} \right) \left(|q_{10}|\, e^{i\,(\omega_2)^1 \theta_{10}} \right) + \left(|q_{11}|\, e^{i\,(\omega_2)^2 \theta_{11}} \right) \left(|q_{11}|\, e^{i\,(\omega_2)^1 \theta_{11}} \right) = 1 \end{cases} \tag{5.29}$$

We first focus on the orthogonality constraints expressed by

$$\left(|u_{00}|\, e^{i\,(\omega_2)^2\theta_{00}}\right)\cdot\left(|u_{10}|\, e^{i\,(\omega_2)^1\theta_{10}}\right)=e^{i\pi}\left(|u_{01}|\, e^{i\,(\omega_2)^2\theta_{01}}\right)\cdot\left(|u_{11}|\, e^{i\,(\omega_2)^1\theta_{11}}\right) \tag{5.30}$$

and apply the logarithm on both sides of the equation to get

$$\begin{aligned}&(\ln|u_{00}|+i\,\theta_{00})+\left(\ln|u_{10}|+i\ (\omega_2)^1\,\theta_{10}\right)-\\&(\ln|u_{01}|+i\,\theta_{01})-\left(\ln|u_{11}|+i\ (\omega_2)^1\,\theta_{11}\right)=i\pi.\end{aligned} \tag{5.31}$$

Therefore, orthogonality reduces to the following pair of constraints

$$\begin{cases}\ln|u_{00}|+\ln|u_{10}|-\ln|u_{01}|-\ln|u_{11}| &= 0\\ \theta_{00}-\theta_{10}-\theta_{01}+\theta_{11} &= \pi\end{cases}. \tag{5.32}$$

Incidentally, we may rewrite the constraints as

$$\begin{pmatrix}1 & 1 & -1 & -1\end{pmatrix}\begin{pmatrix}\ln|u_{00}|\\ \ln|u_{10}|\\ \ln|u_{01}|\\ \ln|u_{11}|\end{pmatrix}=0$$

$$\Rightarrow\begin{pmatrix}\ln|u_{00}|\\ \ln|u_{10}|\\ \ln|u_{01}|\\ \ln|u_{11}|\end{pmatrix}=\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\\ 1 & -1 & 1 & -1\end{pmatrix}\begin{pmatrix}c_0\\ 0\\ c_2\\ c_3\end{pmatrix} \tag{5.33}$$

and

$$\begin{pmatrix}1 & -1 & -1 & 1\end{pmatrix}\begin{pmatrix}\theta_{00}\\ \theta_{10}\\ \theta_{01}\\ \theta_{11}\end{pmatrix}=\pi$$

$$\Rightarrow \begin{pmatrix} \theta_{00} \\ \theta_{10} \\ \theta_{01} \\ \theta_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{pmatrix} \begin{pmatrix} d_0 \\ d_1 \\ \frac{\pi}{4} \\ d_3 \end{pmatrix}, \tag{5.34}$$

hence

$$\mathbf{U} = \begin{pmatrix} e^{c_0+c_2+c_3+i\left(\frac{\pi}{4}+d_0+d_1+d_3\right)} & e^{c_0-c_2+c_3+i\left(-\frac{\pi}{4}+d_0-d_1+d_3\right)} \\ e^{c_0-c_2-c_3+i\left(-\frac{\pi}{4}+d_0+d_1-d_3\right)} & e^{c_0+c_2-c_3+i\left(\frac{\pi}{4}+d_0-d_1-d_3\right)} \end{pmatrix}. \tag{5.35}$$

Finally, a unitary matrix $\mathbf{Q}$ is deduced from $\mathbf{U}$ by simply normalizing the two rows of the matrix $\mathbf{U}$ expressed above so as to ensure that the rows have ℓ_2-norm equal to 1

$$\mathbf{Q} = \begin{pmatrix} \mathbf{q}_0 = \mathbf{u}_0 \cdot \|\mathbf{u}_0\|_{\ell_2}^{-1} \\ \mathbf{q}_1 = \mathbf{u}_1 \cdot \|\mathbf{u}_1\|_{\ell_2}^{-1} \end{pmatrix}, \tag{5.36}$$

from which by construction it follows that

$$\mathbf{Q} \cdot \mathbf{Q}^{\dagger} = \mathbf{I}. \tag{5.37}$$

Having discussed a constructive proof of the weak form of the spectral theorem for matrices, we proceed to discuss in detail the proof of the weak from of the spectral theorem for Hermitian third-order hypermatrices. We point out that the argument also extends quite naturally to arbitrary finite order hypermatrices. For convenience we restrict the discussion here to the third order hypermatrix case. Let us recall that the strong form of the hypermatrix spectral theorem is formulated for an arbitrary $n \times n \times n$ Hermitian hypermatrices $\mathbf{A}$ as follows

$$\begin{cases} \mathbf{A} &= \circ\left(\circ\left(\mathbf{Q}, \mathbf{D}_0, \mathbf{D}_0^T\right), \circ\left(\mathbf{Q}, \mathbf{D}_1, \mathbf{D}_1^T\right)^{(\dagger_3)^2}, \circ\left(\mathbf{Q}, \mathbf{D}_2, \mathbf{D}_2^T\right)^{\dagger_3}\right) \\ \mathbf{\Delta} &= \circ\left(\mathbf{Q}, \mathbf{Q}^{(\dagger_3)^2}, \mathbf{Q}^{\dagger_3}\right) \\ \mathbf{D}_j^{\star^3} &= \circ\left(\mathbf{D}_j^T, \mathbf{D}_j^{T^2}, \mathbf{D}_j\right), \quad 0 \leq j < 3 \end{cases} \tag{5.38}$$

where the $(\dagger_3)^j$ operation corresponds to a third order conjugation applied to the entries of a third order hypermatrix followed by a j-th transpose. The spectral constraints are equivalently written as

$$\left\{\begin{array}{c} \left\langle (\boldsymbol{\mu}_i \star \mathbf{q}_{ik} \star \boldsymbol{\mu}_k)\,,\, (\boldsymbol{\nu}_j \star \mathbf{q}_{ji} \star \boldsymbol{\nu}_i)^{\mathfrak{c}_3^2}\,,\, \left(\boldsymbol{\gamma}_k \star \mathbf{q}_{kj} \star \boldsymbol{\gamma}_j\right)^{\mathfrak{c}_3^1} \right\rangle = a_{ijk} \\ \left\langle \mathbf{q}_{ik},\, (\mathbf{q}_{ji})^{\mathfrak{c}_3^2}\,,\, (\mathbf{q}_{kj})^{\mathfrak{c}_3^1} \right\rangle = \delta_{ijk} \end{array}\right. \tag{5.39}$$

$$\left\{\begin{array}{c} \left\langle (\boldsymbol{\mu}_i \star \boldsymbol{\mu}_k) \star (\boldsymbol{\nu}_j \star \boldsymbol{\nu}_i)^{\mathfrak{c}_3^2} \star \left(\boldsymbol{\gamma}_k \star \boldsymbol{\gamma}_j\right)^{\mathfrak{c}_3^1}\,,\, \mathbf{q}_{ik} \star (\mathbf{q}_{ji})^{\mathfrak{c}_3^2} \star (\mathbf{q}_{kj})^{\mathfrak{c}_3^1} \right\rangle = a_{ijk} \\ \left\langle \mathbf{1}_{n\times 1},\, \mathbf{q}_{ik} \star (\mathbf{q}_{ji})^{\mathfrak{c}_3^2} \star (\mathbf{q}_{kj})^{\mathfrak{c}_3^1} \right\rangle = \delta_{ijk} \end{array}\right. . \tag{5.40}$$

This in turns leads to the weak form of the spectral theorem for third order hypermatrices expressed as follows

$$\left\langle \boldsymbol{\lambda}_{ijk},\, \mathbf{q}_{ijk} \right\rangle = a_{ijk} \text{ and } \left\langle \mathbf{1},\, \mathbf{q}_{ijk} \right\rangle = \delta_{ijk}. \tag{5.41}$$

Theorem (weak form of the third order hypermatrix spectral theorem): the entries of an arbitrary hermitian third order hypermatrix $\mathbf{A}$, admit an expansion of the form

$$\forall\,(i,j,k) \in \mathcal{J}_n, \quad \left\{\begin{array}{rcl} \left\langle \boldsymbol{\lambda}_{ijk},\, \mathbf{q}_{ijk} \right\rangle & = & a_{ijk} \\ \left\langle \mathbf{1},\, \mathbf{q}_{ijk} \right\rangle & = & \delta_{ijk} \end{array}\right. \tag{5.42}$$

where $\mathcal{J}_n$ denotes the indexing set defined by

$$\mathcal{J}_n := \left\{ \underbrace{\binom{n}{1}}_{(i,i,i)} \cup \underbrace{\binom{n}{2}}_{(i,j,j)} \cup \underbrace{\binom{n}{2}}_{(i,i,j)} \cup \underbrace{\binom{n}{3}}_{(i,j,k)} \cup \underbrace{\binom{n}{3}}_{(j,i,k)} \right\},$$

for the $\left(n + 2\binom{n}{2} + 2\binom{n}{3}\right)$ vectors $\left\{\boldsymbol{\lambda}_{ijk}\right\}_{(i,j,k)\in\mathcal{J}_n}$ and the $\left(n + 2\binom{n}{2} + 2\binom{n}{3}\right)$ vectors $\left\{\mathbf{q}_{ijk}\right\}_{(i,j,k)\in\mathcal{J}_n}$.

Proof : The proof is quite analogous to the matrix proof. It starts by establishing that the theorem holds for $2 \times 2 \times 2$ Hermitian hypermatrix as the base case for the induction. Let

$$\mathbf{A}^{\dagger_3} = \mathbf{A} \in \mathbb{C}^{2\times 2\times 2} \tag{5.43}$$

We note that the constraints

$$\forall\,(i,j,k) \in \mathcal{J}_n, \quad a_{ijk} = \left\langle \boldsymbol{\lambda}_{ijk},\, \mathbf{q}_{ijk} \right\rangle \text{ and } \delta_{ijk} = \left\langle \mathbf{1},\, \mathbf{q}_{ijk} \right\rangle \tag{5.44}$$

can be written as

$$\mathbf{M} \cdot \begin{bmatrix} q_{0000} \\ q_{0001} \\ q_{0100} \\ q_{0101} \\ q_{1010} \\ q_{1011} \\ q_{1110} \\ q_{1111} \end{bmatrix} = \begin{bmatrix} a_{000} \\ a_{010} \\ a_{101} \\ a_{111} \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{5.45}$$

where

$$\mathbf{M} = \begin{bmatrix} \lambda_0 & \lambda_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \lambda_0 & \lambda_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \lambda_0 & \lambda_1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \lambda_0 & \lambda_1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}, \tag{5.46}$$

from which we deduce that

$$\mathbf{q} = \begin{bmatrix} q_{0000} \\ q_{0001} \\ q_{0100} \\ q_{0101} \\ q_{1010} \\ q_{1011} \\ q_{1110} \\ q_{1111} \end{bmatrix} = \mathbf{M}^{-1} \cdot \begin{bmatrix} a_{000} \\ a_{010} \\ a_{101} \\ a_{111} \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \tag{5.47}$$

Similarly, the entries of $\boldsymbol{\lambda}$ and $\mathbf{q}$ must be roots of the multivariate rational function

$$\det\left\{\mathbf{M} - \operatorname{diag}\left\{\mathbf{q}^{\star^{-1}} \star \mathbf{a}\right\}\right\} = 0 \tag{5.48}$$

which we think of as expressing a variant of the characteristic equation for Hermitian third-order hypermatrices of dimensions $2 \times 2 \times 2$. We have assumed in the expressions above that $\mathbf{q}$ had no non zero entries and this assumption results in little or no loss in generality since for if $\mathbf{q}$ had zero entries, a small additive perturbation would turn such entries into non-zero entries, while slightly perturbing the corresponding spectral decomposition. Working over the algebraic closed field $\mathbb{C}$ we have therefore reduced the existence of the weak spectral decomposition for hermitian $2 \times 2 \times 2$ matrices to the fundamental theorem of algebra. Having established the base case of the induction, we now work out the remaining part of the induction argument to derive the spectral decomposition of $(n+1) \times (n+1) \times (n+1)$ from the spectral decomposition of $n \times n \times n$ hypermatrices. By the induction hypothesis we assume that we can determine the spectrum of $n \times n \times n$ hypermatrices. For some

given $(n+1)\times(n+1)\times(n+1)$ hypermatrice $\mathbf{A}$ we consider the $n+1$ minors defined by

$$\forall\, 0 \leq t \leq n, \quad \mathbf{A}^{[t]} = \left(a^{[t]}_{i,j,k} = \begin{cases} a_{i,j,k} & \text{if } i,\, j,\, k \in [n] \setminus \{t\} \\ 0 & \text{otherwise} \end{cases} \right) \tag{5.49}$$

for each one of these minors according to the induction hypothesis we assume that we have at our disposal their spectral decomposition expressed as follows

$$\forall\, (i \neq t,\, j \neq t,\, k \neq t) \in \mathcal{J}_n, \quad a^{[t]}_{ijk} = \left(\sum_{0 \leq s \neq t \leq n} \lambda^{[t]}_{ijks}\, q^{[t]}_{ijks} \right) = \left\langle \boldsymbol{\lambda}^{[t]}_{ijk},\, \mathbf{q}^{[t]}_{ijk} \right\rangle \tag{5.50}$$

$$\forall\, (i \neq t,\, j \neq t,\, k \neq t) \in \mathcal{J}_n, \quad \delta^{[t]}_{ijk} = \left(\sum_{0 \leq s \neq t \leq n} q^{[t]}_{ijks} \right) = \left\langle \mathbf{1},\, \mathbf{q}^{[t]}_{ijk} \right\rangle. \tag{5.51}$$

By adding up the weak spectral decomposition of all the minors we have

$$\forall\, (i \neq t,\, j \neq t,\, k \neq t) \in \mathcal{J}_n, \quad a_{ijk} = \sum_{0 \leq s \leq n} \left\langle \boldsymbol{\lambda}^{[s]}_{ijk},\, \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right\rangle \tag{5.52}$$

$$\forall\, (i \neq t,\, j \neq t,\, k \neq t) \in \mathcal{J}_n, \quad \delta_{ijk} = \sum_{0 \leq s \leq n} \left\langle \mathbf{1},\, \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right\rangle \tag{5.53}$$

We may rewrite the constraints as

$$\forall\, (i \neq t,\, j \neq t,\, k \neq t) \in \mathcal{J}_n, \quad a_{ijk} = \left\langle \mathbf{1},\, \sum_{0 \leq s \leq n} \boldsymbol{\lambda}^{[s]}_{ijk} \star \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right\rangle \tag{5.54}$$

$$\forall\, (i \neq t,\, j \neq t,\, k \neq t) \in \mathcal{J}_n, \quad \delta_{ijk} = \left\langle \mathbf{1},\, \sum_{0 \leq s \leq n} \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right\rangle. \tag{5.55}$$

Furthermore, we have

$$a_{ijk} = \left\langle \left(\sum_{0 \leq s \leq n} \boldsymbol{\lambda}^{[s]}_{ijk} \star \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right) \star \left(\sum_{0 \leq s \leq n} \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right)^{\star^{-1}},\, \sum_{0 \leq s \leq n} \frac{\mathbf{q}^{[s]}_{ijk}}{n} \right\rangle. \tag{5.56}$$

From which we conclude that

$$\boldsymbol{\lambda}_{ijk} = \left(\sum_{0 \leq s \leq n} \boldsymbol{\lambda}_{ijk}^{[s]} \star \frac{\mathbf{q}_{ijk}^{[s]}}{n} \right) \star \left(\sum_{0 \leq s \leq n} \frac{\mathbf{q}_{ijk}^{[s]}}{n} \right)^{\star^{-1}} \tag{5.57}$$

and

$$\mathbf{q}_{ijk} = \sum_{0 \leq s \leq n} \frac{\mathbf{q}_{ijk}^{[s]}}{n}. \tag{5.58}$$

In the weak form of the spectral decomposition of the $(n+1) \times (n+1) \times (n+1)$ matrix $\mathbf{A}$ can be expressed as follows

$$\forall\, (i,j,k) \in \mathcal{J}_{n+1}, \quad \left\{ \begin{array}{rcl} \left\langle \boldsymbol{\lambda}_{ijk},\, \mathbf{q}_{ijk} \right\rangle & = & a_{ijk} \\ \left\langle \mathbf{1},\, \mathbf{q}_{ijk} \right\rangle & = & \delta_{ijk} \end{array} \right. \quad \square \tag{5.59}$$

5.3 The strong form of the spectral theorem

We may now discuss a polynomial approach to matrix and third-order hypermatrix spectral decomposition. We begin by formulating without proof in the polynomial framework the strong form of the matrix spectral theorem.

Theorem (strong form of the matrix spectral theorem): $\forall\, a \in \mathbb{C}_{(n,n)}^{x,y}$ such that $a\,(x,y) = a^{\mathfrak{c}_2^1}\,(x,y)$, a admits an expansion of the form

$$\mathbb{E}\left[\left(f\,(R_0)\; q\,(x,R_0) \right) \left(g^{\mathfrak{c}_2^1}\,(R_1)\, q^{\mathfrak{c}_2^1}\,(y,R_1) \right) \right] = n^{-1} a\,(x,y) \mod \left\{ \begin{array}{c} x^n - 1 \\ y^n - 1 \end{array} \right\}, \tag{5.60}$$

where q is subject to the unitary constraint

$$\mathbb{E}\left[q\,(x,R_0)\; q^{\mathfrak{c}_2^1}\,(y,R_1) \right] = n^{-1} \mathcal{I}_{n \times n}\,(x,y) \mod \left\{ \begin{array}{c} x^n - 1 \\ y^n - 1 \end{array} \right\}. \tag{5.61}$$

We further remark that the spectral theorem is equivalent to the statement $\forall\, a \in \mathbb{C}^{x,y}_{(n,n)}$ such that

$$a\left(x,y\right) = a^{\mathfrak{c}_2^1}\left(x,y\right) \mod \left\{ \begin{array}{l} x^n - 1 \\ y^n - 1 \end{array} \right\} \tag{5.62}$$

there exists $q \in \mathbb{C}^{x,y}_{(n,n)}$ such that

$$\left\{ \mathcal{I}_{n\times n}\left(x,y\right),\, a\left(x,y\right) \right\} \subset$$

$$\text{Ideal generated by } \left\{ q\left(x,r\right) \right\}_{r\in\Omega_n} \cap \text{ Ideal generated by } \left\{ q^{\mathfrak{c}_2^1}\left(y,r\right) \right\}_{r\in\Omega_n}. \tag{5.63}$$

Finally, the spectral theorem yields the following fixed-point equation for some unitary polynomial q over $\mathbb{C}^{x,y}_{(n,n)}$,

$$n^{-1} q\left(x,y\right) \equiv \frac{\mathbb{E}\left[a\left(x,R_0\right)\ \mathrm{Inv}\left\{ g^{\mathfrak{c}_2^1}\left(R_1\right) q^{\mathfrak{c}_2^1}\left(y,R_1\right) \right\} \right]}{f\left(y\right)} \mod \left\{ \begin{array}{l} x^n - 1 \\ y^n - 1 \end{array} \right\}. \tag{5.64}$$

We now discuss the generalization of the spectral decomposition to third order hypermatrices. Given a non-zero polynomial $a \in \mathbb{C}^{x,y,z}_{(n,n,n)}$ such that

$$a\left(x,y,z\right) = a^{\mathfrak{c}_3^1}\left(y,z,x\right) = a^{\mathfrak{c}_3^2}\left(z,x,y\right) \mod \left\{ \begin{array}{l} x^n - 1 \\ y^n - 1 \\ z^n - 1 \end{array} \right\}, \tag{5.65}$$

we seek to determine when a admits an expansion of the form

$$\mathbb{E}\left[\left(f_0\left(x,R_0\right)q\left(x,R_0,z\right)f_1\left(R_0,z\right)\right)\left(g_0^{\mathfrak{c}_3^2}\left(y,R_1\right)q^{\mathfrak{c}_3^2}\left(y,R_1,x\right)g_1^{\mathfrak{c}_3^2}\left(R_1,x\right)\right)\times\right.$$

$$\left.\left(h_0^{\mathfrak{c}_3^1}\left(z,R_2\right)q^{\mathfrak{c}_3^1}\left(z,R_2,y\right)h_1^{\mathfrak{c}_3^1}\left(R_2,y\right)\right)\right]\equiv$$

$$a\left(x,y,z\right)\mod\left\{\begin{array}{c}x^n-1\\y^n-1\\z^n-1\end{array}\right\}\tag{5.66}$$

where for $0\leq i<2$, $f_i\left(x,y\right)=f_i\left(y,x\right)$, $g_i\left(x,y\right)=g_i\left(y,x\right)$, and $h_i\left(x,y\right)=h_i\left(y,x\right)$, in addition to q being unitary over $\mathbb{C}_{(n,n,n)}^{x,y,z}$; that is to say

$$\mathbb{E}\left[q\left(x,R_0,z\right)\ q^{\mathfrak{c}_3^2}\left(y,R_1,x\right)\ q^{\mathfrak{c}_3^1}\left(z,R_2,y\right)\right]\equiv$$

$$n^{-1}\,\mathcal{I}_{n\times n\times n}\left(x,\,y,\,z\right)\mod\left\{\begin{array}{c}x^n-1\\y^n-1\\z^n-1\end{array}\right\}.\tag{5.67}$$

Equivalently, the spectral decomposition for third order hypermatrices can also be expressed as an ideal intersection problem as follows

$$\left\{a\left(x,y,z\right),\,\mathcal{I}_{n\times n\times n}\left(x,y,z\right)\right\}\subset\text{Ideal generated by }\left\{q\left(x,r,z\right)\right\}_{r\in\Omega_n}\cap$$

$$\text{Ideal generated by }\left\{q^{\mathfrak{c}_2^2}\left(y,r,x\right)\right\}_{r\in\Omega_n}\cap\ \text{Ideal generated by }\left\{q^{\mathfrak{c}_2^1}\left(z,r,y\right)\right\}_{r\in\Omega_n}.\tag{5.68}$$

The spectral decomposition of third order hypermatrices also yields a fixed-point equation derived as follows, let $u\left(x,y,z\right)$, $v\left(x,y,z\right)$ denote the inverse pair associated with the pair of functions

$$\left(\left(g_0^{\mathfrak{c}_2^2}\left(y,z\right)q^{\mathfrak{c}_2^2}\left(y,z,x\right)g_1^{\mathfrak{c}_2^2}\left(z,x\right)\right);\ \left(h_0^{\mathfrak{c}_2^1}\left(z,x\right)q^{\mathfrak{c}_2^1}\left(z,x,y\right)h_1^{\mathfrak{c}_2^1}\left(x,y\right)\right)\right)$$

over $\mathbb{C}_{(n,n,n)}^{x,y,z}$, we have

$$n^{-1}q\left(x,y,z\right)\equiv\frac{\mathbb{E}\left[a\left(x,R_{0},z\right)\ u\left(x,y,R_{1}\right)\ v\left(R_{2},y,z\right)\right]}{f_{0}\left(x,y\right)\ f_{1}\left(y,z\right)}\mod\left\{\begin{array}{c}x^{n}-1\\y^{n}-1\\z^{n}-1\end{array}\right\} \tag{5.69}$$

Theorem (strong form of the third-order hypermatrix spectral theorem): If for $a\in\mathbb{C}_{(n,n,n)}^{x,y,z}$ the induced functional map

$$q\left(x,y,z\right)\rightarrowtail\mathcal{F}_{a}\left(q\right):=n\frac{\mathbb{E}\left[a\left(x,R_{0},z\right)\ u\left(x,y,R_{1}\right)\ v\left(R_{2},y,z\right)\right]}{f_{0}\left(x,y\right)f_{1}\left(y,z\right)}\mod\left\{\begin{array}{c}x^{n}-1\\y^{n}-1\\z^{n}-1\end{array}\right\} \tag{5.70}$$

(where $\left(u\left(x,y,z\right),\ v\left(x,y,z\right)\right)$ are inverse pairs to

$$\left(\left(g_{0}^{\mathfrak{c}_{2}^{2}}\left(y,z\right)q^{\mathfrak{c}_{2}^{2}}\left(y,z,x\right)g_{1}^{\mathfrak{c}_{2}^{2}}\left(z,x\right)\right);\ \left(h_{0}^{\mathfrak{c}_{2}^{1}}\left(z,x\right)q^{\mathfrak{c}_{2}^{1}}\left(z,x,y\right)h_{1}^{\mathfrak{c}_{2}^{1}}\left(x,y\right)\right)\right)$$

$\mathbb{C}_{(n,n,n)}^{x,y,z}$) is continuous in a bounded domain specified by $\left(\left\|q\right\|_{\ell_{3}}\right)^{3}\leq\kappa$ for some nonzero constant $\kappa>0$ and some choice of symmetric functions

$$\left\{f_{i}\left(x,y\right),\ g_{i}\left(x,y\right),\ h_{i}\left(x,y\right)\right\}_{0\leq i<2}$$

in the variables x, y, it follows that a admits an expansion of the form

$$\mathbb{E}\left[\left(f_{0}\left(x,R_{0}\right)q\left(x,R_{0},z\right)f_{1}\left(R_{0},z\right)\right)\left(g_{0}^{\mathfrak{c}_{3}^{2}}\left(y,R_{1}\right)q^{\mathfrak{c}_{3}^{2}}\left(y,R_{1},x\right)g_{1}^{\mathfrak{c}_{3}^{2}}\left(R_{1},x\right)\right)\right.$$

$$\left.\left(h_{0}^{\mathfrak{c}_{3}^{1}}\left(z,R_{2}\right)q^{\mathfrak{c}_{3}^{1}}\left(z,R_{2},y\right)h_{1}^{\mathfrak{c}_{3}^{1}}\left(R_{2},y\right)\right)\right]\equiv n^{-1}\,a\left(x,y,z\right)\mod\left\{\begin{array}{c}x^{n}-1\\y^{n}-1\\z^{n}-1\end{array}\right\}. \tag{5.71}$$

Proof : The proof of the strong form of the third-order hypermatrix spectral theorem follows as an immediate consequence of the Brouwer fixed-point theorem.

In particular we note that for

$$\mathcal{F}_a : \mathbb{C}^{x,y,z}_{(n,n,n)} \to \mathbb{C}^{x,y,z}_{(n,n,n)},$$

and if there exist $0 < \theta < 1$ such that

$$\|\mathcal{F}_a(q_1) - \mathcal{F}_a(q_0)\|^3_{\ell_3} \leq \theta \, \|q_1 - q_0\|^3_{\ell_3} \tag{5.72}$$

some choice of symmetric functions $\{f_i(x,y), g_i(x,y), h_i(x,y)\}_{0 \leq i < 2}$ it follows that for an arbitrary choice of $q_0 \in \mathbb{C}^{x,y,z}_{(n,n,n)}$ then the iteration defined by

$$q_{n+1} = F_a(q_n) \tag{5.73}$$

determines the spectral decomposition of a.

Chapter 6
Symmetries and the Combinatorial Nullstellensatz method

6.1 Combinatorial problems are symmetry breakings.

We recall that the General Linear group of degree n over $\mathbb{C}$ noted $GL(n, \mathbb{C})$ corresponds to the multiplicative group of invertible matrices. We briefly describe some algebraic and combinatorial problems which are naturally formulated as symmetry breakings over the elements of $GL(n, \mathbb{C})$. In fact, the solutions to many algebraic and combinatorial problems can be thought of as instances of symmetry breakings over the elements of $GL(n, \mathbb{C})$, as illustrated by the following list of classical examples.

- *The matrix diagonalization problem :* amounts to determine $\mathbf{F} \in GL(n, \mathbb{C})$ for some given $n \times n$ matrix $\mathbf{A}$, such that [1]

$$\left(\mathbf{F} \cdot \mathbf{A} \cdot \frac{\text{Adjoint}\{\mathbf{F}\}}{\det\{\mathbf{F}\}}\right)^{2} = \left(\mathbf{F} \cdot \mathbf{A} \cdot \frac{\text{Adjoint}\{\mathbf{F}\}}{\det\{\mathbf{F}\}}\right)^{\star^2} \tag{6.1}$$

- *The unitary matrix subgroup $U(n, \mathbb{C})$ of $GL(n, \mathbb{C})$* : amounts to determining $\mathbf{F} \in GL(n, \mathbb{C})$ for which the following matrix equality holds

$$\mathbf{F} \det\{\mathbf{F}\} = \text{Adjoint}\left\{\mathbf{F}^{\dagger}\right\} \tag{6.2}$$

[1] The $\star$ denotes the entry-wise matrix product operator.

- *The orthogonal matrix subgroup $O(n, \mathbb{R})$ of $GL(n, \mathbb{C})$:* amounts to determining $\mathbf{F} \in GL(n, \mathbb{C})$ which satisfy the matrix constraint

$$\mathbf{F} = s \,\text{Adjoint}\left\{\mathbf{F}^T\right\} \mod \left(s^2 - 1\right) \tag{6.3}$$

- *The permutation matrix subgroup of $GL(n, \mathbb{C})$ (i.e. canonical matrix representation of S_n):* amounts to determining $\mathbf{F} \in GL(n, \mathbb{C})$ such that

$$\begin{cases} \mathbf{F} = \mathbf{F}^{\star^2} \\ \mathbf{F} = s \,\text{Adjoint}\left\{\mathbf{F}^T\right\} \mod \left(s^2 - 1\right) \end{cases} \tag{6.4}$$

- *The nearest orthogonal matrix problem:* amounts to determining elements of $O(n, \mathbb{R})$ which are nearest to the element of a given set of matrices $\mathcal{S} \subset \mathbb{C}^{n \times n}$ i.e.

$$\begin{aligned} \min_{\substack{\mathbf{F} \in \text{GL}(n, \mathbb{R}) \\ \mathbf{A} \in \mathcal{S}}} & \left\{\text{Trace}\left\{(\mathbf{A} - \mathbf{F})^T \cdot (\mathbf{A} - \mathbf{F})\right\}\right\} \\ \text{s.t. } \mathbf{F} &= s \,\text{Adjoint}\left\{\mathbf{F}^T\right\} \mod \left(s^2 - 1\right) \end{aligned} \tag{6.5}$$

- *The Hadamard matrix search problem:* amounts to determine $\mathbf{F} \in GL(n, \mathbb{C})$ such that

$$\begin{cases} \mathbf{F} = \mathbf{F}^{\star^{(-1)}} \\ \mathbf{F} = s\, n^{\frac{2-n}{2}} \,\text{Adjoint}\left\{\mathbf{F}^T\right\} \mod \left(s^2 - 1\right) \end{cases} \tag{6.6}$$

- *The subgraph isomorphism problem:* amounts to determine whether for some given input matrices $\mathbf{A}, \mathbf{B} \in \{0, 1\}^{n \times n}$ there exists $\mathbf{F} \in GL(n, \mathbb{C})$ such that

$$\begin{cases} \left(\mathbf{F}^T \cdot \mathbf{A} \cdot \mathbf{F}\right) \star \mathbf{B} = \mathbf{B} \\ \mathbf{F} = s \,\text{Adjoint}\left\{\mathbf{F}^T\right\} \mod \left(s^2 - 1\right) \cdot \\ \mathbf{F} = \mathbf{F}^{\star^2} \end{cases} \tag{6.7}$$

6.2 The combinatorial nullstellensatz method approach to solving subgraph isomorphism

Given adjacency matrices $\mathbf{A}$ and $\mathbf{B}$ respectively associated with unweighted directed graphs G and H. We say that $G \supseteq H$ i.e. H is subisomorphic to G if the following matrix equality holds for some matrix $\mathbf{P}$.

$$\begin{cases} \left(\mathbf{P}^T \cdot \mathbf{A} \cdot \mathbf{P}\right) \star \mathbf{B} &= \mathbf{B} \\ \mathbf{P}^T \cdot \mathbf{P} &= \mathbf{I} \\ \mathbf{P} \star \mathbf{P} &= \mathbf{P} \end{cases} \tag{6.8}$$

or equivalently

$$\begin{cases} \mathbf{A} \star \left(\mathbf{P} \cdot \mathbf{B} \cdot \mathbf{P}^T\right) &= \left(\mathbf{P} \cdot \mathbf{B} \cdot \mathbf{P}^T\right) \\ \mathbf{P} \cdot \mathbf{P}^T &= \mathbf{I} \\ \mathbf{P} \star \mathbf{P} &= \mathbf{P} \end{cases} \tag{6.9}$$

In order to express the matrix constraints above in the polynomial framework we first express the corresponding adjacency polynomials in their expanded form as follows

$$a\left(x_0,\, x_1\right) = n^{-2} \sum_{0 \leq k_0,\, k_1 < n} \left\langle \mathbf{A},\, \overline{\mathbf{w}^{\star k_0} \cdot \left(\mathbf{w}^{\star k_1}\right)^T} \right\rangle \left(x_0\right)^{k_0} \left(x_1\right)^{k_1} \tag{6.10}$$

and

$$b\left(x_0,\, x_1\right) = n^{-2} \sum_{0 \leq k_0,\, k_1 < n} \left\langle \mathbf{B},\, \overline{\mathbf{w}^{\star k_0} \cdot \left(\mathbf{w}^{\star k_1}\right)^T} \right\rangle \left(x_0\right)^{k_0} \left(x_1\right)^{k_1} \tag{6.11}$$

respectively associated with the graphs G and H, where the set $\left\{\mathbf{w}^{\star k}\right\}_{0 \leq k < n}$ denotes the column vectors of the DFT matrix $\mathbf{W}$. We recall that via the symbolic vector $\mathbf{v}\left(x\right)$ whose entries are polynomials in the variable x expressed by

$$\mathbf{v}\left(x\right) := \left(v_k\left(x\right) = \prod_{0 \leq t \neq k < n} \left(\frac{x - \left(\omega_n\right)^t}{\left(\omega_n\right)^k - \left(\omega_n\right)^t}\right)\right)_{0 \leq k < n}, \tag{6.12}$$

we express the permutation polynomial p by the following vector product of the symbolic vector $\mathbf{v}(x)$ and the symbolic vector $\mathbf{r} = (r_k)_{0 \leq k < n}$ as follows

$$p(x; \mathbf{r}) = \langle \mathbf{v}(x), \mathbf{r} \rangle . \tag{6.13}$$

The existence (respectively the non existence) of solution to the corresponding subgraph isomorphism instance associated with the input binary entry adjacency matrices $\mathbf{A}$ and $\mathbf{B}$ is determined by the polynomial

$$f(\mathbf{r}) = \sum_{0 \leq j_0, j_1 < n} \left[\left(\sum_{0 \leq k_0, k_1 < n} \left(\omega^{j_0}\right)^{k_0} \left(\omega^{j_1}\right)^{k_1} \frac{\left\langle \mathbf{B}, \overline{\mathbf{w}^{\star k_0} \cdot \left(\mathbf{w}^{\star k_1}\right)^T} \right\rangle}{n^2} \right) \times \right.$$

$$\left. \left(1 - \sum_{0 \leq l_0, l_1 < n} \frac{\left\langle \mathbf{A}, \overline{\mathbf{w}^{\star l_0} \cdot \left(\mathbf{w}^{\star l_1}\right)^T} \right\rangle}{n^2} \left\langle \mathbf{r}^{\star l_0}, \mathbf{r}^{\star l_1} \right\rangle_{\mathbf{v}\left(\omega^{j_0}\right) \cdot \mathbf{v}^T\left(\omega^{j_1}\right)} \right) \right]^2 \bmod \left(\mathbf{r}^{\star n} - \mathbf{w}^{\star 0} \right)$$

since the matrices $\mathbf{A}$ and $\mathbf{B}$ have binary entries it follows that

$$f(\mathbf{r}) = \sum_{0 \leq j_0, j_1 < n} \left(\sum_{0 \leq k_0, k_1 < n} \left(\omega^{j_0}\right)^{k_0} \left(\omega^{j_1}\right)^{k_1} \frac{\left\langle \mathbf{B}, \overline{\mathbf{w}^{\star k_0} \cdot \left(\mathbf{w}^{\star k_1}\right)^T} \right\rangle}{n^2} \right) \times$$

$$\left(1 - \sum_{0 \leq l_0, l_1 < n} \frac{\left\langle \mathbf{A}, \overline{\mathbf{w}^{\star l_0} \cdot \left(\mathbf{w}^{\star l_1}\right)^T} \right\rangle}{n^2} \left\langle \mathbf{r}^{\star l_0}, \mathbf{r}^{\star l_1} \right\rangle_{\mathbf{v}\left(\omega^{j_0}\right) \cdot \mathbf{v}^T\left(\omega^{j_1}\right)} \right) \bmod \left(\mathbf{r}^{\star n} - \mathbf{w}^{\star 0} \right)$$

more specifically $G \supseteq H$ if and only if the polynomial f admits an expansion of the form

$$f(\mathbf{r}) = \langle (\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w}_1), \mathbf{g}(\mathbf{r}) \rangle = \sum_{0 \leq k < n} \left(r_k - \omega^{\gamma(k)} \right) g_k(\mathbf{r}) \tag{6.14}$$

for some $\gamma \in S_n$ and $\{g_k\}_{0\leq k<n} \subset \mathbb{C}[\mathbf{r}]$. The natural action of elements of the symmetric group on the polynomial f is defined for some arbitrary $\sigma \in S_n$ by

$$f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right) = \sum_{0\leq j_0, j_1<n} \left(\sum_{0\leq k_0, k_1<n} \left(\omega^{j_0}\right)^{k_0} \left(\omega^{j_1}\right)^{k_1} \frac{\left\langle \mathbf{B},\, \overline{\mathbf{w}^{\star k_0} \cdot \left(\mathbf{w}^{\star k_1}\right)^T} \right\rangle}{n^2} \right) \times$$

$$\left(1 - \sum_{0\leq l_0, l_1<n} \frac{\left\langle \mathbf{A},\, \overline{\mathbf{w}^{\star l_0} \cdot \left(\mathbf{w}^{\star l_1}\right)^T} \right\rangle}{n^2} \left\langle \mathbf{P}_\sigma \cdot \mathbf{r}^{\star l_0},\, \mathbf{P}_\sigma \cdot \mathbf{r}^{\star l_1} \right\rangle_{\mathbf{v}\left(\omega^{j_0}\right)\cdot \mathbf{v}^T\left(\omega^{j_1}\right)} \bmod \left(\mathbf{r}^{\star n} - \mathbf{w}^{\star 0}\right) \right).$$

If the function admits an expansion of the sought after form it would follow that

$$f\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) = \left\langle \left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w}_1\right),\, \mathbf{g}\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) \right\rangle \tag{6.15}$$

$$\Rightarrow f\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) = \left\langle \mathbf{P}_{\sigma^{-1}} \cdot \left(\mathbf{r} - \mathbf{P}_\sigma \cdot \mathbf{P}_\gamma \cdot \mathbf{w}_1\right),\, \mathbf{g}\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) \right\rangle \tag{6.16}$$

$$\Rightarrow f\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) = \left\langle \left(\mathbf{r} - \mathbf{P}_{\sigma\circ\gamma} \cdot \mathbf{w}_1\right),\, \mathbf{P}_\sigma \cdot \mathbf{g}\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) \right\rangle \tag{6.17}$$

and incidentally we shall crucially use the fact that

$$\begin{cases} f\left(\mathbf{r}\right) f\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) & \equiv & 0 \mod \left(\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w}\right) \\ & \text{and} & \\ f\left(\mathbf{r}\right) f\left(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}\right) & \equiv & 0 \mod \left(\mathbf{r} - \mathbf{P}_{\sigma\circ\gamma} \cdot \mathbf{w}\right) \end{cases}. \tag{6.18}$$

Let $\mathrm{Aut}\{f\left(\mathbf{r}\right)\}$ denote the automorphism group of f defined as follows

$$\mathrm{Aut}\left\{f\left(\mathbf{r}\right)\right\} := \left\{\sigma \in S_n, \text{ s.t. } \quad f\left(\mathbf{r}\right) - f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right) = 0\right\}, \tag{6.19}$$

let the set $\mathcal{T}$ denote group quotient $S_n/\mathrm{Aut}\{f(\mathbf{r})\}$ induced by the following partition of S_n

$$S_n = \bigcup_{\sigma\in\mathcal{T}} \sigma\, \mathrm{Aut}\left\{f\left(\mathbf{r}\right)\right\}, \tag{6.20}$$

Theorem (Combinatorial Resolvent): The reduced polynomial

$$f(\mathbf{r}) = \sum_{0 \leq j_0, j_1 < n} \left(\sum_{0 \leq k_0, k_1 < n} \left(\omega^{j_0}\right)^{k_0} \left(\omega^{j_1}\right)^{k_1} \frac{\left\langle \mathbf{B},\ \overline{\mathbf{w}^{\star k_0} \cdot \left(\mathbf{w}^{\star k_1}\right)^T} \right\rangle}{n^2} \right) \times$$

$$\left(1 - \sum_{0 \leq l_0, l_1 < n} \frac{\left\langle \mathbf{A},\ \overline{\mathbf{w}^{\star l_0} \cdot \left(\mathbf{w}^{\star l_1}\right)^T} \right\rangle}{n^2} \left\{ \left\langle \mathbf{r}^{\star l_0},\ \mathbf{r}^{\star l_1} \right\rangle_{\mathbf{v}\left(\omega^{j_0}\right) \cdot \mathbf{v}^T\left(\omega^{j_1}\right)} \bmod \left(\mathbf{r}^{\star n} - \mathbf{w}^{\star 0}\right) \right\} \right)$$

admits an expansion of the form

$$f(\mathbf{r}) = \left\langle (\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w}),\ \mathbf{g}(\mathbf{r}) \right\rangle \tag{6.21}$$

for some $\gamma \in S_n$ and $\mathbf{g} \in (\mathbb{C}[\mathbf{r}])^n$, if and only if

$$\prod_{\sigma \in \mathcal{T}} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \equiv 0 \mod (\mathbf{r} - \mathbf{w}) \tag{6.22}$$

and conversely the polynomial f does not admit an expansion of the sought after form if

$$\prod_{\sigma \in \mathcal{T}} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \neq 0 \mod (\mathbf{r} - \mathbf{w}) \tag{6.23}$$

Proof : It is immediate by Euclidean division that

$$\forall \sigma^{-1} \in S_n, \quad f(\mathbf{r}) = |\kappa_{\sigma^{-1}}| + \left\langle (\mathbf{r} - \mathbf{P}_{\sigma^{-1}} \cdot \mathbf{w}),\ \mathbf{g}_{\sigma^{-1}}(\mathbf{r}) \right\rangle \tag{6.24}$$

$$\Rightarrow f(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}) = |\kappa_{\sigma^{-1}}| + \left\langle \mathbf{P}_{\sigma^{-1}} \cdot (\mathbf{r} - \mathbf{w}),\ \mathbf{g}_{\sigma^{-1}}(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}) \right\rangle \tag{6.25}$$

$$\Rightarrow f(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}) = |\kappa_{\sigma^{-1}}| + \left\langle (\mathbf{r} - \mathbf{w}),\ \mathbf{P}_\sigma \cdot \mathbf{g}_{\sigma^{-1}}(\mathbf{P}_{\sigma^{-1}} \cdot \mathbf{r}) \right\rangle \tag{6.26}$$

and hence

$$\prod_{\sigma \in S_n} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \equiv \prod_{\sigma \in S_n} |\kappa_\sigma| \mod (\mathbf{r} - \mathbf{w})$$

furthermore we note that

$$\prod_{\sigma \in S_n} f(\mathbf{P}_\sigma \cdot \mathbf{r}) = \left(\prod_{\sigma \in \mathcal{T}} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \right)^{\left|\mathrm{Aut}\{f(\mathbf{r})\}\right|} \tag{6.27}$$

$$\Rightarrow \prod_{\sigma \in S_n} f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right) \mod \left(\mathbf{r} - \mathbf{w}\right) = \left(\prod_{\sigma \in \mathcal{T}} |\kappa_\sigma|\right)^{\left|\mathrm{Aut}\{f(\mathbf{r})\}\right|} \tag{6.28}$$

from which it immediately follows that

$$\prod_{\sigma \in \mathcal{T}} f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right) \equiv 0 \mod \left(\mathbf{r} - \mathbf{w}\right) \Leftrightarrow \exists\, \sigma \in S_n \text{ s.t. } \kappa_\sigma = 0. \square \tag{6.29}$$

Finally, the computation of the unique reduced polynomial associated with the combinatorial resolvent

$$\prod_{\sigma \in \mathcal{T}} f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right),$$

which determines the existence of solutions to the subgraph isomorphism instance associated with the input matrices $\mathbf{A}$ and $\mathbf{B}$, require manipulating polynomial expressions whose number of terms is upper bounded by

$$\sum_{0 \leq t \leq |\mathcal{T}|} \binom{n}{t} (n-1)^t \tag{6.30}$$

since the terms in the reduced polynomial associated with the polynomial

$$\prod_{\sigma \in \mathcal{T}} f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right) \mod \left(\mathbf{r}^{\star^n} - \mathbf{w}^{\star^0}\right) \tag{6.31}$$

precisely corresponds to the terms in the polynomial

$$1 + \left(\sum_{\substack{0 \leq i < n \\ 0 < k < n}} \left(r_i\right)^k \right) + \left(\sum_{\substack{(i_0, i_1) \in \binom{[n]}{2} \\ 0 < k_0, k_1 < n}} \left(r_{i_0}\right)^{k_0} \left(r_{i_1}\right)^{k_1} \right) + \cdots + \left(\sum_{\substack{\left(i_0, i_1, \cdots, i_{|\mathcal{T}|-1}\right) \in \binom{[n]}{|\mathcal{T}|} \\ 0 < k_0, k_1, \cdots, k_{|\mathcal{T}|-1} < n}} \prod_{0 \leq j < |\mathcal{T}|} \left(r_{i_j}\right)^{k_j} \right), \tag{6.32}$$

where $\binom{[n]}{m}$ describes set of distinct unordered m-tuples chosen from the integers in the set $\{0, \cdots, n-1\}$. It also follows that if $|\mathcal{T}| \geq n$ than the number of terms in the polynomial $\prod_{\sigma \in \mathcal{T}} f\left(\mathbf{P}_\sigma \cdot \mathbf{r}\right) \mod \left(\mathbf{r}^{\star^n} - \mathbf{w}_0\right)$ is upper bounded by n^n terms. The upper bound on the size of the reduced polynomial corresponds to our measure of the space required to store the certificate. To account for the time required compute the certificate we provide an upper-bound on the number of monomial products and the number of monomial reductions to be performed throughout the procedure. The upper bound on the number of monomial products is given by

$$\sum_{2 \leq m \leq 1+|\mathcal{T}|} \left(\sum_{0 \leq i \leq 2} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq j \leq m} \binom{n}{j} (n-1)^j \right) \tag{6.33}$$

while the upper bound on the number of reduction required is given by

$$\sum_{2 \leq m \leq 1+|\mathcal{T}|} \left[- \sum_{0 \leq j \leq m+2} \binom{n}{i} (n-1)^j + \left(\sum_{0 \leq i \leq 2} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq j \leq m} \binom{n}{j} (n-1)^j \right) \right] \tag{6.34}$$

6.3 A canonical polynomial time reduction of boolean constraints satisfaction problems to symmetry breakings

Consider an arbitrary boolean Constraint Satisfaction Problem (CSP) specified for some boolean n-dimensional boolean column vector $\mathbf{x}$ by the constraint

$$\mathbf{x}^T \cdot \mathbf{A} \cdot \mathbf{x} + \mathbf{b}^T \cdot \mathbf{x} + c = 0, \tag{6.35}$$

for some given matrix $\mathbf{A} \in \mathbb{C}^{n \times n}$, vector $\mathbf{b} \in \mathbb{C}^{n \times 1}$ and a scalar $c \in \mathbb{C}$. The solution to 6.35 is determined by solving n independent instances of symmetry breakings over elements of the permutation group S_n. The n independent

symmetry breaking instances of amount to determine $\mathbf{P} \in GL\left(n, \mathbb{C}\right)$ subject to the constraints

$$\left(\mathbf{P} \cdot \mathbf{v}\right)^T \cdot \mathbf{A} \cdot \left(\mathbf{P} \cdot \mathbf{v}\right) + \mathbf{b}^T \cdot \left(\mathbf{P} \cdot \mathbf{v}\right) + c = 0 \tag{6.36}$$

where

$$\mathbf{v} \in \left\{ \sum_{0 \leq j < k} \mathbf{e}_j \right\}_{0 \leq k \leq n} \text{ and } \left\{ \begin{array}{rcl} \mathbf{P} & = & s \, \text{Adjoint} \left\{ \mathbf{F}^T \right\} \mod \left(s^2 - 1 \right) \\ \mathbf{P} & = & \mathbf{P}^{\star^2} \end{array} \right. . \tag{6.37}$$

where $\left\{ \mathbf{e}_j \right\}_{0 \leq j < n}$ denote the canonical Euclidean basis vectors, in other words the column vectors of the identity matrix. Without loss of generality combinatorial problems can be thought of as systems of boolean CSPs of the form

$$\left\{ \mathbf{x}^T \cdot \mathbf{A}_k \cdot \mathbf{x} + \mathbf{b}_k^T \cdot \mathbf{x} + c_k = 0 \right\}_{0 \leq k < m}, \tag{6.38}$$

for a given set of matrices $\left\{ \mathbf{A}_k \right\}_{0 \leq k < m} \subset \mathbb{C}^{n \times n}$, a set of vectors $\left\{ \mathbf{b}_k \right\}_{0 \leq k < m} \subset \mathbb{C}^{n \times 1}$, and a set of scalars $\left\{ c_k \right\}_{0 \leq k < m} \subset \mathbb{C}$. The constraints amount to determining $\mathbf{P} \in GL\left(n, \mathbb{C}\right)$ subject to the constraints

$$0 = \sum_{0 \leq k < m} \left| \left(\mathbf{P} \cdot \mathbf{v} \right)^T \cdot \mathbf{A}_k \cdot \left(\mathbf{P} \cdot \mathbf{v} \right) + \mathbf{b}_k^T \cdot \left(\mathbf{P} \cdot \mathbf{v} \right) + c_k \right|^2 \tag{6.39}$$

$$\mathbf{v} \in \left\{ \sum_{0 \leq j < k} \mathbf{e}_j \right\}_{0 \leq k \leq n} \text{ and } \left\{ \begin{array}{rcl} \mathbf{P} & = & s \, \text{Adjoint} \left\{ \mathbf{P}^T \right\} \mod \left(s^2 - 1 \right) \\ \mathbf{P} & = & \mathbf{P}^{\star^2} \end{array} \right. . \tag{6.40}$$

6.4 A hardness attenuation paradigm

Recall that determining the existence of solutions to a subgraph isomorphism instance $G_2 \subseteq G_1$ reduces in poly-time (in the number of vertices) to the task of determining if some poly-size (in expanded form) $f \in \mathbb{C}\left[\mathbf{r}\right]$ admits an expansion of the form

$$f\left(\mathbf{r}\right) = \left\langle \left(\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w} \right), \, \mathbf{g}\left(\mathbf{r}\right) \right\rangle \tag{6.41}$$

for some $\gamma \in S_n$ and $\mathbf{g} \in (\mathbb{C}[\mathbf{r}])^n$. Furthermore let $\mathrm{Aut}\{f(\mathbf{r})\}$ denote the automorphism group of f defined by

$$\mathrm{Aut}\{f(\mathbf{r})\} := \{\sigma \in S_n, \text{ s.t. } \quad f(\mathbf{r}) - f(\mathbf{P}_\sigma \cdot \mathbf{r}) = 0\}, \tag{6.42}$$

and let $\mathcal{T}$ denote the group quotient $S_n/\mathrm{Aut}_{\{f(\mathbf{r})\}}$ induced by the following partition of S_n

$$S_n = \bigcup_{\sigma \in \mathcal{T}} \sigma \, \mathrm{Aut}\{f(\mathbf{r})\}. \tag{6.43}$$

Prior to the expansion of the *partial combinatorial resolvent* and crucially assuming that $G_2 \subseteq G_1$ we have that

$$\mathrm{Prob}_{\tau \in S_n}(f(\mathbf{r}) \neq 0 \mod (\mathbf{r} - \mathbf{P}_\tau \cdot \mathbf{w}) \mid G_2 \subseteq G_1) =$$

$$\frac{n! - |\mathrm{Aut}\{f(\mathbf{r})\}|}{n!} = 1 - \left(\frac{n!}{|\mathrm{Aut}\{f(\mathbf{r})\}|}\right)^{-1}$$

furthermore considering the partial resolvent product over permutations in the set $\mathcal{T}\backslash\Gamma$ we have,

$$\mathrm{Prob}_{\tau \in S_n}\left(\prod_{\sigma \in \mathcal{T}\backslash\Gamma} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \neq 0 \mod (\mathbf{r} - \mathbf{P}_\tau \cdot \mathbf{w}) \mid G_2 \subseteq G_1\right) =$$

$$\frac{n! - |\mathrm{Aut}\{f(\mathbf{r})\}|\,|\mathcal{T}\backslash\Gamma|}{n!} = |\Gamma|\left(\frac{n!}{|\mathrm{Aut}\{f(\mathbf{r})\}|}\right)^{-1}$$

for some $\Gamma \subset \mathcal{T}$ and in particular,

$$\mathrm{Prob}_{\tau \in S_n}\left(\prod_{\sigma \in \mathcal{T}} f(\mathbf{P}_\sigma \mathbf{r}) \neq 0 \mod (\mathbf{r} - \mathbf{P}_\tau \cdot \mathbf{w}) \mid G_2 \subseteq G_1\right) = 0.$$

The reduced polynomial associated with the partial combinatorial resolvent

$$\prod_{\sigma \in \mathcal{T}\backslash\Gamma} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \mod \left(\mathbf{r}^{\star^n} - \mathbf{w}^{\star^0}\right)$$

allows us to randomly determine the existence of solution by trying permutations sampled uniformly at random. Assuming that $G_2 \subseteq G_1$, our randomized

permutation trial procedure determines that $G_2 \subseteq G_1$ with probability greater or equal to $(1-p)$ if the arbitrary subset Γ of $\mathcal{T}$ is such that

$$1 - |\Gamma| \left(\frac{n!}{|\mathrm{Aut}\{f(\mathbf{r})\}|} \right)^{-1} \leq 1 - p \Rightarrow |\Gamma| \geq p \frac{n!}{|\mathrm{Aut}\{f(\mathbf{r})\}|}.$$

Consequently, an upper bound on the number of the monomials in the entries of $\mathbf{r}$ with non zero coefficient in the reduced polynomial associated with the partial combinatorial resolvent is given by

$$\sum_{0 \leq t \leq |\mathcal{T} \setminus \Gamma|} \binom{n}{t} (n-1)^t.$$

Furthermore, an upper bound on the number of products of terms as well as the number of monomial reductions required for obtaining the reduced partial combinatorial resolvent are respectively upper bounded by

$$\sum_{2 \leq m \leq |\mathcal{T} \setminus \Gamma| + 2} \left(\sum_{0 \leq i \leq m} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq j \leq 2} \binom{n}{j} (n-1)^j \right) \tag{6.44}$$

and

$$\sum_{2 \leq m \leq |\mathcal{T} \setminus \Gamma| + 2} \left[- \sum_{0 \leq t \leq m+2} \binom{n}{t} (n-1)^t + \left(\sum_{0 \leq i \leq 2} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq j \leq m} \binom{n}{j} (n-1)^j \right) \right]. \tag{6.45}$$

Fortunately, the domain of application of the hardness attenuation framework extends far beyond the specific problem of subgraphs Isomorphism, we discuss bellow two examples of applications of our proposed hardness attenuation framework which also conveniently do not require the use of an Isomorphism oracle and incidentally yields significantly weaker results.

Example 1: We illustrate the hardness attenuation framework on the integer factoring problem. We recall that integer factoring is specified for some given input binary vector $\mathbf{b}$ by the CSP

$$\left(\sum_{0 \leq k < \frac{n}{2}} x_k 2^k \right) \left(\sum_{\frac{n}{2} \leq k < n} x_k 2^{k - \frac{n}{2}} \right) =$$

$$\left(\sum_{0\leq k<\frac{n}{2}} b_k 2^k\right) + 2^{\frac{n}{2}} \mod \left(\mathbf{x}^{\star^2} - \mathbf{x}\right) \tag{6.46}$$

let

$$\boldsymbol{\beta} = \begin{pmatrix} 2^0 \\ \vdots \\ 2^k \\ \vdots \\ 2^{\frac{n}{2}-1} \end{pmatrix} \tag{6.47}$$

the factoring constraint can therefore be expressed as a single quadratic constraint over binary variables

$$\left\langle \mathbf{x}, \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{\beta} \right\rangle \left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \boldsymbol{\beta}, \mathbf{x} \right\rangle = 2^{\frac{n}{2}} + \langle \mathbf{b}, \boldsymbol{\beta} \rangle \mod \left(\mathbf{x}^{\star^2} - \mathbf{x}\right) \tag{6.48}$$

equivalently written as

$$\mathbf{x}^T \cdot \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{\beta}\right) \cdot \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \boldsymbol{\beta}\right)^T \cdot \mathbf{x} = 2^{\frac{n}{2}} + \langle \mathbf{b}, \boldsymbol{\beta} \rangle \mod \left(\mathbf{x}^{\star^2} - \mathbf{x}\right) \tag{6.49}$$

so that the symmetry breaking formulation is expressed as

$$\left(\mathbf{P}_\sigma \cdot \sum_{0\leq k<\tau} \mathbf{e}_k\right)^T \cdot \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{\beta}\right) \cdot \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \boldsymbol{\beta}\right)^T \cdot \left(\mathbf{P}_\sigma \cdot \sum_{0\leq k<\tau} \mathbf{e}_k\right) = N \tag{6.50}$$

for $1 < \tau \leq \frac{n}{2}$ and $N = 2^{\frac{n}{2}} + \langle \mathbf{b}, \boldsymbol{\beta} \rangle$. Let

$$\mathbf{f}_\tau := \sum_{0\leq j<\tau} \mathbf{e}_j$$

which we associate with the single variable polynomial $f_\tau(x) \in \mathbb{C}[x]$ expressed by

$$f_\tau(x) = \sum_{0\leq k<\tau} \prod_{0\leq u\neq k<n} \left(\frac{x - \omega^u}{\omega^k - \omega^u}\right) \tag{6.51}$$

$$\Rightarrow f_\tau(x) = n^{-1} \sum_{0 \le k < n} \frac{1 - \omega^{-k\tau}}{1 - \omega^{-k}} x^k \tag{6.52}$$

$$\Rightarrow f_\tau(x) = n^{-1} \sum_{0 \le k < n} \frac{1 - \left(e^{i2\frac{\pi}{n}}\right)^{-k\tau}}{1 - \left(e^{i2\frac{\pi}{n}}\right)^{-k}} x^k \tag{6.53}$$

$$\Rightarrow f_\tau(x) = n^{-1} \sum_{0 \le k < n} \frac{\left(e^{i\left(\frac{\pi}{n} - \frac{\pi}{n}\right)}\right)^{-k\tau} - \left(e^{i\left(\frac{\pi}{n} + \frac{\pi}{n}\right)}\right)^{-k\tau}}{\left(e^{i\left(\frac{\pi}{n} - \frac{\pi}{n}\right)}\right)^{-k} - \left(e^{i\left(\frac{\pi}{n} + \frac{\pi}{n}\right)}\right)^{-k}} x^k \tag{6.54}$$

$$\Rightarrow f_\tau(x) = n^{-1} \sum_{0 \le k < n} e^{i\frac{\pi}{n}(1-\tau)k} \frac{\left(e^{-i\frac{\pi}{n}}\right)^{-k\tau} - \left(e^{i\frac{\pi}{n}}\right)^{-k\tau}}{\left(e^{-i\frac{\pi}{n}}\right)^{-k} - \left(e^{i\frac{\pi}{n}}\right)^{-k}} x^k \tag{6.55}$$

Hence

$$f_\tau(x) = n^{-1} \sum_{0 \le k < n} \frac{\sin\left(\frac{\pi}{n} k\tau\right)}{\sin\left(\frac{\pi}{n} k\right)} \left(x\, e^{i\frac{\pi}{n}(1-\tau)}\right)^k. \tag{6.56}$$

We further recall that a permutation of the elements of Ω_n can be encoded as a polynomial via the symbolic vector $\mathbf{v}(x)$ whose entries are polynomials in the variable x expressed by

$$\mathbf{v}(x) := \left(v_k(x) = \prod_{0 \le t \ne k < n} \left(\frac{x - (\omega_n)^t}{(\omega_n)^k - (\omega_n)^t}\right)\right)_{0 \le k < n},$$

and the permutation polynomial will be expressed by the vector product

$$p(x; \mathbf{r}) = \langle \mathbf{v}(x), \mathbf{r} \rangle \tag{6.57}$$

so a solution to the solution to factoring problem is determined by the reduced polynomial associated with

$$g_\tau(\mathbf{r}) = -\left(2^{\frac{n}{2}} + \langle \mathbf{b}, \boldsymbol{\beta} \rangle\right) +$$

$$\sum_{0 \le j_0, j_1 < n} \left[f_\tau\left(p\left(\omega^{j_0}; \mathbf{r}\right)\right) f_\tau\left(p\left(\omega^{j_1}; \mathbf{r}\right)\right) \bmod \left(\mathbf{r}^{\star^n} - \mathbf{w}^{\star^0}\right) \times \right.$$

$$\left. n^{-1} \sum_{0 \le k_0, k_1 < n} \left\langle \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{\beta}\right) \cdot \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \boldsymbol{\beta}\right)^T, \overline{\mathbf{w}^{\star^{k_0}} \cdot \left(\mathbf{w}^{\star^{k_1}}\right)^T} \right\rangle \left(\omega^{j_0}\right)^{k_0} \left(\omega^{j_1}\right)^{k_1} \right] \tag{6.58}$$

when the number of 1s in the binary solution vector $\mathbf{x}$ is equal to the parameter τ and exceed or equals the number of 0s, in the alternatively case where the number of 0s in the binary solution $\mathbf{x}$ is equal to the parameter τ and exceed the number of 1s we have that the solution to the factoring problem is determined by the reduced polynomial associated with

$$g_\tau(\mathbf{r}) = -\left(2^{\frac{n}{2}} + \langle \mathbf{b}, \boldsymbol{\beta} \rangle\right) + \sum_{0 \leq j_0, j_1 < n} \left[\left(1 - f_\tau\left(p\left(\omega^{j_0}; \mathbf{r}\right)\right)\right)\left(1 - f_\tau\left(p\left(\omega^{j_1}; \mathbf{r}\right)\right)\right) \bmod \left(\mathbf{r}^{\star^n} - \mathbf{w}^{\star^0}\right) \times n^{-1} \sum_{0 \leq k_0, k_1 < n} \left\langle \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \boldsymbol{\beta}\right) \cdot \left(\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \boldsymbol{\beta}\right)^T, \overline{\mathbf{w}^{\star^{k_0}} \cdot \left(\mathbf{w}^{\star^{k_1}}\right)^T} \right\rangle \left(\omega^{j_0}\right)^{k_0} \left(\omega^{j_1}\right)^{k_1} \right] \tag{6.59}$$

admitting an expansion of the form

$$g_\tau(\mathbf{r}) = \langle (\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w}), \mathbf{g}_\tau(\mathbf{r}) \rangle \tag{6.60}$$

for some $\gamma \in S_n$ and $\{g_{\tau,t}\}_{0 \leq t < n} \subset \mathbb{C}[\mathbf{r}]$. We may assume without loss of generality that we know the value of τ, since the computation for the $\frac{n}{2}$ different values of τ can be performed in parallel. Fortunately we know that the automorphism group of $f_\tau(p(x; \mathbf{r}))$ is determined by the set of permutations which map 1s to 1s and 0s to 0s. Incidentally there will be $\tau!(n-\tau)!$ such permutations. Furthermore we note that the composition of the permutation prescribed by the map

$$\forall\, 0 \leq j < n, \quad r_j \to r_{\left(j + \frac{n}{2} \mod \frac{n}{2}\right)} \tag{6.61}$$

with each one of the $\tau!(n-\tau)!$ permutations which map 1s to 1s and 0s to 0s, must yield a new member of the automorphism group of g_τ by the commutativity property of integer multiplication, hence

$$|\mathrm{Aut}\{g_\tau(\mathbf{r})\}| = 2\,\tau!(n-\tau)!\,. \tag{6.62}$$

Let the set $\mathcal{T}$ denote ${}^{S_n}/_{\mathrm{Aut}\{f(\mathbf{r})\}}$ induced by the following partition of S_n

$$S_n = \bigcup_{\sigma \in \mathcal{T}} \sigma \,\mathrm{Aut}\left\{g_\tau\left(\mathbf{r}\right)\right\}, \tag{6.63}$$

by the Lagrange theorem

$$|\mathcal{T}| = 2^{-1}\binom{n}{\tau}. \tag{6.64}$$

Incidentally, the number of monomials in the entries of $\mathbf{r}$ with non zero coefficients is upper bounded by

$$\sum_{0 \leq t \leq 2^{-1}\binom{n}{\tau} - |\Gamma|} \binom{n}{t} (n-1)^t .$$

while the number of products of terms as well as the number of monomial reductions required for computing the partial combinatorial resolvent are respectively upper bounded by

$$\sum_{2 \leq m \leq 1 + 2^{-1}\binom{n}{\tau} - |\Gamma|} \left(\sum_{0 \leq i \leq m} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq t \leq 2} \binom{n}{t} (n-1)^t \right) \tag{6.65}$$

while the upper bound on the number of reduction required is given by

$$\sum_{2 \leq m \leq 1 + 2^{-1}\binom{n}{\tau} - |\Gamma|} \left[- \left(\sum_{0 \leq j \leq m+2} \binom{n}{i} (n-1)^j \right) + \left(\sum_{0 \leq i \leq 2} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq j \leq m} \binom{n}{j} (n-1)^j \right) \right] \tag{6.66}$$

and finally

$$\mathrm{Prob}_{\gamma \in S_n} \left(\prod_{\sigma \in \mathcal{T} \backslash \Gamma} g_\tau \left(\mathbf{P}_\sigma \cdot \mathbf{r} \right) \neq 0 \mod \left(\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w} \right) \right) =$$

$$\frac{n! - |\mathrm{Aut}\left\{g_\tau\left(\mathbf{r}\right)\right\}| \, |\mathcal{T} \backslash \Gamma|}{n!} = 2\,|\Gamma| \, \binom{n}{\tau}^{-1}$$

Example 2: We now apply the hardness attenuation framework to the Hadamard

matrix search problem. We start by considering the $\sqrt{n} \times \sqrt{n}$ matrix $\mathbf{H}$ expressed by

$$\mathbf{H} = \left(\begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \mathbf{1}_{\frac{\sqrt{n}}{2} \times 1} \right) \cdot \mathbf{e}_0^T + \sum_{0 < k < \sqrt{n}} \left(\begin{pmatrix} 1 \\ -1 \end{pmatrix} \otimes \mathbf{1}_{\frac{\sqrt{n}}{2} \times 1} \right) \cdot \mathbf{e}_k^T \tag{6.67}$$

we think of the matrix as encoded with a polynomial in a single variable expressed by

$$h(x) = \sum_{0 \leq i\sqrt{n}+j < n} h_{i,j} \prod_{0 \leq u\sqrt{n}+v \neq i\sqrt{n}+j < n} \left(\frac{x - \omega_n^{u\sqrt{n}+v}}{\omega_n^{i\sqrt{n}+j} - \omega_n^{u\sqrt{n}+v}} \right) \tag{6.68}$$

and we consider the equation

$$\sum_{0 \leq k < \sqrt{n}} h\left(p\left(x_0 \cdot \left(\omega_{\sqrt{n}} \right)^{\frac{k}{\sqrt{n}}}; \mathbf{r} \right) \right) h\left(p\left(\left(\omega_{\sqrt{n}} \right)^k \cdot (x_1)^{\frac{1}{\sqrt{n}}}; \mathbf{r} \right) \right) \equiv$$

$$\sqrt{n}\, \mathcal{I}_{\sqrt{n} \times \sqrt{n}}(x_0, x_1) \mod \left\{ \begin{array}{c} \mathbf{r}^{\star^n} - \mathbf{1}_{n \times 1} \\ \mathbf{x}^{\star^{\sqrt{n}}} - \mathbf{1}_{2 \times 1} \end{array} \right\}. \tag{6.69}$$

We recall that for

$$\mathbf{v}(x) := \left(v_k(x) = \prod_{0 \leq t \neq k < n} \left(\frac{x - (\omega_n)^t}{(\omega_n)^k - (\omega_n)^t} \right) \right)_{0 \leq k < n}, \tag{6.70}$$

we recall the following property for the polynomial encoding the permutation of the roots of unity

$$\forall\, 0 \leq t < n, \quad (p(x; \mathbf{r}))^t = \left\langle \mathbf{v}(x), \mathbf{r}^{\star^t} \right\rangle. \tag{6.71}$$

To determine the existence of Hadamard matrix of size $\sqrt{n} \times \sqrt{n}$ it suffice to determine that the polynomial

$$f(\mathbf{r}) = \sum_{(x_0, x_1) \in \Omega_{\sqrt{n}} \times \Omega_{\sqrt{n}}} \left[\sqrt{n}\, \mathcal{I}_{\sqrt{n} \times \sqrt{n}}(x_0, x_1) - \right.$$

$$\left. \sum_{0 \leq k < \sqrt{n}} h\left(p\left(x_0 \cdot \left(\omega_{\sqrt{n}} \right)^{\frac{k}{\sqrt{n}}}; \mathbf{r} \right) \right) h\left(p\left(\left(\omega_{\sqrt{n}} \right)^k \cdot (x_1)^{\frac{1}{\sqrt{n}}}; \mathbf{r} \right) \right) \right]^2$$

admits an expansion of the form

$$f(\mathbf{r}) = \langle (\mathbf{r} - \mathbf{P}_\gamma \cdot \mathbf{w}),\ \mathbf{g}(\mathbf{r}) \rangle \tag{6.72}$$

for some $\gamma \in S_n$ and $\mathbf{g} \in (\mathbb{C}[\mathbf{r}])^n$. By construction we have that

$$|\mathrm{Aut}\{f(\mathbf{r})\}| \geq \left(\frac{n}{2} + \sqrt{n}\right)! \left(\frac{n}{2} - \sqrt{n}\right)! \tag{6.73}$$

and hence

$$\mathcal{T} \leq \binom{n}{\frac{n}{2} - \sqrt{n}} \tag{6.74}$$

furthermore the partial combinatorial resolvent is expressed by

$$\left(\prod_{\sigma \in \mathcal{T} \backslash \Gamma} f(\mathbf{P}_\sigma \cdot \mathbf{r}) \right) \bmod \left(\mathbf{r}^{\star^n} - \mathbf{w}^{\star^n} \right).$$

Incidentally the number of the terms in the corresponding reduced polynomial is upper bounded by

$$\sum_{0 \leq t \leq \binom{n}{\frac{n}{2} - \sqrt{n}} - |\Gamma|} \binom{n}{t} (n-1)^t.$$

while the number of monomial products and monomial reductions required for computing the partial combinatorial resolvent are respectively upper bounded by

$$\sum_{4 \leq m \leq 3 + \binom{n}{\frac{n}{2} - \sqrt{n}} - |\Gamma|} \left(\sum_{0 \leq i \leq m} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq t \leq 4} \binom{n}{t} (n-1)^t \right) \tag{6.75}$$

while the upper bound on the number of reduction required is given by

$$\sum_{4 \leq m \leq 3 + \binom{n}{\frac{n}{2} - \sqrt{n}} - |\Gamma|} \left[- \left(\sum_{0 \leq j \leq m+4} \binom{n}{i} (n-1)^j \right) + \right.$$

$$\left. \left(\sum_{0 \leq i \leq 4} \binom{n}{i} (n-1)^i \right) \left(\sum_{0 \leq j \leq m} \binom{n}{j} (n-1)^j \right) \right] \tag{6.76}$$

while the randomized tradeoff is expressed by the probability

$$\text{Prob}_{\tau \in S_n} \left(\prod_{\sigma \in \mathcal{T} \backslash \Gamma} f\left(\mathbf{P}_\sigma \cdot \mathbf{P}_\tau \cdot \mathbf{w}\right) \neq 0 \,|\, \exists\, \mathbf{H} \in \Omega_2^{\sqrt{n} \times \sqrt{n}} \text{s.t. } \frac{\mathbf{H}^T \cdot \mathbf{H}}{\sqrt{n}} = \mathbf{I} \right) \leq$$

$$\frac{n! - \left|\text{Aut}\left\{f\left(\mathbf{r}\right)\right\}\right| \left|\mathcal{T} \backslash \Gamma\right|}{n!} = \left|\Gamma\right| \binom{n}{\frac{n}{2} - \sqrt{n}}^{-1} \tag{6.77}$$

Chapter 7
Conclusion

We have described here a polynomial encoding which provides a unified framework for discussing the algebra and the spectral analysis of matrices and hypermatrices. In addition to describing some algorithms for performing orthogonalization and spectral analysis of hypermatrices, we have presented some computational aspects, more specifically the important role of symmetries in Alon's Combinatorial Nullstellensatz method for solving combinatorial problems. It remains to determine in our furture work if the framework introduced here can be extended to less general family of combinatorial problems and most importantly yield comparable ressource performance. We also plan to investigate in subsequent work approximation algorithms inspired by the Alon's Combinatorial Nullstellensatz method.

References

[1] N. Alon. Combinatorial Nullstellensatz. Combinatorics, Probability and Computing, 8:7–29, 1999.

[2] N. Alon, I. Dinur, E. Friedgut, B. Sudakov. Graph products, Fourier analysis and spectral techniques, Geom. Funct. Anal. 14 (2004) 913–940.

[3] P. Bhattacharya. A new three-dimensional transform using a ternary product. *IEEE Trans. Signal Processing*, 43(12):pp.3081–3084, 1995.

[4] B. Buchberger. An algorithmic criterion for the solvability of a system of algebraic equations. *Aequationes Mathematicae 4*, pages pp.374–383, 1970.

[5] R. C. Bose, D. M. Mesner (1959), "On linear associative algebras corresponding to association schemes of partially balanced designs", Annals of Mathematical Statistics 30 (1): 21–38

[6] S.R. Bulò and M. Pelillo. New bounds on the clique number of graphs based on spectral hypergraph theory, T. Stützle ed., *Learning and Intelligent Optimization*, Springer Verlag, Berlin, (2009) pp. 45-48.

[7] S.R. Bulò and M. Pelillo. A generalization of the Motzkin-Straus theorem to hypergraphs, *Optim. Lett.* **3** (2009) 187-295.

[8] K. Braman. Third-order tensors as linear operators on a space of matrices, *Linear Algebra and Its Applications*, 433 (2010) 1241-1253.

[9] A. Cayley. On the theory of linear transformations, *Cambridge Math. J.*, 4 (1845) 1-16.

[10] J. Cooper and A. Dutle. Spectral of Hypergraphs, Department of Mathematics, University of South Carolina, June 2011, Arxiv preprint arXiv:1106.4856, 2011.

[11] C. H. Thomas, Leiserson, C. E., Rivest, L. Ronald , Stein, Clifford (2009) [1990]. Introduction to Algorithms (3rd ed.). MIT Press and McGraw-Hill. ISBN 0-262-03384-4.

[12] D. A. Cox, J. B. Little. D. O'Shea. *Ideals, Varieties, and Algorithms Third Edition, 2007*. Springer, 2007.

[13] D. Cartwright and B. Sturmfels. The number of eigenvalues of a tensor, to appear in: *Linear Algebra and Its Applications*.

[14] P. Comon, G. Golub, L.-H. Lim and B. Mourrain, "Symmetric tensors and symmetric tensor rank", *SIAM Journal on Matrix Analysis and Application*, 30 (2008) 1254-1279.

[15] L. D. Lathauwer, B. D. Moor and J. Vandewalle. On the best rank-1 and rank-$(R_1, R_2, \cdots, R_N)$ approximation of higher-order tensor, *SIAM J. Matrix Anal. Appl.*, 21 (2000) 1324-1342.

[16] R. P. Feynman. The Space-Time Formulation of Nonrelativistic Quantum Mechanics. Reviews of Modern Physics 20 (1948) 367–387.

[17] S. Friedland, S. Gaubert and L. Han. Perron-Frobenius theorem for nonnegative multilinear forms and extensions, to appear in: *Linear Algebra and Its Applications*.

[18] I.M. Gelfand, M.M. Kapranov and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants* Birkhauser, Boston, 1994.

[19] E. K. Gnang, A. Elgammal, V. Retakh. A Spectral Theory for Tensors, Annales de la faculté des sciences de Toulouse Sér. 6, 20 no. 4, p. 801-841, 2011.

[20] C.D. Godsil, B.D. McKay, Constructing cospectral graphs, Aequationes Math. 25 (1982) 257–268.

[21] R. A. Harshman. Foundations of the parafac procedure: Models and conditions for an explanatory multi-modal factor analysis. *UCLA working papers in phonetics*, 1970.

[22] J. Hastad. Tensor rank is np-complete. *J. Algorithms*, 11(4):644–654, 1990.

[23] L.-H. Lim and C. Hillar. Most tensor problems are np hard. *Preprint arXiv:0911.1393v2*, 2009.

[24] S. Hu, Z. Huang, C. Ling and L. Qi, "E-Determinants of tensors", arXiv Preprint 1109.0348v3 [math.NA] 13 Sep 2011.

[25] S. Hu, Z. Huang, H. Ni and L. Qi. Positive definiteness of diffusion kurtosis imaging, to appear in: *Inverse Problems and Imaging*.

[26] S. Hu, Z. Huang and L. Qi. Finding the spectral radius of a nonnegative tensor, Department of Applied Mathematics, The Hong Kong Polytechnic University, December 2010. arXiv: 1111.2138v1 [math.NA] 9 Nov 2011.

[27] S. Hu, Z. Huang and L. Qi. Finding extreme Z-eigenvalues of tensors via sequential SDPs, Department of Mathematics, Tianjin University, December 2011.

[28] S. Hu and L. Qi, Algebraic connectivity of an even uniform hypergraph, to appear in: *Journal of Combinatorial Optimization*.

[29] S. Hu and L. Qi, "Convergence of a second order Markov chain", Department of Applied Mathematics, The Hong Kong Polytechnic University, July, 2011, Revised: December 2011.

[30] M.E. Kilmer, C.D. Martin, and L. Perrone. A third-order generalization of the matrix svd as a product of third-order tensors. Technical Report Technical Report Number TR-2008-4, Tufts University Department of Computer Science, Medford, MA, October 2008.

[31] J. Kollár. Sharp Effective Nullstellensatz , Journal of the American Mathematical Society 1 (1988): 963–975

[32] T. G. Kolda, B. W. Bader, and J. P. Kenny. Higher-order web link analysis using multilinear algebra. In *ICDM '05: Proceedings of the Fifth IEEE International Conference on Data Mining*, pages 242–249, Washington, DC, USA, 2005. IEEE Computer Society.

[33] T. G. Kolda and J. Sun. Scalable tensor decompositions for multiaspect data mining. In *ICDM 2008: Proceedings of the 8th IEEE International Conference on Data Mining*, pages 363–372, December 2008.

[34] E. Kranakis: Invited Talk: Symmetry and Computability in Anonymous Networks. SIROCCO 1996: 1-16

[35] M.E. Kilmer, K. Braman, N. Hao and R.C. Hoover. Third order tensors as operators on matrices: a theoretical and computational framework with applications in imaging, Department of Computer Science, Tufts University, March 2011.

[36] T.G. Kolda and B.W. Bader. Tensor decompositions and applications, *SIAM Review*, 51 (2009) 455-500.

[37] T.G. Kolda and J.R. Mayo. Shifted power method for computing tensor eigenpairs, *SIAM J. Matrix Analysis*, 32 (2011) 1095-1124.

[38] L. D. Lathauwer, B. de Moor, and J. Vandewalle. Independent component analysis and (simultaneous) third-order tensor diagonalization. *IEEE Transactions on Signal Processing*, 49:2262–2271, October 2001.

[39] L. D. Lathauwer, B. D. Moor, and J. Vandewalle. A multilinear singular value decomposiiton. *SIAM Journal On Matrix Analysis and Applications*, 21(4):1253–1278, 2000.

[40] L. D. Lathauwer, B. D. Moor, and J. Vandewalle. On the best rank-1 and rank-(r1, r2, ..., rn) approximation of higher-order tensors. *SIAM Journal On Matrix Analysis and Applications*, 21(4):1324–1342, 2000.

[41] L.-H. Lim. Singular values and eigenvalues of tensors: a variational approach. *Proceedings of the IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing*, CAMSAP05(1):pp.129–132, 2005.

[42] L.-H. Lim. Singular values and eigenvalues of tensors: a variational approach, *Proceedings of the IEEE International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP '05)*, 1 (2005) 129-132.

[43] G. Li, L. Qi and G. Yu. Semismoothness of the maximum eigenvalue function of a symmetric tensor and its application, to appear in: *Linear Algebra and Its Applications*.

[44] G. Li, L. Qi and G. Yu. The Z-eigenvalues of a symmetric tensor and its application to spectral hypergraph theory, Department of Applied Mathematics, University of New South Wales, December 2011.

[45] J.A. De Loera, J. Lee, P.N. Malkin, and S. Margulies. Hilbert's Nullstellensatz and an algorithm for proving combinatorial infeasibility. http://arxiv.org/abs/0801.3788

[46] J. a. Loera, J. Lee, S. Margulies, and S. Onn. 2009. Expressing combinatorial problems by systems of polynomial equations and hilbert's nullstellensatz. Comb. Probab. Comput. 18, 4 (July 2009), 551-582.

[47] J. A. De Loera, J. Lee, P. N. Malkin, and S. Margulies. 2011. Computing infeasibility certificates for combinatorial problems through Hilbert's Nullstellensatz. J. Symb. Comput. 46, 11 (November 2011), 1260-1283.

[48] L. Lovász. Stable sets and polynomials. Discrete Mathematics, 124:137–153, 1994.

[49] L.-H. Lim, M. Ng and L. Qi. The Spectral Theory of Tensors and Its Applications, *Numerical Linear Algebra with Applications*. http://sites.google.com/site/tensorspectrum/

[50] S. Margulies. 2008. Computer Algebra, Combinatorics, and Complexity: Hilbert's Nullstellensatz and Np-Complete Problems. Ph.D. Dissertation. University of California at Davis, Davis, CA, USA. AAI3336295.

[51] D. M. Mesner, P. Bhattacharya Association schemes on triples and a ternary algebra. J. Comb. Theory, Ser. A 55(2): 204-234 (1990)

[52] D. M. Mesner, P. Bhattacharya A ternary algebra arising from association schemes on triples Journal of Algebra 01/1994; 164(1):595-613.

[53] K.J. Pearson, Essentially positive tensors, *International Journal of Algebra*, 9 (2010) 421-427.

[54] L. Qi. Eigenvalues of a real supersymmetric tensor. *Journal of Symbolic Computation*, 40:pp.1302–1324, 2005.

[55] L. Qi. Rank and eigenvalues of a supersymmetric tensor, the multivariate homogeneous polynomial and the algebraic hypersurface it defines. *Journal of Symbolic Computation*, 41(12):pp.1309–1327, 2006.

[56] L. Qi. Eigenvalues and invariants of tensors. *Journal of Mathematical Analysis and Applications*, 325:pp.1363–1377, 2007.

[57] L. Qi. Eigenvalues of a real supersymmetric tensor, *J. Symbolic Computation*, 40 (2005) 1302-1324.

[58] L. Qi. Rank and eigenvalues of a supersymmetric tensor, the multivariate homogeneous polynomial and the algebraic hypersurface it defines, *Journal of Symbolic Computation*, 41 (2006) 1309-1327.

[59] L. Qi. Eigenvalues and invariants of tensors, *Journal of Mathematical Analysis and Applications*, 325 (2007) 1363-1377.

[60] L. Qi, The best rank-one approximation ratio of a tensor space, *SIAM Journal on Matrix Analysis and Applications*, 32 (2011) 430-432.

[61] L. Qi, H.H. Dai and D. Han. Conditions for strong ellipticity and M-eigenvalues, *Frontiers of Mathematics in China*, 4 (2009) 349-364.

[62] L. Qi, D. Han and E.X. Wu. Principal invariants and inherent parameters of diffusion kurtosis tensors, *Journal of Mathematical Analysis and Applications*, 349 (2009) 165-180.

[63] L. Qi, W. Sun and Y. Wang. Numerical multilinear algebra and its applications, *Frontiers of Mathematics in China*, 2 (2007) 501-526.

[64] S. Ben-Israel, E. Ben-Sasson, D. R. Karger: Breaking local symmetries can dramatically reduce the length of propositional refutations. Electronic Colloquium on Computational Complexity (ECCC) 17: 68 (2010)

[65] J. A. Schwenk .Almost all trees are cospectral. New directions in the theory of graphs (Proc. Third Ann Arbor Conf., Univ. Michigan, Ann Arbor, Mich., 1971), pp. 275–307. Academic Press, New York, 1973.

[66] T. Tao, Higher order Fourier analysis, Graduate Studies in Mathematics, 142 American Mathematical Society, 2012 ISBN-10: 0-8218-8986-9

[67] L.R. Tucker. Some mathematical notes on three-mode factor analysis. *Psychometrika*, 31:279–311, 1966.

[68] C. Van Loan, Future dirctions in tensor-based computation and modeling, Workshop Report in Arlington, Virginia at National Science Foundation, February 20-21, 2009. http://www.cs.cornell.edu/cv/TenWork/Home.htm.

[69] M.E. Kilmer and C.D. Moravitz Martin. Decomposing a tensor. *SIAM News*, 37(9), 2004.