


On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials III: Actions by Classical Groups

Zhili Chen ✉ 

Center for Quantum Software and Information, University of Technology Sydney, Australia

Joshua A. Grochow ✉ 


Departments of Computer Science and Mathematics, University of Colorado Boulder, CO, USA

Youming Qiao ✉ 

Center for Quantum Software and Information, University of Technology Sydney, Australia

Gang Tang ✉ 

Center for Quantum Software and Information, University of Technology Sydney, Australia

Chuanqi Zhang ✉ 

Center for Quantum Software and Information, University of Technology Sydney, Australia

Abstract

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

Our main results are as follows. First, for orthogonal and symplectic groups acting on 3-way arrays, the isomorphism problems reduce to the corresponding problems over the general linear group. Second, for orthogonal and unitary groups, 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 $d > 3$. For unitary groups, the preceding result implies that LOCC classification of tripartite quantum states is at least as difficult as LOCC classification of d -partite quantum states for any d . Lastly, we also show that the graph isomorphism problem reduces to the tensor isomorphism problem over orthogonal and unitary groups.

2012 ACM Subject Classification Theory of computation → Algebraic complexity theory

Keywords and phrases complexity class, tensor isomorphism, polynomial isomorphism, group isomorphism, local operations and classical communication

Digital Object Identifier 10.4230/LIPIcs.ITCS.2024.31

Related Version *Full Version:* <https://arxiv.org/abs/2306.03135> [5]

Funding *Joshua A. Grochow:* Supported by NSF CAREER grant CISE-2047756.

Youming Qiao: Partially supported by the Australian Research Council DP200100950 and LP220100332.

Gang Tang: Partially supported by the Australian Research Council LP220100332 and the Sydney Quantum Academy, Sydney, NSW, Australia.

Chuanqi Zhang: Partially supported by the the Australian Research Council DP200100950 and the Sydney Quantum Academy, Sydney, NSW, Australia.

Acknowledgements We thank the anonymous reviewers for their careful reading and helpful suggestions.



© Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang; licensed under Creative Commons License CC-BY 4.0

15th Innovations in Theoretical Computer Science Conference (ITCS 2024).

Editor: Venkatesan Guruswami; Article No. 31; pp. 31:1–31:23

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Previously in [13–15, 17, 27], isomorphism problems of tensors, groups, and polynomials *over direct products of general linear groups* were studied from the complexity-theoretic viewpoint. In particular, a complexity class **TI** was defined in [15], and several isomorphism problems, including those for tensors, groups, and polynomials, were shown to be **TI**-complete. The equivalence between polynomials and 3-tensors was shown subsequently but independently in [27]; some problems over products of general linear groups with monomial groups were also shown to be **TI**-complete [7].

In this paper, 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. There are several motivations to study tensor isomorphism over classical groups from statistical data analysis and quantum information. This introduction section is organised as follows. We will first review d -way arrays and some natural group actions on them in Section 1.1, and describe motivations to study these actions over classical groups in Section 1.2. We will then present our main results in Section 1.3, and give an overview of the proofs in Section 1.4. We conclude this introduction with a brief overview of the series of works this paper belongs to, a discussion on the results, and some open problems in Section 1.5.

1.1 Review of d -way arrays and some group actions on them

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

► **Definition 1.** *Let $\mathrm{GL}(n, \mathbb{F})$ be the general linear group of degree n over \mathbb{F} . We define an action of $\mathrm{GL}(n_1, \mathbb{F}) \times \dots \times \mathrm{GL}(n_d, \mathbb{F})$ on $\mathbb{T}(n_1 \times \dots \times n_d, \mathbb{F})$, denoted as \circ , as follows. Let $\mathbf{g} = (g_1, \dots, g_d)$, where $g_k \in \mathrm{GL}(n_k, \mathbb{F})$ over $k \in [d]$. The action of \mathbf{g} sends $\mathbf{A} = (a_{i_1, \dots, i_d})$ to $\mathbf{g} \circ \mathbf{A} = (b_{i_1, \dots, i_d})$, where $b_{i_1, \dots, i_d} = \sum_{j_1, \dots, j_d} a_{j_1, \dots, j_d} (g_1)_{i_1, j_1} (g_2)_{i_2, j_2} \dots (g_d)_{i_d, j_d}$.*

There are several group actions of direct products of general linear 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 $A \in \mathbb{M}(n, \mathbb{F})$, (1) $(P, Q) \in \mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$ sends A to $P^t A Q$, (2) $P \in \mathrm{GL}(n, \mathbb{F})$ sends A to $P^{-1} A P$, and (3) $P \in \mathrm{GL}(n, \mathbb{F})$ sends A to $P^t A P$. 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 [15, Sec. 2.2] for more discussion of why these five capture all possibilities within a certain natural class).

► **Definition 2.** *We define five actions of (direct products of) general linear groups on 3-way arrays. Note that in the following, \circ is from Definition 1.*

1. *Given $\mathbf{A} \in \mathbb{T}(l \times m \times n, \mathbb{F})$, $(P, Q, R) \in \mathrm{GL}(l, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$ sends \mathbf{A} to $(P, Q, R) \circ \mathbf{A}$;*
2. *Given $\mathbf{A} \in \mathbb{T}(l \times l \times m, \mathbb{F})$, $(P, Q) \in \mathrm{GL}(l, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$ sends \mathbf{A} to $(P, P, Q) \circ \mathbf{A}$;*
3. *Given $\mathbf{A} \in \mathbb{T}(l \times l \times m, \mathbb{F})$, $(P, Q) \in \mathrm{GL}(l, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$ sends \mathbf{A} to $(P, P^{-t}, Q) \circ \mathbf{A}$;*
4. *Given $\mathbf{A} \in \mathbb{T}(l \times l \times l, \mathbb{F})$, $P \in \mathrm{GL}(l, \mathbb{F})$ sends \mathbf{A} to $(P, P, P^{-t}) \circ \mathbf{A}$;*
5. *Given $\mathbf{A} \in \mathbb{T}(l \times l \times l, \mathbb{F})$, $P \in \mathrm{GL}(l, \mathbb{F})$ sends \mathbf{A} to $(P, P, P) \circ \mathbf{A}$.*

These five actions arise naturally 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 (noncommutative) cubic forms. For details on these interpretations, we refer the reader to [15, Sec. 2.2].

For a group \mathcal{G} acting on a set S , the isomorphism problem for this action asks to decide, given $s, t \in S$, whether s and t are in the same \mathcal{G} -orbit. For example, GRAPH ISOMORPHISM is the isomorphism problem for the action of the symmetric group S_n on $2^{\binom{[n]}{2}}$, the power set of the set of size-2 subsets of $[n]$.

To help specify which of the five actions we are talking about, we use the following shorthand notation from multilinear algebra¹. 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 2 and vice versa.

1.2 Motivations for isomorphism problems of d -way arrays over classical groups

The term “classical groups” appeared in Weyl’s classic [34], though there are multiple competing possibilities for what this term should mean formally [20]. In this paper, 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. Note that for the orthogonal group $O(n, \mathbb{R})$, there are essentially three actions instead of five (because $P^{-t} = P$ for $P \in O(n, \mathbb{R})$).

Actions of classical groups on d -way arrays have appeared in several areas of computational and applied mathematics [24]. In this subsection we examine some of these applications from statistical data analysis and quantum information.

Warm up: singular value decompositions. Consider the action of $(A, B) \in U(n, \mathbb{C}) \times U(m, \mathbb{C})$ on $C \in M(n \times m, \mathbb{C})$ by sending C to A^*CB , where A^* denotes the conjugate transpose of A . The orbits of this action are determined by the Singular Value Theorem, which states that every $C \in M(n \times m, \mathbb{C})$ can be written as A^*DB where $A \in U(n, \mathbb{C})$, $B \in U(m, \mathbb{C})$, and $D \in M(n \times m, \mathbb{C})$ is a rectangular diagonal matrix. Furthermore, the diagonal entries of D are non-negative real numbers, called the singular values of C . Similar results hold for $O(n, \mathbb{R}) \times O(m, \mathbb{R})$ acting on $\mathbb{R}^n \otimes \mathbb{R}^m$.

This example illustrates that the orbit structure of $U(n, \mathbb{C}) \times U(m, \mathbb{C})$ on $M(n \times m, \mathbb{C})$ is different from the action of $GL(n, \mathbb{C}) \times GL(m, \mathbb{C})$ on $M(n \times m, \mathbb{C})$. 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).

Orthogonal isomorphism of tensors from data analysis. The singular value decomposition is the basis for the Eckart–Young Theorem [10], 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 generalisation of such a result to d -way arrays, $d > 2$, is a central problem in statistical analysis of multiway data [9].

¹ See [24] 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.

Due to the close relation between singular value decompositions 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 [8,9,18,28]. 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 characterise orbits as in the matrix case. In the literature, d -way arrays under orthogonal group actions are sometimes called Cartesian tensors [31].

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 $T(n_1 \times \cdots \times n_d, \mathbb{C}) \cong \mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_d}$ are called pure states, and two pure states are called locally-unitary (LU) equivalent, if they are in the same orbit under the natural action of $\mathbf{U} := U(n_1, \mathbb{C}) \times \cdots \times U(n_d, \mathbb{C})$ (where the i -th factor of the group acts on the i -th tensor factor). By Bennett *et al.* [3], the LU equivalence of pure states also captures their equivalence under local operations and classical communication (LOCC), which means that LU-equivalent states are inter-convertible by reasonable physical operations.

A completely positive map is a function $f : M(n, \mathbb{C}) \rightarrow M(n, \mathbb{C})$ of the form $f(A) = \sum_{i \in [m]} B_i A B_i^*$ for some complex matrices $B_i \in M(n, \mathbb{C})$; 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, \dots, B_m) and (B'_1, \dots, B'_m) define the same completely positive map if and only if there exists $S = (s_{i,j}) \in U(m, \mathbb{C})$ such that $\forall i \in [m]$, $B_i = \sum_{j \in [m]} s_{i,j} B'_j$ [26, Theorem 8.2]. And two quantum channels $f, g : M(n, \mathbb{C}) \rightarrow M(n, \mathbb{C})$ are called unitarily equivalent if there exists $T \in U(n, \mathbb{C})$ such that for any $A \in M(n, \mathbb{C})$, $T^* f(A) T = g(T^* A T)$. Thus, two matrix tuples (B_1, \dots, B_m) and (B'_1, \dots, B'_m) define the unitarily equivalent quantum channels if and only if their corresponding 3-way arrays in $T(n \times n \times m, \mathbb{C})$ are in the same orbit under a natural action of $U(n, \mathbb{C}) \times U(m, \mathbb{C})$.

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 $A, B \in M(d \times n, q)$, decide if there exist $C \in GL(d, q)$ and $P \in S_n$, such that $A = CBP$. One algorithm for this problem, under some conditions on A and B , from [2] 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 [2], 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 ([5, Proposition 3.1]), 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 $\mathbf{A} = (a_{i,j,k}) \in \mathbb{T}(n \times n \times n, \mathbb{C})$, construct its matrix flattening $B = (b_{i,j}) \in \mathbb{M}(n \times n^2, \mathbb{C})$, 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 $\mathbb{U}(n, \mathbb{C}) \times \mathbb{U}(n, \mathbb{C}) \times \mathbb{U}(n, \mathbb{C})$. 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 [21].

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 [30], we chose a TI-complete problem ALTERNATING TRILINEAR FORM ISOMORPHISM [17], and carried out experiments using the Gröbner basis method for this problem, implemented in Magma [4]. For some details of these experiments see our full version [5, 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 219.7GB memory, yet still did not complete with a solution. Over the orthogonal group for odd n , the data are shown in Table 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.

■ **Table 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.

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

1.3 Our results

In this paper we study the complexity-theoretic aspects of TENSOR ISOMORPHISM under classical groups. We focus on the following two 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 d -way arrays. What are the relations between the isomorphism problems defined by these actions?

Questions of the first type were implicitly studied in [14, 15, 19] 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 \mathbf{A}_G encoding this graph following Edmonds, Tutte and Lovász [11, 25, 32], and it is shown in [19] that G and H are isomorphic (a notion based on the symmetric groups S_n) if and only if \mathbf{A}_G and \mathbf{A}_H are isomorphic (under a product of general linear groups).

Questions of the second type were studied in [13, 15] for GL. For example, one main result in [13, 15] is to show the polynomial-time equivalence of the five isomorphism problems for 3-way arrays under (direct products of) general linear groups (cf. Section 1.1).

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 on this paper.

Results on relations between different groups. Our first group of results 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 $GL(n, \mathbb{F})$ naturally via permutation matrices. We use \leq to denote the subgroup relation. When we say “reduces”, briefly, we mean: polynomial-time computable kernel reductions [12] (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 [33], 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 [15, Sec. 2.3] for details on these notions.

► **Theorem 3.** *Suppose a group family $\mathcal{G} = \{\mathcal{G}_n\}$ satisfies that $S_n \leq \mathcal{G}_n \leq GL(n, \mathbb{F})$, 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 $\mathcal{G}_n \leq GL(n, \mathbb{F})$. We say that \mathcal{G}_n *preserves a bilinear form*, if there exists some $A \in M(n, \mathbb{F})$, such that $\mathcal{G}_n = \{T \in GL(n, \mathbb{F}) \mid T^t A T = A\}$. For example, orthogonal and symplectic groups are defined as preserving full-rank symmetric and skew-symmetric forms.

► **Theorem 4.** *Let $\mathcal{G} = \{\mathcal{G}_n \mid \mathcal{G}_n \leq GL(n, \mathbb{F})\}$ be a group family preserving a polynomial-time-constructible family of bilinear forms,² and consider one of the five actions of GL on 3-way arrays in Definition 2. The restricted \mathcal{G} -isomorphism problem for this action reduces to the GL-isomorphism problem for this action.*

► **Remark 5.** Recall from Section 1.2 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 [12] (mapping matrices to matrices) from ORTHOGONAL EQUIVALENCE OF MATRICES to GENERAL LINEAR EQUIVALENCE OF MATRICES. In contrast, Theorem 4 shows that for 3-way arrays, orthogonal isomorphism does reduce to general-linear isomorphism.

Results on relations between different actions. Our second group of results 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 Section 1.5, and leave open the questions for more general bilinear-form-preserving groups.

We begin with the five actions in Definition 2.

► **Theorem 6.** *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 2 are polynomial-time equivalent to one another.*

Our second result in this group is a reduction from d -way arrays to 3-way arrays.

► **Theorem 7.** *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 That is, the function $\Phi: \mathbb{N} \rightarrow M(n, \mathbb{F})$ 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 3.

An application in quantum information. As introduced in Section 1.2, LU equivalence, characterises the equivalence of quantum states under local operations and classical communication (LOCC). We refer the interested reader to the nice paper [6] for the LOCC notion, as well as the classification of three-qubit states based on LOCC [1].

By the work of Bennett *et al.* [3], 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 7 can then be interpreted as saying that classifying tripartite quantum states under LOCC equivalence is as difficult as classifying d -partite quantum states. This may be compared with the result in [35], 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 [15]; in the next section we discuss how our proof here differs from the one there.)

1.4 Overview of the proofs of main results

In the following, we present proof outlines for Theorems 3, 4, 6, and 7. While their proofs are inspired the strategies of previous results [13, 15, 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 7 requires not only using a quiver different from that in the proof of [15, Theorem 1.2], but also a completely new and much simpler argument.

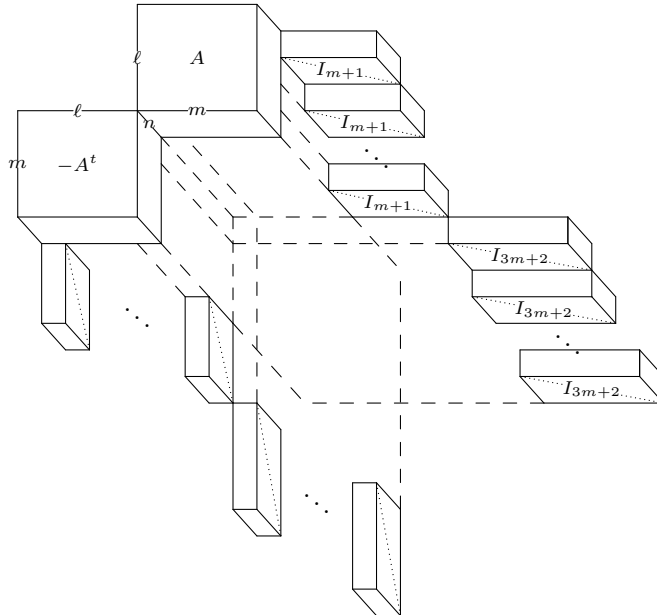
About Theorem 3. For Theorem 3, we start with DIRECTED GRAPH ISOMORPHISM (DGI), which is GI-complete. We then use a natural construction of 3-way arrays from directed graphs as recently studied in [23], which takes an arc (i, j) and constructs an elementary matrix $E_{i,j}$. By [23, Observation 6.1, Proposition 6.2], DGI reduces to the isomorphism problem of $U \otimes U \otimes W$ under $\text{GL}(U) \times \text{GL}(W)$. Theorem 3 is shown by observing that the proofs of [23, Observation 6.1, Proposition 6.2] carry over to all subgroups of $\text{GL}(U)$ and $\text{GL}(W)$ that contain the corresponding symmetric groups; see our full version [5, Section 3] for a detailed proof.

About Theorem 4. For Theorem 4, let us consider the isomorphism problem of $U \otimes V \otimes W$ under $\text{O}(U) \times \text{O}(V) \times \text{O}(W)$. Let $a = \dim(U)$, $b = \dim(V)$, and $c = \dim(W)$. That is, given $\mathbf{A}, \mathbf{B} \in \text{T}(a \times b \times c, \mathbb{F})$, we want to decide if there exists $(R, S, T) \in \text{O}(a, \mathbb{F}) \times \text{O}(b, \mathbb{F}) \times \text{O}(c, \mathbb{F})$, such that $(R, S, T) \circ \mathbf{A} = \mathbf{B}$. Our goal is to reduce this problem to an isomorphism problem of $U' \otimes V' \otimes W'$ under $\text{GL}(U') \times \text{GL}(V') \times \text{GL}(W')$. The idea is to encode the requirements of R, S, T being orthogonal by adding identity matrices. We then construct tensor systems $(\mathbf{A}, I_1, I_2, I_3)$ and $(\mathbf{B}, I_1, I_2, I_3)$ where $I_1 \in \text{M}(a, \mathbb{F})$, $I_2 \in \text{M}(b, \mathbb{F})$, and $I_3 \in \text{M}(c, \mathbb{F})$ are the identity matrices, and the goal is to decide if there exists $(R, S, T) \in \text{GL}(a, \mathbb{F}) \times \text{GL}(b, \mathbb{F}) \times \text{GL}(c, \mathbb{F})$ such that $(R, S, T) \circ \mathbf{A} = \mathbf{B}$, $R^t R = I_1$, $S^t S = I_2$, and $T^t T = I_3$. Such a problem falls into the tensor system framework in [13]; a main result of [13, Theorem 1.1] can be rephrased as a reduction from TENSOR SYSTEM ISOMORPHISM to 3-TENSOR ISOMORPHISM; see our full version [5, Section 4] for a detailed proof.

About Theorem 6. For Theorem 6, polynomial-time reductions for the five actions under GL were devised in [13, 15]. The main proof technique is a gadget construction, first proposed in [13], 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 $A \in T(\ell \times m \times n, \mathbb{F})$, and take the frontal slices of A as $(A_1, \dots, A_n) \in M(\ell \times m, \mathbb{F})$. Then construct $(A'_1, \dots, A'_n) \in M(\ell + m, \mathbb{F})$, where $A'_i = \begin{bmatrix} 0 & A_i \\ -A_i^t & 0 \end{bmatrix}$, and let the corresponding 3-way array be $A' \in T((\ell + m) \times (\ell + m) \times n, \mathbb{F})$. Similarly, starting from $B \in T(\ell \times m \times n, \mathbb{F})$, we can construct B' in the same way. The wish here is that A and B are unitarily isomorphic in $U \otimes V \otimes W$ if and only if A' and 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 $(R, S) \in U(U') \times U(W')$ from A' to 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 is an illustration from [15]. It can be



■ **Figure 1** Pictorial representation of the reduction for Theorem 6; credit for the figure goes to the authors of [15], reproduced here with their permission.

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 [15]. 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. Still, some technical difficulties remain. For example, 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. As another

example, the proof in [13] relies on the Krull–Schmidt theorem for quiver representations (under general linear group actions). Fortunately, in our context we can replace that with a result of Sergeichuk [29, Theorem 3.1] so that the proof can go through. Finally, we also require the use of the Singular Value Theorem to handle certain degenerate cases.

About Theorem 7. For Theorem 7, at a high level we follow the strategy of reduction from d -TENSOR ISOMORPHISM to 3-TENSOR ISOMORPHISM from [15], but we find that the construction there does not quite work in the setting of orthogonal or unitary group actions. As in [15], we shall reduce d -TENSOR ISOMORPHISM to ALGEBRA ISOMORPHISM, which reduces to 3-TENSOR ISOMORPHISM by Theorem 6. As in [15], we also use path algebras. However, they 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. This then gives us the reduction from d -TENSOR ORTHOGONAL ISOMORPHISM to ORTHOGONAL ALGEBRA ISOMORPHISM, and similarly in the unitary case.

1.5 Summary and future directions

Context within recent developments on the complexity of TENSOR ISOMORPHISM. Following [14, 15], this paper contributes to building up the complexity theory around TENSOR ISOMORPHISM and closely related problems. That is, [15] introduced TI-completeness and showed that many isomorphism problems, under the action of a product of general linear groups, were TI-complete. Then [14] focused on applications of tensor techniques for reductions around p -GROUP ISOMORPHISM. Several recent works further enrich this theory, such as [7, 17] showing more problems to be TI-complete, and [16] providing more efficient reductions between the five actions by general linear groups.

Some remarks on our results and techniques for more matrix groups. In this paper, 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 1.4, the proof strategies of our results are adapted from previous works [13, 15, 23], although certain non-trivial adaptations were necessary, especially for the proofs of Theorem 6 and 7, 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 $AB^t = I$.

Complexity classes $\text{TI}_{\mathcal{G}}$. 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 [22], and the latter leads to the complexity class TI [15]. Based on Theorems 6 and 7, it may be interesting to define $\text{TI}_{\mathcal{G}}$, 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 $\text{TI}_{\text{GL}} = \text{TI}$ by definition, and $\text{TI}_{\text{S}} = \text{GI}$, 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 [36]). Then a special case of Theorem 3 can be reformulated as $\text{TI}_{\text{S}} \subseteq \text{TI}_{\text{O}} \cap \text{TI}_{\text{U}}$, and special cases of Theorem 4 can be reformulated as $\text{TI}_{\text{O}}, \text{TI}_{\text{Sp}} \subseteq \text{TI}_{\text{GL}}$. It may be interesting to investigate $\text{TI}_{\mathcal{G}}$ with \mathcal{G} being other subgroups of GL, such as special linear, affine, and Borel or parabolic subgroups.

Open questions. With this notation in hand, we highlight the following questions left open by our work:

► **Open Question 8.** Which, if any, of $\text{TI}_{\text{O}}, \text{TI}_{\text{U}}, \text{TI}_{\text{Sp}}$ 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 $\text{GI} \subseteq \text{TI}_{\text{Sp}} \cap \text{TI}_{\text{SL}}$ 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 $\text{SL}_n \cap S_n = A_n$ (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 9.** Is TI_{SL} contained in TI? Are they equal?

► **Open Question 10.** Is $\text{TI}_{\text{U}} \subseteq \text{TI}$? And the same question for unitary versus general linear group actions over finite fields.

► **Open Question 11.** 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 $O(p, q)$, 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?

Paper organisation. After presenting some preliminaries in Section 2, we prove the main results: Theorem 6 in Section 3, and Theorem 7 in Section 4. For detailed proofs of Theorem 3 and Theorem 4, we refer the reader to our full version [5, Section 3, Section 4].

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 logspace computable. For arbitrary fields, the reductions are in logspace 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 $\alpha \in \text{Aut}_{\mathbb{K}}(\mathbb{F})$ 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 $\alpha = \text{complex conjugation}$. Whether V^* denotes linear or antilinear maps should be evident from context.

Some subgroups of general linear groups. Let V be a vector space over a field \mathbb{F} . Let $\text{GL}(V)$ be the general linear group over V , which consists of all invertible linear maps on V . Let $\phi : V \times V \rightarrow \mathbb{F}$ 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. Then $\text{GL}(V)$ acts on ϕ naturally, by $M \in \text{GL}(V)$ sends ϕ to $\phi \circ M$, defined as $(\phi \circ M)(v, v') = \phi(M(v), M(v'))$. The subgroup of $\text{GL}(V)$ that preserves ϕ is denoted as $\mathcal{G}(V, \phi) := \{M \in \text{GL}(V) \mid \phi \circ M = \phi\}$.

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 $\text{U}(n, \mathbb{C})$.
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 $\text{O}(n, \mathbb{R})$.
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 $\text{Sp}(2n, \mathbb{F})$.

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

Matrices. Let $M(l \times m, \mathbb{F})$ be the linear space of $l \times m$ matrices over \mathbb{F} , and $M(n, \mathbb{F}) := M(n \times n, \mathbb{F})$. Given $A \in M(l \times m, \mathbb{F})$, denote by A^t the transpose of A . Given $A \in \text{GL}(n, \mathbb{F})$, 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 $E_{i,j} \in M(n, \mathbb{F})$ be the *elementary matrix* where the (i, j) th entry is 1, and the remaining entries are 0. For $i \neq j$, the matrix $E_{i,j} - E_{j,i}$ is called an *elementary alternating matrix*.

3-way arrays and some group actions on them. Let $T(\ell \times m \times n, \mathbb{F})$ be the linear space of $\ell \times m \times n$ 3-way arrays over \mathbb{F} . Given $\mathbf{A} \in T(\ell \times m \times n, \mathbb{F})$, the (i, j, k) th entry of \mathbf{A} is denoted as $A(i, j, k) \in \mathbb{F}$. We can slice \mathbf{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 $A_1, \dots, A_n \in M(\ell \times m, \mathbb{F})$, where $A_k(i, j) = A(i, j, k)$. Similarly, we also obtain the *horizontal* slices by slicing along the first coordinate, and the *lateral* slices by slicing along the second coordinate.

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

Tensors. Let V_1, \dots, 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 $(a_1, b_1; a_2, b_2; \dots; a_c, b_c)$ supported by (V_1, \dots, V_c) is an element in $V_1^{\otimes a_1} \otimes V_1^{*\otimes b_1} \otimes V_2^{\otimes a_2} \otimes V_2^{*\otimes b_2} \otimes \dots \otimes V_c^{\otimes a_c} \otimes V_c^{*\otimes b_c}$. We say

31:12 Isomorphism Problems over Classical Groups

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 $a_1 = \dots = a_c = 1$ and $b_1 = \dots = b_c = 0$. The group $\text{GL}(V_1) \times \dots \times \text{GL}(V_c)$ acts naturally on the space $V_1^{\otimes a_1} \otimes V_1^{*\otimes b_1} \otimes V_2^{\otimes a_2} \otimes V_2^{*\otimes b_2} \otimes \dots \otimes V_c^{\otimes a_c} \otimes V_c^{*\otimes b_c}$. 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 $V_1^{\otimes a_1} \otimes V_1^{*\otimes b_1} \otimes V_2^{\otimes a_2} \otimes V_2^{*\otimes b_2} \otimes \dots \otimes V_c^{\otimes a_c} \otimes V_c^{*\otimes b_c}$. After fixing the basis of each V_i , T can be represented as a multiway array $R_T \in \mathbb{T}(d_1^{\times(a_1+b_1)} \times \dots \times d_c^{\times(a_c+b_c)})$ and the elements in $\text{GL}(V_i) \cong \text{GL}(d_i, \mathbb{F})$ can be represented as invertible $d_i \times d_i$ matrices. The action of (A_1, \dots, A_c) on R_T can be explicitly written following Definition 1, using A_i for a_i directions and A_i^{-t} for b_i directions.

3 Proof of Theorem 6

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 [13, 15]. We follow their proof strategies, but as mentioned in Section 1.4, certain technical difficulties need to be dealt with.

In Section 3.1, 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 3.2, 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 3.3 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 3.4, we reduce $U \otimes U \otimes W$ to $U \otimes U \otimes U^*$ and $U \otimes U \otimes U$.

3.1 Reduction to plain UNITARY 3-TENSOR ISOMORPHISM

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 rephrasing [13, Theorem 1.1], as in our full version [5, Theorem 4.1], and then proving the following new result in the unitary setting.

► **Theorem 12** (Unitary version of [13, Theorem 1.1]). *Let $S = \{S_1, \dots, S_c\}$ and $T = \{T_1, \dots, T_c\}$ be two tensor systems supported by $\{V_1, \dots, V_m\}$, 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 $U(V_1) \times \dots \times U(V_m)$ if and only if $r(S)$ and $r(T)$ are isomorphic under $U(U) \times U(V) \times U(W)$. The algorithm r runs in time polynomial in the maximum dimension over U, V, W , and this maximum dimension is upper bounded by $\text{poly}(\sum_{i \in [m]} \dim(V_i), 2^{\text{poly}(c)})$.*

This follows the same proof as [13, Theorem 1.1], outlined in our full version [5, Appendix B], with one change, based on the following result.

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

► **Theorem 13** (Sergeichuk [29, Theorem 3.1]). *Let $\mathbf{C} = (C_1, \dots, C_m) \in M(l \times n, \mathbb{F})$. 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 j th 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 j th 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 14.** *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 12. With Corollary 14, the proof of [13, Theorem 1.1] goes through for this unitary setting, by replacing the use of the Krull–Schmidt theorem for quiver representations ([13, pp. 20]) with Theorem 13.

The case of orthogonal groups follows similarly by using [29, 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 12.

► **Proposition 15.** *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 $\mathbf{A} \in V \otimes V \otimes W$, we can construct a tensor system consisting of one tensor \mathbf{A} and two vector spaces $\{V, W\}$, with two arcs from V to \mathbf{A} , and one arc from W to \mathbf{A} . Starting from two tensors $\mathbf{A}_1, \mathbf{A}_2 \in V \otimes V \otimes W$, we consider the corresponding tensor systems, and ask for unitary isomorphism of these tensor systems. Then by Theorem 12, they can be reduced to the plain 3-tensor unitary isomorphism in time $\text{poly}(\dim(V), \dim(W))$, 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. ◀

3.2 Reduction from UNITARY 3-TI to BILINEAR FORM UNITARY PSUEDOISOMETRY $(V \otimes V \otimes W)$

We mainly follow the construction in [15] to show that there is a reduction from UNITARY 3-TENSOR ISOMORPHISM $(U \otimes V \otimes W)$ to BILINEAR FORM UNITARY PSEUDOISOMETRY $(V' \otimes V' \otimes W')$. In addition, we prove that the reduction from [15] preserves the unitary property in both directions.

► **Proposition 16.** *Given two 3-tensors $\mathbf{A}, \mathbf{B} \in U \otimes V \otimes W$, where $\dim(U) = l \leq \dim(V) = m$ and $\dim(W) = n$. There is a reduction $r : U \otimes V \otimes W \rightarrow V' \otimes V' \otimes W'$ with $\dim(V') = l + 5m + 3$ and $\dim(W') = n + l(m + 1) + m(3m + 2)$ such that \mathbf{A} and \mathbf{B} are unitarily isomorphic if and only if $r(\mathbf{A})$ and $r(\mathbf{B})$ are unitarily isomorphic, where frontal slices of $r(\mathbf{A})$ and $r(\mathbf{B})$ are skew-symmetric matrices.*

31:14 Isomorphism Problems over Classical Groups

Proof.

The reduction. We use the gadget in [13] and [15] to present this reduction. Here we use matrix format to illustrate our construction, and the picture of this construction is shown in Figure 1. Denote the i th frontal slice of \mathbf{A} by $A_i \in M(l \times m, \mathbb{C})$, where $i \in [n]$. Let the i th frontal slice of $r(\mathbf{A})$ be $\hat{A}_i \in M(l + 5m + 3, \mathbb{C})$, 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 $E_{s, l+m+t} - E_{l+m+t, s}$, 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 $E_{l+s, l+m+m+1+t} - E_{l+m+m+1+t, l+s}$, 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 $r(\mathbf{A})$ 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 i th horizontal slice of $-\mathbf{A}$. Thus, $m + 1 \leq \text{rank}(L_i) \leq 2m + 1$.
- 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 \mathbf{A} with size $l \times n$. Therefore, $3m + 2 \leq \text{rank}(L_i) \leq 3m + 2 + l \leq 4m + 2$.
- For the next $m + 1$ slices, L_i has a block I_l after rearranging the columns, so $\text{rank}(L_i) = l \leq m$.
- For the last $3m + 2$ slices, similarly, L_i has a block I_m after rearranging the columns, so $\text{rank}(L_i) = m$.

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 $P \in U(l + 5m + 3, \mathbb{C})$ and $Q \in U(n + l(m + 1) + m(3m + 2), \mathbb{C})$ such that $P^t r(\mathbf{A}) P = r(\mathbf{B}) Q$. 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 $P_{1,1} \in M(l, \mathbb{C})$, $P_{2,2} \in M(m, \mathbb{C})$ and $P_{3,3} \in M(4m + 3, \mathbb{C})$. By ranks of lateral slices of $r(\mathbf{B})$

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-triangular unitary

matrix, $P_{1,1}, P_{2,2}$ and $P_{3,3}$ are unitary matrices. Since the aim is to check if \mathbf{A} and \mathbf{B} are isomorphic, we only consider the first n frontal slices of $r(\mathbf{A})$ and $r(\mathbf{B})$, which contains \mathbf{A} and \mathbf{B} respectively. After applying P on lateral slices and horizontal slices of $r(\mathbf{A})$, 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 $r(\mathbf{B})$, and have $P^t r(\mathbf{A}) P = r(\mathbf{B})^Q$. Note that only the block (1, 2) and (2, 1) are non-zero blocks in the first n slices of $r(\mathbf{B})$ and $P^t r(\mathbf{A}) P$, 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 $P_{1,1}^t \mathbf{A} P_{2,2} = \mathbf{B}^{Q_{1,1}}$ where $P_{1,1}^t, P_{2,2}$ and $Q_{1,1}$ are unitary.

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

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

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

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

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

where $E_i \in M(l \times (m + 1), \mathbb{C})$. 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 \mathbf{E} to be $L_i \in M(l \times l(m + 1), \mathbb{C})$ where $i \in [m + 1]$. Apply a proper permutation π on the columns of L_i and have the matrix $L'_i = L_i T_\pi = [\mathbf{0} \dots I_l \dots \mathbf{0}]$ where $T_\pi \in M(l(m + 1), \mathbb{C})$ is the permutation matrix and the i th block of L'_i is the identity matrix $I_l \in M(l, \mathbb{C})$. After left multiplying L'_i by P^t , we have $P^t L'_i = [\mathbf{0} \dots P^t \dots \mathbf{0}]$. Now we define a diagonal matrix T'_1 as $\text{diag}(P^t, \dots, P^t)$, which gives us $P^t L'_i = L'_i T'_1 \iff P^t L_i = L_i T_\pi T'_1 T_\pi^t$. Then we set S_1 to be the identity matrix and T_1 to be $T_\pi T'_1 T_\pi^t$, and it yields $P^t \mathbf{E} S_1 = \mathbf{E}^{T_1}$, 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. \blacktriangleleft

3.3 Reduction from UNITARY 3-TENSOR ISOMORPHISM to UNITARY MATRIX SPACE CONJUGACY ($\mathbf{V} \otimes \mathbf{V}^* \otimes \mathbf{W}$)

A 3-way array $\mathbf{A} \in \mathbb{T}(l \times m \times n, \mathbb{F})$ is *non-degenerate* if along each direction, the slices are linearly independent.

► **Lemma 17.** *For any 3-way array $\mathbf{A} \in \mathbb{T}(l \times m \times n, \mathbb{C})$, there are unitary matrices $T_1 \in \mathbb{U}(l, \mathbb{C})$, $T_2 \in \mathbb{U}(m, \mathbb{C})$ and $T_3 \in \mathbb{U}(n, \mathbb{C})$ such that*

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

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

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

$$A' = [A_1 \quad \dots \quad A_n].$$

We denote the maximum number of linearly independent horizontal slices of \mathbf{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 \mathbf{A} sends \mathbf{A} to

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

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

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

► **Lemma 18.** *Given two 3-tensors $\mathbf{A}, \mathbf{B} \in U \otimes V \otimes W$ where $l = \dim(U)$, $m = \dim(V)$ and $n = \dim(W)$, there is a reduction r such that \mathbf{A} and \mathbf{B} are unitarily isomorphic if and only if $r(\mathbf{A})$ and $r(\mathbf{B})$ are unitarily isomorphic, where $r(\mathbf{A})$ and $r(\mathbf{B})$ are non-degenerate.*

We note that this reduction is one of the few in the paper 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 17, we can find unitary matrices $S_1 \in \mathbb{U}(l, \mathbb{C})$, $S_2 \in \mathbb{U}(m, \mathbb{C})$ and $S_3 \in \mathbb{U}(n, \mathbb{C})$ to extract the $l' \times m' \times n'$ non-degenerate tensor $\tilde{\mathbf{A}}$ of \mathbf{A} . There are similar unitary matrices $T_1 \in \mathbb{U}(l, \mathbb{C})$, $T_2 \in \mathbb{U}(m, \mathbb{C})$ and $T_3 \in \mathbb{U}(n, \mathbb{C})$ for \mathbf{B} as well. Then we claim \mathbf{A} and \mathbf{B} are unitarily isomorphic if and only if $r(\mathbf{A}) = \tilde{\mathbf{A}}$ and $r(\mathbf{B}) = \tilde{\mathbf{B}}$ are unitarily isomorphic.

For the if direction, assume $\tilde{P} \tilde{\mathbf{A}} \tilde{Q} = \tilde{B}^{\tilde{R}}$ where $\tilde{P} \in \mathbb{U}(l', \mathbb{C})$, $\tilde{Q} \in \mathbb{U}(m', \mathbb{C})$ and $\tilde{R} \in \mathbb{U}(n', \mathbb{C})$. It yields that $P' \mathbf{A}' Q' = B'^{R'}$ where $A' = \begin{bmatrix} \tilde{\mathbf{A}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$ and $B' = \begin{bmatrix} \tilde{\mathbf{B}} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$, and $P' =$

$\text{diag}(\tilde{P}, I_{l-l'}), Q' = \text{diag}(\tilde{Q}, I_{m-m'})$ and $R' = \text{diag}(\tilde{R}, I_{n-n'})$. 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 $PAQ = B^R$.

For the only if direction, suppose $PAQ = B^R$ for $P \in U(l, \mathbb{C}), Q \in U(m, \mathbb{C})$ and $R \in U(n, \mathbb{C})$, which follows that $P'A'Q' = B'^{R'}$ for $A' = \begin{bmatrix} \tilde{A} & 0 \\ 0 & 0 \end{bmatrix}$ and $B' = \begin{bmatrix} \tilde{B} & 0 \\ 0 & 0 \end{bmatrix}$, 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 $A'Q'$ and $B'^{R'}$ are $\mathbf{0}$ and the first l' slices of $A'Q'$ are linearly independent, so we derive that $P_{2,1} = \mathbf{0}$. We can conclude that Q' and R' are block-lower-triangular 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{A} and \tilde{B} by $\tilde{P}\tilde{A}\tilde{Q} = \tilde{B}\tilde{R}$. ◀

► **Corollary 19.** *Given two 3-tensors $A, B \in V \otimes V \otimes W$, there is a reduction r such that A, B are unitarily isomorphic if and only if $r(A), r(B) \in V \otimes V \otimes W'$ are unitarily pseudo-isometric bilinear forms, and such that the frontal slices of $r(A)$ and $r(B)$ are linearly independent.*

Based on Lemma 18, we will show that the UNITARY 3-TENSOR ISOMORPHISM ($U \otimes V \otimes W$) can be reduced to UNITARY MATRIX SPACE CONJUGACY ($V' \otimes V'^* \otimes W'$).³

► **Proposition 20.** *There is a reduction $r : U \otimes V \otimes W \rightarrow V' \otimes V'^* \otimes W$ where $\dim(U) = l, \dim(V) = m, \dim(W) = n$ and $\dim(V') = l + m$ such that two tensors $A, B \in U \otimes V \otimes W$ are unitarily isomorphic if and only if $r(A), r(B) \in V' \otimes V'^* \otimes W$ are unitarily conjugate matrix spaces.*

Proof.

The reduction. Denote the i th 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 $\hat{A}_i \in M(l + m, \mathbb{C})$ is the i th frontal slice of $r(A)$.

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 $r(A)$ and $r(B)$ are isomorphic.

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

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

³ 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 $U(V') \times U(W')$ on $V' \otimes V'^* \otimes W'$ or the action of $U(V') \times GL(W')$ on the same space. In this paper 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 $U(V') \times U(W')$ acting.

31:18 Isomorphism Problems over Classical Groups

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

$$\begin{bmatrix} A_i P_{2,1} & A_i P_{2,2} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & P_{1,1} B'_i \\ \mathbf{0} & P_{2,1} B'_i \end{bmatrix},$$

where $A_i P_{2,1} = \mathbf{0}$ and $A_i P_{2,2} = P_{1,1} B'_i$ 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 \mathbf{A} is non-degenerate, $P_{2,1}$ must be a zero matrix. Thus, P is a block-upper-triangular matrix, which results in $P_{1,1}$ and $P_{2,2}$ are unitary. Therefore, we have that $P_{1,1}^{-1} \mathbf{A} P_{2,2} = \mathbf{B}^Q$ for $P_{1,1} \in \mathbf{U}(l, \mathbb{C})$, $P_{2,2} \in \mathbf{U}(m, \mathbb{C})$ and $Q \in \mathbf{U}(n, \mathbb{C})$.

For the only if direction. Suppose $PAQ = \mathbf{B}^R$ where $P \in \mathbf{U}(l, \mathbb{C})$, $Q \in \mathbf{U}(m, \mathbb{C})$ and $R \in \mathbf{U}(n, \mathbb{C})$. 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 $P'^{-1} r(\mathbf{A}) P' = r(\mathbf{B})^{Q'}$. ◀

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

3.4 Reduction from UNITARY 3-TENSOR ISOMORPHISM to UNITARY ALGEBRA ISO. ($V \otimes V \otimes V^*$) and UNITARY EQUIVALENCE OF NONCOMMUTATIVE CUBIC FORMS ($V \otimes V \otimes V$)

► **Proposition 22.** *There is a reduction from BILINEAR FORM UNITARY PSEUDO-ISOMETRY to UNITARY ALGEBRA ISOMORPHISM and to UNITARY EQUIVALENCE OF NONCOMMUTATIVE CUBIC FORMS.*

In symbols, there are reductions

$$r : V \otimes V \otimes W \rightarrow V' \otimes V' \otimes V'^* \quad \text{and} \quad r' : V \otimes V \otimes W \rightarrow V' \otimes V' \otimes V'$$

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

Proof.

The construction. Given a tensor $\mathbf{A} \in V \otimes V \otimes W$ whose frontal slices are A_i , construct an array $\mathbf{A}' \in \mathbf{T}((l+m) \times (l+m) \times (l+m), \mathbb{C})$ 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 $\hat{\mathbf{A}}$ represent the tensor in $V' \otimes V' \otimes V'^*$ corresponding to entries defined by \mathbf{A}' , and denote $\tilde{\mathbf{A}}$ by the tensor in $V' \otimes V' \otimes V'$ corresponding to entries defined by \mathbf{A}' . Note that by Corollary 19, we can always assume that the frontal slices of \mathbf{A} are linearly independent, so the last m slices of \mathbf{A}' are linearly independent as well. We will show that $\mathbf{A}, \mathbf{B} \in V \otimes V \otimes W$ are isomorphic if and only if $\hat{\mathbf{A}}, \hat{\mathbf{B}} \in V' \otimes V' \otimes V'^*$ are isomorphic, and \mathbf{A}, \mathbf{B} are isomorphic if and only if $\tilde{\mathbf{A}}, \tilde{\mathbf{B}} \in V' \otimes V' \otimes V'$ are isomorphic.

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

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

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

Since the last m slices of $\hat{\mathbf{A}}$ 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 $P^t \hat{\mathbf{A}} P$ and $\hat{\mathbf{B}}^{\hat{P}^t}$ yields that $P_{1,1}^t \mathbf{A} P_{1,1} = \mathbf{B}^{P_{2,2}^t}$, 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. \blacktriangleleft

4 Proof of Theorem 7

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

Let \mathbf{A}, \mathbf{B} be two d -way arrays in $T(n_1 \times \cdots \times n_d, \mathbb{F})$. We will exhibit an algorithm T such that $T(\mathbf{A})$ is an algebra on \mathbb{F}^m where $m = \text{poly}(n_1, \dots, n_d)$, and such that \mathbf{A} and \mathbf{B} are unitarily isomorphic as d -tensors if and only if $T(\mathbf{A})$ and $T(\mathbf{B})$ are unitarily isomorphic as algebras. We can then apply Theorem 6 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.

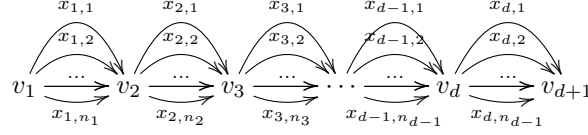
Background on quivers and path algebras. A *quiver* is a directed multigraph $G = (V, E, s, t)$, where V is the vertex set, E is the arrow set, and $s, t : E \rightarrow V$ are two maps indicating the source and target of an arrow.

A path in G is the concatenation of edges $p = e_1, e_2, \dots, e_n$, 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 $\text{Path}_{\mathbb{F}}(G)$, is the free algebra generated by $V \cup E$ modulo the relations generated by:

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 paper we make use of the following quiver. Note that this is different from the quiver used in [15]; 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 [15] does so).



■ **Figure 2** The quiver G we use in this paper.

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

Proof of Theorem 7. Let $f, g \in U_1 \otimes U_2 \otimes \dots \otimes U_d$ be two tensors, where $U_i = \mathbb{F}^{n_i}$ for $i \in [d]$. We can encode f in $\text{Path}_{\mathbb{F}}(G)$ as follows. Recall that e_i denotes the i th standard basis vector. Suppose $f = \sum_{(i_1, \dots, i_d)} \alpha_{i_1, \dots, i_d} e_{i_1} \otimes \dots \otimes e_{i_d}$, where the summation is over $(i_1, \dots, i_d) \in [n_1] \times \dots \times [n_d]$ and $\alpha_{i_1, \dots, i_d} \in \mathbb{F}$. Then let $\hat{f} \in \text{Path}_{\mathbb{F}}(G)$ be defined as $\hat{f} = \sum_{(i_1, \dots, i_d)} \alpha_{i_1, \dots, i_d} x_{1,i_1} x_{2,i_2} \dots x_{d,i_d}$, where $(i_1, \dots, i_d) \in [n_1] \times \dots \times [n_d]$.

Let $R_f := \text{Path}_{\mathbb{F}}(G)/(\hat{f})$ and $R_g := \text{Path}_{\mathbb{F}}(G)/(\hat{g})$. 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 $(P_1, \dots, P_d) \in U(n_1, \mathbb{C}) \times \dots \times U(n_d, \mathbb{C})$ be a tensor isomorphism from f to g . Then P_i naturally acts on the linear space $\langle x_{i,1}, \dots, x_{i,n_i} \rangle$, and together with the identity matrix I_{d+1} acting on $\langle v_1, \dots, v_{d+1} \rangle$. It's straightforward to show that they form an algebra isomorphism from R_f to R_g , which is essentially the same as [15]; see our full version [5, Section 6] for a detailed proof.

Algebra isomorphism implies tensor isomorphism. This part of the proof is new, compared to the corresponding part in [15].

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

Note that $\text{Path}_{\mathbb{F}}(G)$ is linearly spanned by paths in G , so it is naturally graded, and we use $\text{Path}_{\mathbb{F}}(G)_{\ell}$ denotes the linear space of $\text{Path}_{\mathbb{F}}(G)$ 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 $\text{Path}_{\mathbb{F}}(G)/(\hat{f})$, $(v_1, \dots, v_{d+1}, x_{i,j},$ paths of length 2, $\dots,$ 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, \dots, 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

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

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 $(x_{i,1}, \dots, x_{i,n_i})$, and let the resulting (invertible) matrix be P_i . These matrices P_1, \dots, 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 d th roots. We can then obtain $(1/\alpha^{1/d} \cdot P_1, 1/\alpha^{1/d} \cdot P_2, \dots, 1/\alpha^{1/d} \cdot P_d) \cdot f = g$.

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. ◀

References

- 1 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.
- 2 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.
- 3 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.
- 4 W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system I: the user language. *J. Symb. Comput.*, pages 235–265, 1997.
- 5 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.
- 6 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.
- 7 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>.
- 8 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.

- 9 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.
- 10 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.
- 11 Jack Edmonds. Paths, trees, and flowers. *Canadian Journal of mathematics*, 17(3):449–467, 1965. doi:10.4153/CJM-1965-045-4.
- 12 Lance Fortnow and Joshua A. Grochow. Complexity classes of equivalence problems revisited. *Inform. and Comput.*, 209(4):748–763, 2011. Also available as arXiv:0907.4775 [cs.CC]. doi:10.1016/j.ic.2011.01.006.
- 13 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.
- 14 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.
- 15 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. Part of the preprint arXiv:1907.00309 [cs.CC]. Preliminary version appeared at ITCS '21, DOI:10.4230/LIPICs.ITCS.2021.31. doi:10.1137/21M1441110.
- 16 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. doi:10.48550/arXiv.2306.16317.
- 17 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. Extended abstract appeared in STACS '21 DOI:10.4230/LIPICs.STACS.2021.38. doi:10.46298/jgcc.2022.14.1.9431.
- 18 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.
- 19 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.
- 20 Jim Humphreys. What are “classical groups”? <https://mathoverflow.net/questions/50610/what-are-classical-groups>.
- 21 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.
- 22 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.
- 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.
- 24 Lek-Heng Lim. Tensors in computations. *Acta Numerica*, 30:555–764, 2021. doi:10.1017/S0962492921000076.
- 25 László Lovász. On determinants, matchings, and random algorithms. In Lothar Budach, editor, *Fundamentals of Computation Theory, FCT 1979, Proceedings of the Conference on Algebraic, Arithmetic, and Categorical Methods in Computation Theory, Berlin/Wendisch-Rietz, Germany, September 17-21, 1979*, pages 565–574. Akademie-Verlag, Berlin, 1979.

- 26 M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000. doi:10.1017/CB09780511976667.
- 27 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>.
- 28 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.
- 29 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.
- 30 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.
- 31 George Frederick James Temple. *Cartesian Tensors: an introduction*. Courier Corporation, 2004.
- 32 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.
- 33 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 11th 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.
- 34 H. Weyl. *The classical groups: their invariants and representations*, volume 1. Princeton University Press, 1946 (1997). doi:10.2307/j.ctv3hh48t.
- 35 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.
- 36 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.