Tensor Isomorphism over Some Matrix Groups and Its Applications

by

Zhili Chen

A thesis submitted in satisfaction of the

requirements for the degree of

Master of Science (Research)

in the

Faculty of Engineering and Information Technology

at the

University of Technology Sydney

December 2023

Certificate of Original Authorship

I, Zhili Chen, declare that this thesis is submitted in fulfilment of the requirements for the award of Master of Science (Research), in the School of Computer Science, Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Production Note:
Signature removed prior to publication.

Signature of Author

List of Publications

This thesis is based on the following paper.

[CGQ+23]: **Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang.** On the complexity of isomorphism problems for tensors, groups, and polynomials III: actions by classical groups. To appear in 15th In- novations in Theoretical Computer Science Conference (ITCS 2024), 2023, arXiv:2306.03135.

Abstract

Tensor Isomorphism over Some Matrix Groups and Its Applications

by

Zhili Chen

Master of Science (Research)

University of Technology Sydney

We study the complexity of isomorphism problems for d-way arrays under natural actions by different matrix groups such as the general linear group, unitary group, orthogonal group and symplectic group. Such problems naturally relate to statistical data analysis and quantum information. We study two types of complexity-theoretic questions. First, for a fixed action type (congruence, conjugacy, etc.), we relate the complexity of the isomorphism problem over classical groups to that over symmetric group or general linear group. Second, for a fixed group type (orthogonal or unitary), we compare the complexity of deciding isomorphism under different actions.

Our main results are as follows. First, for orthogonal (symplectic) group acting on 3-way arrays, the isomorphism problem reduces to the corresponding problem over the general linear group. Second, for orthogonal (unitary) group, the isomorphism problems of five natural actions on 3-way arrays are polynomial-time equivalent, and the d-tensor isomorphism problem reduces to the 3-tensor isomorphism problem for any fixed $d > 3$. The preceding result for unitary groups implies that determining tripartite quantum states equivalence under local operations and classical communication (LOCC) is at least as difficult as determining d-partite quantum states equivalence under LOCC for any constant d. Lastly, we also show that the graph isomorphism problem reduces to the tensor isomorphism problem over orthogonal and unitary groups.

Acknowledgements

First and foremost I would like to express my deepest gratitude to my supervisor Youming Qiao, who gave me the chance to participate in this project. Without him this thesis would not have been possibly started. I am thankful for his patient guidance, detailed feedback, and insightful discussions, which significantly contributed to the development of this thesis and several talks. His dedication to research has taught me the importance of rigorous thinking, precise expression, and enduring patience in the pursuit of knowledge.

I would also like to express my appreciation to my co-supervisor, Troy Lee, with whom I engaged in insightful discussions throughout my Master's program. Additionally, I am grateful for the opportunity he provided me to serve as his tutor, which not only enriched my academic experience but also supported my living expenses.

It's very fortune for me to collaborate with Chuanqi Zhang and Gang Tang, who have a highly strong impact on enhancing my scientific skills. I extend my thanks for our extensive discussions over the past two years and the invaluable perspectives gained during this process.

I am honored to work alongside other collaborators, particularly Joshua Grochow. I would also like to express my gratitude to other excellent researchers, including Bin Cheng, Miklos Santha, Yan Peng, and Zhicheng Zhang, for our engaging discussions and shared insights. I am grateful to my defense committees, Bo Liu and Ryan Mann, for reviewing this thesis.

Contents

Chapter 1

Introduction

This introduction chapter is organized as follows. We will first review the history of Graph Isomorphism in Section 1.1.1 and then focus on the background of Tensor Isomorphism in Section 1.1.2. We introduce Tensor Isomorphism over *classical groups* and describe motivations to study these actions over classical groups in Section 1.2. We then present our main results in Section 1.3 and provide an application of our results on *Local Operation and Classical Communication* (LOCC) in Section 1.4. Finally, we give an overview of the proofs and list technical obstacles in Section 1.5.

1.1 Background

1.1.1 Graph Isomorphism

Graph Isomorphism is one of the most well-known problems in computational complexity, which asks to decide if there is an edge-preserving bijection between vertex sets of two given graphs.

Graph Isomorphism is known to be an NP problem. It was shown to be in coAM [Sch88], which implies that Graph Isomorphism is not a NP-complete problem unless polynomial hierarchy collapses to the second level. Besides, Babai's quasi-polynomial algorithm also implies that exponential time hierarchy collapses if Graph

Isomorphism is NP-complete [Bab16]. Some NP-intermediate candidatures such as Linear Programming and Primes, which were proved to be actually problems in P [Hač80, AKS19]. Given that the best algorithm for Graph Isomorphism is not yet in the polynomial time, Graph Isomorphism is believed to be in the NP-intermediate.

In addition, Graph Isomorphism also appeared in *zero-knowledge proofs*. The zero-knowledge proof scheme designed by Goldreich, Micali and Wigderson is based on Graph Isomorphism [GMW91]. This prototype was generalized to other proof systems based on isomorphism problems such as Alternating Trilinear Form Equivalence and Matrix Code Equivalence [TDJ+22, CNP+23].

Besides the theoretical result [Bab16], Graph Isomorphism has been known to be easily solvable in practice for a long time [McK81, MP14]. Therefore, it's natural to ask if there are any isomorphism type problems harder than Graph Isomorphism. There are some proposed problems listed by Babai [Bab16], including Group Isomorphism, Permutational Code Equivalence and Permutation Group Conjugacy.

In fact, most isomorphism problems can be formulated as algorithmic problems for *group actions*. Given a group $\mathcal{G}$ acting on a set S, the isomorphism problem for this action asks to decide, given $s, t \in S$, whether there is a group element $g \in \mathcal{G}$ such that g sends s to t. Given an element s, the subset containing all elements sent from s by an arbitrary group element g is said to be the *orbit* of s, i.e., $\{s' \in S \mid s' = s \circ g, g \in \mathcal{G}\}$. Graph Isomorphism was represented as the isomorphism problem for the action of the symmetric group S_n on $2^{\binom{[n]}{2}}$ [Luk82], the power set of the set of size-2 subsets of $[n]$, which represents all pairs of vertices in the graph.

1.1.2 Tensor Isomorphism

Isomorphism problems of *tensors, groups, and polynomials* over direct products of *general linear groups*, which can also be formulated as isomorphism problems by general linear group actions, are considered to be a natural linear algebraic analogue for Graph Isomorphism. Previously in [FGS19, GQ23a, GQ21, GQT22, RST22], isomorphism problems of tensors, groups, and polynomials over direct products of general linear groups were studied from the complexity-theoretic viewpoint. In particular, it turns out that Tensor Isomorphism occupies the central position among above problems, and hence a complexity class TI was defined in [GQ23a], which contains problems polynomial-time reducible to Tensor Isomorphism.

More specifically, several isomorphism problems, including those for tensors, groups, and polynomials, were shown to be reducible to 3-Tensor Isomorphism [FGS19]. Another work first showed the reversed direction: 3-Tensor Isomorphism is reducible to all those problems [GQ23a]. Another result from this work indicates that d-Tensor Isomorphism is reducible to 3-Tensor Isomorphism. The above results imply that those isomorphism problems for tensors, groups, and polynomials are TI-complete, including 3-Tensor Isomorphism. It was also proved in [GQ23a] that Graph Isomorphism is polynomial-time reducible to 3-Tensor Isomorphism. It gives theoretical evidence such that TI is a harder class than GI.

There is another group of results by Agrawal, Kayal and Saxena [KS06,AS05,AS06], who demonstrated some reductions between Ring Isomorphism, Cubic Form Equivalence and isomorphism problems for commutative, unital, associative algebras. The equivalence between polynomials and 3-tensors was shown subsequently but independently in [RST22]; some problems over products of general linear groups with monomial groups were also shown to be TI-complete [D'A23]. Therefore, a wide class of problems were shown to be equivalent and TI-complete. Recently, a breakthrough on group isomorphism by Sun [Sun23] can be transferred to an asymptotically faster algorithm for TI over finite fields [GQ23b].

TI-complete problems arise in many areas, including cryptography, quantum information, machine learning and computational algebra. Thus, studying complexity of these problems helps us better understand many potential applications. Specifically, in cryptography, several isomorphism problems were suggested strong enough to be assumptions for digital signature scheme [Pat96, JQSY19, TDJ+22]. In quantum information, it was showed that determining SLOCC equivalences of d-partite pure states, $d > 3$, can be reduced to determining such equivalences for tripartite pure states [GQ23a].

1.2 Tensor Isomorphism over Matrix Groups

In this thesis, we study isomorphism problems of tensors, groups, and polynomials over some *classical groups*, such as *orthogonal, unitary, and symplectic groups*, from the computational complexity viewpoint. We denote those problems by Tensor $\mathcal{G}$-Isomorphism, where $\mathcal{G}$ is some matrix group. For convenience, we denote Tensor Isomorphism as Tensor $\mathcal{G}$-Isomorphism for $\mathcal{G}$ being the general linear group.

1.2.1 Classical Groups

Let V be a vector space over a field $\mathbb{F}$. Let $\mathrm{GL}(V)$ be the general linear group over V, which consists of all invertible linear maps on V. Classical groups are subgroups of general linear groups, which preserves some forms. Let $\phi : V \times V \to \mathbb{F}$ be a bilinear or sesquilinear form on V. In the case when ϕ is sesquilinear, $\mathbb{F}$ is a quadratic extension of a subfield $\mathbb{K}$; sesquilinear means that it is linear in one argument and anti-linear in the other, i.e., $\forall u, v \in V, \forall \alpha, \beta \in \mathbb{F}, \phi(u\alpha, v\beta) = \alpha^*\phi(u, v)\beta$. Then $\mathrm{GL}(V)$ acts on ϕ naturally, by $M \in \mathrm{GL}(V)$ sending ϕ to $\phi \circ M$, defined as $(\phi \circ M)(v, v') = \phi(M(v), M(v'))$. The subgroup of $\mathrm{GL}(V)$ that preserves ϕ is denoted as $\mathcal{G}(V, \phi) := \{M \in \mathrm{GL}(V) \mid \phi \circ M = \phi\}$.

It is well-known that some classical groups arise as $\mathcal{G}(V, \phi)$.

(1) Let $\mathbb{F} = \mathbb{C}$. Let ϕ be the sesquilinear form on $V = \mathbb{C}^n$ defined as $\phi(u, v) = \sum_{i \in [n]} u_i^* v_i$, where u_i^* is the complex conjugate of u_i. Then $\mathcal{G}(V, \phi)$ is the unitary group $\mathrm{U}(n, \mathbb{C})$.

(2) Let $\mathbb{F} = \mathbb{R}$. Let ϕ be the symmetric bilinear form on $V = \mathbb{R}^n$ defined as $\phi(u, v) = \sum_{i \in [n]} u_i v_i$. Then $\mathcal{G}(V, \phi)$ is the orthogonal group $\mathrm{O}(n, \mathbb{R})$.

(3) Let ϕ be the skew-symmetric bilinear form on $V = \mathbb{F}^{2n}$, defined as $\phi(u, v) = \sum_{i\in[n]}(u_i v_{2n-i+1} - u_{n+i} v_{n-i+1})$. Then $\mathcal{G}(V, \phi)$ is the symplectic group $\mathrm{Sp}(2n, \mathbb{F})$.

Depending on the underlying fields, orthogonal groups may indicate some families of groups preserving different (non-congruent) symmetric forms. In this thesis we always use orthogonal groups and unitary groups w.r.t. the standard bilinear or sesquilinear form as defined above.

1.2.2 Motivation

There are several motivations to study tensor isomorphism over classical groups from statistical data analysis and quantum information.

The term "classical groups" appeared in Weyl's classic [Wey97], though there are multiple competing possibilities for what this term should mean formally [Hum]. In this thesis, we will be mostly concerned with *groups consisting of elements that preserve a bilinear or sesquilinear form*, which include orthogonal groups O, symplectic groups Sp, and unitary groups U, among others. As subgroups of GL, they act naturally on d-way arrays.

Actions by classical groups on d-way arrays have arisen in several areas of computational and applied mathematics [Lim21]. In this subsection we examine some of these applications mainly from statistical data analysis and quantum information.

Warm up: singular value decomposition. We introduce motivations by considering the action on 2-way arrays (matrices), i.e., the action of $(A, B) \in \mathrm{U}(n, \mathbb{C}) \times \mathrm{U}(m, \mathbb{C})$ on $C \in \mathrm{M}(n \times m, \mathbb{C})$ sending C to $A^* C B$, where A^* denotes the conjugate transpose of A. The equivalences of matrices under this action are determined by the Singular Value Theorem, which states that every $C \in \mathrm{M}(n \times m, \mathbb{C})$ can be written as $A^* D B$ where $A \in \mathrm{U}(n, \mathbb{C})$, $B \in \mathrm{U}(m, \mathbb{C})$, and $D \in \mathrm{M}(n \times m, \mathbb{C})$ is a rectangular diagonal matrix. Furthermore, the diagonal entries of D are non-negative real numbers, called the singular values of C. Similar result holds for $\mathrm{O}(n, \mathbb{R}) \times \mathrm{O}(m, \mathbb{R})$ acting on $\mathbb{R}^n \otimes \mathbb{R}^m$.

This example indicates that the equivalent classes of unitary matrix groups on matrices is different from the action of general linear matrix groups on matrices. Indeed, the former is determined by singular values (of which there are continuum many choices) and the latter is determined by rank (of which there are only finitely many choices). Motivated by this point, we can question if this will hold for d-way arrays where $d \leq 3$?

Orthogonal isomorphism of tensors from data analysis. The singular value decomposition is the basis for the Eckart–Young Theorem [EY36], which states that the best rank-r approximation of a real matrix C is the one obtained by summing up the rank-1 components corresponding to the largest r singular values. To obtain a generalization of such a result to d-way arrays, $d > 2$, is a central problem in statistical analysis of multiway data [DSL08].

Due to the close relation between singular value decomposition and orthogonal groups acting on matrices, it may not be surprising that the orthogonal equivalence of real d-way arrays is studied in this context [DLDMV00, DSL08, HU17, Sei18]. For example, one question is to study the relation between "higher-order singular values" and orbits under orthogonal group actions. From the perspective of the orthogonal equivalence of d-way arrays, such higher-order singular values are natural isomorphism invariants, though they do not characterize orbits as in the matrix case. In the literature, d-way arrays under orthogonal group actions are sometimes called Cartesian tensors [Tem04].

Unitary isomorphism of tensors from quantum information. We now turn to $\mathbb{F} = \mathbb{C}$ and consider the action of a product of unitary groups; such actions arise in at least two distinct ways in quantum information, which we highlight here: as LU or LOCC equivalence of quantum states, and as unitary equivalence of quantum channels.

In quantum information, unit vectors in $\mathrm{T}(n_1 \times \cdots \times n_d, \mathbb{C}) \cong \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_d}$ are called pure states, and two pure states are called local unitary (LU) equivalent, if they are in the same orbit under the natural action of $\mathbf{U} := \mathrm{U}(n_1, \mathbb{C}) \times \cdots \times \mathrm{U}(n_d, \mathbb{C})$ (where the i-th factor of the group acts on the i-th tensor factor). By Bennett *et al.* [BPR+00], the LU equivalence of pure states also captures their equivalence under local operations and classical communication (LOCC), which means that LU-equivalent states are interconvertible by reasonable physical operations.

A completely positive map is a function $f : \mathrm{M}(n, \mathbb{C}) \to \mathrm{M}(n, \mathbb{C})$ of the form $f(A) = \sum_{i\in[m]} B_i A B_i^*$ for some complex matrices $B_i \in \mathrm{M}(n, \mathbb{C})$; quantum channels are given precisely by the completely positive maps that are also "trace-preserving", in the sense that $\sum_{i\in[m]} B_i^* B_i = I_n$. Two tuples of matrices $(B_1, \ldots, B_m)$ and $(B_1', \ldots, B_m')$ define the same completely positive map if and only if there exists $S = (s_{i,j}) \in \mathrm{U}(m, \mathbb{C})$ such that $\forall i \in [m]$, $B_i = \sum_{j\in[m]} s_{i,j} B_j'$ [NC00, Theorem 8.2]. And two quantum channels $f, g : \mathrm{M}(n, \mathbb{C}) \to \mathrm{M}(n, \mathbb{C})$ are called unitarily equivalent if there exists $T \in \mathrm{U}(n, \mathbb{C})$ such that for any $A \in \mathrm{M}(n, \mathbb{C})$, $T^* f(A) T = g(T^* A T)$. Thus, two matrix tuples $(B_1, \ldots, B_m)$ and $(B_1', \ldots, B_m')$ define the unitarily equivalent quantum channels if and only if their corresponding 3-way arrays in $\mathrm{T}(n \times n \times m, \mathbb{C})$ are in the same orbit under a natural action of $\mathrm{U}(n, \mathbb{C}) \times \mathrm{U}(m, \mathbb{C})$.

Classical groups arising from Code Equivalence. Classical groups may appear even when we start with general linear or symmetric groups. Here is an example from code equivalence. Recall that the (permutation linear) code equivalence problem asks the following: given two matrices $A, B \in \mathrm{M}(d \times n, q)$, decide if there exist $C \in \mathrm{GL}(d, q)$ and $P \in \mathrm{S}_n$, such that $A = CBP$. One algorithm for this problem, under some conditions on A and B, from [BOST19] goes as follows. Suppose it is the case that $A = CBP$. Then $AA^t = CBPP^t B^t C^t = CBB^t C^t$. This means that AA^t and BB^t are congruent. Assuming that AA^t and BB^t are full-rank, then up to a change of basis, we can set that $AA^t = BB^t =: F$, so any such C must lie in a classical group preserving the form F. We are then reduced to the problem of asking whether A and B are equivalent up to some C from a classical group and some P from a permutation group. This problem, as shown in [BOST19], reduces to Graph Isomorphism.

Some preliminary remarks on the algorithms for Tensor Isomorphism over classical groups. Although we show that Orthogonal TI and Unitary TI are still GI-hard (Theorem 3.4), from the current literature it seems that orthogonal and unitary isomorphism of tensors are easier than general-linear isomorphism. There are currently two reasons for this: the first is mathematical, and the second is based on practical algorithmic experience, which we now discuss.

One mathematical reason why these problems may be easier is that there are easily computable isomorphism invariants for such actions, while such invariants are not known for general-linear group actions. Here is one construction of a quite effective invariant in the unitary case. From $\mathrm{A} = (a_{i,j,k}) \in \mathrm{T}(n \times n \times n, \mathbb{C})$, construct its matrix flattening $B = (b_{i,j}) \in \mathrm{M}(n \times n^2, \mathbb{C})$, where $b_{i,j\cdot n+k} = a_{i,j,k}$. Then it can be verified easily that $|\det(BB^*)|$ is a polynomial-time computable isomorphism invariant for the unitary group action $\mathrm{U}(n, \mathbb{C}) \times \mathrm{U}(n, \mathbb{C}) \times \mathrm{U}(n, \mathbb{C})$. However, it is not known whether such isomorphism invariants for the general linear group action exist—if they did, they would break the pseudo-random assumption for this action proposed in [JQSY19].

Practically speaking, current techniques seem much more effective at solving tensor isomorphism-style problems over the orthogonal group than over the general linear group. It is not hard to formulate Tensor Isomorphism and related problems over general linear and some classical groups as solving systems of polynomial equations. Motivated by cryptographic applications [TDJ+22], we chose a TI-complete problem Alternating Trilinear Form Isomorphism [GQT22], and carried out experiments using the Gröbner basis method for this problem, implemented in Magma [BJP97]. For some details of these experiments see Appendix A. We fixed the underlying field order as 32771 (a large prime that is close to a power of 2). Over the general linear group for $n = 7$, the solver ran for about 3 weeks on a server, eating 219.7 GB memory, yet still did not complete with a solution. Over the orthogonal group for odd n, the data are shown in Table 1.1. In particular, the solver returns a solution for $n = 21$ in about 3.6 hours, a sharp contrast to the difficulty met when solving the problem under the general linear group action.

n	7	9	11	13	15	17	19	21
Time (in s)	0.396	5.039	37.120	140.479	524.520	1764.179	4720.129	12959.799

Table 1.1: The experiment results of the Gröbner basis method to solve the problem of isomorphism of alternating trilinear forms under the action of the orthogonal group.

1.3 Results

In this thesis, we study relations between Tensor Isomorphism under classical groups and that of other groups from complexity-theoretic aspects. We focus on the following three types of questions:

(1) Consider two classical groups $\mathcal{G}$ and $\mathcal{H}$, and fix the way they act on d-way arrays. What are the relations between the isomorphism problems defined by these groups?

(2) Fix a classical group $\mathcal{G}$, and consider its different actions on 3-way arrays. What are the relations between the isomorphism problems defined by these actions?

(3) Fix a classical group $\mathcal{G}$. What are the relations between d-Tensor Isomorphism and 3-Tensor Isomorphism?

Questions of the first type were implicitly studied in [HQ21, GQ23a, GQ21] for some classes of d-way arrays, with the groups being either general linear or symmetric groups. For example, starting from a graph G, one can construct a 3-way array A_G encoding this graph following Edmonds, Tutte and Lovász [Tut47,Edm65,Lov79], and it is shown in [HQ21] that G and H are isomorphic (a notion based on the symmetric groups S_n) if and only if A_G and A_H are isomorphic (under a product of general linear groups).

Questions of the second type were studied in [FGS19,GQ23a] for GL. For example, one main result in [FGS19,GQ23a] is to show the polynomial-time equivalence of the five isomorphism problems for 3-way arrays under (direct products of) general linear groups (cf. Chapter 2).

Questions of the third type were studied in [GQ23a] for GL. It was showed in [GQ23a] that d-Tensor Isomorphism reduces to 3-Tensor Isomorphism in polynomial time.

Still, to the best of our knowledge, these types of questions have not been studied for orthogonal, unitary, and symplectic groups, which are the focus in this thesis.

1.3.1 Relations between Different Groups

Our first result shows that isomorphism problems of tensors under classical groups are sandwiched between the celebrated Graph Isomorphism problem and the more familiar Tensor Isomorphism problem under GL. We use S_n to denote the symmetric group of degree n, and view S_n as a subgroup of $\mathrm{GL}(n, \mathbb{F})$ naturally via permutation matrices. We use $\leq$ to denote the subgroup relation. When we say "reduces", briefly, we mean: polynomial-time computable kernel reductions [FG11] (there is a polynomial-time function r sending (A, B) to $(r(A), r(B))$, such that the map $(A, B) \mapsto (r(A), r(B))$ is a many-one reduction of isomorphism problems), that are typically polynomial-size projections ("p-projections") in the sense of Valiant [Val79], functorial (on isomorphisms), and containments in the sense of the literature on wildness. Some reductions that use a non-degeneracy condition may not be p-projections. See [GQ23a, Sec. 2.3] for details on these notions.

Theorem 1.1. *Suppose a group family $\mathcal{G} = \{\mathcal{G}_n\}$ satisfies that $\mathrm{S}_n \leq \mathcal{G}_n \leq \mathrm{GL}(n, \mathbb{F})$, where here S_n denotes the group of $n \times n$ permutation matrices. Then Graph Isomorphism reduces to Bilinear Form $\mathcal{G}$-Pseudo-isometry, that is, the isomorphism problem for the action of $\mathcal{G}(U) \times \mathcal{G}(V)$ on $U \otimes U \otimes V$.*

Let $\mathcal{G}_n \leq \mathrm{GL}(n, \mathbb{F})$. We say that $\mathcal{G}_n$ *preserves a bilinear form*, if there exists some $A \in \mathrm{M}(n, \mathbb{F})$, such that $\mathcal{G}_n = \{T \in \mathrm{GL}(n, \mathbb{F}) \mid T^t A T = A\}$. For example, orthogonal and symplectic groups are defined as preserving full-rank symmetric and skew-symmetric forms.

Theorem 1.2. *Let $\mathcal{G} = \{\mathcal{G}_n \mid \mathcal{G}_n \leq \mathrm{GL}(n, \mathbb{F})\}$ be a group family preserving a polynomial-time-constructible family of bilinear forms,*[1] *and consider one of the five actions of* GL *on* 3*-way arrays in Definition 1.4. The restricted $\mathcal{G}$-isomorphism problem for this action reduces to the* GL*-isomorphism problem for this action.*

Remark 1.3. Recall from Section 1.2.2 that the orthogonal equivalence of matrices (determined by singular values) is more involved than the general-linear equivalence of matrices (determined by ranks) over $\mathbb{R}$. By a counting argument, there is unconditionally no polynomial-size kernel reduction [FG11] (mapping matrices to matrices) from Orthogonal Equivalence of Matrices to General Linear Equivalence of Matrices. In contrast, Theorem 1.2 shows that for 3-way arrays, orthogonal isomorphism does reduce to general-linear isomorphism.

1.3.2 Relations between Different Actions.

Our second result is concerned with different actions of the same group on d-way arrays. Our main results are for the real orthogonal groups and complex unitary groups; we discuss some difficulties encountered with symplectic groups in Chapter 7, and leave opening the questions for more general bilinear-form-preserving groups.

We begin with the five actions in Definition 1.4.

Group actions on arrays. Let $\mathrm{T}(\ell \times m \times n, \mathbb{F})$ be the linear space of $\ell \times m \times n$ 3-way arrays over $\mathbb{F}$. Given $\mathrm{A} \in \mathrm{T}(\ell \times m \times n, \mathbb{F})$, the (i, j, k)th entry of A is denoted as $\mathrm{A}(i, j, k) \in \mathbb{F}$. We can slice A along one direction and obtain several matrices, which are called slices. For example, slicing along the third coordinate, we obtain the *frontal* slices, namely n matrices $A_1, \ldots, A_n \in \mathrm{M}(l \times m, \mathbb{F})$, where $A_k(i, j) = \mathrm{A}(i, j, k)$. Similarly, we also obtain the *horizontal* slices by slicing along the first coordinate, and the *lateral* slices by slicing along the second coordinate.

[1] That is, the function $\Phi \colon \mathbb{N} \to \mathrm{M}(n, \mathbb{F})$ giving a matrix for the form preserved by $\mathcal{G}_n$ is computable in polynomial time. We note that no such restriction was needed in Theorem 1.1.

A 3-way array allows for group actions in three directions. Given $P \in \mathrm{M}(\ell, \mathbb{F})$ and $Q \in \mathrm{M}(m, \mathbb{F})$, let $P\mathrm{A}Q$ be the $\ell \times m \times n$ 3-way array whose kth frontal slice is PA_kQ. For $R = (r_{i,j}) \in \mathrm{M}(n, \mathbb{F})$, let A^R be the $\ell \times m \times n$ 3-way array whose kth frontal slice is $\sum_{k' \in [n]} r_{k',k} A_{k'}$.

There are several group actions of direct products of matrix groups on d-way arrays, based on interpretations of d-way arrays as different multilinear algebraic objects. For example, there are three well-known natural actions on matrices: for $A \in \mathrm{M}(n, \mathbb{F})$, (1) $(P, Q) \in \mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$ sends A to $P^t AQ$, (2) $P \in \mathrm{GL}(n, \mathbb{F})$ sends A to $P^{-1}AP$, and (3) $P \in \mathrm{GL}(n, \mathbb{F})$ sends A to $P^t AP$. These three actions endow A with different algebraic or geometric interpretations: (1) a linear map from a vector space V to another vector space W, (2) a linear map from V to itself, and (3) a bilinear map from $V \times V$ to $\mathbb{F}$.

Analogously, there are five natural actions on 3-way arrays, which we collect in the following definition (see [GQ23a, Sec. 2.2] for more discussion of why these five capture all possibilities within a certain natural class).

Definition 1.4. We define five actions of (direct products of) some matrix groups on 3-way arrays.

(1) Given $\mathrm{A} \in \mathrm{T}(l \times m \times n, \mathbb{F})$, $(P, Q, R) \in \mathcal{G}(l, \mathbb{F}) \times \mathcal{G}(m, \mathbb{F}) \times \mathcal{G}(n, \mathbb{F})$ sends A to $P^t \mathrm{A}^R Q$;

(2) Given $\mathrm{A} \in \mathrm{T}(l \times l \times m, \mathbb{F})$, $(P, Q) \in \mathcal{G}(l, \mathbb{F}) \times \mathcal{G}(m, \mathbb{F})$ sends A to $P^t \mathrm{A}^Q P$;

(3) Given $\mathrm{A} \in \mathrm{T}(l \times l \times m, \mathbb{F})$, $(P, Q) \in \mathcal{G}(l, \mathbb{F}) \times \mathcal{G}(m, \mathbb{F})$ sends A to $P^t \mathrm{A}^Q P^{-t}$;

(4) Given $\mathrm{A} \in \mathrm{T}(l \times l \times l, \mathbb{F})$, $P \in \mathcal{G}(l, \mathbb{F})$ sends A to $P^t \mathrm{A}^{P^{-t}} P$;

(5) Given $\mathrm{A} \in \mathrm{T}(l \times l \times l, \mathbb{F})$, $P \in \mathcal{G}(l, \mathbb{F})$ sends A to $P^t \mathrm{A}^P P$,

where P^{-t} denotes the transpose inverse of P.

Considering the matrix group as the general linear group, these five actions naturally arise in, by viewing 3-way arrays as encoding, respectively: (1) tensors or matrix spaces (up to equivalence), (2) p-groups of class 2 and exponent p, quadratic polynomial maps, or bilinear maps, (3) matrix spaces up to conjugacy, (4) algebras, and (5) trilinear forms or (non-commutative) cubic forms. For details on these interpretations, we refer the reader to [GQ23a, Sec. 2.2]. Note that for the orthogonal group $\mathrm{O}(n, \mathbb{R})$, there are essentially three actions instead of five (because $P^{-t} = P$ for $P \in \mathrm{O}(n, \mathbb{R})$).

To help specify which of the five actions we are talking about, we use the following shorthand notation from multilinear algebra[2]. Let $U \cong \mathbb{F}^l$, $V \cong \mathbb{F}^m$ and $W \cong \mathbb{F}^n$. The dual space of a vector space U is denoted as U^*. Then action (1) is referred to as $U \otimes V \otimes W$, (2) is $U \otimes U \otimes V$, (3) is $U \otimes U^* \otimes V$, (4) is $U \otimes U \otimes U^*$, and (5) is $U \otimes U \otimes U$. Note that from this shorthand notation, one can directly read off the action as in Definition 1.4 and vice versa. Then we have the following result that different actions of unitary groups (or orthogonal groups) on arrays are equivalent.

Theorem 1.5. *Let $\mathcal{G}$ be either the unitary over $\mathbb{C}$ or orthogonal over $\mathbb{R}$ group family. Then the five isomorphism problems corresponding to the five actions of $\mathcal{G}$ on 3-way arrays in Definition 1.4 are polynomial-time equivalent to one another.*

1.3.3 d-Tensor $\mathcal{G}$-Isomorphism to 3-Tensor $\mathcal{G}$-Isomorphism

Our third result is a reduction from the isomorphism problem over some classical group $\mathcal{G}$ for d-way arrays to that for 3-way arrays. Here, we also constrict the classical group $\mathcal{G}$ to be either the orthogonal groups or unitary groups. To prove the correctness of this reduction, we utilized different techniques from those in [GQ23a].

Theorem 1.6. *Let $\mathcal{G}$ be the unitary over $\mathbb{C}$ or orthogonal over $\mathbb{R}$ group family. For any fixed $d \geq 1$, d-Tensor $\mathcal{G}$-Isomorphism reduces to 3-Tensor $\mathcal{G}$-Isomorphism.*

[2]See [Lim21] for a nice survey of various viewpoints of tensors. For us, we have to start with the d-way array viewpoint, because we wish to study the relations between different actions, and the constructions are more intuitively described by examining the arrays.

1.4 Application

An application in quantum information. As introduced in Section 1.2.2, LU equivalence, characterizes the equivalence of quantum states under local operations and classical communication (LOCC). We refer the interested reader to the nice paper [CLM+14] for the LOCC notion, as well as the classification of three-qubit states based on LOCC [ABLS01].

By the work of Bennett *et al.* [BPR+00], LOCC equivalence of pure quantum states is the same as the equivalence of unit vectors in $V_1 \otimes V_2 \otimes \cdots \otimes V_d$ where V_i are vector spaces over $\mathbb{C}$. Our Theorem 1.6 can then be interpreted as saying that classifying tripartite quantum states under LOCC equivalence is as difficult as classifying d-partite quantum states under LOCC equivalence. This may be compared with the result in [ZLQ18], which states that classifying d-partite states reduces to classifying tensor networks of tripartite or bipartite tensors. (We note that the analogous result for SLOCC, via the general linear group action, was shown in [GQ23a]; in the next section we discuss how our proof here differs from the one there.)

1.5 Techniques

1.5.1 Overview of the Proofs

In the following, we present proof outlines for Theorems 1.1, 1.2, 1.5, and 1.6. While these proofs are inspired the strategies of previous results [FGS19, GQ23a, LQW+23], new technical ingredients are indeed needed, such as the Singular Value Theorem, and a certain Krull–Schmidt type result for matrix tuples under unitary group actions. We also wish to highlight that, Theorem 1.6 requires not only using a quiver different from that in the proof of [GQ23a, Theorem 1.2], but also a completely new and much simpler argument.

About Theorem 1.1. For Theorem 1.1, we start with Directed Graph Isomorphism (DGI), which is GI-complete. We then use a natural construction of 3-way arrays from directed graphs as recently studied in [LQW+23], which takes an arc (i, j) and constructs an elementary matrix $\mathrm{E}_{i,j}$. By [LQW+23, Observation 6.1, Proposition 6.2], DGI reduces to the isomorphism problem of $U \otimes U \otimes W$ under $\mathrm{GL}(U) \times \mathrm{GL}(W)$. Theorem 1.1 is shown by observing that the proofs of [LQW+23, Observation 6.1, Proposition 6.2] carry over to all subgroups of $\mathrm{GL}(U)$ and $\mathrm{GL}(W)$ that contain the corresponding symmetric groups.

About Theorem 1.2. For Theorem 1.2, let us consider the isomorphism problem of $U \otimes V \otimes W$ under $\mathrm{O}(U) \times \mathrm{O}(V) \times \mathrm{O}(W)$. Let $a = \dim(U)$, $b = \dim(V)$, and $c = \dim(W)$. That is, given $\mathrm{A}, \mathrm{B} \in \mathrm{T}(a \times b \times c, \mathbb{F})$, we want to decide if there exists $(R, S, T) \in \mathrm{O}(a, \mathbb{F}) \times \mathrm{O}(b, \mathbb{F}) \times \mathrm{O}(c, \mathbb{F})$, such that $(R, S, T) \circ \mathrm{A} = \mathrm{B}$. Our goal is to reduce this problem to an isomorphism problem of $U' \otimes V' \otimes W'$ under $\mathrm{GL}(U') \times \mathrm{GL}(V') \times \mathrm{GL}(W')$. The idea is to encode the requirements of R, S, T being orthogonal by adding identity matrices. We then construct tensor systems $(\mathrm{A}, I_1, I_2, I_3)$ and $(\mathrm{B}, I_1, I_2, I_3)$ where $I_1 \in \mathrm{M}(a, \mathbb{F})$, $I_2 \in \mathrm{M}(b, \mathbb{F})$, and $I_3 \in \mathrm{M}(c, \mathbb{F})$ are the identity matrices, and the goal is to decide if there exists $(R, S, T) \in \mathrm{GL}(a, \mathbb{F}) \times \mathrm{GL}(b, \mathbb{F}) \times \mathrm{GL}(c, \mathbb{F})$ such that $(R, S, T) \circ \mathrm{A} = \mathrm{B}$, $R^t R = I_1$, $S^t S = I_2$, and $T^t T = I_3$. Such a problem falls into the tensor system framework in [FGS19]; a main result of [FGS19, Theorem 1.1] can be rephrased as a reduction from Tensor System Isomorphism for 3-tensors or 2-tensors to 3-Tensor Isomorphism.

About Theorem 1.5. For Theorem 1.5, polynomial-time reductions for the five actions under GL were devised in [FGS19, GQ23a]. The main proof technique is a gadget construction, first proposed in [FGS19], which we call the Furtony–Grochow–Sergeichuk gadget, or FGS gadget for short. Roughly speaking, this gadget has the effect of reducing isomorphism over block-upper-triangular invertible matrices to that over general invertible matrices. We will explain why this is useful for our purpose, and the structure of this gadget, in the following.

First, let us examine a setting when we wish to restrict to consider only block-upper-triangular matrices. Suppose we wish to reduce isomorphism of $U \otimes V \otimes W$ to that of $U' \otimes U' \otimes W'$. One naive idea is to set $U' = U \oplus V$ and $W' = W$, and perform the following construction. Let $\mathtt{A} \in \mathrm{T}(\ell \times m \times n, \mathbb{F})$, and take the frontal slices of $\mathtt{A}$ as $(A_1, \ldots, A_n) \in \mathrm{M}(\ell \times m, \mathbb{F})$. Then construct $(A'_1, \ldots, A'_n) \in \mathrm{M}(\ell + m, \mathbb{F})$, where $A'_i = \begin{bmatrix} 0 & A_i \\ -A_i^t & 0 \end{bmatrix}$, and let the corresponding 3-way array be $\mathtt{A}' \in \mathrm{T}((\ell + m) \times (\ell + m) \times n, \mathbb{F})$. Similarly, starting from $\mathtt{B} \in \mathrm{T}(\ell \times m \times n, \mathbb{F})$, we can construct $\mathtt{B}'$ in the same way. The wish here is that $\mathtt{A}$ and $\mathtt{B}$ are unitarily isomorphic in $U \otimes V \otimes W$ if and only if $\mathtt{A}'$ and $\mathtt{B}'$ are unitarily isomorphic in $U' \otimes U' \otimes W'$. It can be verified that the only if direction holds easily, but the if direction is tricky. This is because, if we start with some isomorphism $(R, S) \in \mathrm{U}(U') \times \mathrm{U}(W')$ from $\mathtt{A}'$ to $\mathtt{B}'$, R may mix the U and V parts of U'.

This problem—more generally, the problem of two parts of the vector space potentially mixing in undesired ways—is solved by the FGS gadget, which attaches identity matrices of appropriate ranks to prevent such mixing. Figure 1.1 is an illustration from [GQ23a]. It can be verified that, because of the identity matrices I_{m+1} and I_{3m+2}, an isomorphism R in the U' part has to be block-upper-triangular, and the blocks would yield the desired isomorphism for the U and W parts.

This was done for the general linear group case in [GQ23a]. For the unitary group case, this almost goes through, because if a unitary matrix is block-upper-triangular, then it is actually block-diagonal, and the blocks are unitary too. Now the gadgets cause some problem for the only if direction (which was easy in the GL case), so we must verify carefully that the added gadgets allow for extending the original orthogonal or unitary transformations to bigger ones. Still, some technical difficulties remain. We discuss how we get around these difficulties in the next section.

About Theorem 1.6. For Theorem 1.6, at a high level we follow the strategy of reduction from d-Tensor Isomorphism to 3-Tensor Isomorphism from [GQ23a], but we find that the construction there does not quite work in the setting of orthogonal

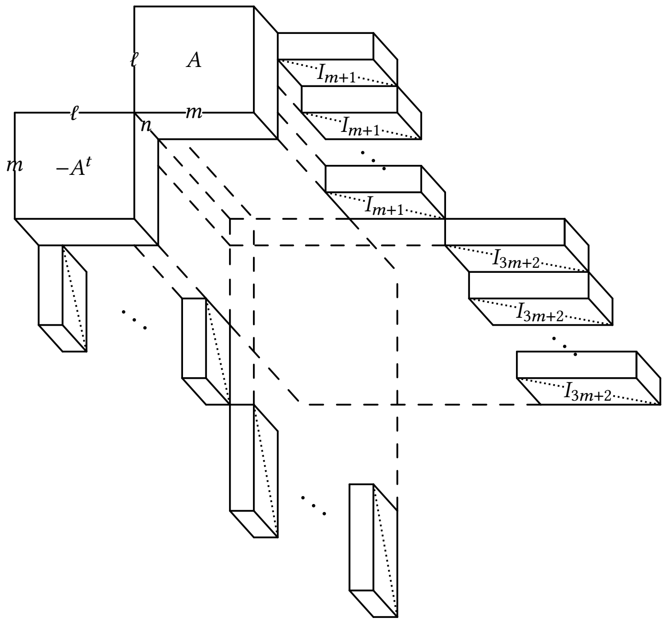

Figure 1.1: Pictorial representation of the reduction for Theorem 1.5; credit for the figure goes to the authors of [GQ23a], reproduced here with their permission.

or unitary group actions. As in [GQ23a], we shall reduce d-Tensor Isomorphism to Algebra Isomorphism, which reduces to 3-Tensor Isomorphism by Theorem 1.5. As in [GQ23a], we also use path algebras, but we use a different path algebra construction. We discuss the difference of our construction in the next section. Together with the result in Theorem 1.5, this then gives us the reduction from d-Tensor Orthogonal Isomorphism to Orthogonal Algebra Isomorphism, and similarly in the unitary case.

1.5.2 Issues and Solutions

Issue with Tensor System Isomorphism The proof in [FGS19] relies on the Krull–Schmidt Theorem for quiver representations (under general linear group actions), which states that if two matrix tuples are isomorphic then the decomposed matrix tuples are also isometric. However, we found it's not feasible to directly apply Krull–

Schmidt Theorem on the isomorphism over classical group. Fortunately, in our context we can replace that with a result of Sergeichuk [Ser98, Theorem 3.1] so that the proof can go through.

Issue with Degenerating Tensors The proofs in [GQ23a] degenerate tensors to demonstrate that isomorphism problems under some special actions are TI-hard. Since it's proved in the general linear group context, degenerating tensors is completed by naturally utilizing general linear matrices. As for the unitary group or orthogonal group, we require the use of the Singular Value Theorem to handle certain degenerate cases. However, we still haven't found any solutions for the symplectic group case.

Issues with the Path Algebra Constriction The proofs in [GQ23a] use Mal'cev's result on the conjugacy of the Wedderburn complements of the Jacobson radical, and this result seems not to hold if we require the conjugating matrix to be orthogonal or unitary. To get around this, our main technical contribution is to develop a related but in fact *simpler* path algebra construction, that avoids the use of the aforementioned deep algebraic results, and works not only in the GL setting, but extends to the orthogonal and unitary settings as well.

Chapter 2

Preliminaries

Fields. All our reductions are constant-free p-projections (that is, the only constants they use other than copying the ones already present in the input are $\{0, 1, -1\}$). When the fields are representable on a Turing machine, our reductions are log space computable. For arbitrary fields, the reductions are in log space in the Blum–Shub–Smale model over the corresponding field.

Linear algebra. All vector spaces in this article are finite dimensional. Let V be a vector space over a field $\mathbb{F}$. The dual of V, V^*, consists of all linear or anti-linear forms over $\mathbb{F}$. In this case when anti-linear is considered, $\mathbb{F}$ is a quadratic extension of a subfield $\mathbb{K}$, there is thus an automorphism $\alpha \in \mathrm{Aut}_{\mathbb{K}}(\mathbb{F})$ of order two, and anti-linear means $f(\lambda v) = \alpha(\lambda)f(v)$. An example is $\mathbb{F} = \mathbb{C}$ and $\mathbb{K} = \mathbb{R}$, and α=complex conjugation. Whether V^* denotes linear or antilinear maps should be evident from context.

Matrices. Let $\mathrm{M}(l \times m, \mathbb{F})$ be the linear space of $l \times m$ matrices over $\mathbb{F}$, and $\mathrm{M}(n, \mathbb{F}) := \mathrm{M}(n \times n, \mathbb{F})$. Given $A \in \mathrm{M}(l \times m, \mathbb{F})$, denote by A^t the transpose of A. Given $A \in \mathrm{GL}(n, \mathbb{F})$, denote by A^{-1} the inverse of A and by A^{-t} the inverse transpose of A.

We use I_n to denote the $n \times n$ *identity matrix*, and if it is clear from the context, we may drop the subscript n. For $(i, j) \in [n] \times [n]$, let $\mathrm{E}_{i,j} \in \mathrm{M}(n, \mathbb{F})$ be the *elementary* *matrix* where the (i,j)th entry is 1, and the remaining entries are 0. For $i \neq j$, the matrix $\mathrm{E}_{i,j} - \mathrm{E}_{j,i}$ is called an *elementary alternating matrix*.

Arrays Let $\mathbb{F}$ be a field, and let $n_1, \ldots, n_d \in \mathbb{N}$. For $n \in \mathbb{N}$, $[n] := \{1, 2, \ldots, n\}$. We use $\mathrm{T}(n_1 \times \cdots \times n_d, \mathbb{F})$ to denote the linear space of d-way arrays with $[n_j]$ being the range of the jth index. That is, an element in $\mathrm{T}(n_1 \times \cdots \times n_d, \mathbb{F})$ is of the form $\mathrm{A} = (a_{i_1,\ldots,i_d})$ where $\forall j \in [d]$, $i_j \in [n_j]$, and $a_{i_1,\ldots,i_d} \in \mathbb{F}$. Note that 2-way arrays are just matrices. Let $\mathrm{M}(n \times m, \mathbb{F}) := \mathrm{T}(n \times m, \mathbb{F})$, and $\mathrm{M}(n, \mathbb{F}) := \mathrm{M}(n \times n, \mathbb{F})$.

Definition 2.1. Let $\mathcal{G}(n, \mathbb{F})$ be some matrix group of degree n over $\mathbb{F}$. We define an action of $\mathcal{G}(n_1, \mathbb{F}) \times \cdots \times \mathcal{G}(n_d, \mathbb{F})$ on $\mathrm{T}(n_1 \times \cdots \times n_d, \mathbb{F})$, denoted as $\circ$, as follows. Let $\mathbf{g} = (g_1, \ldots, g_d)$, where $g_k \in \mathcal{G}(n_k, \mathbb{F})$ over $k \in [d]$. The action of $\mathbf{g}$ sends $\mathrm{A} = (a_{i_1,\ldots,i_d})$ to $\mathbf{g} \circ \mathrm{A} = (b_{i_1,\ldots,i_d})$, where $b_{i_1,\ldots,i_d} = \sum_{j_1,\ldots,j_d} a_{j_1,\ldots,j_d} (g_1)_{i_1,j_1} (g_2)_{i_2,j_2} \cdots (g_d)_{i_d,j_d}$.

Tensors. Let $V_1, \ldots, V_c$ be vector spaces over $\mathbb{F}$. Let $a_i, b_i, i \in [c]$ be non-negative integers, such that for each i, $a_i + b_i > 0$. A tensor T of type $(a_1, b_1; a_2, b_2; \ldots; a_c, b_c)$ supported by $(V_1, \ldots, V_c)$ is an element in $V_1^{\otimes a_1} \otimes V_1^{*\otimes b_1} \otimes V_2^{\otimes a_2} \otimes V_2^{*\otimes b_2} \otimes \cdots \otimes V_c^{\otimes a_c} \otimes V_c^{*\otimes b_c}$. We say that V_i's are the supporting vector spaces of T, and a_i (resp. b_i) is the multiplicity of T at V_i (resp. V_i^*). (By convention $V^{\otimes 0} := \mathbb{F}$; note that $U \otimes \mathbb{F} \cong U$, since our tensor products are over $\mathbb{F}$.)

The order of T is $\sum_{i \in [c]} (a_i + b_i)$. We say that T is *plain*, if $a_1 = \cdots = a_c = 1$ and $b_1 = \cdots = b_c = 0$. The group $\mathrm{GL}(V_1) \times \cdots \times \mathrm{GL}(V_c)$ acts naturally on the space $V_1^{\otimes a_1} \otimes V_1^{*\otimes b_1} \otimes V_2^{\otimes a_2} \otimes V_2^{*\otimes b_2} \otimes \cdots \otimes V_c^{\otimes a_c} \otimes V_c^{*\otimes b_c}$. Two tensors in this space are isomorphic if they are in the same orbit under this group action.

From tensors to multiway arrays. For $i \in [c]$, let V_i be a dimension-d_i vector space over $\mathbb{F}$. Let T be a tensor in $V_1^{\otimes a_1} \otimes V_1^{*\otimes b_1} \otimes V_2^{\otimes a_2} \otimes V_2^{*\otimes b_2} \otimes \cdots \otimes V_c^{\otimes a_c} \otimes V_c^{*\otimes b_c}$. After fixing the basis of each V_i, T can be represented as a multiway array $R_T \in \mathrm{T}(d_1^{\times(a_1+b_1)} \times \cdots \times d_c^{\times(a_c+b_c)})$ and the elements in $\mathrm{GL}(V_i) \cong \mathrm{GL}(d_i, \mathbb{F})$ can be represented as invertible $d_i \times d_i$ matrices. The action of $(A_1, \ldots, A_c)$ on R_T can be explicitly written following Definition 2.1, using A_i for a_i directions and A_i^{-t} for b_i directions.

Chapter 3

Relations between Tensor Isomorphisms over Different Matrix Groups

We first give notions regarding tensor system in Section 3.1. We then show that Graph Isomorphism reduces to 3-Tensor $\mathcal{G}$-Isomorphism in Section 3.2.1 by adapting results from [LQW+23], where $\mathcal{G}$ is any group family containing the family of symmetric groups. We prove that there is a reduction from 3-Tensor $\mathcal{G}$-Isomorphism to 3-Tensor Isomorphism in Section 3.2.2, where $\mathcal{G}$ preserves a family of polynomial-time-constructible bilinear forms.

3.1 Preparations

The key to the reduction from 3-Tensor $\mathcal{G}$-Isomorphism to 3-Tensor Isomorphism is [FGS19, Theorem 1.1]. For this, we need the tensor system notion in [FGS19]. This notion is also related to tensor networks, and we refer the reader to [FGS19] for further references.

Tensor systems and [FGS19, Theorem 1.1]. Let $V = \{V_1, \ldots, V_c\}$ be a set of vector spaces over a field $\mathbb{F}$. Let $T = \{T_1, \ldots, T_n\}$ be a set of tensors, such that T_i is supported by a subset of V_j's in V.

The types of T_i's can be recorded by a bipartite graph (with directed, possibly parallel arcs) as follows. Let $B_T = (T \cup V, E)$ be a bipartite graph, where E is a multiset whose elements are from $V \times T$ and $T \times V$. The arcs in E are as follows. Suppose the multiplicity of T_i at V_j (resp. V_j^*) is $a_{i,j}$ (resp. $b_{i,j}$). Then the multiplicity of (V_j, T_i) (resp. (T_i, V_j)) in E is $a_{i,j}$ (resp. $b_{i,j}$). For an example, see Figure 3.1.

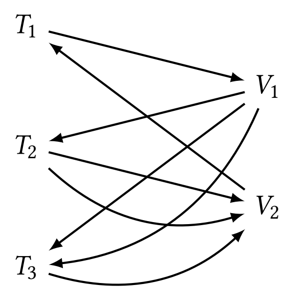

Figure 3.1: The bipartite graph encoding a system of three tensors over two $\mathbb{F}$-vector spaces V_1, V_2: $T_1 \in V_1^* \otimes V_2$, $T_2 \in V_1 \otimes V_2^* \otimes V_2^*$, and $T_3 \in V_1 \otimes V_1 \otimes V_2^*$.

Let $S = \{S_1, \ldots, S_c\}$ and $T = \{T_1, \ldots, T_c\}$ be two tensor systems of the same type. That is, their underlying bipartite graphs are the same up to renaming S_i with T_j. We say that S and T are isomorphic if and only if there exists $A = (A_1, \ldots, A_c) \in \mathrm{GL}(V_1) \times \cdots \times \mathrm{GL}(V_c)$ such that (the relevant components of) A sends S_i to T_i for every $i \in [c]$.

Theorem 3.1 (Rephrase of [FGS19, Theorem 1.1]). *Let $S = \{S_1, \ldots, S_c\}$ and $T = \{T_1, \ldots, T_c\}$ be two tensor systems supported by $\{V_1, \ldots, V_m\}$, where each S_i and T_i is of order ≤ 3. Then there exists an algorithm A that takes S and T and outputs two plain 3-tensors $A(S)$ and $A(T)$ supported by vector spaces $\{U, V, W\}$, such that S and T are isomorphic as tensor systems if and only if $A(S)$ and $A(T)$ are isomorphic. The algorithm runs in time polynomial in the dimension of U, V, W, and this maximum dimension is at most* $\mathrm{poly}(\sum_{i\in[m]} \dim(V_i), 2^{\mathrm{poly}(c)})$.

Here we give an outline for the proof of Theorem 3.1. The goal here is to give a guided exposition of some main technical steps in the proof of [FGS19, Theorem 1.1], so the reader may verify the parameters in conjunction with [FGS19] more easily. This requires us to examine the constructions in [FGS19] to compute the parameters explicitly. Combining Proposition 3.2 in Section 3.1 and Proposition 3.3 in Section 3.1, we show the correctness of Theorem 3.1

Step 1: Block isomorphism and plain isomorphism

The first notion is the block isomorphism of 3-tensors. Let A and B be two plain 3-tensors in $U \otimes V \otimes W$. Let $U = U_1 \oplus \cdots \oplus U_e$, $V = V_1 \oplus \cdots \oplus V_f$, and $W = W_1 \oplus \cdots \oplus W_g$ be direct sum decompositions. Let $\mathcal{E} \leq \mathrm{GL}(U)$ be the subgroup of $\mathrm{GL}(U)$ that preserves this direct sum decomposition, that is, E consists of those invertible linear maps that sends U_i to U_i for every $i \in [e]$. Similarly let $\mathcal{F}$ (resp. $\mathcal{G}$) be the subgroup of $\mathrm{GL}(V)$ (resp. $\mathrm{GL}(W)$) preserving the direct sum decomposition. We say that A and B are *block-isomorphic* with respect to these direct sum decompositions if A and B are in the same orbit under $\mathcal{E} \times \mathcal{F} \times \mathcal{G}$.

Proposition 3.2 (Rephrase of [FGS19, Theorem 2.1])**.** *Let $U = U_1 \oplus \cdots \oplus U_e$, $V = V_1 \oplus \cdots \oplus V_f$, and $W = W_1 \oplus \cdots \oplus W_g$ be direct sum decompositions of vector spaces U, V, and W. Then there exists an algorithm B that takes $\mathrm{A}, \mathrm{B} \in U \otimes V \otimes W$ and outputs vector spaces U', V', W' and $B(\mathrm{A}), B(\mathrm{B}) \in U' \otimes V' \otimes W'$ such that* A *and* B *are block-isomorphic if and only if $B(\mathrm{A})$ and $B(\mathrm{B})$ are isomorphic. The algorithm runs in time polynomial in the maximum dimension over U, V, W, and this maximum dimension is upper bounded by* $\mathrm{poly}(\dim(U), \dim(V), \dim(W), 2^e, 2^f, 2^g)$.

Step 2: Linked-block isomorphism and block isomorphism

The second notion is the linked-block isomorphism of 3-tensors. Again, let A and B be two plain 3-tensors in $U \otimes V \otimes W$. Let $U = U_1 \oplus \cdots \oplus U_e$, $V = V_1 \oplus \cdots \oplus V_f$, and

$W = W_1 \oplus \cdots \oplus W_g$ be direct sum decompositions. Let $\mathcal{E} \leq \mathrm{GL}(U)$, $\mathcal{F} \leq \mathrm{GL}(V)$ and $\mathcal{G} \leq \mathrm{GL}(W)$ be defined as in Section 3.1.

Let $I_U = [e]$, $I_V = [f]$, and $I_W = [g]$. Suppose two binary relations $\sim$ and $\bowtie$ on $I_U \cup I_V \cup I_W$ satisfy the following: (1) $\sim$ is an equivalence relation; (2) if $a \bowtie b$ then $a \nsim b$; and (3) if $a \bowtie b$, then $b \bowtie c \iff a \sim c$.

For convenience, we shall use X_a to denote U_a, V_a, or W_a depending on whether $a \in I_U$, $a \in I_V$, or $a \in I_W$. Briefly speaking, $a \sim b$ denotes that the corresponding two blocks are acted covariantly, and $a \bowtie b$ denotes that the corresponding two blocks are acted contravariantly. So if $a \sim b$ or $a \bowtie b$, then $\dim(X_a) = \dim(X_b)$.

Given such binary relations $\sim$ and $\bowtie$, we define a block-isomorphism X between A and B to be a *linked-block-isomorphism* if for any $a, b \in I_U \cup I_V \cup I_W$, the following conditions for decompositions of U, V and W holds:

$$X_a = X_b \text{ if } a \sim b, \qquad X_a = X_b^{-t} \text{ if } a \bowtie b.$$

Proposition 3.3 (Rephrase of [FGS19, Theorem 4.1]). *Let $U = U_1 \oplus \cdots \oplus U_e$, $V = V_1 \oplus \cdots \oplus V_f$, and $W = W_1 \oplus \cdots \oplus W_g$ be direct sum decompositions of vector spaces U, V, and W and these decompositions satisfy conditions with respect to some binary relations $\sim$ and $\bowtie$ for $I_U \cup I_V \cup I_W$. Then there exists an algorithm B that takes $\mathrm{A}, \mathrm{B} \in U \otimes V \otimes W$ and outputs vector spaces U', V', W' and $B(\mathrm{A}), B(\mathrm{B}) \in U' \otimes V' \otimes W'$, where $U' = U'_1 \oplus \cdots \oplus U'_{\mathrm{poly}(e)}$, $V' = V'_1 \oplus \cdots \oplus V'_{\mathrm{poly}(f)}$, and $W' = W'_1 \oplus \cdots \oplus W'_{\mathrm{poly}(g)}$ such that* A *and* B *are linked-block-isomorphic if and only if $B(\mathrm{A})$ and $B(\mathrm{B})$ are block-isomorphic. The algorithm runs in time polynomial in the maximum dimension over U, V, W, and this maximum dimension is upper bounded by* $\mathrm{poly}(e, f, g) \cdot \max(\dim(U), \dim(V), \dim(W))$.

Following that tensor system isomorphism is naturally represented by linked-block isomorphism for 3-tensors, tensor system isomorphism reduces to block isomorphism for 3-tensors by Proposition 3.3. Then the tensor system isomorphism problem reduces to 3-Tensor Isomorphism.

3.2 Detailed Proofs

3.2.1 Graph Isomorphism to Tensor Isomorphism over Classical Group

Our goal is to reduce the directed graph isomorphism problem DGI, which is GI-complete [KST93], to the isomorphism problem of $U \otimes U \otimes V$ under $\mathcal{G}(U) \times \mathcal{G}(V)$ where $\mathcal{G} = \{\mathcal{G}(n, \mathbb{F})\}$ is a family of subgroups of the general linear groups that contains the symmetric groups. Note that S_n is naturally embedded in $\mathrm{GL}(n, \mathbb{F})$ by taking the matrix representation of permutations. In this section, we also view $\mathcal{G}(n, \mathbb{F})$ as a matrix group.

Recall that two directed graphs $G = ([n], E)$ and $H = ([n], F)$ are isomorphic, if there exists a bijective map $f : [n] \to [n]$, such that $(i, j) \in E$ if and only if $(f(i), f(j)) \in F$.

We rephrase [LQW+23, Proposition 6.1, Proposition 6.2] to adapt them to our context in the following proposition, which would conclude our proof of Theorem 1.1.

Proposition 3.4. *Given two directed graphs $G = ([n], E)$ and $H = ([n], F)$, and a group family $\mathcal{G} = \{\mathcal{G}(n, \mathbb{F})\}$ satisfying that $\mathrm{S}_n \leq \mathcal{G}(n, \mathbb{F}) \leq \mathrm{GL}(n, \mathbb{F})$. We can efficiently construct two 3-tensors S_G and S_H associated with G and H, respectively, such that S_G is isomorphic to S_H in $U \otimes U \otimes W$ under the action of $\mathcal{G}(U) \times \mathcal{G}(W)$ if and only if G is isomorphic to H.*

Proof. **The construction.** For directed graph $G = ([n], E)$, we construct the associated 3-way array $\mathrm{S}_G \in \mathrm{T}(n \times n \times |E|, \mathbb{F})$ by setting its frontal slices as $(\mathrm{E}_{i,j} \mid (i, j) \in E)$, where edges in E are ordered lexicographically. We also construct $\mathrm{S}_H \in \mathrm{T}(n \times n \times |F|, \mathbb{F})$ associated with $H = ([n], F)$ in the same way. Let $m = |E| = |F|$. We will show that $G \cong H$ as graphs iff S_G and S_H are in the same orbit of $\mathcal{G}(U) \times \mathcal{G}(V)$ acting on $U \otimes U \otimes V$, where $U = \mathbb{F}^n, V = \mathbb{F}^m$.

The if direction. Let $\sigma \in \mathrm{S}_n$ be an isomorphism from G to H, and let $\tau \in \mathrm{S}_m$ be the induced permutation of edges. Then the permutation matrices corresponding to σ and τ yield an isomorphism from S_G to S_H. Note that here we need to use the condition that $\mathcal{G}$ contains symmetric groups.

The only if direction. Let $T \in \mathcal{G}(n, \mathbb{F}) \leq \mathrm{GL}(n, \mathbb{F})$ and $R \in \mathcal{G}(m, \mathbb{F}) \leq \mathrm{GL}(m, \mathbb{F})$ such that $T^t \mathrm{S}_G T = \mathrm{S}_H^R$. Denote by A_r the rth frontal slice of S_H^R. Let $t_{i,j} \in \mathbb{F}$ be the (i, j)th entry of T. Then for each $(i, j) \in E$, let $r \in [m]$ be the index corresponding to the edge $(i, j) \in E$. Then we have:

$$T^t \mathrm{E}_{i,j} T = \begin{bmatrix} t_{1,i} \\ \vdots \\ t_{n,i} \end{bmatrix} \begin{bmatrix} t_{1,j} & \cdots & t_{n,j} \end{bmatrix} = [t_{k,i} t_{\ell,j}]_{k,\ell \in [n]} = A_r.$$

Note that for each $r \in [m]$, A_r is a linear combination of the frontal slices of S_H. Since the slices of S_H are of the form $E_{i,j}$, and these are linearly independent, it follows that if the (k, ℓ)th entry $t_{k,i} t_{\ell,j}$ of A_r is non-zero for some $r \in [m]$, then $\mathrm{E}_{k,\ell}$ must be present with nonzero coefficient in this linear combination, and therefore we must have $(k, \ell) \in F$.

Next, as T is invertible, there exists a permutation $\sigma \in \mathrm{S}_n$ such that $t_{\sigma(i),i} \neq 0$ for all $i \in [n]$ (for otherwise, considering the expression of $\det T$ as a sum over permutations, we would get $\det T = 0$). In particular, $t_{\sigma(i),i} t_{\sigma(j),j} \neq 0$ for any $i, j \in [n]$. Combining with the previous paragraph, we get that for $(i, j) \in E$, $(\sigma(i), \sigma(j)) \in F$. In other words, σ is an injective map from vertices of G to vertices of H which preserves arcs. Finally, the invertibility of T and R ensures that the frontal slices of S_G and S_H have the same number, which means G and H have the same edge size, and hence that σ in fact induces a bijection on arcs. This shows that G is isomorphic to H, as claimed. ■

3.2.2 Isomorphism over Classical Group to Isomorphism over General Linear Group

Let $\{\phi_n : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}\}$ be a family of bilinear forms. Suppose $\mathcal{G}(n, \mathbb{F}) \le \mathrm{GL}(n, \mathbb{F})$ preserves ϕ_n. For convenience, we only consider one action in Definition 1.4, and the reader will see that the other four actions follow essentially the same line of arguments. Our goal is to decide whether $\mathtt{A}, \mathtt{B} \in \mathrm{T}(l \times m \times n, \mathbb{F})$ are in the same orbit under the action of $\mathcal{G}(l, \mathbb{F}) \times \mathcal{G}(m, \mathbb{F}) \times \mathcal{G}(n, \mathbb{F})$. We would like to reduce to the isomorphism problem of $U \otimes V \otimes W$ under $\mathrm{GL}(U) \times \mathrm{GL}(V) \otimes \mathrm{GL}(W)$ where the dimensions of U, V, W are polynomial in l, m, n.

Given Theorem 3.1, we now proceed to the proof of Theorem 1.2.

Proof of Theorem 1.2. Let $\Phi_l \in \mathrm{M}(l, \mathbb{F}), \Phi_m \in \mathrm{M}(m, \mathbb{F})$ and $\Phi_n \in \mathrm{M}(n, \mathbb{F})$ be the matrix representations of bilinear forms ϕ_l, ϕ_m and ϕ_n, respectively. Then we construct $S = \{\mathtt{A}, \Phi_l, \Phi_m, \Phi_n\}$ and $T = \{\mathtt{B}, \Phi_l, \Phi_m, \Phi_n\}$, which is viewed as tensor systems as follows. Let $U' = \mathbb{F}^l$, $V' = \mathbb{F}^m$, and $W' = \mathbb{F}^n$. Then $\mathtt{A} \in U' \otimes V' \otimes W'$, $\Phi_l \in U' \otimes U'$, $\Phi_m \in V' \otimes V'$, and $\Phi_n \in W' \otimes W'$. It is clear that $\mathtt{A}$ and $\mathtt{B}$ are $\mathcal{G}$-isomorphic if and only if the two tensor systems S and T are GL-isomorphic.

Every tensor in the above tensor systems is of order ≤ 3, and each has only $c = 4 = O(1)$ components, so we can apply Theorem 1.2 to obtain two plain tensors $r(S)$ and $r(T)$ in $U \otimes V \otimes W$, where $\dim(U)$, $\dim(V)$ and $\dim(W)$ are at most by $\mathrm{poly}(l+n+m)$. Furthermore, S and T are isomorphic as tensor systems if and only if $r(S)$ and $r(T)$ are isomorphic as plain tensors. This concludes the proof. ∎

Chapter 4

The Equivalences of Five Actions

We first introduce the notion of *non-degenerate* arrays in Section 4.1. Then we show the polynomial-time equivalence between the isomorphism problems of $U \otimes V \otimes W$, $U \otimes U \otimes V$, $U \otimes U^* \otimes V$, $U \otimes U \otimes U$, and $U \otimes U \otimes U^*$ under orthogonal and unitary groups in Section 4.2. We only present the proofs for unitary groups as proofs for orthogonal groups are similar. To prove this, we first present reductions from $U \otimes U \otimes V$, $U \otimes U^* \otimes V$, $U \otimes U \otimes U$, and $U \otimes U \otimes U^*$ to $U \otimes V \otimes W$, and then we present reductions for the opposite direction.

4.1 Preparations

A 3-way array $\mathrm{A} \in \mathrm{T}(l \times m \times n, \mathbb{F})$ is non-degenerate if along all directions including the frontal direction, the horizontal direction and the lateral direction, slices are linearly independent. Then we show a reduction from Unitary Tensor Isomorphism for degenerate arrays to Unitary Tensor Isomorphism for non-degenerate arrays.

Lemma 4.1. *For any 3-way array* $\mathrm{A} \in \mathrm{T}(l \times m \times n, \mathbb{C})$*, there are unitary matrices* $T_1 \in \mathrm{U}(l, \mathbb{C}), T_2 \in \mathrm{U}(m, \mathbb{C})$ *and* $T_3 \in \mathrm{U}(n, \mathbb{C})$ *such that*

$$(T_1 \mathrm{A} T_2)^{T_3} = \begin{bmatrix} \tilde{\mathrm{A}} & 0 \\ 0 & 0 \end{bmatrix},$$

where $\tilde{\mathrm{A}}$ *is a non-degenerate array of size* $l' \times m' \times n'$.

Proof. First, we consider the horizontal slices of A. Let $(A_1, \ldots, A_n)$ be the corresponding matrix tuple of frontal slices of A. Then we construct the $l \times mn$ matrix

$$A' = \begin{bmatrix} A_1 & \ldots & A_n \end{bmatrix}.$$

We denote the maximum number of linearly independent horizontal slices of A by l'; it follows that the rank of A' is l'. Applying a singular value decomposition on A', we have

$$A' = U\Sigma V^*,$$

where U and V are unitary matrices of size $l \times l$ and $mn \times mn$, respectively, and $\Sigma = \begin{bmatrix} \hat{\Sigma} \\ \mathbf{0} \end{bmatrix}$ for a full-rank rectangular diagonal matrix $\hat{\Sigma}$ of size $l' \times mn$. Multiplying A' by $T_1 = U^{-1}$, we have

$$T_1 A' = \Sigma V^*,$$

where the first l' rows of ΣV^* are linearly independent and the last $l - l'$ rows are zero. It follows that acting T_1 on the horizontal slices of A sends A to

$$T_1 \mathrm{A} = \begin{bmatrix} \hat{\mathrm{A}} \\ 0 \end{bmatrix},$$

where the horizontal slices of $\hat{\mathrm{A}} \in \mathrm{T}(l' \times m \times n, \mathbb{C})$ are linearly independent.

We can similarly find unitary matrices T_2, T_3 for the other two directions. ■

Lemma 4.2. *Given two 3-tensors* $\mathrm{A}, \mathrm{B} \in U \otimes V \otimes W$ *where* $l = \dim(U), m = \dim(V)$ *and* $n = \dim(W)$*, there is a reduction* r *such that* A *and* B *are unitarily isomorphic if and only if* $r(\mathrm{A})$ *and* $r(\mathrm{B})$ *are unitarily isomorphic, where* $r(\mathrm{A})$ *and* $r(\mathrm{B})$ *are non-degenerate.*

We note that this reduction is one of the few in the thesis that is explicitly *not* a p-projection (similar to how the reduction of a matrix to row echelon form is not a p-projection).

Proof. By Lemma 4.1, we can find unitary matrices $S_1 \in \mathrm{U}(l, \mathbb{C}), S_2 \in \mathrm{U}(m, \mathbb{C})$ and $S_3 \in \mathrm{U}(n, \mathbb{C})$ to extract the $l' \times m' \times n'$ non-degenerate tensor $\tilde{\mathrm{A}}$ of A. There are similar unitary matrices $T_1 \in \mathrm{U}(l, \mathbb{C}), T_2 \in \mathrm{U}(m, \mathbb{C})$ and $T_3 \in \mathrm{U}(n, \mathbb{C})$ for B as well. Then we claim A and B are unitarily isomorphic if and only if $r(\mathrm{A}) = \tilde{\mathrm{A}}$ and $r(\mathrm{B}) = \tilde{\mathrm{B}}$ are unitarily isomorphic.

For the if direction, assume $\tilde{P}\tilde{\mathrm{A}}\tilde{Q} = \tilde{\mathrm{B}}^{\tilde{R}}$ where $\tilde{P} \in \mathrm{U}(l', \mathbb{C}), \tilde{Q} \in \mathrm{U}(m', \mathbb{C})$ and $\tilde{R} \in \mathrm{U}(n', \mathbb{C})$. It yields that $P'\mathrm{A}'Q' = \mathrm{B}'^{R'}$ where $\mathrm{A}' = \begin{bmatrix} \tilde{\mathrm{A}} & 0 \\ 0 & 0 \end{bmatrix}$ and $\mathrm{B}' = \begin{bmatrix} \tilde{\mathrm{B}} & 0 \\ 0 & 0 \end{bmatrix}$, and $P' = \mathrm{diag}(\tilde{P}, I_{l-l'}), Q' = \mathrm{diag}(\tilde{Q}, I_{m-m'})$ and $R' = \mathrm{diag}(\tilde{R}, I_{n-n'})$. Then we set P to be $T_1^{-1}P'S_1$, Q to be $S_2Q'T_2^{-1}$ and R to be $T_3R'S_3^{-1}$, where P, Q and R are unitary matrices. It's easy to check that $P\mathrm{A}Q = \mathrm{B}^R$.

For the only if direction, suppose $P\mathrm{A}Q = \mathrm{B}^R$ for $P \in \mathrm{U}(l, \mathbb{C}), Q \in \mathrm{U}(m, \mathbb{C})$ and $R \in \mathrm{U}(n, \mathbb{C})$, which follows that $P'\mathrm{A}'Q' = \mathrm{B}'^{R'}$ for $\mathrm{A}' = \begin{bmatrix} \tilde{\mathrm{A}} & 0 \\ 0 & 0 \end{bmatrix}$ and $\mathrm{B}' = \begin{bmatrix} \tilde{\mathrm{B}} & 0 \\ 0 & 0 \end{bmatrix}$, and $P' = T_1PS_1^{-1}, Q' = S_2^{-1}QT_2$, and $R' = T_3^{-1}RS_3$. Write P' as $\begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix}$ where $P_{1,1}$ is of size $l' \times l'$. Observe that the last $l - l'$ horizontal slices of $\mathrm{A}'Q'$ and $\mathrm{B}'^{R'}$ are $\mathbf{0}$ and the first l' slices of $\mathrm{A}'Q'$ are linearly independent, so we derive that $P_{2,1} = \mathbf{0}$. We can conclude that Q' and R' are block-lower-trianglular matrices in the same way. Therefore, $\tilde{P}, \tilde{Q}$ and $\tilde{R}$ are unitary, where $\tilde{P}$ is the first $l' \times l'$ submatrix of P', $\tilde{Q}$ is the first $m' \times m'$ submatrix of Q' and $\tilde{R}$ is the first $n' \times n'$ submatrix of R'. Thus, $\tilde{P}, \tilde{Q}$ and $\tilde{R}$ form a unitary isomorphism between $\tilde{\mathrm{A}}$ and $\tilde{\mathrm{B}}$ by $\tilde{P}\tilde{\mathrm{A}}\tilde{Q} = \tilde{\mathrm{B}}^{\tilde{R}}$. ■

Corollary 4.3. *Given two 3-tensors* $\mathrm{A}, \mathrm{B} \in V \otimes V \otimes W$*, there is a reduction* r *such that* A, B *are unitarily isomorphic if and only if* $r(\mathrm{A}), r(\mathrm{B}) \in V \otimes V \otimes W'$ *are unitarily pseudo-isometric bilinear forms, and such that the frontal slices of* $r(\mathrm{A})$ *and* $r(\mathrm{B})$ *are linearly independent.*

Note that the above results also work for orthogonal groups.

4.2 Detailed Proofs

Recall that we need to show the polynomial-time equivalence between the isomorphism problems of $U \otimes V \otimes W$, $U \otimes U \otimes V$, $U \otimes U^* \otimes V$, $U \otimes U \otimes U$, and $U \otimes U \otimes U^*$ under orthogonal and unitary groups. We present the proofs for unitary groups, and the proofs for orthogonal groups follow the same line.

The equivalences for GL were proved in [FGS19, GQ23a]. We follow their proof strategies, but as mentioned in Section 1.5, certain technical difficulties need to be dealt with.

In Section 4.2.1, we reduce $U \otimes U \otimes V$, $U \otimes U^* \otimes V$, $U \otimes U \otimes U$, and $U \otimes U \otimes U^*$ to $U \otimes V \otimes W$. This is done through the tensor system framework with the adaptation to unitary isomorphism.

In Section 4.2.2, we reduce $U \otimes V \otimes W$ to $U \otimes U \otimes W$. This requires a careful check due to the introduction of the gadget.

In Section 4.2.3 we reduce $U \otimes V \otimes W$ to $U \otimes U^* \otimes W$. This requires the Singular Value Theorem as a new ingredient.

In Section 4.2.4, we reduce $U \otimes U \otimes W$ to $U \otimes U \otimes U^*$ and $U \otimes U \otimes U$.

4.2.1 Others to $U \otimes V \otimes W$

In this section, we will reduce unitary isomorphism problems of $U \otimes U \otimes V$, $U \otimes U^* \otimes V$, $U \otimes U \otimes U$, and $U \otimes U \otimes U^*$ to $U \otimes V \otimes W$ with a polynomial dimension blow-up. This requires the following unitary version of Theorem 3.1, so we begin with its proof.

Theorem 4.4 (Unitary version of [FGS19, Theorem 1.1]). *Let $S = \{S_1, \ldots, S_c\}$ and $T = \{T_1, \ldots, T_c\}$ be two tensor systems supported by $\{V_1, \ldots, V_m\}$, where every S_i and T_i is of order ≤ 3. Then there exists an algorithm r that takes S and T and outputs two 3-tensors $r(S)$ and $r(T)$ supported by vector spaces $\{U, V, W\}$, such that S and T are isomorphic as tensor systems under $\mathrm{U}(V_1) \times \cdots \times \mathrm{U}(V_m)$ if and only if $r(S)$ and $r(T)$ are isomorphic under $\mathrm{U}(U) \times \mathrm{U}(V) \times \mathrm{U}(W)$. The algorithm r runs in time polynomial in the* *maximum dimension over U, V, W, and this maximum dimension is upper bounded by* $\mathrm{poly}(\sum_{i\in[m]} \dim(V_i), 2^{\mathrm{poly}(c)})$.

This follows the same proof as [FGS19, Theorem 1.1], outlined in Section 3.1, with one change, based on the following result.

We say that two matrix tuples $(C_1, \dots, C_m) \in \mathrm{M}(l \times n, \mathbb{F})^m$ and $(D_1, \dots, D_m) \in \mathrm{M}(l \times n, \mathbb{F})^m$ are unitarily equivalent, if there exist unitary matrices $L \in \mathrm{U}(l, \mathbb{F})$ and $R \in \mathrm{U}(n, \mathbb{F})$, such that for any $i \in [m]$, $LC_iR = D_i$.

Theorem 4.5 (Sergeichuk [Ser98, Theorem 3.1])**.** *Let $\mathbf{C} = (C_1, \dots, C_m) \in \mathrm{M}(l \times n, \mathbb{F})$. Suppose $\mathbf{C}$ is unitarily equivalent to $\mathbf{D} = (D_1, \dots, D_m)$, such that each D_i is block-diagonal with k blocks, with the jth block of size $d_j \times d_j$. Furthermore, let $\mathbf{D}_j = (D_{1,j}, \dots, D_{m,j})$ be the m-tuple of $d_j \times d_j$ matrices consisting of the jth block from each D_i, and suppose $\mathbf{D}_j$ is not unitarily equivalent to a block-diagonal tuple. Then the isomorphism types of $\mathbf{D}_i$'s and the multiplicities of each isomorphism type are uniquely determined by $\mathbf{C}$, that is, they are the same regardless of the choice of decomposition.*

From the above theorem, the following corollary is immediate:

Corollary 4.6. *If $\left(\begin{bmatrix} A_1 & 0 \\ 0 & B_1 \end{bmatrix}, \dots, \begin{bmatrix} A_m & 0 \\ 0 & B_m \end{bmatrix}\right)$ and $\left(\begin{bmatrix} A_1 & 0 \\ 0 & C_1 \end{bmatrix}, \dots, \begin{bmatrix} A_m & 0 \\ 0 & C_m \end{bmatrix}\right)$ are unitarily equivalent, then $(B_1, \dots, B_m)$ and $(C_1, \dots, C_m)$ are unitarily equivalent.*

Proof of Theorem 4.4. With Corollary 4.6, the proof of [FGS19, Theorem 1.1] goes through for this unitary setting, by replacing the use of the Krull–Schmidt theorem for quiver representations ([FGS19, pp. 20]) with Theorem 4.5.

The case of orthogonal groups follows similarly by using [Ser98, Theorem 4.1] instead. ■

We utilize the tensor system to construct reductions to plain 3-tensor unitary isomorphism, and then prove their correctness by Theorem 4.4.

Proposition 4.7. *The unitary isomorphism problems on* $V \otimes V \otimes W$, $V \otimes V^* \otimes W$, $V \otimes V \otimes V$ *and* $V \otimes V \otimes V^*$ *are polynomial-time reducible to* Unitary 3-Tensor Isomorphism *on* $U' \otimes V' \otimes W'$ *where* $\dim(U')$, $\dim(V')$ *and* $\dim(W')$ *are at most polynomial in* $\dim(V)$ *and* $\dim(W)$.

Proof. The reduction is based on the observation that tensor systems can encode these isomorphism problems. For example, for $\mathrm{A} \in V \otimes V \otimes W$, we can construct a tensor system consisting of one tensor A and two vector spaces $\{V, W\}$, with two arcs from V to A, and one arc from W to A. Starting from two tensors $\mathrm{A}_1, \mathrm{A}_2 \in V \otimes V \otimes W$, we consider the corresponding tensor systems, and ask for unitary isomorphism of these tensor systems. Then by Theorem 4.4, they can be reduced to the plain 3-tensor unitary isomorphism in time $\mathrm{poly}(\dim(V), \dim(W))$, as these are tensor systems with only 1 tensor each. It can be seen that this works for $V \otimes V^* \otimes W$, $V \otimes V \otimes V$, and $V \otimes V \otimes V^*$. This concludes the proof. ∎

4.2.2 $U \otimes V \otimes W$ to $V \otimes V \otimes W$

We mainly follow the construction in [GQ23a] to show that there is a reduction from Unitary 3-Tensor Isomorphism ($U \otimes V \otimes W$) to Unitary Bilinear Form Pseudoisometry ($V' \otimes V' \otimes W'$). In addition, we prove that the reduction from [GQ23a] preserves the unitary property in both directions.

Proposition 4.8. *Given two 3-tensors* $\mathrm{A}, \mathrm{B} \in U \otimes V \otimes W$, *where* $\dim(U) = l \leq \dim(V) = m$ *and* $\dim(W) = n$. *There is a reduction* $r : U \otimes V \otimes W \to V' \otimes V' \otimes W'$ *with* $\dim(V') = l + 5m + 3$ *and* $dim(W') = n + l(m+1) + m(3m+2)$ *such that* A *and* B *are unitarily isomorphic if and only if* $r(\mathrm{A})$ *and* $r(\mathrm{B})$ *are unitarily isomorphic, where frontal slices of* $r(\mathrm{A})$ *and* $r(\mathrm{B})$ *are skew-symmetric matrices.*

Proof. **The reduction.** We use the gadget in [FGS19] and [GQ23a] to present this reduction. Here we use matrix format to illustrate our construction, and the picture of this construction is shown in Figure 1.1. Denote the ith frontal slice of A by $A_i \in$

$\mathrm{M}(l \times m, \mathbb{C})$, where $i \in [n]$. Let the ith frontal slice of $r(\mathrm{A})$ be $\hat{A}_i \in \mathrm{M}(l + 5m + 3, \mathbb{C})$, where $i \in [n + l(m + 1) + m(3m + 2)]$. Then $\hat{A}_i$ is constructed as follows:

- For $i \in [n]$, $\hat{A}_i$ is of the form $\begin{bmatrix} \mathbf{0} & A_i & \mathbf{0} \\ -A_i^t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$.
- For $i \in [n + 1, n + l(m + 1)]$, let $\hat{A}_i$ be the elementary alternating matrix $\mathrm{E}_{s,l+m+t} - \mathrm{E}_{l+m+t,s}$, where $s = \lceil (i - n)/(m + 1) \rceil$ and $t = i - n - (s - 1)(m + 1)$.
- For $i \in [n + l(m + 1), n + l(m + 1) + m(3m + 2)]$, let $\hat{A}_i$ be the elementary alternating matrix $\mathrm{E}_{l+s,l+m+m+1+t} - \mathrm{E}_{l+m+m+1+t,l+s}$, where $s = \lceil (i - n - l(m+1))/(3m+2) \rceil$ and $t = i - n - l(m + 1) - (s - 1)(3m + 2)$.

Denote lateral slices of $r(\mathrm{A})$ by L_i, where $i \in [l + 5m + 3]$. Then we check the ranks of these lateral slices:

- For the first l slices, the lateral slice L_i is a block matrix with two non-zero blocks. One block is $-I_{m+1}$, and another block of size $m \times n$ is the transpose of the ith horizontal slice of $-\mathrm{A}$. Thus, $m + 1 \leq \mathrm{rank}(L_i) \leq 2m + 1$.
- For the following m slices, L_i is a block matrix with two non-zero blocks. One block is $-I_{3m+2}$ and the other one is the $(i - n)$th lateral slice of A with size $l \times n$. Therefore, $3m + 2 \leq \mathrm{rank}(L_i) \leq 3m + 2 + l \leq 4m + 2$.
- For the next $m + 1$ slices, L_i has a block I_l after rearranging the columns, so $\mathrm{rank}(L_i) = l \leq m$.
- For the last $3m + 2$ slices, similarly, L_i has a block I_m after rearranging the columns, so $\mathrm{rank}(L_i) = m$.

Now we consider the ranks of linear combinations of the above slices. There are four observations that help prove the correctness of the reduction:

- If the combination contains L_i for $1 \leq i \leq l$, since the resulting matrix has at least one identity matrix I_{m+1} in the $(l + m + 1)$th row to $(l + 2m + 1)$th row, it has the rank at least $m + 1$.

- If the combination doesn't contain L_i for $l+1 \leq i \leq l+m+1$, the resulting matrix has rank at most $3m+1$, because there are at most $l+5m+3-3m-2 \leq 3m+1$ non-zero rows.
- If the combination involves L_i for $l+1 \leq i \leq l+m+1$, the resulting matrix has rank at least $3m+2$, because there is at least one identity matrix I_{3m+2} in the last $3m+2$ rows.
- If the combination involves L_i for $1 \leq i \leq l$ and L_i for $l+1 \leq i \leq l+m+1$, the resulting matrix has rank at least $4m+3$, because there are at least one identity matrix I_{3m+2} in the last $3m+2$ rows and one identity matrix I_{m+1} in the $(l+m+1)$th row to $(l+2m+1)$th row.

The if direction. Assume there are $P \in \mathrm{U}(l+5m+3, \mathbb{C})$ and $Q \in \mathrm{U}(n+l(m+1)+m(3m+2), \mathbb{C})$ such that $P^t r(\mathrm{A}) P = r(\mathrm{B})^Q$. Then we write P as $P = \begin{bmatrix} P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,1} & P_{2,2} & P_{2,3} \\ P_{3,1} & P_{3,2} & P_{3,3} \end{bmatrix}$, where $P_{1,1} \in \mathrm{M}(l, \mathbb{C})$, $P_{2,2} \in \mathrm{M}(m, \mathbb{C})$ and $P_{3,3} \in \mathrm{M}(4m+3, \mathbb{C})$. By ranks of lateral slices of $r(\mathrm{B})$ and the above observations, it's easy to have that $P_{2,1} = \mathbf{0}$, $P_{1,2} = \mathbf{0}$, $P_{1,3} = \mathbf{0}$ and $P_{2,3} = \mathbf{0}$. Therefore, P is of the form $\begin{bmatrix} P_{1,1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & P_{2,2} & \mathbf{0} \\ P_{3,1} & P_{3,2} & P_{3,3} \end{bmatrix}$. As P is a block-lower-trianglular unitary matrix, $P_{1,1}, P_{2,2}$ and $P_{3,3}$ are unitary matrices. Since the aim is to check if A and B are isomorphic, we only consider the first n frontal slices of $r(\mathrm{A})$ and $r(\mathrm{B})$, which contains A and B respectively. After applying P on lateral slices and horizontal slices of $r(\mathrm{A})$, we have the first n frontal slices as follows:

$$\begin{bmatrix} P_{1,1}^t & \mathbf{0} & P_{3,1}^t \\ \mathbf{0} & P_{2,2}^t & P_{3,2}^t \\ \mathbf{0} & \mathbf{0} & P_{3,3}^t \end{bmatrix} \begin{bmatrix} \mathbf{0} & A_i & \mathbf{0} \\ -A_i^t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P_{1,1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & P_{2,2} & \mathbf{0} \\ P_{3,1} & P_{3,2} & P_{3,3} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & P_{1,1}^t A_i P_{2,2} & \mathbf{0} \\ -P_{2,2}^t A_i^t P_{1,1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

Then we apply the unitary matrix Q on the frontal slices of $r(\mathrm{B})$, and have $P^t r(\mathrm{A}) P = r(\mathrm{B})^Q$. Note that only the block $(1,2)$ and $(2,1)$ are non-zero blocks in the first n slices of $r(\mathrm{B})$ and $P^t r(\mathrm{A}) P$, so we have that only the first $n \times n$ submatrix $Q_{1,1}$ of Q is non-zero in the first n columns, which implies that $Q_{1,1}$ is unitary from the fact that Q is unitary. Therefore, it is enough to give the isomorphism $P_{1,1}^t \mathrm{A} P_{2,2} = \mathrm{B}^{Q_{1,1}}$ where $P_{1,1}^t, P_{2,2}$ and $Q_{1,1}$ are unitary.

The only if direction. Assume $P\mathrm{A}Q = \mathrm{B}^R$ for some $P \in \mathrm{U}(l, \mathbb{C}), Q \in \mathrm{U}(m, \mathbb{C})$ and $R \in \mathrm{U}(n, \mathbb{C})$. We claim that there are two unitary matrices $\hat{P} = \mathrm{diag}(P, Q, S_1, S_2) \in \mathrm{U}(l + 5m + 3, \mathbb{C})$ and $\hat{Q} = \mathrm{diag}(R, T_1, T_2) \in \mathrm{U}(n + l(m + 1) + m(3m + 2), \mathbb{C})$ such that $\hat{P}^t r(\mathrm{A}) \hat{P} = r(\mathrm{B})^{\hat{Q}}$, where $S_1 \in \mathrm{U}(m + 1, \mathbb{C}), S_2 \in \mathrm{U}(3m + 2, \mathbb{C}), T_1 \in \mathrm{U}(l(m + 1), \mathbb{C})$ and $T_2 \in \mathrm{U}(m(3m + 2), \mathbb{C})$.

Due to the fact that $P\mathrm{A}Q = \mathrm{B}^R$, it's straightforward to check the first n frontal slices of $\hat{P}^t r(\mathrm{A}) \hat{P}$ and $r(\mathrm{B})^{\hat{Q}}$ are equal. Then we consider the remaining gadget slices. Let $\overline{r(\mathrm{A})}$ and $\overline{r(\mathrm{B})}$ be tensors constructed by the $(m+1)$th frontal slice to $(m+l(m+1))$th frontal slice of $r(\mathrm{A})$ and $r(\mathrm{B})$, respectively. Consider $\overline{r(\mathrm{A})}$ and $\overline{r(\mathrm{B})}$ from the frontal view:

$$\begin{bmatrix} 0 & 0 & \mathrm{E} & 0 \\ 0 & 0 & 0 & 0 \\ -\mathrm{E} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix},$$

where $\mathrm{E} \in \mathrm{T}(l \times (m+1) \times l(m+1), \mathbb{C})$. Then we apply $\hat{P}$ on the lateral and horizontal slices of $\overline{r(\mathrm{A})}$,

$$\begin{bmatrix} P^t & & & \\ & Q^t & & \\ & & S_1^t & \\ & & & S_2^t \end{bmatrix} \begin{bmatrix} \mathbf{0} & \mathbf{0} & E_i & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -E_i & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P & & & \\ & Q & & \\ & & S_1 & \\ & & & S_2 \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & P^t E_i S_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -S_1^t E_i P & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

where $E_i \in \mathrm{M}(l \times (m + 1), \mathbb{C})$. Observe that P^t acts on the horizontal direction of E, so it requires designing proper S_1 and T_1 to remove the effect of P. Let the lateral slice of E to be $L_i \in \mathrm{M}(l \times l(m + 1), \mathbb{C})$ where $i \in [m + 1]$. Apply a proper permutation π on the columns of L_i and have the matrix $L_i' = L_i T_\pi = \begin{bmatrix} \mathbf{0} \dots I_l \dots \mathbf{0} \end{bmatrix}$ where $T_\pi \in$

$\mathrm{M}(l(m+1),\mathbb{C})$ is the permutation matrix and the ith block of L'_i is the identity matrix $I_l \in \mathrm{M}(l,\mathbb{C})$. After left multiplying L'_i by P^t, we have $P^t L'_i = \begin{bmatrix}\mathbf{0}\dots P^t \dots \mathbf{0}\end{bmatrix}$. Now we define a diagonal matrix T'_1 as $\mathrm{diag}(P^t,\dots,P^t)$, which gives us $P^t L'_i = L'_i T'_1 \iff P^t L_i = L_i T_\pi T'_1 T^t_\pi$. Then we set S_1 to be the identity matrix and T_1 to be $T_\pi T'_1 T^t_\pi$, and it yields $P^t \mathrm{E} S_1 = \mathrm{E}^{T_1}$, where S_1 and T_1 are unitary.

It remains to check the last $m(3m+2)$ frontal slices, which uses the similar method as above, and this produces unitary matrix S_2 and T_2. Now we have the unitary matrix S and T as desired. ■

4.2.3 $U \otimes V \otimes W$ to $V \otimes V^* \otimes W$

Based on Lemma 4.2, we will show that the Unitary 3-Tensor Isomorphism ($U \otimes V \otimes W$) can be reduced to Unitary Matrix Space Conjugacy ($V' \otimes V'^* \otimes W'$).[1]

Proposition 4.9. *There is a reduction $r : U \otimes V \otimes W \to V' \otimes V'^* \otimes W$ where $\dim(U) = l$, $\dim(V) = m$, $\dim(W) = n$ and $\dim(V') = l+m$ such that two tensors $\mathrm{A}, \mathrm{B} \in U \otimes V \otimes W$ are unitarily isomorphic if and only if $r(\mathrm{A}), r(\mathrm{B}) \in V' \otimes V'^* \otimes W$ are unitarily conjugate matrix spaces.*

Proof. **The reduction.** Denote the ith frontal slice of A by A_i. We construct the reduction in the following way:

$$\hat{A}_i = \begin{bmatrix} \mathbf{0} & A_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix},$$

where $\hat{A}_i \in \mathrm{M}(l+m,\mathbb{C})$ is the ith frontal slice of $r(\mathrm{A})$.

[1]We note that there is some ambiguity in the name here, which where the notation helps. Namely, "unitary conjugacy of matrix spaces" could mean either the action of $\mathrm{U}(V')\times\mathrm{U}(W')$ on $V'\otimes V'^*\otimes W'$ or the action of $\mathrm{U}(V')\times\mathrm{GL}(W')$ on the same space. In this thesis we do not consider such "mixed" actions, though they are certainly interesting for future research. As a mnemonic, if we think of the matrix space itself as "unitary", in the sense of having a unitary structure, this lends itself to the interpretation of $\mathrm{U}(V')\times\mathrm{U}(W')$ acting.

Without loss of generality, we can always assume A and B are non-degenerate. Then we will show that A and B are isomorphic if and only if $r(\mathrm{A})$ and $r(\mathrm{B})$ are isomorphic.

For the if direction. We assume that $r(\mathrm{A})$ and $r(\mathrm{B})$ are unitarily isomorphic, so there are $P \in \mathrm{U}(l+m, \mathbb{C})$ and $Q \in \mathrm{U}(n, \mathbb{C})$ such that $P^{-1}r(\mathrm{A})P = r(\mathrm{B})^Q$. Let P be a block matrix:

$$\begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix},$$

where $P_{1,1}$ is of size $l \times l$. Let $r(\mathrm{B})^Q$ be $r(\mathrm{B})'$ and the ith frontal slice of $r(\mathrm{B})'$ be B_i'. Since $r(\mathrm{A})P = Pr(\mathrm{B})'$, we have that

$$\begin{bmatrix} A_iP_{2,1} & A_iP_{2,2} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & P_{1,1}B_i' \\ \mathbf{0} & P_{2,1}B_i' \end{bmatrix},$$

where $A_iP_{2,1} = \mathbf{0}$ and $A_iP_{2,2} = P_{1,1}B_i'$ for all $i \in [n]$. It follows that every row of $P_{2,1}$ is in the intersection of right kernels of A_i. Since A is non-degenerate, $P_{2,1}$ must be a zero matrix. Thus, P is a block-upper-trianglular matrix, which results in $P_{1,1}$ and $P_{2,2}$ are unitary. Therefore, we have that $P_{1,1}^{-1}\mathrm{A}P_{2,2} = \mathrm{B}^Q$ for $P_{1,1} \in \mathrm{U}(l, \mathbb{C}), P_{2,2} \in \mathrm{U}(m, \mathbb{C})$ and $Q \in \mathrm{U}(n, \mathbb{C})$.

For the only if direction. Suppose $P\mathrm{A}Q = \mathrm{B}^R$ where $P \in \mathrm{U}(l, \mathbb{C}), Q \in \mathrm{U}(m, \mathbb{C})$ and $R \in \mathrm{U}(n, \mathbb{C})$. Then we define P' and Q' as follows

$$P' = \begin{bmatrix} P^{-1} & \mathbf{0} \\ \mathbf{0} & Q \end{bmatrix} \quad \text{and} \quad Q' = R,$$

where P' and R' are unitary. We can straightforwardly check that $P'^{-1}r(\mathrm{A})P' = r(\mathrm{B})^{Q'}$.

■

We can similarly apply the strategy in this section to construct the reduction from Unitary 3-Tensor Isomorphism ($U \otimes V \otimes W$) to Bilinear Form Unitary Pseudo-isometry ($V \otimes V \otimes W$). We record this as the following result.

Proposition 4.10. *There is a reduction* $r : U \otimes V \otimes W \to V' \otimes V' \otimes W$ *where* $\dim(U) = l$, $\dim(V) = m$, $\dim(W) = n$ *and* $\dim(V') = l + m$ *such that two tensors* $\mathrm{A}, \mathrm{B} \in U \otimes V \otimes W$ *are unitarily isomorphic if and only if* $r(\mathrm{A}), r(\mathrm{B}) \in V' \otimes V' \otimes W$ *are unitarily pseudo-isometric bilinear forms.*

4.2.4 $U \otimes V \otimes W$ to $V \otimes V \otimes V^*$ and $V \otimes V \otimes V$

In this section, we demonstrate that there are reductions from $U \otimes V \otimes W$ to $V \otimes V \otimes V^*$ and $V \otimes V \otimes V$. Since it was proved that $U \otimes V \otimes W$ reduces to $V \otimes V \otimes W$ in Section 4.2.2, we only need to show reductions from $V \otimes V \otimes W$ to $V \otimes V \otimes V^*$ and $V \otimes V \otimes V$.

Proposition 4.11. *There is a reduction from* Bilinear Map Unitary Pseudo-isometry *to* Unitary Algebra Isomorphism *and to* Unitary Equivalence of Noncommutative Cubic Forms.

In symbols, there are reductions

$$r : V \otimes V \otimes W \to V' \otimes V' \otimes V'^* \quad \textit{and} \quad r' : V \otimes V \otimes W \to V' \otimes V' \otimes V'$$

where $\dim(V') = \dim(V) + \dim(W)$ *such that two bilinear forms* $\mathrm{A}, \mathrm{B} \in V \otimes V \otimes W$ *are unitarily pseudo-isometric if and only if* $r(\mathrm{A})$ *and* $r(\mathrm{B})$ *are unitarily isomorphic algebras, if and only if* $r'(\mathrm{A})$ *and* $r'(\mathrm{B})$ *are unitarly equivalent noncommutative cubic forms.*

Proof. **The construction.** Given a tensor $\mathrm{A} \in V \otimes V \otimes W$ whose frontal slices are A_i, construct an array $\mathrm{A}' \in \mathrm{T}((l+m) \times (l+m) \times (l+m), \mathbb{C})$ of which the frontal slices are

$$A_i' = \mathbf{0} \text{ for } i \in [l] \quad \text{ and } \quad A_i' = \begin{bmatrix} A_{i-l} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \text{ for } i \in [l+1, l+m]\,.$$

Let $\hat{\mathrm{A}}$ represent the tensor in $V' \otimes V' \otimes V'^*$ corresponding to entries defined by A', and denote $\tilde{\mathrm{A}}$ by the tensor in $V' \otimes V' \otimes V'$ corresponding to entries defined by A'. Note that by Corollary 4.3, we can always assume that the frontal slices of A are linearly independent, so the last m slices of A' are linearly independent as well. We will show that $\mathrm{A}, \mathrm{B} \in V \otimes V \otimes W$ are isomorphic if and only if $\hat{\mathrm{A}}, \hat{\mathrm{B}} \in V' \otimes V' \otimes V'^*$ are isomorphic, and A, B are isomorphic if and only if $\tilde{\mathrm{A}}, \tilde{\mathrm{B}} \in V' \otimes V' \otimes V'$ are isomorphic.

The only if direction. Given $P \in \mathrm{U}(l, \mathbb{C})$ and $Q \in \mathrm{U}(m, \mathbb{C})$ such that $P^t \mathrm{A} P = \mathrm{B}^Q$, set $\hat{P}$ and $\tilde{P}$ to be $\mathrm{diag}(P, Q^t)$ and $\mathrm{diag}(P, Q^{-1})$ respectively, where $\hat{P}$ and $\tilde{P}$ are unitary. Then we can straightforwardly derive that $\hat{P}^t \hat{\mathrm{A}} \hat{P} = \hat{\mathrm{B}}^{\hat{P}^t}$ and $(\tilde{P}^t \tilde{\mathrm{A}} \tilde{P})^{\tilde{P}} = \tilde{\mathrm{B}}$.

The if direction. We first consider the $V' \otimes V' \otimes V'^*$ case. Assume there is a matrix $P \in \mathrm{U}(l+m, \mathbb{C})$ such that $P^t \hat{\mathrm{A}} P = \hat{\mathrm{B}}^{P^t}$. Then we write P as $\begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix}$, where $P_{1,1} \in \mathrm{M}(l, \mathbb{C})$. Consider the first l slices B_i'' of $\hat{\mathrm{B}}^{P^t}$,

$$B_i'' = P^t \hat{\mathrm{A}}_i P = \mathbf{0}.$$

Since the last m slices of $\hat{\mathrm{A}}$ are linearly independent, we will have that $P_{2,1} = \mathbf{0}$. It follows that $P_{1,1}$ and $P_{2,2}$ are unitary. The equivalence of the last m slices of $P^t \hat{\mathrm{A}} P$ and $\hat{\mathrm{B}}^{P^t}$ yields that $P_{1,1}^t \mathrm{A} P_{1,1} = \mathrm{B}^{P_{2,2}^t}$, which completes the proof of the if direction for $V' \otimes V' \otimes V'^*$.

The proof for the if direction of $V' \otimes V' \otimes V'$ case is similar to the above. ■

Chapter 5

d-Tensor $\mathcal{G}$-Isomorphism to 3-Tensor $\mathcal{G}$-Isomorphism

In this chapter, we present some background for algebras in Section 5.1. Then we show a reduction from Unitary d-Tensor Isomorphism to Uniatry 3-Tensor Isomorphism in Section 5.2. Since proofs for orthogonal groups are similar, we only present the proofs for unitary groups.

5.1 Preparations

In this section, we introduce notions of *quivers* and *path algebras* as those notions are required for converting Unitary d-Tensor Isomorphism to the isomorphism for algebras.

A *quiver* is a directed multigraph $G = (V, E, s, t)$, where V is the vertex set, E is the arrow set, and $s, t : E \to V$ are two maps indicating the source and target of an arrow.

A path in G is the concatenation of edges $p = e_1, e_2, \ldots, e_n$, where $e_i \in E$ for $i \in [n]$, such that $s(e_{i+1}) = t(e_i)$ for $i \in [n-1]$. $s(p) = s(e_1)$ is the source of p, $t(p) = t(e_n)$ is the target of p and $l(p) = n$ is the length of p. For a consistent notation including the vertex, we define the source $s(v)$ and target $t(v)$ for each vertex $v \in V$

by $s(v) = t(v) = v$, and we regard the length $l(v)$ of every vertex v as 0. Note that V consists of paths of length 0, and E consists of paths of length 1.

Let $\mathbb{F}$ be a field. The *path algebra* of G, denoted as $\mathrm{Path}_{\mathbb{F}}(G)$, is the free algebra whose bases are generated by $V \cup E$ modulo the relations:

(1) For $v, v' \in V$, $vv' = v$ if $v = v'$, and 0 otherwise.

(2) For $v \in V$ and $e \in E$, $ve = e$ if $v = s(e)$, and 0 otherwise. And $ev = e$ if $v = t(e)$, and 0 otherwise.

(3) For $e, e' \in E$, $ee' = 0$ if $t(e) \neq s(e')$.

In this thesis we make use of the following quiver. Note that this is different from the quiver used in [GQ23a]; this difference leads to some significant simplifications in the argument, and allows the argument to go through for unitary and orthogonal groups (it is unclear to us whether the original argument in [GQ23a] does so). Note

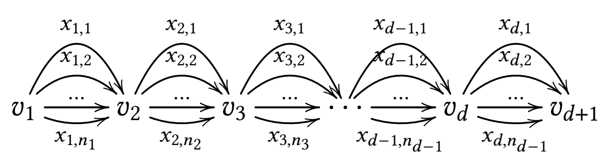

Figure 5.1: The quiver G we use in this thesis.

that $G = (V, E, s, t)$ where $V = \{v_1, \ldots, v_{d+1}\}$, $E = \{x_{i,j} \mid i \in [d], j \in [n_i]\}$, $s(x_{i,j}) = v_i$ and $t(x_{i,j}) = v_{i+1}$.

5.2 Detailed Proofs

Let A, B be two d-way arrays in $\mathrm{T}(n_1 \times \cdots \times n_d, \mathbb{F})$. We will exhibit an algorithm T such that $T(\mathrm{A})$ is an algebra on $\mathbb{F}^m$ where $m = \mathrm{poly}(n_1, \ldots, n_d)$, and such that A and B are unitarily isomorphic as d-tensors if and only if $T(\mathrm{A})$ and $T(\mathrm{B})$ are unitarily isomorphic as algebras. We can then apply Theorem 1.5 to reduce to Unitary 3-

Tensor Isomorphism. Therefore, in the following we focus on the step of reducing Unitary d-Tensor Isomorphism to Unitary Algebra Isomorphism.

We present the proof for unitary groups, and the argument is essentially the same for orthogonal groups.

Proof of Theorem 1.6. Let $f, g \in U_1 \otimes U_2 \otimes \cdots \otimes U_d$ be two tensors, where $U_i = \mathbb{F}^{n_i}$ for $i \in [d]$. We can encode f in $\mathrm{Path}_{\mathbb{F}}(G)$ as follows. Recall that e_i denotes the ith standard basis vector. Suppose $f = \sum_{(i_1,\ldots,i_d)} \alpha_{i_1,\ldots,i_d} e_{i_1} \otimes \cdots \otimes e_{i_d}$, where the summation is over $(i_1, \ldots, i_d) \in [n_1] \times \cdots \times [n_d]$ and $\alpha_{i_1,\ldots,i_d} \in \mathbb{F}$. Then let $\hat{f} \in \mathrm{Path}_{\mathbb{F}}(G)$ be defined as $\hat{f} = \sum_{(i_1,\ldots,i_d)} \alpha_{i_1,\ldots,i_d} x_{1,i_1} x_{2,i_d} \ldots x_{d,i_d}$, where $(i_1, \ldots, i_d) \in [n_1] \times \cdots \times [n_d]$.

Let $R_f := \mathrm{Path}_{\mathbb{F}}(G)/(\hat{f})$ and $R_g := \mathrm{Path}_{\mathbb{F}}(G)/(\hat{g})$. We will show that f and g are unitarily isomorphic as tensors if and only if R_f and R_g are unitarily isomorphic as algebras.

Tensor isomorphism implies algebra isomorphism. Let $(P_1, \ldots, P_d) \in \mathrm{U}(n_1, \mathbb{C}) \times \cdots \times \mathrm{U}(n_d, \mathbb{C})$ be a tensor isomorphism from f to g. Then P_i naturally acts on the linear space $\langle x_{i,1}, \ldots, x_{i,n_i} \rangle$. Together with the identity matrix I_{d+1} acting on $\langle v_1, \ldots, v_{d+1} \rangle$, we claim that they form an algebra isomorphism from R_f to R_g.

We will show that this is a homomorphism, and then verify that it is indeed an isomorphism. This part is essentially the same as [GQ23a].

To show that it is a homomorphism, we first examine the quiver relations. This homomorphism $R_f \to R_g$ is induced by a linear map, this map P is defined by $P(v_i) = v_i$ and

$$P(x_{i,j}) = \sum_{k=1}^{n_i} (P_i)_{jk} y_{i,k} \quad \text{for } i = 1, \ldots, d-1,$$

where $y_{1,1}, \ldots, y_{d,n_d}, v_1, \ldots, v_d$ denote generators of R_g. Let $x_{1,1}, \ldots, x_{d,n_d}, v_1, \ldots, v_d$ be generators of R_f, and then the following quiver relations need to be checked:

$$v_i v_{i'} = \delta_{i,i'} v_i$$

$$v_i x_{i',j} = \delta_{i,i'} x_{i',j}$$

$$x_{i,j}v_{i'} = \delta_{i+1,i'}x_{i,j}$$
$$x_{i,j}x_{i',j'} = 0 \quad \text{if } i+1 \neq i'.$$

It's not hard to examine the first three which involve the v_i, as

$$\begin{aligned}
P(v_i v_{i'}) &= P(v_i)P(v_{i'}) = v_i v_{i'} = \delta_{i,i'}P(v_i),\\
P(v_i x_{i',j}) &= P(v_i)P(x_{i',j}) = v_i \sum_{k=1}^{n_{i'}} (P'_i)_{jk} y_{i',k} = \delta_{i,i'}P(x_{i',j}),\\
P(x_{i,j}v_{i'}) &= P(x_{i,j})P(v_{i'}) = \sum_{k=1}^{n_i} (P_i)_{jk} y_{i,k} v_{i'} = \delta_{i+1,i'}P(x_{i,j}).
\end{aligned}$$

For the last relation,

$$\begin{aligned}
P(x_{i,j}x_{i',j'}) &= P(x_{i,j})P(x_{i',j'})\\
&= \sum_{k=1}^{n_i} (P_i)_{jk} y_{i,k} \sum_{k=1}^{n_{i'}} (P_{i'})_{j'k} y_{i',k}\\
&= \sum_{k=1}^{n_i} \sum_{k=1}^{n_{i'}} (P_i)_{jk} (P_{i'})_{j'k} y_{i,k} y_{i',k}\\
&= 0 \quad \text{if } i+1 \neq i'.
\end{aligned}$$

Therefore, the map $R_f \longrightarrow R_g$ induced by P is an algebra homomorphism.

Let $n = \max_i\{n_i\}$. To prove the map $R_f \longrightarrow R_g$ is an algebra isomorphism, it requires to check the dimension of R_f first:

$$\begin{aligned}
\dim(R_f) &= \#\{v_i\} + \sum_{i=1}^{d} \sum_{j=0}^{d-i} \#\{\text{paths from } v_i \text{ to } v_{i+j}\}\\
&= d + \sum_{i=1}^{d} \sum_{j=0}^{d-i} \prod_{k=i}^{i+j} n_j\\
&\leq d + \sum_{i=1}^{d} \sum_{j=0}^{d-i} n^d\\
&\leq O(d^2 n^d).
\end{aligned}$$

If d is fixed, the dimension of R_f is polynomial with n. Next, as P is an isomorphism of $(\sum_{i=1}^{d} n_i + d)$-vector spaces, it follows that $R_f \longrightarrow R_g$ induced by P is surjective on all the generators of R_g and hence it's surjective on the whole R_g. Finally, since $\dim(R_f) = \dim(R_g) < \infty$, the map $R_f \to R_g$ is a bijection and it's naturally an algebra isomorphism from R_f to R_g.

Algebra isomorphism implies tensor isomorphism. This part of the proof is new, compared to the corresponding part in [GQ23a].

Let $\phi : \mathrm{Path}_{\mathbb{F}}(G)/(\hat{f}) \to \mathrm{Path}_{\mathbb{F}}(G)/(\hat{g})$ be an algebra isomorphism, which is determined by the images of $v_i, x_{j,k}$ under ϕ.

Note that $\mathrm{Path}_{\mathbb{F}}(G)$ is linearly spanned by paths in G, so it is naturally graded, and we use $\mathrm{Path}_{\mathbb{F}}(G)_\ell$ denotes the linear space of $\mathrm{Path}_{\mathbb{F}}(G)$ spanned by paths of length exactly ℓ.

First, note that $\phi(\hat{f}) = \alpha \cdot \hat{g}$+a linear combination of quiver relations, where $\alpha \in \mathbb{F}$.

Second, we claim that the coefficient of v_i in $\phi(x_{j,k})$ must be zero for any i, j, k. If not, suppose $\phi(x_{j,k}) = \gamma \cdot v_i + M$ where $\gamma \neq 0$, and M denotes other terms not containing v_i. On the one hand, $\phi(x_{j,k}^2) = 0$ because $x_{j,k}^2 = 0$ by the quiver relations. On the other hand, $\phi(x_{j,k})^2 = (\gamma \cdot v_i + M)^2 = \gamma^2 \cdot v_i^2 + M' = \gamma^2 \cdot v_i + M'$ where M' denotes other terms, which cannot contain v_i. So $\phi(x_{j,k})^2$ is nonzero, contradicting $\phi(x_{j,k}^2) = 0$ and ϕ being an algebra isomorphism.

By the above, it follows for any path P (a product of $x_{i,j}$'s) of length $\ell \geq 1$, $\phi(P)$ is a linear combination of paths of length $\geq \ell$. This implies that, if we express ϕ in the linear basis of $\mathrm{Path}_{\mathbb{F}}(G)/(\hat{f})$, $(v_1, \ldots, v_{d+1}, x_{i,j}, \text{paths of length } 2, \ldots, \text{paths of length } d)$, then ϕ is a block-lower-triangular matrix, where the each block is determined by the path lengths. That is, the first block is indexed by $(v_1, \ldots, v_{d+1})$, the second block is indexed by $(x_{i,j})$, the third block is indexed by paths of length 2, and so on.

Third, we claim that for $1 \leq i < j \leq d+1$, the coefficient of $x_{i,k}$ in $\phi(x_{j,k'})$ must be zero. If not, then let P be a path of length $d - i$ starting from v_{i+1}. Because of the block-lower-triangular matrix structure and that ϕ is an isomorphism, we know that there exists a path P' of length $d - i$, such that the coefficient of P in $\phi(P')$ is nonzero. Then $\phi(x_{j,k'} \cdot P') = \phi(x_{j,k'}) \cdot \phi(P') = (\beta \cdot x_{i,k} + M) \cdot (\gamma \cdot P + N) = \beta \cdot \gamma \cdot x_{i,k} \cdot P + L$, where M, N and L denote appropriate other terms, and $\beta, \gamma \in \mathbb{F}$ are non-zero. Note that $x_{i,k} \cdot P$ cannot be cancelled from other terms. This implies that $\phi(x_{j,k'} \cdot P')$ is non-zero. However, $x_{j,k'} \cdot P'$ has to be zero because P' is of length $d - i$, so it starts from some variable $x_{i+1,k''}$. This leads to the desired contradiction.

By the above, if we restrict ϕ to the linear subspace $\langle x_{i,j} \rangle$ in the linear basis

$$(x_{1,1}, \ldots, x_{1,n_1}, \ldots, x_{d,1}, \ldots, x_{n_d}),$$

then ϕ is again in the block-lower-triangular form, where the blocks are determined by the first index of $x_{i,j}$. That is, the first block is indexed by $x_{1,j}$ for all j, the second block is indexed by $x_{2,j}$ for all j, and so on.

We now can take the diagonal block of ϕ on $(x_{i,1}, \ldots, x_{i,n_i})$, and let the resulting (invertible) matrix be P_i. These matrices $P_1, \ldots, P_d$ together determine a linear map ψ on $\langle x_{i,j} \rangle$. By comparing degrees, we see that $\psi(\hat{f}) = \alpha \cdot \hat{g}$. Now suppose $\mathbb{F}$ contains dth roots. We can then obtain $(1/\alpha^{1/d} \cdot P_1, 1/\alpha^{1/d} \cdot P_2, \ldots, 1/\alpha^{1/d} \cdot P_d) \cdot f = g$.

Getting back to our original goal, we see that if ψ is unitary, then the block-lower-triangular form of ψ implies that it is actually block-diagonal, and the diagonal blocks are all unitary as well. This shows that P_i's are unitary, and f and g are unitarily isomorphic. ■

Chapter 6

Application to LOCC Equivalence

In this chapter, we first introduce some equivalences for quantum entanglement and their relations in Section 6.1. Then we discuss motivations of studying quantum entanglement in Section 6.2. Some relative works related to determining equivalences of quantum entanglement are presented in Section 6.3. Our result is presented in Section 6.4.

6.1 Background on Equivalences for Quantum Entanglement

Local Operation and Classical Communication is a natural protocol from the physical operation viewpoint, where local operation is performed on each part and classical information is sent to other parts. For example, an LOCC protocol for two parties is showed in Figure 6.1.

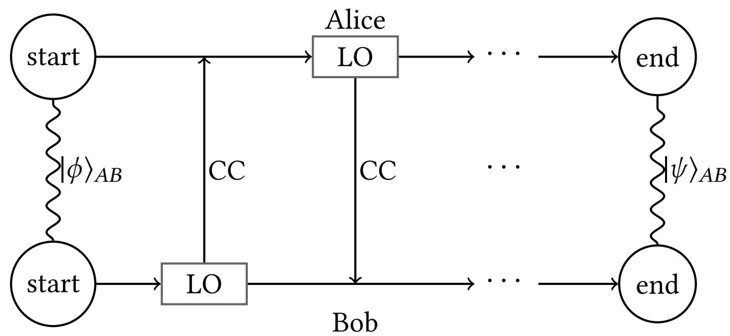

Figure 6.1: LOCC protocol with two parties

In the beginning, Alice and Bob share an entanglement $|\phi\rangle$. After multiple rounds of local operations and classical communications, they obtained a new entanglement $|\psi\rangle$. For those pairs of entanglement, we have the following type of equivalence–*LOCC equivalence*.

Definition 6.1. Given $|\phi\rangle, |\psi\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \cdots \otimes \mathbb{C}^{n_d}$:

(1) $|\phi\rangle$ is said to be LOCC convertible to $|\psi\rangle$ (denoted as $|\phi\rangle \xrightarrow{\text{LOCC}} |\psi\rangle$) if there is a LOCC protocol converting $|\phi\rangle$ to $|\psi\rangle$.

(2) $|\phi\rangle, |\psi\rangle$ are said to be LOCC equivalent (denoted as $|\phi\rangle \xLeftrightarrow{\text{LOCC}} |\psi\rangle$) if $|\phi\rangle \xrightarrow{\text{LOCC}} |\psi\rangle$ and $|\phi\rangle \xleftarrow{\text{LOCC}} |\psi\rangle$.

Stochastic local operations and classical communications (SLOCC) relaxes LOCC by only requiring that the initial state can be transformed to the terminal start by local operations and classical communication with non-zero probability. An example of SLOCC is presented in Figure 6.2.

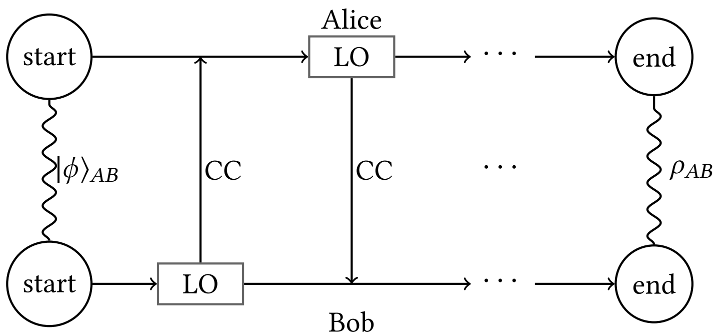

Figure 6.2: SLOCC protocol with two parties

If the resulting quantum state ρ_{AB} can be represented as the linear combination as a pure state $|\psi\rangle$ and other pure states, i.e., $\rho_{AB} = p_0|\psi\rangle\langle\psi| + \sum_i p_i|\psi_i\rangle\langle\psi_i|$, then we say $|\phi\rangle$ is SLOCC convertible to $|\psi\rangle$. Then we similarly present the following definition of SLOCC equivalence.

Definition 6.2. Given $|\phi\rangle, |\psi\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \cdots \otimes \mathbb{C}^{n_d}$:

(1) $|\phi\rangle$ is said to be SLOCC convertible to $|\psi\rangle$ (denoted as $|\phi\rangle \xrightarrow{\text{SLOCC}} |\psi\rangle$) if there is a SLOCC protocol converting $|\phi\rangle$ to $|\psi\rangle$.

(2) $|\phi\rangle, |\psi\rangle$ are said to be SLOCC equivalent (denoted as $|\phi\rangle \overset{\text{SLOCC}}{\Longleftrightarrow} |\psi\rangle$) if $|\phi\rangle \xrightarrow{\text{SLOCC}} |\psi\rangle$ and $|\phi\rangle \xleftarrow{\text{SLOCC}} |\psi\rangle$.

There are other two types of equivalences, which are related to LOCC equivalence and SLOCC equivalence. The first equivalence is called *LU equivalence*, which is similar to our definition for Unitary Tensor Isomorphism.

Definition 6.3. Given two d-partite pure states $|\phi\rangle, |\psi\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \cdots \otimes \mathbb{C}^{n_d}$:

$|\phi\rangle, |\psi\rangle$ are said to be LU equivalent ($|\phi\rangle \overset{\text{LU}}{\Longleftrightarrow} |\psi\rangle$) if $\exists$ d *unitary matrices* $U_1 \in \mathrm{U}(\mathbb{C}^{n_1}), U_2 \in \mathrm{U}(\mathbb{C}^{n_2}), \ldots, U_d \in \mathrm{U}(\mathbb{C}^{n_d})$ s.t.

$$|\phi\rangle = U_1 \otimes U_2 \cdots \otimes U_d|\psi\rangle.$$

The local unitary (LU) equivalence is the finest relation between quantum states, and it's related to LOCC equivalence. For pure states, the LU equivalence is the same as the LOCC equivalence [BPR+00].

Theorem 6.4 ([BPR+00]). $|\phi\rangle \overset{\text{LOCC}}{\Longleftrightarrow} |\psi\rangle$ *if and only if* $|\phi\rangle \overset{\text{LU}}{\Longleftrightarrow} |\psi\rangle$.

Another equivalence is similar to Tensor Isomorphism.

Definition 6.5. Given two d-partite pure states $|\phi\rangle, |\psi\rangle \in \mathbb{C}^{n_1} \otimes \mathbb{C}^{n_2} \cdots \otimes \mathbb{C}^{n_d}$:

$|\phi\rangle, |\psi\rangle$ are said to be LI equivalent ($|\phi\rangle \overset{\text{LI}}{\Longleftrightarrow} |\psi\rangle$) if $\exists$ d *invertible matrices* $A_1 \in \mathrm{GL}(\mathbb{C}^{n_1}), A_2 \in \mathrm{GL}(\mathbb{C}^{n_2}), \ldots, A_d \in \mathrm{GL}(\mathbb{C}^{n_d})$ s.t.

$$|\phi\rangle = A_1 \otimes A_2 \cdots \otimes A_d |\psi\rangle.$$

Similarly, by [DVC00], two d-partite states $|\phi\rangle, |\psi\rangle \in \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_d}$ are SLOCC equivalent if they are LI equivalent.

Theorem 6.6 ([DVC00]). $|\phi\rangle \overset{\text{SLOCC}}{\Longleftrightarrow} |\psi\rangle$ *if and only if* $|\phi\rangle \overset{\text{LI}}{\Longleftrightarrow} |\psi\rangle$.

6.2 Multipartite Entanglement

Multipartite quantum entanglement plays a crucial role in quantum algorithms [JL03, BM11], quantum computation [BBD+09], and many-body quantum systems [AFOV08].

Interestingly, it is generally regarded that d-partite entanglement, $d \geq 3$, is more difficult to understand than bipartite entanglement. That is, there are nice and clean criteria to decide if two bipartite states are equivalent under local unitary (LU, by Schmidt coefficients), local operations and classical communication (LOCC, by Nielsen's theorem [Nie99]), or stochastic local operations and classical communication (SLOCC, by Schmidt ranks). However, to decide whether two d-partite pure states, $d \geq 3$, are equivalent under LU, LOCC, or SLOCC, no such clean and complete criteria are known.

This prompted Walter, Gross and Eisert to suggest that we may have to "come to terms with the fact that a canonical theory of multipartite entanglement may not exist" in [WGE16]. The distinction between bipartite and multipartite entanglement naturally leads one to wonder about the role of the part number in the complexity of quantum entanglement. For example, now that classifying tripartite states seems more difficult than classifying bipartite states, would classifying 4-partite states be more difficult than classifying tripartite states?

6.3 Previous Works

There has been an intensive study of LU and LI equivalences of multipartite states. We refer the readers to the great survey on multipartite entanglement by Walter, Gross, and Eisert [WGE16]. In particular, the above characterizations by group actions naturally lead to algebraic and geometric techniques such as in [VDDMV02, Kra10a, Kra10b, Lan11, GW13].

From classifications up to 4 qubits [DVC00, VDDMV02, DdGMO22, BDD+10] and results on algebraic invariants up to 5 qubits [LT05, BLT03, HLT14], it is commonly understood that SLOCC classification becomes more difficult with more qubits. The result in [GQ23a], in contrast, shows that if we stick with 3 particles, but allow the dimension of their individual state spaces to grow—i.e., use 3 qu*d*its rather than many qu*b*its—SLOCC classification is already as hard as the 3 qu*d* case.

In [ZLQ18], Zangi, Li, and Qiao presented a procedure that transforms a d-partite state to a *set* of bipartite and tripartite states, such that two d-partite states are LU and LI equivalent if and only if the resulting sets of states are. They achieved their result by a technique called quantum state concentration, which takes the form of a tree tensor network structure [SDV06], and concluded that "multipartite entanglement is no more complex than the tripartite entangled states of high enough dimensions."

6.4 Our Result

Our result in Theorem 1.6 implies that *classifying LU equivalence of d-partite pure states, $d > 3$, can be reduced to classifying LU equivalence for tripartite pure states.* Formally, we have the following.

Theorem 6.7. *Let $d > 3$, $n_1, \ldots, n_d \in \mathbb{N}$, $\vec{n} = (n_1, \ldots, n_d)$, and $N = \prod_{i \in [d]} n_i$. Then there exists a map $F_{\mathrm{LU},d,\vec{n}}$ sending d-partite pure states in $V = \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_d}$ to tripartite pure states in $\mathbb{C}^{m_1} \otimes \mathbb{C}^{m_2} \otimes \mathbb{C}^{m_3}$, such that*

(1) *For $i \in [3]$, m_i is upper bounded by a polynomial in N, and*

(2) *Two pure states $|\phi\rangle, |\psi\rangle \in V$ are LU equivalent if and only if $F_{\mathrm{LU},d,\vec{n}}(|\phi\rangle)$ and $F_{\mathrm{LU},d,\vec{n}}(|\psi\rangle)$ are LU equivalent.*

Compared to [ZLQ18], our result transforms a d-partite state to a *single* tripartite state. Perhaps more interestingly, we utilize some new techniques, including path algebras from representation theory of associative algebras, and gadget constructions from computational complexity theory. We hope that these techniques will find other uses in quantum information and computation.

Chapter 7

Conclusion

Our works are concluded in Section 7.1. Then some open problems are proposed in Section 7.2. We discuss our further plans in Section 7.3.

7.1 Summary

7.1.1 Recent Developments on TI

Following [GQ23a, GQ21], this thesis contributes to building up the complexity theory around Tensor Isomorphism and closely related problems. That is, [GQ23a] introduced TI-completeness and showed that many isomorphism problems, under the action of a product of general linear groups, were TI-complete. Then [GQ21] focused on applications of tensor techniques for reductions around p-Group Isomorphism. Several recent works further enrich this theory, such as [GQT22, D'A23] showing more problems to be TI-complete, and [GQ23b] providing more efficient reductions between the five actions by general linear groups.

7.1.2 Our Results and Techniques for More Matrix Groups

In this thesis, we examine isomorphism problems of d-way arrays under various actions of different subgroups of the general linear group from a complexity-theoretic viewpoint. We show that for 3-way arrays, the isomorphism problems over orthogonal and symplectic groups reduce to that over the general linear group. We also show that for orthogonal and unitary groups, the five isomorphism problems corresponding to the five natural actions are polynomial-time equivalent, and d-TENSOR ISOMORPHISM reduces to 3-TENSOR ISOMORPHISM.

As seen in Section 1.5, the proof strategies of our results are adapted from previous works [FGS19, GQ23a, LQW+23], although certain non-trivial adaptations were necessary, especially for the proofs of Theorem 1.5 and 1.6, beyond careful examinations of previous proofs. Interestingly, in extending the proof strategies from these previous works to our main results, we also encountered some obstacles that would seem are more generally obstacles to reaching a uniform result for all classical groups. For example, the reduction from orthogonal and symplectic to general linear seems not work for unitary—the standard linear-algebraic gadgets have no way to force complex conjugation—and the reductions between the five actions on 3-way arrays seem not work for symplectic. One stumbling block (pun intended) in the symplectic case is that even a symplectic block-*diagonal* matrix (let alone a symplectic block-triangular matrix) need not have its individual blocks be symplectic. For example, the matrix $A \oplus B$, with A, B both $n \times n$, is symplectic iff $AB^t = I$.

7.1.3 Complexity Classes $\mathsf{TI}_{\mathcal{G}}$

To put some of these remaining questions in a larger framework, we introduce a notation that highlights the role of the group doing the acting. Previously in computational complexity, the most studied isomorphism problems are over symmetric groups (such as GRAPH ISOMORPHISM) and over general linear groups (such as tensor, group, and polynomial isomorphism problems). The former leads to the complexity class GI [KST93], and the latter leads to the complexity class TI [GQ23a]. Based on Theorems 1.5 and 1.6, it may be interesting to define $\mathsf{TI}_{\mathcal{G}}$, where $\mathcal{G}$ is a family of matrix groups, consisting of all problems polynomial-time reducible to the 3-tensor isomorphism problem over $\mathcal{G}$. Let S, GL, O, U, Sp be the symmetric, general linear, orthogonal (over $\mathbb{R}$), unitary (over $\mathbb{C}$), and symplectic group families. Then $\mathsf{TI}_{\mathrm{GL}} = \mathsf{TI}$ by definition, and $\mathsf{TI}_{\mathrm{S}} = \mathsf{GI}$, as asking if two 3-tensors are the same up to permuting the coordinates is just the colored 3-partite 3-uniform hypergraph isomorphism problem, a GI-complete problem (by the methods of [ZKT85]). Then a special case of Theorem 1.1 can be reformulated as $\mathsf{TI}_{\mathrm{S}} \subseteq \mathsf{TI}_{\mathrm{O}} \cap \mathsf{TI}_{\mathrm{U}}$, and special cases of Theorem 1.2 can be reformulated as $\mathsf{TI}_{\mathrm{O}}, \mathsf{TI}_{\mathrm{Sp}} \subseteq \mathsf{TI}_{\mathrm{GL}}$.

7.2 Open Problems

It may be interesting to investigate $\mathsf{TI}_{\mathcal{G}}$ with $\mathcal{G}$ being other subgroups of GL, such as special linear, affine, and Borel or parabolic subgroups. With this notation in hand, we highlight the following questions left open by our work:

Open Question 7.1. Which, if any, of $\mathsf{TI}_{\mathrm{O}}, \mathsf{TI}_{\mathrm{U}}, \mathsf{TI}_{\mathrm{Sp}}$ are equal to TI?

As a warm-up in this direction, one may ask which of these classes is not only GI-hard, but contains Code Equivalence (permutational or monomial).

We suspect that $\mathsf{GI} \subseteq \mathsf{TI}_{\mathrm{Sp}} \cap \mathsf{TI}_{\mathrm{SL}}$ as well, for the following reason. Although the symplectic groups Sp_n and the special linear groups SL_n do not contain the symmetric group S_n given by $n \times n$ permutation matrices, they do contain isomorphic copies of $S_{n'}$ for $n' \geq \Omega(n)$. In particular, Sp_{2n} contains S_n as the subgroup $\{A \oplus A^T : A \in S_n\}$, and $\mathrm{SL}_n \cap S_n = A_n$ (and contains an isomorphic copy of S_{n-2}, where even $\pi \in S_{n-2}$ get embedded as $P_\pi \oplus I_2$ and odd π get embedded as $P_\pi \oplus \tau$, where $\tau = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$).

Open Question 7.2. Is $\mathsf{TI}_{\mathrm{SL}}$ contained in TI? Are they equal?

Open Question 7.3. Is $\mathsf{TI}_{\mathrm{U}} \subseteq \mathsf{TI}$? And the same question for unitary versus general linear group actions over finite fields.

Open Question 7.4. What is the complexity of various problems in TI when restricted from GL to other form-preserving groups? A notable family of such groups is the mixed orthogonal groups $\mathrm{O}(p,q)$, defined over $\mathbb{R}$ by preserving a real symmetric form of signature (p,q). But more generally, what about form-preserving groups for forms that are neither symmetric nor skew-symmetric?

7.3 Future Plans

We have studied the equivalence between different tensor isomorphism under action of matrix groups over field. However, if we replace the field with the ring, we might find other interesting applications. For example, Calabi-Yau threefold is a well-studied class of geometric spaces. One open problem in the superstring theory asks if the number of topologically distinct Calabi-Yau threefolds is finite. This problem is naturally related to the problem of classifying Calabi-Yau threefolds. It appears that determining the equivalence of two Calabi-Yau threefolds can be formulated as a type of tensor equivalence ($V \otimes V \otimes V$) under actions of groups over ring [JTT22].

By adapting the construction in [FGS19] and [GQ23a], we can show that tensor isomorphism problems under five different actions of groups over ring are equivalent. We only need to overcome an issue in the ring case. We substitute Knull-Schmidt Theorem used in [FGS19] to Knull-Schmidt Theorem over modules to demonstrate subcomponents of two isomorphic matrix tuples over ring are isomorphic. This result indicates that determining the equivalence of two Calabi-Yau threefolds is as hard as other equivalence problems.

Besides this, some problems are also based on the isomorphism of algebraic structures under actions of matrix groups over ring. Studying the relation between those isomorphism problems and tensor isomorphism under groups over ring is also an interesting aspect. For example, the goal of LATTICE ISOMORPHISM is to decide if two lattices are isomorphic by the action of matrices in the general linear over integer. It was first studied by Plesken and Souvigbier [PS97]. Then the asymptotic complexity of this problem was studied in [DSSV09], and it's also shown in this paper that GRAPH ISOMORPHISM reduces to LATTICE ISOMORPHISM. This problem is known to be in SZK by [HR14].

Now we might wonder if there are any algorithms solving other 3-tensor equivalence problems under actions of groups over ring. It turns out there is an algorithm designed to compute stabilizers of 3-tensor under some action ($V \otimes V \otimes V^*$) of groups over ring [GS80a, GS80b]. If we can adapt this algorithm to solve the 3-tensor isomorphism problem under this action, then we can utilize an algebraic algorithm to decide other related problems such as the equivalence of Calabi-Yau threefolds.

Appendix A

Polynomial systems for Tensor Isomorphism and related problems

We provide more details for the Gröbner basis experiments described in Section 1.2.2.

Let us first examine how to formulate Tensor Isomorphism as solving a system of polynomial equations. Let $\mathrm{A}, \mathrm{B} \in \mathrm{T}(n \times n \times n, \mathbb{F})$ be two 3-way arrays. Let X, Y, Z be three $n \times n$ variable matrices. Then $X\mathrm{A}^{Z}Y = \mathrm{B}$ can be seen as encoding n^3 many cubic polynomials in $3n^2$ many variables, whose coefficients are determined by the entries of A and B. To ensure that X, Y, Z are invertible, we introduce new variables x, y, z, and include polynomials $\det(X) \cdot x = 1$, $\det(Y) \cdot y = 1$, and $\det(Z) \cdot z = 1$. (This is similar to [GGPS23], although there instead of using the determinant they introduce twice as many new variables, and equations $XX' = X'X = I$ and similarly for Y and Z. This reduces degree compared to our equations here, but at the expense of many more variables). This gives a system of polynomial equations, which has a solution over $\mathbb{F}$ if and only if A and B are isomorphic as tensors over $\mathbb{F}$. Then this problem can be solved by e.g. the Gröbner basis algorithm.

Of course the above is just one approach. Indeed, from the Gröbner basis viewpoint, it is more desirable to consider $X\mathrm{A}Y = \mathrm{B}^{Z}$, so we get quadratic equations rather than cubic ones. Interested readers may refer [TDJ+22] for more optimizations as such.

The instances we do experiments on are drawn as follows. Note that if A and B are both random instances, then with high probability they are not isomorphic. To get isomorphic pairs instead, we can sample a random A and random invertible matrices R, S, T, and set $\mathrm{B} = (R, S, T) \circ \mathrm{A}$. (This is the setting used in cryptographic schemes based on TI-hardness, e.g., [JQSY19].) The pair (A, B) is then set as the input.

If orthogonal isomorphism is needed, we can set $X^t X = I$ which is a system of quadratic equations. We can also sample a random orthogonal matrix over $\mathbb{F}_q$ by existing functionality of Magma.

We now introduce the exact problem to be tackled by our actual experiments. Let $\phi, \psi : \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ be two alternating trilinear forms. We say that ϕ, ψ are isomorphic, if there exists $A \in \mathrm{GL}(n, q)$, such that $\phi(Au, Av, Aw) = \psi(u, v, w)$ for any $u, v, w \in \mathbb{F}_q^n$. To decide whether two alternating trilinear forms are isomorphic is known to be TI-complete [GQT22]. This problem can be similarly formulated as solving systems of polynomial equations, and some technical issues also follow the ideas as described above.

Bibliography

[ABLS01] Antonio Acín, Dagmar Bruß, Maciej Lewenstein, and Anna Sanpera. Classification of mixed three-qubit states. *Physical Review Letters*, 87(4):040401, 2001. doi:10.1103/PhysRevLett.87.040401.

[AFOV08] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. Entanglement in many-body systems. *Rev. Mod. Phys.*, 80:517–576, May 2008. doi:10.1103/RevModPhys.80.517.

[AKS19] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Errata: PRIMES is in P [MR2123939]. *Ann. of Math. (2)*, 189(1):317–318, 2019. doi:10.4007/annals.2019.189.1.6.

[AS05] Manindra Agrawal and Nitin Saxena. Automorphisms of finite rings and applications to complexity of problems. In *STACS 2005, 22nd Annual Symposium on Theoretical Aspects of Computer Science, Stuttgart, Germany, February 24-26, 2005, Proceedings*, pages 1–17, 2005. doi:10.1007/978-3-540-31856-9_1.

[AS06] Manindra Agrawal and Nitin Saxena. Equivalence of f-algebras and cubic forms. In *STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science, Marseille, France, February 23-25, 2006, Proceedings*, pages 115–126, 2006. doi:10.1007/11672142_8.

[Bab16] László Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual ACM SIGACT Symposium on*

Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016, pages 684–697, 2016. doi:10.1145/2897518.2897542. arXiv:1512.03547, version 2.

[BBD+09] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009. doi:10.1038/nphys1157.

[BDD+10] L. Borsten, D. Dahanayake, M. J. Duff, A. Marrani, and W. Rubens. Four-qubit entanglement classification from string theory. *Phys. Rev. Lett.*, 105:100507, Sep 2010. doi:10.1103/PhysRevLett.105.100507.

[BJP97] W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system I: the user language. *J. Symb. Comput.*, pages 235–265, 1997.

[BLT03] Emmanuel Briand, Jean-Gabriel Luque, and Jean-Yves Thibon. A complete set of covariants of the four qubit system. *Journal of Physics A: Mathematical and General*, 36(38):9915, sep 2003. doi:10.1088/0305-4470/36/38/309.

[BM11] D. Bruß and C. Macchiavello. Multipartite entanglement in quantum algorithms. *Phys. Rev. A*, 83:052313, May 2011. doi:10.1103/PhysRevA.83.052313.

[BOST19] Magali Bardet, Ayoub Otmani, and Mohamed Saeed-Taha. Permutation code equivalence is not harder than graph isomorphism when hulls are trivial. In *2019 IEEE International Symposium on Information Theory (ISIT)*, pages 2464–2468. IEEE, 2019. doi:10.1109/ISIT.2019.8849855.

[BPR+00] Charles H Bennett, Sandu Popescu, Daniel Rohrlich, John A Smolin, and Ashish V Thapliyal. Exact and asymptotic measures of multipartite pure-state entanglement. *Physical Review A*, 63(1):012307, 2000. doi:10.1103/PhysRevA.63.012307.

[CGQ+23] Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang. On the complexity of isomorphism problems for tensors, groups, and polynomials III: actions by classical groups. 2023, arXiv:2306.03135.

[CLM+14] Eric Chitambar, Debbie Leung, Laura Mančinska, Maris Ozols, and Andreas Winter. Everything you always wanted to know about LOCC (but were afraid to ask). *Communications in Mathematical Physics*, 328:303–326, 2014. doi:10.1007/s00220-014-1953-9.

[CNP+23] Tung Chou, Ruben Niederhagen, Edoardo Persichetti, Tovohery Hajatiana Randrianarisoa, Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Take your MEDS: digital signatures from matrix code equivalence. In *Progress in cryptology—AFRICACRYPT 2023*, volume 14064 of *Lecture Notes in Comput. Sci.*, pages 28–52. Springer, Cham, [2023] ©2023. doi:10.1007/978-3-031-37679-5_2.

[D'A23] Giuseppe D'Alconzo. Monomial isomorphism for tensors and applications to code equivalence problems. Cryptology ePrint Archive, Paper 2023/396, 2023. URL `https://eprint.iacr.org/2023/396`.

[DdGMO22] Heiko Dietrich, Willem A. de Graaf, Alessio Marrani, and Marcos Origlia. Classification of four qubit states and their stabilisers under slocc operations. *Journal of Physics A: Mathematical and Theoretical*, 55(9):095302, feb 2022. doi:10.1088/1751-8121/ac4b13.

[DLDMV00] Lieven De Lathauwer, Bart De Moor, and Joos Vandewalle. A multilinear singular value decomposition. *SIAM journal on Matrix Analysis and Applications*, 21(4):1253–1278, 2000. doi:10.1137/S0895479896305696.

[DSL08] Vin De Silva and Lek-Heng Lim. Tensor rank and the ill-posedness of the best low-rank approximation problem. *SIAM Journal on Matrix Analysis and Applications*, 30(3):1084–1127, 2008. doi:10.1137/06066518X.

[DSSV09] Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin. Complexity and algorithms for computing Voronoi cells of lattices. *Math. Comp.*, 78(267):1713–1731, 2009. doi:10.1090/S0025-5718-09-02224-8.

[DVC00] Wolfgang Dür, Guifre Vidal, and J Ignacio Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62(6):062314, 2000. doi:10.1103/PhysRevA.62.062314.

[Edm65] Jack Edmonds. Paths, trees, and flowers. *Canadian Journal of mathematics*, 17(3):449–467, 1965. doi:10.4153/CJM-1965-045-4.

[EY36] Carl Eckart and Gale Young. The approximation of one matrix by another of lower rank. *Psychometrika*, 1(3):211–218, 1936. doi:10.1007/BF02288367.

[FG11] Lance Fortnow and Joshua A. Grochow. Complexity classes of equivalence problems revisited. *Inform. and Comput.*, 209(4):748–763, 2011. doi:10.1016/j.ic.2011.01.006. Also available as arXiv:0907.4775 [cs.CC].

[FGS19] Vyacheslav Futorny, Joshua A. Grochow, and Vladimir V. Sergeichuk. Wildness for tensors. *Linear Algebra and its Applications*, 566:212–244, 2019. doi:10.1016/j.laa.2018.12.022.

[GGPS23] Nicola Galesi, Joshua A. Grochow, Toniann Pitassi, and Adrian She. On the algebraic proof complexity of Tensor Isomorphism. In *Computational Complexity Conference (CCC) 2023*, 2023. Preprint arXiv:2305.19320 [cs.CC].

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity for all languages in NP have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991. doi:10.1145/116825.116852.

[GQ21] Joshua A. Grochow and Youming Qiao. On p-group isomorphism: Search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. In Valentine Kabanets, editor, *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference)*, volume 200 of *LIPIcs*, pages 16:1–16:38. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. doi:10.4230/LIPIcs.CCC.2021.16.

[GQ23a] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: Tensor Isomorphism-completeness. *SIAM J. Comput.*, 52:568–617, 2023. doi:10.1137/21M1441110. Part of the preprint arXiv:1907.00309 [cs.CC]. Preliminary version appeared at ITCS '21, DOI:10.4230/LIPIcs.ITCS.2021.31.

[GQ23b] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials IV: linear-length reductions and their applications. *CoRR*, abs/2306.16317, 2023, arXiv:2306.16317. doi:10.48550/arXiv.2306.16317.

[GQT22] Joshua A Grochow, Youming Qiao, and Gang Tang. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. *journal of Groups, Complexity, Cryptology*, 14, 2022. doi:10.46298/jgcc.2022.14.1.9431. Extended abstract appeared in STACS '21 DOI:10.4230/LIPIcs.STACS.2021.38.

[GS80a] Fritz Grunewald and Daniel Segal. Some general algorithms. I. Arithmetic groups. *Ann. of Math. (2)*, 112(3):531–583, 1980. doi:10.2307/1971091.

[GS80b] Fritz Grunewald and Daniel Segal. Some general algorithms. II. Nilpotent groups. *Ann. of Math. (2)*, 112(3):585–617, 1980. doi:10.2307/1971092.

[GW13] Gilad Gour and Nolan R Wallach. Classification of multipartite entanglement of all finite dimensionality. *Physical Review Letters*, 111(6):060502, 2013. doi:10.1103/PhysRevLett.111.060502.

[Hač80] L. G. Hačijan. Polynomial algorithms in linear programming. *Zh. Vychisl. Mat. i Mat. Fiz.*, 20(1):51–68, 260, 1980.

[HLT14] Frédéric Holweck, Jean-Gabriel Luque, and Jean-Yves Thibon. Entanglement of four qubit systems: A geometric atlas with polynomial compass I (the finite world). *Journal of Mathematical Physics*, 55(1):012202, 01 2014. doi:10.1063/1.4858336.

[HQ21] Xiaoyu He and Youming Qiao. On the Baer–Lovász–Tutte construction of groups from graphs: Isomorphism types and homomorphism notions. *Eur. J. Comb.*, 98:103404, 2021. doi:10.1016/j.ejc.2021.103404.

[HR14] Ishay Haviv and Oded Regev. On the lattice isomorphism problem. In Chandra Chekuri, editor, *Proceedings of the Twenty-Fifth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2014, Portland, Oregon, USA, January 5-7, 2014*, pages 391–404. SIAM, 2014. doi:10.1137/1.9781611973402.29.

[HU17] Wolfgang Hackbusch and André Uschmajew. On the interconnection between the higher-order singular values of real tensors. *Numerische Mathematik*, 135:875–894, 2017. doi:10.1007/s00211-016-0819-9.

[Hum] Jim Humphreys. What are “classical groups”? https://mathoverflow.net/questions/50610/what-are-classical-groups.

[JL03] Richard Jozsa and Noah Linden. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 459(2036):2011–2032, 2003. doi:10.1098/rspa.2002.1097.

[JQSY19] Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I*, pages 251–281, 2019. doi:10.1007/978-3-030-36030-6_11.

[JTT22] Vishnu Jejjala, Washington Taylor, and Andrew Turner. Identifying equivalent calabi–yau topologies: A discrete challenge from math and physics for machine learning, 2022, arXiv:2202.07590.

[Kra10a] B Kraus. Local unitary equivalence of multipartite pure states. *Physical Review Letters*, 104(2):020504, 2010.

[Kra10b] Barbara Kraus. Local unitary equivalence and entanglement of multipartite pure states. *Physical Review A*, 82(3):032121, 2010. doi:10.1103/PhysRevLett.104.020504.

[KS06] Neeraj Kayal and Nitin Saxena. Complexity of ring morphism problems. *Computational Complexity*, 15(4):342–390, 2006. doi:10.1007/s00037-007-0219-8.

[KST93] Johannes Köbler, Uwe Schöning, and Jacobo Torán. *The graph isomorphism problem: its structural complexity*. Birkhauser Verlag, Basel, Switzerland, Switzerland, 1993. doi:10.1007/978-1-4612-0333-9.

[Lan11] JM Landsberg. *Tensors: Geometry and Applications: Geometry and Applications*, volume 128. American Mathematical Soc., 2011.

[Lim21] Lek-Heng Lim. Tensors in computations. *Acta Numerica*, 30:555–764, 2021. doi:10.1017/S0962492921000076.

[Lov79] László Lovász. On determinants, matchings, and random algorithms. In Lothar Budach, editor, *Fundamentals of Computation Theory, FCT 1979, Proceedings of the Conference on Algebraic, Arthmetic, and Categorial Methods in Computation Theory, Berlin/Wendisch-Rietz, Germany, September 17-21, 1979*, pages 565–574. Akademie-Verlag, Berlin, 1979.

[LQW+23] Yinan Li, Youming Qiao, Avi Wigderson, Yuval Wigderson, and Chuanqi Zhang. Connections between graphs and matrix spaces. *Israel Journal of Mathematics*, 256(2):513–580, 2023.

[LT05] Jean-Gabriel Luque and Jean-Yves Thibon. Algebraic invariants of five qubits. *Journal of Physics A: Mathematical and General*, 39(2):371, dec 2005. doi:10.1088/0305-4470/39/2/007.

[Luk82] Eugene M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comput. Syst. Sci.*, 25(1):42 – 65, 1982. doi:10.1016/0022-0000(82)90009-5.

[McK81] Brendan D. McKay. Practical graph isomorphism. *Congr. Numer.*, 30:45–87, 1981.

[MP14] Brendan D. McKay and Adolfo Piperno. Practical graph isomorphism, II. *Journal of Symbolic Computation*, 60(0):94 – 112, 2014. doi:http://dx.doi.org/10.1016/j.jsc.2013.09.003.

[NC00] M. Nielsen and I. Chuang. *Quantum computation and quantum information.* Cambridge University Press, 2000. doi:10.1017/CBO9780511976667.

[Nie99] Michael A Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83(2):436, 1999. doi:10.1103/PhysRevLett.83.436.

[Pat96] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, pages 33–48, 1996. doi:10.1007/3-540-68339-9_4.

[PS97] W. Plesken and B. Souvignier. Computing isometries of lattices. volume 24, pages 327–334. 1997. doi:10.1006/jsco.1996.0130. Computational algebra and number theory (London, 1993).

[RST22] Krijn Reijnders, Simona Samardjiska, and Monika Trimoska. Hardness estimates of the Code Equivalence Problem in the rank metric. In *WCC 2022: The Twelfth International Workshop on Coding and Cryptography*, 2022. Cryptology ePrint Archive, Paper 2022/276, `https://eprint.iacr.org/2022/276`.

[Sch88] Uwe Schöning. Graph isomorphism is in the low hierarchy. *J. Comput. System Sci.*, 37(3):312–323, 1988. doi:10.1016/0022-0000(88)90010-4.

[SDV06] Y-Y Shi, L-M Duan, and Guifre Vidal. Classical simulation of quantum many-body systems with a tree tensor network. *Physical Review A*, 74(2):022320, 2006. doi:10.1103/PhysRevA.74.022320.

[Sei18] Anna Seigal. Gram determinants of real binary tensors. *Linear Algebra and its Applications*, 544:350–369, 2018. doi:10.1016/j.laa.2018.01.019.

[Ser98] Vladimir V Sergeichuk. Unitary and Euclidean representations of a quiver. *Linear Algebra and its Applications*, 278(1-3):37–62, 1998. doi:10.1016/S0024-3795(98)00006-8.

[Sun23] Xiaorui Sun. Faster isomorphism for p-groups of class 2 and exponent p. In *STOC'23—Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 433–440. ACM, New York, [2023] ©2023. doi:10.1145/3564246.3585250.

[TDJ+22] Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. Practical post-quantum signature schemes from isomorphism problems of trilinear forms. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 582–612. Springer, 2022. doi:10.1007/978-3-031-07082-2_21.

[Tem04] George Frederick James Temple. *Cartesian Tensors: an introduction.* Courier Corporation, 2004.

[Tut47] W. T. Tutte. The factorization of linear graphs. *Journal of the London Mathematical Society*, s1-22(2):107–111, 1947. doi:10.1112/jlms/s1-22.2.107.

[Val79] Leslie G. Valiant. Completeness classes in algebra. In Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho, editors, *Proceedings of the 11h Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*, pages 249–261. ACM, 1979. doi:10.1145/800135.804419.

[VDDMV02] Frank Verstraete, Jeroen Dehaene, Bart De Moor, and Henri Verschelde. Four qubits can be entangled in nine different ways. *Physical Review A*, 65(5):052112, 2002. doi:10.1103/PhysRevA.65.052112.

[Wey97] H. Weyl. *The classical groups: their invariants and representations*, volume 1. Princeton University Press, 1946 (1997). doi:10.2307/j.ctv3hh48t.

[WGE16] Michael Walter, David Gross, and Jens Eisert. Multipartite entanglement. *Quantum Information: From Foundations to Quantum Technology Applications*, pages 293–330, 2016. Extended version available at arXiv:1612.02437.

[ZKT85] V. N. Zemlyachenko, N. M. Korneenko, and R. I. Tyshkevich. Graph isomorphism problem. *J. Soviet Math.*, 29(4):1426–1481, May 1985. doi:10.1007/BF02104746.

[ZLQ18] SM Zangi, Jun-Li Li, and Cong-Feng Qiao. Quantum state concentration and classification of multipartite entanglement. *Physical Review A*, 97(1):012301, 2018. doi:10.1103/PhysRevA.97.012301.