ON THE COMPLEXITY OF ISOMORPHISM PROBLEMS FOR TENSORS, GROUPS, AND POLYNOMIALS I: TENSOR ISOMORPHISM-COMPLETENESS *

JOSHUA A. GROCHOW† AND YOUMING QIAO ‡

Abstract. We study the complexity of isomorphism problems for tensors, groups, and polynomials. These problems have been studied in multivariate cryptography, machine learning, quantum information, and computational group theory. We show that these problems are all polynomial-time equivalent, creating bridges between problems traditionally studied in myriad research areas. This prompts us to define the complexity class TI, namely problems that reduce to the Tensor Isomorphism (TI) problem in polynomial time. Our main technical result is a polynomial-time reduction from d-tensor isomorphism to 3-tensor isomorphism. In the context of quantum information, this result gives multipartite-to-tripartite entanglement transformation procedure, that preserves equivalence under stochastic local operations and classical communication (SLOCC).

Key words. isomorphism problems, tensor isomorphism, group isomorphism, polynomial isomorphism, complexity class, completeness

MSC codes. 68Q15, 81P45, 68Q17

1. Introduction.

Although Graph Isomorphism (GI) is perhaps the most well-studied isomorphism problem in computational complexity—even going back to Cook's and Levin's initial investigations into NP (see [3, Sec. 1])—it has long been considered to be solvable in practice [76, 77], and Babai's recent quasi-polynomial-time breakthrough is one of the theoretical gems of the last several decades [6].

However, several isomorphism problems for tensors, groups, and polynomials seem to be much harder to solve, both in practice—they've been suggested as difficult enough to support cryptography [59, 84]—and in theory: the best known worst-case upper bounds are barely improved from brute force (e. g., [69, 90]). As these problems arise in a variety of areas, from multivariate cryptography and machine learning, to quantum information and computational algebra, getting a better understanding of their complexity is an important goal with many potential applications. These isomorphism problems are the focus of this paper.

Our first set of results shows that all these isomorphism problems from many research areas are equivalent under polynomial-time reductions, creating bridges between different disciplines. The Tensor Isomorphism (TI) problem turns out to occupy a central position among these problems, leading us to define the complexity class TI, consisting of those problems polynomial-time reducible to the Tensor Isomorphism problem.

More specifically, we first present a polynomial-time reduction from d-Tensor Isomorphism to 3-Tensor Isomorphism. This result may be viewed as corresponding to the k-SAT to 3-SAT reduction in the setting of Tensor Isomorphism, but the proof is much more involved. This result also has a natural application to quantum information: it gives a procedure that turns multipartite entanglements to tripartite entanglements while preserving equivalence under stochastic local operations and classical communication (SLOCC).

*An extended abstract of this paper appeared in the 12th Innovations in Theoretical Computer Science Conference [52].

Funding: Both authors were supported by NSF grant DMS-1750319. J. A. G was partly funded by NSF CAREER grant CCF-2047756. Y. Q. was partly supported by Australian Research Council DP200100950.

†Departments of Computer Science and Mathematics, University of Colorado, Boulder (jgrochow@colorado.edu).

‡Centre for Quantum Software and Information, University of Technology Sydney (youming.qiao@uts.edu.au).

We then demonstrate that various isomorphism problems for polynomials, general algebras, groups, and tensors all turn out to be TI-complete. One important reference here is the recent work [42], in which they showed that several such problems reduce to 3TI. Our contribution is to show that these problems are also 3TI-hard. Another set of related works are [1,2,62] by Agrawal, Kayal, and Saxena, who showed some equivalences and reductions between Ring Isomorphism (commutative with unit), Cubic Form Equivalence, and isomorphism of commutative, unital, associative algebras [1,2,62]. Here we greatly expand these and show a much wider class of problems are equivalent (see Thm. 1.4=Thm. B and Fig. 1).

In a follow-up paper [51], we study search and counting to decision reductions, apply the results of the present paper to Group Isomorphism in the matrix group model, and obtain a nilpotency class reduction for Group Isomorphism.

All these results together lay the foundation for an emerging theory of the complexity class TI that in some cases parallels, and in some cases deviates from, the complexity theory of the class GI, namely the set of problems that are polynomial-time reducible to Graph Isomorphism [64]. From the theory perspective, this theory reveals a family of algorithmic problems demonstrating highly interesting complexity-theoretic properties. From the practical perspective, this theory could serve as a guidance for, and facilitate dialogue among, researchers from diverse research areas including cryptography, machine learning, quantum information, and computational algebra. Indeed, some of our results already have natural applications to quantum information and computational group theory.

In the remainder of this section we shall present these results in detail, starting from an introduction of these problems and their origins.

1.1. Isomorphism testing problems from several areas. Let $\mathbb{F}$ be a field. Let $\mathrm{GL}(n,\mathbb{F})$ denote the general linear group of degree n over $\mathbb{F}$, and $\mathrm{M}(n,\mathbb{F})$ the linear space of $n\times n$ matrices. For a finite field $\mathbb{F}_q$, we may also write $\mathrm{GL}(n,\mathbb{F}_q)$ and $\mathrm{M}(n,\mathbb{F}_q)$ as $\mathrm{GL}(n,q)$ and $\mathrm{M}(n,q)$.

Multivariate cryptography. In 1996, Patarin [84] proposed identification and signature schemes based on a family of problems called "isomorphism of polynomials." A specific problem, called *isomorphism of (quadratic) polynomials with two secrets* (IP2S), asks the following. Let $\vec{f} = (f_1,\dots,f_m)$ and $\vec{g}=(g_1,\dots,g_m)$ be two tuples of homogeneous quadratic polynomials, where $f_i, g_j \in \mathbb{F}[x_1,\dots,x_n]$. Recall an m-tuple of polynomials in n variables can be viewed as a polynomial map from $\mathbb{F}^n$ to $\mathbb{F}^m$. It is natural to ask whether $\vec{f}$ and $\vec{g}$ represent the same polynomial map up to change of basis, or more specifically, whether there exists $P\in\mathrm{GL}(n,\mathbb{F})$ and $Q\in\mathrm{GL}(m,\mathbb{F})$, such that $Q\circ\vec{f}\circ P=\vec{g}$. Since then, the IP2S problem, and its variant isomorphism of (quadratic) polynomials with one secret (IP1S), have been intensively studied in multivariate cryptography (see [13, 57] and references therein).

Machine learning. In machine learning, it is natural to view a sequential data stream as a path. This leads to the use of the *signature* tensor of a path $\phi:[0,1]\to\mathbb{R}^n$, first introduced by Chen [29] to extract features of data. This is the basic idea of the signature tensor method, which has been pursued by in a series of works; see [30, 72, 81] and references therein. The algorithmic problem of reconstructing the path from the signature tensor is of considerable interest; see, e. g., [73,86]. In this context, the following problem was recently studied by Pfeffer, Seigal, and Sturmfels [86], called the Tensor Congruence problem: given two 3-tensors $\mathtt{A}=(a_{ijk}), \mathtt{B}=(b_{ijk})\in\mathbb{F}^{n\times n\times n}$, decide whether there exists $P\in\mathrm{GL}(n,\mathbb{F})$, such that the congruence action of P sends $\mathtt{A}$ to $\mathtt{B}$. More specifically, this action of $P=(p_{ij})$ sends $\mathtt{A}=(a_{ijk})$ to $\mathtt{A}'=(a'_{ijk})$, where $a'_{ijk}=\sum_{i',j',k'} a_{i'j'k'}p_{i,i'}p_{j,j'}p_{k,k'}$.

Quantum information. Let $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_d$, where $\mathcal{H}_i = \mathbb{C}^{n_i}$. Let $\rho = |\phi\rangle\langle\phi|$ and $\tau = |\psi\rangle\langle\psi|$ be two pure quantum states, where $|\phi\rangle, |\psi\rangle \in \mathcal{H}$. In quantum information, a natural question is to decide whether ρ can be converted to τ using local operations and classical communication statistically (SLOCC), i. e., with non-zero probability [12,36]. It is well-known by [36] that ρ and τ are interconvertible via SLOCC if and only if there exist $T_i \in \mathrm{GL}(\mathcal{H}_i)$, such that $(T_1 \otimes \dots T_m)|\phi\rangle = |\psi\rangle$. Therefore, given pure quantum states ρ and τ, whether ρ and τ are inverconvertible via SLOCC can be cast as an isomorphism testing problem, called the d-Tensor Isomorphism problem (see Definition 1.1).

Computational group theory. In computational group theory, a notoriously difficult problem is to test isomorphism of finite p-groups, namely groups of prime power order (see, e. g., [82]). Here, the groups are represented succinctly, e. g., by generating sets of permutations or matrices over finite fields. Indeed, testing isomorphism of p-groups is considered to be a bottleneck to testing isomorphism of general groups [8, 28, 49]. Even for p-groups of class 2 and exponent p, current methods are still quite limited to instances of small size.

Theoretical computer science. As already mentioned, Agrawal, Kayal, and Saxena studied isomorphism and automorphism problems of rings, algebras, and polynomials [1, 2, 62], motivated by several problems including Primality Testing, Polynomial Factorization, and Graph Isomorphism. Later, motivated by cryptographic applications and algebraic complexity, Kayal studied the Polynomial Equivalence problems (possibly under affine projections) and solved certain important special cases [60,61] (see also [48]). Among these problems, we will be mostly concerned with the following two. First, the Algebra Isomorphism problem for commutative, unital, associative algebras over a field $\mathbb{F}$, asks whether two such algebras, given by structure constants, are isomorphic. Second, the Cubic Form Equivalence problem asks whether two homogeneous cubic polynomials over $\mathbb{F}$ are equivalent under the natural action of the general linear group by change of basis on the variables.

Practical complexity of these problems. The preceding isomorphism testing problems are of great interest to researchers from seemingly unrelated areas. Furthermore, they pose considerable challenges for practical computations at the present stage. The latter is in sharp contrast to Graph Isomorphism, for which very effective practical algorithms have existed for some time [76, 77]. Indeed, the problems we consider have been proposed to be difficult enough for cryptographic purposes [59, 84]. As further evidence of their practical difficulty, current algorithms implemented for testing isomorphism of p-groups of class 2 and exponent p can handle groups of dimension 20 over $\mathbb{F}_{13}$, but absolutely not for groups of dimension 200 over $\mathbb{F}_{13}$, even though in this case the input can still be stored in only a few megabytes.[1] In [86, arXiv version 1], computations on special cases of the Tensor Congruence problem were performed in Macaulay2 [45], but these could not go beyond small examples either.

A note on terminology. Before introducing our results formally, a terminological note is in order: we shall call valence-d tensors d-way arrays, and tensors will be understood to be d-way arrays considered under a specific group action. The reason for this change of terminology will be clearer in the following. We remark that it is not uncommon to see such differences in the terminologies around tensors, see, e. g., the preface of [68].

We follow a natural convention: when $\mathbb{F}$ is finite, a fixed algebraic extension of a finite field such as $\overline{\mathbb{F}}_p$, the rationals, or a fixed algebraic extension of the rationals such as $\overline{\mathbb{Q}}$, we consider the

[1] We thank James B. Wilson, who maintains a suite of algorithms for p-group isomorphism testing [24], for communicating this insight to us from his hands-on experience. We of course maintain responsibility for any possible misunderstanding, or lack of knowledge regarding the performance of other implemented algorithms.

usual model of Turing machines; when $\mathbb{F}$ is $\mathbb{R}$, $\mathbb{C}$, the p-adic rationals $\mathbb{Q}_p$, or other more "exotic" fields, we work in the Blum–Shub–Smale model over $\mathbb{F}$.

1.2. Main results.

1.2.1. Defining the Tensor Isomorphism complexity class.

Given the diversity of the isomorphism problems from Sec. 1.1, the first main question addressed in this paper is

> Is there a unifying framework that accommodates the many difficult isomorphism testing problems arising in practice?

Such a framework would help to explain the difficulties from various areas when dealing with these isomorphism problems, and facilitate dialogue among researchers from different fields.

At first sight, this seems quite difficult: these problems concern very different mathematical objects, ranging from sets of quadratic equations, to algebras, to finite groups, to tensors, and each of them has its own rich theory.

Despite these obstacles, our first main result shows that those problems in Sec. 1.1 arising in many fields—from computational group theory to cryptography to machine learning—are equivalent under polynomial-time reductions. In proving the first main result, the d-Tensor Isomorphism problem occupies a central position. This leads us to define the complexity class TI, consisting of problems reducible to TI, much in vein of the introduction of the Graph Isomorphism complexity class GI [64].

Definition 1.1 (The d-Tensor Isomorphism problem). *d-Tensor Isomorphism over a field $\mathbb{F}$ is the problem: given two d-way arrays $\mathtt{A} = (a_{i_1,\dots,i_d})$ and $\mathtt{B} = (b_{i_1,\dots,i_d})$, where $i_k \in [n_k]$ for $k \in [d]$, and $a_{i_1,\dots,i_d}, b_{i_1,\dots,i_d} \in \mathbb{F}$, decide whether there are $P_k \in \mathrm{GL}(n_k, \mathbb{F})$ for $k \in [d]$, such that for all $i_1, \dots, i_d$,*

$$a_{i_1,\dots,i_d} = \sum_{j_1,\dots,j_d} b_{j_1,\dots,j_d} (P_1)_{i_1,j_1} (P_2)_{i_2,j_2} \cdots (P_d)_{i_d,j_d}. \quad (1.1)$$

Our first main result resolves an open question well-known to the experts:[2]

Theorem 1.2 (=Cor. A). *d-Tensor Isomorphism reduces to 3-Tensor Isomorphism in time $O(n^d)$.*

Thm. 1.2 is also key to the application to quantum information as in Sec. 1.4.

Thus, while the 2TI problem is easy (it's just matrix rank), 3TI already captures the complexity of dTI for any fixed d. This phenomenon is reminiscent of the transition in hardness from 2 to 3 in k-SAT, k-Coloring, k-Matching, and many other NP-complete problems. It is interesting that an analogous phenomenon—a transition to some sort of "universality" from 2 to 3—occurs in the setting of isomorphism problems, which we believe are not NP-complete over finite fields (indeed, they cannot be unless PH collapses).

Definition 1.3 (TI). *For any field $\mathbb{F}$, $\mathsf{TI}_{\mathbb{F}}$ denotes the class of problems that are polynomial-time Turing (Cook) reducible to d-Tensor Isomorphism over $\mathbb{F}$, for some constant d. A problem is $\mathsf{TI}_{\mathbb{F}}$-complete, if it is in $\mathsf{TI}_{\mathbb{F}}$, and d-Tensor Isomorphism over $\mathbb{F}$ for any d reduces to this problem.*

By Thm. 1.2, we may take $d = 3$ without loss of generality. When we write TI without mentioning the field, the result holds for any field.

[2] We asked several experts who knew of the question, but we were unable to find a written reference. Interestingly, Oldenburger [83] worked on what we would call d-Tensor Isomorphism as far back as the 1930s. We would be grateful for any prior written reference to the question of whether dTI reduces to 3TI.

1.2.2. TI-complete problems. Our second main result shows the wide applicability and robustness of the TI class.

THEOREM 1.4 (Informal statement of part of Theorem B). *All the problems mentioned in Sec. 1.1 are* TI*-hard:* IP2S, TENSOR CONGRUENCE, CUBIC FORM EQUIVALENCE *(over fields of characteristic not 2 or 3),* ALGEBRA ISOMORPHISM *for commutative, unital, associative algebras, and* GROUP ISOMORPHISM *for p-groups of class 2 and exponent p given by matrix generators (over* $\mathbb{F}_{p^e}$*).*

In combination with the results of [42], we conclude that they are in fact TI*-complete.*

REMARK 1.5. *Our results allow us to mostly answer a question from Saxena's thesis [91, p. 86]. Namely, Agrawal & Saxena [1] gave a reduction from* CUBIC FORM EQUIVALENCE *to* RING ISOMORPHISM *for commutative, unital, associative algebras over* $\mathbb{F}$*, under the assumption that every element of* $\mathbb{F}$ *has a cube root in* $\mathbb{F}$*. For finite fields* $\mathbb{F}_q$*, the only such fields are those for which* $q = p^{2e+1}$ *and* $p \equiv 2 \pmod 3$*, which is asymptotically half of all primes. As explained after the proof of [1, Thm. 5], the use of cube roots seems inherent in their reduction, and Saxena asked whether such a reduction could be done over arbitrary fields. Using our results in conjunction with [42], we get a new such reduction—very different from the previous one [1]—which works over any field of characteristic not 2 or 3.*

Here, we would also like to point out that some of the polynomial-time equivalences in Thm. 1.4, though perhaps expected by some experts, were not *a priori* clear. To get a sense for the non-obviousness of the equivalences of problems in Theorem 1.4, let us postulate the following hypothetical question. Recall that two matrices $A, B \in \mathrm{M}(n, \mathbb{F})$ are called *equivalent* if there exist $P, Q \in \mathrm{GL}(n, \mathbb{F})$ such that $P^{-1}AQ = B$, and they are *conjugate* if there exists $P \in \mathrm{GL}(n, \mathbb{F})$ such that $P^{-1}AP = B$. Can we reduce testing MATRIX CONJUGACY to testing MATRIX EQUIVALENCE? Of course since they are both in P there is a trivial reduction; to avoid this, let us consider only reductions r which send a matrix A to a matrix $r(A)$ such that A and B are conjugate iff $r(A)$ and $r(B)$ are equivalent. Nearly all reductions between isomorphism problems that we are aware of have this form (so-called "kernel reductions" [41]; cf. functorial reductions [5]). This turns out to be essentially impossible. The reason is that the equivalence class of a matrix is completely determined by its rank, while the conjugacy class of a matrix is determined by its rational canonical form. Among $n \times n$ matrices there are only $n + 1$ equivalence classes, but there are at least $|\mathbb{F}|^n$ rational canonical forms, coming from the choice of minimal polynomial/companion matrix. Even when $\mathbb{F}$ is a finite field, such a reduction would thus require an exponential increase in dimension, and when $\mathbb{F}$ is infinite, such a reduction is impossible regardless of running time.

Nonetheless, for *linear spaces* of matrices (one form of 3-way arrays; see Sec. 2.2), conjugacy testing does indeed reduce to equivalence testing! We say two subspaces $\mathcal{A}, \mathcal{B} \subseteq \mathrm{M}(n, \mathbb{F})$ are *conjugate* if there exists $P \in \mathrm{GL}(n, \mathbb{F})$ such that $P\mathcal{A}P^{-1} = \{PAP^{-1} : A \in \mathcal{A}\} = \mathcal{B}$, and analogously for equivalence. This is in sharp contrast to the case of single matrices. In the above setting, it means that there exists a polynomial-time computable map ϕ from $\mathrm{M}(n, \mathbb{F})$ to *subspaces of* $\mathrm{M}(s, \mathbb{F})$, such that A, B are conjugate up to a scalar if and only if $\phi(A), \phi(B) \leq \mathrm{M}(s, \mathbb{F})$ are equivalent as matrix spaces. Such a reduction may not be clear at first sight.

1.2.3. The relation between TENSOR ISOMORPHISM **and** GRAPH ISOMORPHISM**.** After introducing the TI class, it is natural to compare this class with the corresponding class for GRAPH ISOMORPHISM, GI.

Already by using known reductions [42,48,71,85], GRAPH ISOMORPHISM and PERMUTATIONAL CODE EQUIVALENCE reduce to 3-TENSOR ISOMORPHISM (see App. B). For the inverse direction, we have the following connection.

COROLLARY 1.6. *Let* $\mathtt{A}$ *and* $\mathtt{B}$ *be two 3-tensors over* $\mathbb{F}_q$*, and let* n *be the sum of the lengths of all three sides. To decides whether* $\mathtt{A}$ *and* $\mathtt{B}$ *are isomorphic reduces to solving* GI *for graphs of size* $q^{O(n)}$*.*

Therefore, if GI is in P, then $3TI_{\mathbb{F}_q}$ can be solved in $q^{O(n)}$ time, where n is the sum of the lengths of all three sides. More generally, if $GI \in \mathsf{TIME}(2^{O(\log n)^c})$ then $3TI_{\mathbb{F}_q} \in \mathsf{TIME}(q^{O(n^c)})$. The current value of c for GI is 3 [6] (see [53] for the analysis of c); improving c to be less than 2 would improve over the current state of the art for both GpI and 3TI.

In Fig. 1 we summarize the relationships between GI, TI, and many more isomorphism testing problems.

1.3. An overview of proof strategies and techniques.

1.3.1. The main new technique. Our main new technique, used to show the reduction from dTI to 3TI (Thm. 1.2=Thm. A), is a simultaneous generalization of our reduction from 3TI to ALGEBRA ISOMORPHISM and the technique Grigoriev used [47] to show that isomorphism in a certain restricted class of algebras is equivalent to GI. In brief outline: a 3-way array $\mathtt{A}$ specifies the structure constants of an algebra with basis $x_1, \dots, x_n$ via $x_i \cdot x_j := \sum_k \mathtt{A}(i,j,k) x_k$, and this is essentially how we use it in the reduction from 3TI to ALGEBRA ISOMORPHISM. For arbitrary $d \geq 3$, we would like to similarly use a d-way array $\mathtt{A}$ to specify how d-tuples of elements in some algebra $\mathcal{A}$ multiply. The issue is that for $\mathcal{A}$ to be an algebra, our construction must still specify how *pairs* of elements multiply. The basic idea is to let pairs (and triples, and so on, up to $(d-2)$-tuples) multiply "freely" (that is, without additional relations), and then to use $\mathtt{A}$ to rewrite any product of $d-1$ generators as a linear combination of the original generators. While this construction as described already gives one direction of the reduction (if $\mathtt{A} \cong \mathtt{B}$, then $\mathcal{A} \cong \mathcal{B}$), the other direction is trickier. For that, we modify the construction to an algebra in which short products (less than $d-2$ generators) do not quite multiply freely, but almost. After the fact, we found out that this construction generalizes the one used by Grigoriev [47] to show that GI was equivalent ALGEBRA ISOMORPHISM for a certain restricted class of algebras (see Sec. 1.6 for a comparison).

1.3.2. The proof strategy for Theorem 1.4=B. Let us now explain briefly on the proof of Thm. B=Thm. 1.4. The first step is to realize all of these problems in a single unifying viewpoint. That is, all these equivalence relations underlying these isomorphism testing problems can be realized as the orbits of certain natural group actions by direct products of general linear groups on 3-way arrays. We shall explain this in detail in Sec. 3. Here, we only demonstrate five group actions on 3-way arrays, and indicate how those practical problems correspond to some of these actions.

To introduce these five group actions, it is instructive to first examine the more familiar cases of matrices. There are three natural group actions on $\mathrm{M}(n,\mathbb{F})$: 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^tAQ, (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^tAP. These three actions endow A with different algebraic/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 $\mathbb{F}$.

The five group actions on 3-way arrays referred to above are precisely analogous to the matrix setting. For a 3-way array $\mathtt{A} = (a_{i,j,k})$, $i,j,k \in [n]$, $a_{i,j,k} \in \mathbb{F}$, these actions are (1) $(P_1, P_2, P_3) \in \mathrm{GL}(n,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F})$ acts on $\mathtt{A}$ according to Equation 1.1 with $d=3$; (2) $(P_1, P_2) \in \mathrm{GL}(n,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F})$ acts on $\mathtt{A}$ as (P_1^{-t}, P_1, P_2) in (1), where P^{-t} denotes the transpose of the inverse of P; (3) $(P_1, P_2) \in \mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F})$ acts on $\mathtt{A}$ as (P_1, P_1, P_2) in (1); (4) $P \in \mathrm{GL}(n, \mathbb{F})$ acts on $\mathtt{A}$ as (P, P, P) in (1); and (5) $P \in \mathrm{GL}(n, \mathbb{F})$ acts on $\mathtt{A}$ as (P, P, P^{-t}) in (1).

These five actions endow various families of 3-way arrays with different algebraic/geometric meanings, including 3-tensors, bilinear maps, matrix (associative or Lie) algebras, and trilinear forms, a.k.a. non-commutative cubic forms. It is then not difficult to cast each of the problems in Thm. 1.4 as (a special case of) the problem of deciding whether two 3-way arrays are in the same orbit under one of the five group actions; see Sec. 2.2 for detailed explanations.[3]

The first step only provides the context for proving Thm. 1.4. After the first step, we need to devise polynomial-time reductions among those isomorphism testing problems for 3-way arrays under these five group actions, often with certain restrictions on the 3-way array structures. The two basic ideas for these reductions are a gadget construction from [42], and the "embedding" technique from [43]. To implement these ideas, however, usually involves detailed and complicated computations. For example, in the proof of Theorem 1.4, we use a gadget construction from [42] for the reduction from Tensor Isomorphism to IP2S in Section 5. To show that this gadget works in our setting, we need a proof strategy that is different from that in [42].

1.4. An implication to quantum information. Quantum information is the study of information-theoretic properties of quantum states and channels, such as entanglement, non-classical correlations, and the uses of quantum states and channels for various computational tasks. A pure quantum particle takes states in a Hilbert space (=complex vector space, along with an inner product) V; a pure multi-particle system takes states in the tensor product of the corresponding Hilbert spaces $V_1 \otimes V_2 \otimes \cdots \otimes V_k$.

A fundamental relation between k-partite quantum states is that of equivalence under *stochastic local operations and classical communication* (SLOCC) [12, 36]. If we imagine each particle is held by a different party, a "local operation" is an operation that a single party i can perform on its state in V_i. Although the definition of SLOCC involves combining this with classical communication, an equivalent definition is that two k-particle states $\psi, \phi \in V_1 \otimes \cdots \otimes V_k$ are SLOCC-equivalent if they are in the same orbit under the action of the product of general linear groups $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \cdots \times \mathrm{GL}(V_k)$ [36].[4] Deciding SLOCC equivalence (of un-normalized quantum states) is thus precisely the same as TI.

In this light, we may interpret our Thm. A as saying that SLOCC equivalence classes for k-partite entanglement can be simulated by SLOCC equivalence classes of tripartite entanglement. This might at first seem surprising, since bipartite entanglement is much better understood than tripartite or higher entanglement, so one might naively expect that 4-partite entanglement should be more complicated than tripartite, and so on. Our results show that in fact the tripartite case is already universal. This may be compared with a recent result in [108], which gives a transformation of multipartite states to a *set* of tripartite or bipartite states, interrelated by a *tensor network*, whereas our reduction produces a single tripartite state.

1.5. Outlook. In light of Babai's breakthrough on GI [6], it is natural to consider "what's next?" for isomorphism problems. That is, what isomorphism problems stand as crucial bottlenecks

[3]While problems in Thm. 1.4 only use three out of those five actions, the other two actions also lead to problems that arise naturally, including Matrix Algebra Conjugacy from [26], Matrix Lie Algebra Conjugacy from [48], and Bilinear Map Isotopism from [21]; see Sec. 2.2 and Sec. 1.6.

[4]Some authors use the action by the product of *special* linear groups $\mathrm{SL}(V_i)$ instead, but the difference is actually that physicists typically consider *normalized* quantum states, which are elements in the corresponding projective space $\mathbb{P}(V_1 \otimes \cdots \otimes V_k)$. Because the difference between $\mathrm{SL}(V_i)$ and $\mathrm{GL}(V_i)$ is merely scalar matrices, and scalar matrices act trivially on projective space, the equivalence relation is the same.

to further improvements on GI, and what isomorphism problems should naturally draw our attention for further exploration? Of course, one of the main open questions in the area remains whether or not GI is in P. Babai [6, arXiv ver., Sec. 13.2 & 13.4] already lists several isomorphism problems for further study, including GROUP ISOMORPHISM, PERMUTATIONAL CODE EQUIVALENCE (of linear codes), and PERMUTATION GROUP CONJUGACY. The reader may see where these sit in Fig. 1.

Based on the results above, we propose TI as a natural problem to study, both "after" GI, and to make further progress on GI itself. In particular, TI stands as a key bottleneck to put GI in P, because of the following. First, Babai suggested [6] that GROUP ISOMORPHISM (GPI) in the Cayley table model is a key bottleneck[5] to putting GI into P. Second, it has been long believed that p-groups of class 2 and exponent p are the hardest cases of GPI (for a number of reasons, see, e. g., [10, 54, 96, 106]). Third, by Baer's correspondence [10], isomorphism for such groups is equivalent[6] to ALTERNATING MATRIX SPACE ISOMETRY (see Section 2.2). Finally, by our main Thm. B, ALTERNATING MATRIX SPACE ISOMETRY over $\mathbb{F}_{p^e}$ is $\mathsf{TI}_{\mathbb{F}_{p^e}}$-complete.

This then relates TI over finite fields to the believed-to-be-hardest instances of GPI, which in turn, as Babai suggested, is a key bottleneck for further progress on GI. We thus view the study of TI as a natural continuation of the study of GI. Furthermore, the main techniques for GI, namely the group-theoretic techniques and the combinatorial ones, also have corresponding techniques in the TI setting, although they are perhaps more complicated and less efficient than in the setting of GI. We explain this in detail in Sec. 1.6.2. Such considerations lead us to believe that TI is harder than GI both in theory and in practice, though at present it is not clear to us how to prove this formally.

This theory for TI is far from complete, and many questions remain, largely inspired by the study of GI. In Sec. 7, we first discuss on a possible theory of universality for basis-explicit linear structures, in analogy with explicit combinatorial structures [109, Section 15]. While not yet complete, this is another exciting reason to study TENSOR ISOMORPHISM and related problems, and it motivates some interesting open questions. Then we pose several natural open problems.

1.6. More related works and further discussions.

1.6.1. Further related works. While most of the related works have already been introduced before, we collect some of the key ones here for further discussions and comparisons.

The most closely related work is that of Futorny, Grochow, and Sergeichuk [42]. They show that a large family of isomorphism problems on 3-way arrays—including those involving multiple 3-way arrays simultaneously, or 3-way arrays that are partitioned into blocks, or 3-way arrays where some of the blocks or sides are acted on by the same group (e. g., MATRIX SPACE ISOMETRY)—all reduce to 3TI. Our work complements theirs in that all our reductions for Thm. B go in the opposite direction, reducing 3TI to other problems. Furthermore, the resulting 3-way arrays from our reductions for Thm. B usually satisfy certain structural constraints, which allows for versatile mathematical interpretations. Some of our other results relate GI and CODE EQUIVALENCE to 3TI; the latter problems were not considered in [42]. Thm. A considers d-tensors for any $d \geq 3$,

[5]Indeed, the current-best upper bounds on these two problems are now quite close: $n^{O(\log n)}$ for GPI (originally due to [39, 78] – Miller attributes this to Tarjan – with improved constants [89, 90, 105]), and $n^{O(\log^2 n)}$ for GI [6] (see [53] for calculation of the exponent).

[6]Specifically, solving ALTERNATING MATRIX SPACE ISOMETRY over $\mathbb{F}_p$ in time $p^{O(n+m)}$ is equivalent to testing isomorphism for p-groups of class 2 and exponent p in time polynomial in the group order, i.e. polynomial time in the Cayley table model.

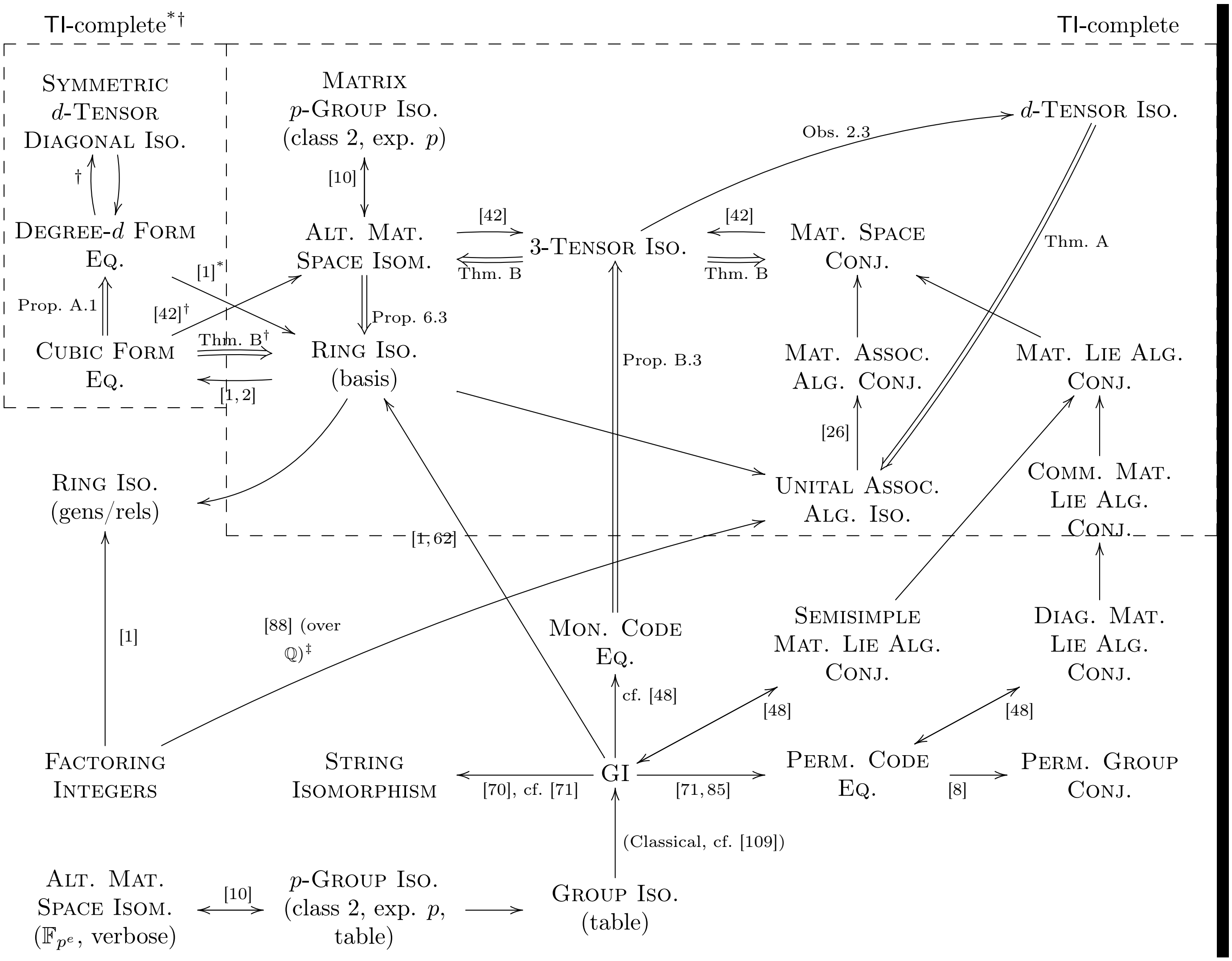


Fig. 1. *Summary of key isomorphism problems.* $A \to B$ *indicates that* A *reduces to* B*, i. e.,* $A \leq_m^p B$*.* $A \Rightarrow B$ *indicates a new result. Unattributed arrows indicate* A *is clearly a special case of* B*. Note that the definition of ring used in [1] is commutative, finite, and unital; by "algebra" we mean an algebra (not necessarily associative, let alone commutative nor unital) over a field. The reductions between* Ring Iso. *(in the basis representation) and* Degree-d Form Eq. *and* Unital Associative Algebra Isomorphism *are for rings over a field. The equivalences between* Alternating Matrix Space Isometry *and* p-Group Isomorphism *are for matrix spaces over* $\mathbb{F}_{p^e}$*. Some* TI*-complete problems from Thm. B are left out for clarity.*

* *These results only hold over fields where every element has a dth root. In particular,* Degree d Form Equivalence *and* Symmetric d-Tensor Isomorphism *are* TI*-complete over fields with* d*-th roots. A finite field* $\mathbb{F}_q$ *has this property if and only if* d *is coprime to* $q-1$*.*

† *These results only hold over rings where* $d!$ *is a unit.*

‡ *Assuming the Generalized Riemann Hypothesis, Rónyai [88] shows a Las Vegas randomized polynomial-time reduction from factoring square-free integers—probably not much easier than the general case—to isomorphism of 4-dimensional algebras over* $\mathbb{Q}$*. Despite the additional hypotheses, this is notable as the target of the reduction is algebras of* constant *dimension, in contrast to all other reductions in this figure.*

which were not considered in [42].

In [1, 2], Agrawal and Saxena considered Cubic Form Equivalence and testing isomorphism of commutative, associative, unital algebras. They showed that GI reduces to Algebra Isomorphism; Commutative Algebra Isomorphism reduces to Cubic Form Equivalence; and Homogeneous Degree-d Form Equivalence reduces to Algebra Isomorphism assuming that the underlying field has dth root for every field element. By combining a reduction from [42], Prop. 5.1, and Cor. 6.5, we get a new reduction from Cubic Form Equivalence to Algebra Isomorphism that works over any field in which 3! is a unit, which is fields of characteristic 0 or $p > 3$.

There are several other works which consider related isomorphism problems. Grigoriev [47] showed that GI is equivalent to isomorphism of unital, associative algebras A such that the radical $R(A)$ squares to zero and $A/R(A)$ is abelian. Interestingly, we show TI-completeness for *conjugacy* of *matrix* algebras with the same abstract structure (even when $A/R(A)$ is only 1-dimensional). Note the latter problem is equivalent to asking whether two representations of A are equivalent up to automorphisms of A. The proof of Thm. A uses algebras in which $R(A)^d = 0$ when reducing from dTI; it also uses Grigoriev's result in one step. For isomorphism problems where the group acting is a complex torus $(\mathbb{C}^\times)^d = \mathrm{GL}_1(\mathbb{C})^d$, Bürgisser, Doğan, Makam, Walter, and Wigderson [27] solve the problem in polynomial time. Their results seem incomparable to ours: they consider arbitrary actions of complex tori, whereas we consider only certain actions of direct products of $\mathrm{GL}_n(\mathbb{F})$ for larger n and arbitrary fields $\mathbb{F}$.

If we ask when two representations of a finitely generated algebra are equivalent (*not* up to automorphisms of A, only up to the usual basis change in the vector space being acted on), Brooksbank and Luks [23] give a polynomial-time algorithm; Chistov, Ivanyos, and Karpinski [31] give an alternative polynomial-time algorithm for the same problem over finite fields, or the algebraic or real closure of a number field. These algorithms also handle simultaneous conjugacy or equivalence of matrix tuples (rather than matrix spaces, as we consider here). A normal form for these problems are constructed by [97].

Brooksbank and Wilson [26] showed a reduction from Associative Algebra Isomorphism (when given by structure constants) to Matrix Algebra Conjugacy. Grochow [48], among other things, showed that GI and CodeEq reduce to Matrix Lie Algebra Conjugacy, which is a special case of Matrix Space Conjugacy.

In [62], Kayal and Saxena considered testing isomorphism of finite rings when the rings are given by structure constants. This problem generalizes testing isomorphism of algebras over finite fields. They put this problem in $\mathsf{NP}\cap\mathsf{coAM}$ [62, Thm. 4.1], reduce GI to this problem [62, Thm. 4.4], and prove that counting the number of ring automorphism (#RA) is in $\mathsf{FP}^{\mathsf{AM}\cap\mathsf{coAM}}$ [62, Thm. 5.1]. They also present a ZPP reduction from GI to #RA, and show that the decision version of the ring automorphism problem is in P.

1.6.2. Combinatorial and group-theoretic techniques for GI and TI. Comparing with Graph Isomorphism also offers one way to see why isomorphism problems for 3-way arrays are difficult. Indeed, the techniques for GI face great difficulty when dealing with isomorphism problems for multi-way arrays. Recall that most algorithms for GI, including Babai's [6], are built on two families of techniques: group-theoretic, and combinatorial. One of the main differences is that the underlying group action for GI is a permutation group acting on a combinatorial structure, whereas the underlying group actions for isomorphism problems for 3-way arrays are matrix groups acting on (multi)linear structures.

Already in moving from permutation groups to matrix groups, we find many new computational difficulties that arise naturally in basic subroutines used in isomorphism testing. For example, the membership problem for permutation groups is well-known to be efficiently solvable by Sims's algorithm [98] (see, e. g., [95] for a textbook treatment), while for matrix groups this was only recently shown to be solvable with a number-theoretic oracle over finite fields of odd characteristic [7]. Correspondingly, when moving from combinatorial structures to (multi)linear algebraic structures, we also find severe limitation on the use of most combinatorial techniques, like individualizing a vertex. For example, it is quite expensive to enumerate all vectors in a vector space, while it is usually considered efficient to go through all elements in a set. Similarly, within a set, any subset has a unique complement, whereas within $\mathbb{F}_q^n$, a subspace can have up to $q^{\Theta(n^2)}$ complements.

Given all the differences between the combinatorial and linear-algebraic worlds, it may be surprising that combinatorial techniques for Graph Isomorphism can nonetheless be useful for Group Isomorphism. Indeed, Li and Qiao [69] adapted the individualisation and refinement technique, as used by Babai, Erdős and Selkow [9], to tackle Alternating Matrix Space Isometry over $\mathbb{F}_q$. This algorithm was recently shown [22] to practically improve over the default algorithms in Magma [19]. However, this technique, though helpful to improve from the brute-force $q^{n^2} \cdot \mathrm{poly}(n, \log q)$ time, seems still limited to getting *average-case* $q^{O(n)}$-time algorithms.

1.7. Organization of the paper. In Sec. 2 we present certain preliminaries. In Sec. 3, we first present a more detailed version of Thm. 1.4 (Thm. B). For this, we give a detailed introduction to more isomorphism problems on 3-way arrays, and their algebraic and geometric interpretations in Sec. 2.2. We prove Thm. A in Sec. 4. We then present the proof for Thm. B in Sec. 5 and 6. In Sec. 7, we put forward a theory of universality for basis-explicit linear structures, in analogy with [109]. We also propose several open problems for further study.

In Appendix A we give a reduction from Cubic Form Equivalence to Degree-d Form Equivalence for any $d \geq 3$ (for $d > 6$ this is easy; for $d = 4$ it requires some work). In Appendix B we present the reductions from Graph Isomorphism and CodeEq to Tensor Isomorphism.

2. Preliminaries.

Font	Object	Space of objects
$A, B, \dots$	matrix	$\mathrm{M}(n,\mathbb{F})$ or $\mathrm{M}(\ell \times n,\mathbb{F})$
$\mathbf{A}, \mathbf{B}, \dots$	matrix tuple	$\mathrm{M}(n,\mathbb{F})^m$ or $\mathrm{M}(\ell \times n,\mathbb{F})^m$
$\mathcal{A}, \mathcal{B}, \dots$	matrix space	[Subspaces of $\mathrm{M}(n,\mathbb{F})$ or $\Lambda(n,\mathbb{F})$]
$\mathtt{A}, \mathtt{B}, \dots$	3-way array	$\mathrm{T}(\ell \times n \times m,\mathbb{F})$

Table 1
Summary of notation related to 3-way arrays and tensors.

2.1. Notation, and review of some mathematical notions.

Vector spaces. Let $\mathbb{F}$ be a field. In this paper we only consider finite-dimensional vector spaces over $\mathbb{F}$. We use $\mathbb{F}^n$ to denote the vector space of length-n *column* vectors. The ith standard basis vector of $\mathbb{F}^n$ is denoted as $\vec{e_i}$. Depending on the context, $\mathbf{0}$ may denote the zero vector space, a zero vector, or an all-zero matrix. Let S be a subset of vectors. We use $\langle S \rangle$ to denote the subspace spanned by elements in S.

Matrices. Let $\mathrm{M}(\ell \times n,\mathbb{F})$ be the linear space of $\ell \times n$ matrices over $\mathbb{F}$, and $\mathrm{M}(n,\mathbb{F}) := \mathrm{M}(n \times n,\mathbb{F})$. Given $A \in \mathrm{M}(\ell \times n,\mathbb{F})$, A^t denotes the transpose of A.

A matrix $A \in \mathrm{M}(n,\mathbb{F})$ is *symmetric*, if for any $u, v \in \mathbb{F}^n$, $u^t A v = v^t A u$, or equivalently $A = A^t$. That is, A represents a symmetric bilinear form. A matrix $A \in \mathrm{M}(n,\mathbb{F})$ is *alternating*, if for any

$u \in \mathbb{F}^n$, $u^t A u = 0$. That is, A represents an alternating bilinear form. Note that in characteristic $\neq 2$, alternating is the same as skew-symmetric, but in characteristic 2 they differ (in characteristic 2, skew-symmetric=symmetric). The linear space of $n \times n$ alternating matrices over $\mathbb{F}$ is denoted by $\Lambda(n, \mathbb{F})$.

The $n \times n$ *identity matrix* is denoted by I_n, and when n is clear from the context, we may just write I. The *elementary matrix* $E_{i,j}$ is the matrix with the (i, j)th entry being 1, and other entries being 0. The (i, j)*-th elementary alternating matrix* is the matrix $E_{i,j} - E_{j,i}$.

Some groups. The general linear group of degree n over a field $\mathbb{F}$ is denoted by $\mathrm{GL}(n, \mathbb{F})$. The symmetric group of degree n is denoted by S_n. The natural embedding of S_n into $\mathrm{GL}(n, \mathbb{F})$ is to represent permutations by permutation matrices. A monomial matrix in $\mathrm{M}(n, \mathbb{F})$ is a matrix where each row and each column has exactly one non-zero entry. All monomial matrices form a subgroup of $\mathrm{GL}(n, \mathbb{F})$ which we call the monomial subgroup, denoted by $\mathrm{Mon}(n, \mathbb{F})$, which is isomorphic to the semi-direct product $\mathbb{F}^n \rtimes S_n$. The subgroup of $\mathrm{GL}(n, \mathbb{F})$ consisting diagonal matrices is called the diagonal subgroup, denoted by $\mathrm{diag}(n, \mathbb{F})$.

Nilpotent groups. If A, B are two subsets of a group G, then $[A, B]$ denotes the sub*group* generated by all elements of the form $[a, b] = aba^{-1}b^{-1}$, for $a \in A, b \in B$. The *lower central series* of a group G is defined as follows: $\gamma_1(G) = G$, $\gamma_{k+1}(G) = [\gamma_k(G), G]$. A group is *nilpotent* if there is some c such that $\gamma_{c+1}(G) = 1$; the smallest such c is called the *nilpotency class* of G, or sometimes just "class" when it is understood from context. A finite group is nilpotent if and only if it is the product of its Sylow subgroups; in particular, all groups of prime power order are nilpotent.

Matrix tuples. We use $\mathrm{M}(\ell \times n, \mathbb{F})^m$ to denote the linear space of m-tuples of $\ell \times n$ matrices. Boldface letters like $\mathbf{A}$ and $\mathbf{B}$ denote matrix tuples. Let $\mathbf{A} = (A_1, \dots, A_m), \mathbf{B} = (B_1, \dots, B_m) \in \mathrm{M}(\ell \times n, \mathbb{F})^m$. Given $P \in \mathrm{M}(\ell, \mathbb{F})$ and $Q \in \mathrm{M}(n, \mathbb{F})$, $P\mathbf{A}Q := (PA_1Q, \dots, PA_mQ) \in \mathrm{M}(\ell, \mathbb{F})$. Given $R = (r_{i,j})_{i,j \in [m]} \in \mathrm{M}(m, \mathbb{F})$, $\mathbf{A}^R := (A'_1, \dots, A'_m) \in \mathrm{M}(m, \mathbb{F})$ where $A'_i = \sum_{j \in [m]} r_{j,i} A_j$.

REMARK 2.1. *In particular, note that A'_i corresponds to the entries in the ith* column *of R. While this choice is immaterial (we could have chosen the opposite convention), all of our later calculations are consistent with this convention.*

Given $\mathbf{A}, \mathbf{B} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$, we say that $\mathbf{A}$ and $\mathbf{B}$ are *equivalent*, if there exist $P \in \mathrm{GL}(\ell, \mathbb{F})$ and $Q \in \mathrm{GL}(n, \mathbb{F})$, such that $P\mathbf{A}Q = \mathbf{B}$. Let $\mathbf{A}, \mathbf{B} \in \mathrm{M}(n, \mathbb{F})^m$. Then $\mathbf{A}$ and $\mathbf{B}$ are *conjugate*, if there exists $P \in \mathrm{GL}(n, \mathbb{F})$, such that $P^{-1}\mathbf{A}P = \mathbf{B}$. And $\mathbf{A}$ and $\mathbf{B}$ are *isometric*, if there exists $P \in \mathrm{GL}(n, \mathbb{F})$, such that $P^t\mathbf{A}P = \mathbf{B}$. Finally, $\mathbf{A}$ and $\mathbf{B}$ are pseudo-isometric, if there exist $P \in \mathrm{GL}(n, \mathbb{F})$ and $R \in \mathrm{GL}(m, \mathbb{F})$, such that $P^t\mathbf{A}P = \mathbf{B}^R$.

Matrix spaces. Linear subspaces of $\mathrm{M}(\ell \times n, \mathbb{F})$ are called matrix spaces. Calligraphic letters like $\mathcal{A}$ and $\mathcal{B}$ denote matrix spaces. By a slight abuse of notation, for $\mathbf{A} \in \mathrm{M}(\ell \times n, \mathbb{F})^m$, we use $\langle \mathbf{A} \rangle$ to denote the subspace spanned by those matrices in $\mathbf{A}$.

3-way arrays. Let $\mathrm{T}(\ell \times n \times m, \mathbb{F})$ be the linear space of $\ell \times n \times m$ 3-way arrays over $\mathbb{F}$. We use the fixed-width teletype font for 3-way arrays, like $\mathtt{A}$, $\mathtt{B}$, etc..

Given $\mathtt{A} \in \mathrm{T}(\ell \times n \times m, \mathbb{F})$, we can think of $\mathtt{A}$ as a 3-dimensional table, where the (i, j, k)th entry is denoted as $\mathtt{A}(i, j, k) \in \mathbb{F}$. We can slice $\mathtt{A}$ along one direction and obtain several matrices, which are then called slices. For example, slicing along the first coordinate, we obtain the *horizontal* slices, namely ℓ matrices $A_1, \dots, A_\ell \in \mathrm{M}(n \times m, \mathbb{F})$, where $A_i(j, k) = \mathtt{A}(i, j, k)$. Similarly, we also obtain the *lateral* slices by slicing along the second coordinate, and the *frontal* slices by slicing along the third coordinate.

We will often represent a 3-way array as a matrix whose entries are vectors. That is, given

$\mathtt{A} \in \mathrm{T}(\ell \times n \times m, \mathbb{F})$, we can write

$$\mathtt{A} = \begin{bmatrix} w_{1,1} & w_{1,2} & \dots & w_{1,n} \\ w_{2,1} & w_{2,2} & \dots & w_{2,n} \\ \vdots & \ddots & \ddots & \vdots \\ w_{\ell,1} & w_{\ell,2} & \dots & w_{\ell,n} \end{bmatrix},$$

where $w_{i,j} \in \mathbb{F}^m$, so that $w_{i,j}(k) = \mathtt{A}(i,j,k)$. Note that, while $w_{i,j} \in \mathbb{F}^m$ are column vectors, in the above representation of $\mathtt{A}$, we should think of them as along the direction "orthogonal to the paper." Following [66], we call $w_{i,j}$ the *tube fibers* of $\mathtt{A}$. Similarly, we can have the *row fibers* $v_{i,k} \in \mathbb{F}^n$ such that $v_{i,k}(j) = \mathtt{A}(i,j,k)$, and the *column fibers* $u_{j,k} \in \mathbb{F}^\ell$ such that $u_{j,k}(i) = \mathtt{A}(i,j,k)$.

Given $P \in \mathrm{M}(\ell, \mathbb{F})$ and $Q \in \mathrm{M}(n, \mathbb{F})$, let $P\mathtt{A}Q$ be the $\ell \times n \times m$ 3-way array whose kth frontal slice is PA_kQ. For $R = (r_{i,j}) \in \mathrm{GL}(m, \mathbb{F})$, let $\mathtt{A}^R$ be the $\ell \times n \times m$ 3-way array whose kth frontal slice is $\sum_{k' \in [m]} r_{k',k} A_{k'}$. Note that these notations are consistent with the notations for matrix tuples above, when we consider the matrix tuple $\mathbf{A} = (A_1, \dots, A_k)$ of frontal slices of $\mathtt{A}$.

Let $\mathtt{A} \in \mathrm{T}(\ell \times n \times m, \mathbb{F})$ be a 3-way array. We say that $\mathtt{A}$ is *non-degenerate* as a 3-tensor if the horizontal slices of $\mathtt{A}$ are linearly independent, the lateral slices are linearly independent, and the frontal slices are linearly independent. Let $\mathbf{A} = (A_1, \dots, A_m) \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ be a matrix tuple consisting of the frontal slices of $\mathtt{A}$. Then it is easy to see that the frontal slices of $\mathtt{A}$ are linearly independent if and only if $\dim(\langle \mathbf{A} \rangle) = m$. The lateral (resp., horizontal) slices of $\mathtt{A}$ are linearly independent if and only if the intersection of the right (resp., left) kernels of A_i is zero.

OBSERVATION 2.2. *There is a polynomial-time function r that takes 3-way arrays to non-degenerate 3-way arrays, and such that $\mathtt{A} \cong \mathtt{B}$ as 3-tensors if and only if $r(\mathtt{A}) \cong r(\mathtt{B})$ as 3-tensors.*

Multi-way arrays. For $d \geq 3$, we use similar notation to 3-way arrays, which we will not belabor. Here we merely observe:

OBSERVATION 2.3. *For any $d' \geq d$, d-TI reduces to d'-TI.*

Proof. Given an $n_1 \times \cdots \times n_d$ d-way array $\mathtt{A}$, we may treat it as a d'-way array $\tilde{\mathtt{A}}$ of format $n_1 \times \cdots \times n_d \times 1 \times 1 \times \cdots \times 1$. If $\mathtt{A} \cong \mathtt{B}$ as d-tensors, say via $(P_1, \dots, P_d)$, then $\tilde{\mathtt{A}} \cong \tilde{\mathtt{B}}$ as d'-tensors via $(P_1, \dots, P_d, 1, 1, \dots, 1)$. Conversely, if $\tilde{\mathtt{A}} \cong \tilde{\mathtt{B}}$ via $(P_1, \dots, P_d, \alpha_{d+1}, \dots, \alpha_{d'})$, then $\mathtt{A} \cong \mathtt{B}$ via $(\alpha_{d+1}\alpha_{d+2} \cdots \alpha_{d'} P_1, \dots, P_d)$. That is, all that can "go wrong" under this embedding is multiplication by scalars, but those scalars can be absorbed into any one of the P_i. ∎

Algebras and their algorithmic representations. An algebra A consists of a vector space V and a bilinear map $\circ : V \times V \to V$. This bilinear map defines the product $\circ$ in this algebra. Note that we do not assume A to be unital (having an identity), associative, alternating, nor satisfying the Jacobi identity. In the literature, an algebra without such properties is sometimes called a non-associative algebra (but also, as usual, associative algebras are a special case of non-associative algebras).

As in Section 1, after fixing an ordered basis $(b_1, \dots, b_n)$ where $b_i \in \mathbb{F}^n$ of $V \cong \mathbb{F}^n$, this bilinear map $\circ$ can be represented by an $n \times n \times n$ 3-way array $\mathtt{A}$, such that $b_i \circ b_j = \sum_{k \in [n]} \mathtt{A}(i,j,k) b_k$. This is the structure constant representation of $\mathtt{A}$. Algorithms for associative algebras and Lie algebras have been studied intensively in this model, e. g., [33, 58].

It is also natural to consider matrix spaces that are closed under multiplication or commutator. More specifically, let $\mathcal{A} \subseteq \mathrm{M}(n, \mathbb{F})$ be a matrix space. If $\mathcal{A}$ is closed under multiplication, that is, for any $A, B \in \mathcal{A}$, $AB \in \mathcal{A}$, then $\mathcal{A}$ is a matrix (associative) algebra with the product being the matrix multiplication. If $\mathcal{A}$ is closed under commutator, that is, for any $A, B \in \mathcal{A}$, $[A, B] = AB - BA \in \mathcal{A}$, then $\mathcal{A}$ is a matrix Lie algebra with the product being the commutator. Algorithms for matrix algebras and matrix Lie algebras have also been studied, e. g., [37, 55, 58].

2.2. Tensor notation, five group actions on 3-way arrays, and the corresponding mathematical objects. In Section 1.2, we briefly defined five group actions on 3-way arrays with the help of Equation 1.1. However, the formulas for these group actions on 3-way arrays are somewhat unwieldy; our experience suggests that they are more easily digested when presented in the context of some of the natural interpretations of 3-way arrays as mathematical objects, which will also allow us to connect them back to the problems of Section 1.1. In the case of 3-way arrays, we will see below several interpretations of the action (1.1).

3-tensors. A 3-way array $\mathtt{A}(i,j,k)$, where $i \in [\ell]$, $j \in [n]$, and $k \in [m]$, is naturally identified as a vector in $\mathbb{F}^\ell \otimes \mathbb{F}^n \otimes \mathbb{F}^m$. Letting $\vec{e_i}$ denote the ith standard basis vector of $\mathbb{F}^n$, a standard basis of $\mathbb{F}^\ell \otimes \mathbb{F}^n \otimes \mathbb{F}^m$ is $\{\vec{e_i} \otimes \vec{e_j} \otimes \vec{e_k}\}$. Then $\mathtt{A}$ represents the vector $\sum_{i,j,k} \mathtt{A}(i,j,k)\vec{e_i} \otimes \vec{e_j} \otimes \vec{e_k}$ in $\mathbb{F}^\ell \otimes \mathbb{F}^n \otimes \mathbb{F}^m$. The natural action (1.1) by $\mathrm{GL}(\ell,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F}) \times \mathrm{GL}(m,\mathbb{F})$ corresponds to changes of basis of the three vector spaces in the tensor product. The problem of deciding whether two 3-way arrays are the same under this action is called 3-TENSOR ISOMORPHISM.[7] This problem has been studied as far back as the 1930s [83].

Cubic forms, trilinear forms, and tensor congruence. From a 3-way array $\mathtt{A}$ we can also construct a cubic form (=homogeneous degree 3 polynomial) $\sum_{i,j,k} \mathtt{A}(i,j,k)x_i x_j x_k$, where x_i are formal variables. If we consider the variables as commuting—or, equivalently, if $\mathtt{A}$ is symmetric, meaning it is unchanged by permuting its three indices—we get an ordinary cubic form; if we consider them as non-commuting, we get a trilinear form (or "non-commutative cubic form"). In either case, the natural notion of isomorphism here comes from the action of $\mathrm{GL}(n,\mathbb{F})$ on the n variables x_i, in which $P \in \mathrm{GL}(n,\mathbb{F})$ transforms the preceding form into $\sum_{ijk} \mathtt{A}(i,j,k)(\sum_{i'} P_{ii'}x_{i'})(\sum_{j'} P_{jj'}x_{j'})(\sum_{k'} P_{kk'}x_{k'})$. In terms of 3-way arrays, we get $(P \cdot \mathtt{A})(i',j',k') = \sum_{ijk} \mathtt{A}(i,j,k)P_{ii'}P_{jj'}P_{kk'}$. The corresponding isomorphism problems are called CUBIC FORM EQUIVALENCE (in the commutative case) and TRILINEAR FORM EQUIVALENCE. This is identical to the TENSOR CONGRUENCE problem from [86] (where they worked over $\mathbb{R}$).

Matrix spaces. Given a 3-way array $\mathtt{A}$, it is natural to consider the linear span of its frontal slices, $\mathcal{A} = \langle A_1, \dots, A_m \rangle$, also called a *matrix space*. One convenience of this viewpoint is that the action of $\mathrm{GL}(m,\mathbb{F})$ becomes implicit: it corresponds to change of basis *within* the matrix space $\mathcal{A}$. This allows us to generalize the three natural equivalence relations on matrices to matrix spaces: (1) two $\ell \times n$ matrix spaces $\mathcal{A}$ and $\mathcal{B}$ are *equivalent* if there exists $(P,Q) \in \mathrm{GL}(\ell,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F})$ such that $P\mathcal{A}Q = \mathcal{B}$, where $P\mathcal{A}Q := \{PAQ : A \in \mathcal{A}\}$; (2) two $n \times n$ matrix spaces $\mathcal{A}, \mathcal{B}$ are *conjugate* if there exists $P \in \mathrm{GL}(n,\mathbb{F})$ such that $P\mathcal{A}P^{-1} = \mathcal{B}$; and (3) they are *isometric* if $P\mathcal{A}P^t = \mathcal{B}$. The corresponding decision problems, when $\mathcal{A}$ is given by a basis $A_1, \dots, A_d$, are MATRIX SPACE EQUIVALENCE, MATRIX SPACE CONJUGACY, and MATRIX SPACE ISOMETRY, respectively.

As in the case of isometry of matrices, wherein skew-symmetric and symmetric matrices play a special role, the same is true for isometry of matrix spaces. We say a matrix space $\mathcal{A}$ is symmetric if every matrix $A \in \mathcal{A}$ is symmetric, and similarly for skew-symmetric or alternating. SYMMETRIC MATRIX SPACE ISOMETRY is equivalent to the IP2S problem (discussed in Section 1.1). ALTERNATING MATRIX SPACE ISOMETRY is another particular case of interest, being in many ways a linear-algebraic analogue of GI [69], in addition to its close relation with GROUP ISOMORPHISM for

[7] Some authors call this TENSOR EQUIVALENCE; we use "ISOMORPHISM" both because this is the natural notion of isomorphism for such objects, and because we will be considering many different equivalence relations on essentially the same underlying objects.

p-groups of class 2 and exponent p, which we discuss below.

Interesting cases of Matrix Space Conjugacy arise naturally whenever we have an algebra A (say, associative or Lie) that is given to us as a subalgebra of the algebra $\mathrm{M}(n, \mathbb{F})$ of $n \times n$ matrices. Two such matrix algebras can be isomorphic as abstract algebras, but the more natural notion of "isomorphism of matrix algebras" is that of conjugacy, which respects both the algebra structure and the presentation in terms of matrices. This is the linear-algebraic analogue of permutational isomorphism (=conjugacy) of permutation groups, and has been studied for matrix Lie algebras [48] and associative matrix algebras [26]. (For those who know what a representation is: it also turns out to be equivalent to asking whether two representations of an algebra A are equivalent up to automorphisms of A, a problem which naturally arises as a subroutine in, e. g., Group Isomorphism, where it is often known as Action Compatibility, e. g., [49].)

Bilinear and quadratic maps. From an $\ell \times n \times m$ 3-way array $\mathtt{A}$, we may also construct a bilinear map (=system of m bilinear forms) $f_{\mathtt{A}} : \mathbb{F}^\ell \times \mathbb{F}^n \to \mathbb{F}^m$, sending $(u, v) \in \mathbb{F}^\ell \times \mathbb{F}^n$ to $(u^t A_1 v, \dots, u^t A_m v)^t$, where the A_k are the frontal slices of $\mathtt{A}$. The group action defining Matrix Space Equivalence is equivalent to the action of $\mathrm{GL}(\ell, \mathbb{F}) \times \mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$ on such bilinear maps. This problem was recently studied under the name "testing isotopism of bilinear maps" in [21], in the context of testing isomorphism of graded algebras.

If, in the above, we have $\ell = n$ and we treat the two input spaces as the same, we may consider the natural action of $\mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$ on such bilinear maps. Two such bilinear maps that are essentially the same up to basis changes in $\mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$ are sometimes called pseudo-isometric [25].

Finite p-groups. When the frontal slices A_k are skew-symmetric, Baer's correspondence [10] gives a bijection between finite p-groups of class 2 and exponent p, that is, in which $g^p = 1$ for all g and in which $[G, G] \le Z(G)$, and their corresponding skew-symmetric bilinear maps $G/Z(G) \times G/Z(G) \to [G, G]$, given by $(gZ(G), hZ(G)) \mapsto [g, h] = ghg^{-1}h^{-1}$. Two such groups are isomorphic if and only if their corresponding bilinear maps are pseudo-isometric, if and only if, using the matrix space terminology, the matrix spaces they span are isometric.

Algebras. We may also consider a 3-way array $\mathtt{A}(i, j, k)$, $i, j, k \in [n]$, as the structure constants of an algebra (which need not be associative, commutative, nor unital), say with basis $x_1, \dots, x_n$, and with multiplication given by $x_i \cdot x_j = \sum_k \mathtt{A}(i, j, k) x_k$, and then extended (bi)linearly. Here the natural notion of equivalence comes from the action of $\mathrm{GL}(n, \mathbb{F})$ by change of basis on the x_i. Despite the seeming similarity of this action to that on cubic forms, it turns out to be quite different: given $P \in \mathrm{GL}(n, \mathbb{F})$, let $\vec{x}' = P\vec{x}$; then we have $x'_i \cdot x'_j = (\sum_i P_{i'i} x_i) \cdot (\sum_j P_{j'j} x_j) = \sum_{i,j} P_{i'i} P_{j'j} x_i \cdot x_j = \sum_{i,j,k} P_{i'i} P_{j'j} \mathtt{A}(i, j, k) x_k = \sum_{i,j,k} P_{i'i} P_{j'j} \mathtt{A}(i, j, k) \sum_{k'} (P^{-1})_{kk'} x_{k'}$. Thus $\mathtt{A}$ becomes $(P \cdot \mathtt{A})(i', j', k') = \sum_{ijk} \mathtt{A}(i, j, k) P_{i'i} P_{j'j} (P^{-1})_{kk'}$. The inverse in the third factor here is the crucial difference between this case and that of cubic or trilinear forms above, similar to the difference between matrix conjugacy and matrix isometry. The corresponding isomorphism problem is called Algebra Isomorphism.

Special cases of Algebra Isomorphism that are of interest include those of unital, associative algebras (commutative, e. g., as studied in [1, 2, 62], and non-commutative, such as group algebras) and Lie algebras.

Summary of the problems. The isomorphism problems of the above structures all have 3-way arrays as the underlying object, but are determined by different group actions. It is not hard to see that there are essentially five group actions in total: 3-Tensor Isomorphism, Matrix Space Conjugacy, Matrix Space Isometry, Trilinear Form Equivalence, and Algebra Isomorphism. It turns out that these cover all the natural isomorphism problems on 3-way arrays in which the group acting is a product of $\mathrm{GL}(n,\mathbb{F})$ (where n is the side length of the arrays), which we discuss next.

Tensor notation. To see that aforementioned problems exhaust the distinct isomorphism problems coming from change-of-basis on 3-way arrays (without introducing multiple arrays, or block structure, or going to subgroups of $\mathrm{GL}(n,\mathbb{F})$), and to keep track of the relation between all the above problems, we use standard mathematical notation for spaces of tensors (however, we won't actually need the full abstract definition here; for a formal introduction see, e. g., [68]).

Much as the three natural equivalence relations on matrices differ by how the groups act on the rows and columns, the same is true for tensors, but on the rows, columns, and depths (the "row-like" sub-arrays which are "perpendicular to the page"). There are two aspects to the notation: first, we keep track of which group is acting where by introducing names U, V, W for the different vector spaces involved (this is also the standard basis-free notation, e. g., [68]) and the groups acting on them, viz. $\mathrm{GL}(U), \mathrm{GL}(V), \mathrm{GL}(W)$, etc. Thus, while it is possible that $\dim U = \dim V$ and thus $\mathrm{GL}(U) \cong \mathrm{GL}(V)$, the notation helps make clear which group is acting where. Second, to take into account the contragradient ("inverse") action, given a vector space V, V^* denotes its dual space, consisting of the linear functions $V \to \mathbb{F}$. $\mathrm{GL}(V)$ acts on V^* by sending a linear function $\ell \in V^*$ to the function $(g \cdot \ell)(v) = \ell(g^{-1}(v))$. In this notation, the three different actions on matrices correspond to the notations

$$U \otimes V \text{ (left-right action)} \qquad V \otimes V^* \text{ (conjugacy)} \qquad V \otimes V \text{ (isometry).}$$

When we have a matrix *space* $\mathcal{A} \subseteq M(n \times m, \mathbb{F})$ instead of a single matrix A, we introduce an additional vector space W, which is naturally isomorphic to $\mathcal{A}$ as a vector space. The action of $\mathrm{GL}(W)$ on W serves to change basis *within* the matrix space, while leaving the space itself unchanged. In this notation, the problems we mention above are listed in Table 2.

Notation	Name	Group Action
$U \otimes V \otimes W$	MATRIX SPACE EQUIVALENCE 3-TENSOR ISOMORPHISM	$\mathcal{A} \mapsto g\mathcal{A}h^{-1}$
$V \otimes V \otimes W$	MATRIX SPACE ISOMETRY BILINEAR MAP PSEUDO-ISOMETRY	$\mathcal{A} \mapsto g\mathcal{A}g^T$
$V \otimes V^* \otimes W$	MATRIX SPACE CONJUGACY	$\mathcal{A} \mapsto g\mathcal{A}g^{-1}$
$V \otimes V \otimes V$	TRILINEAR FORM EQUIVALENCE	$f(\vec{x}) \mapsto f(g^{-1}\vec{x})$
$V \otimes V \otimes V^*$	ALGEBRA ISOMORPHISM	$\mu(\vec{x}, \vec{y}) \mapsto g\mu(g^{-1}\vec{x}, g^{-1}\vec{y})$

TABLE 2
The cast of isomorphism problems on 3-way arrays. We show below how this exhausts the possibilities.

To see that the family of problems in Table 2 exhausts the possible isomorphism problems on (undecorated) 3-way arrays, we note that in this notation there are some "different-looking" isomorphism problems that are trivially equivalent. The first is re-ordering the spaces: the isomorphism problem for $V \otimes V \otimes W$ is trivially equivalent to that for $V \otimes W \otimes V$, simply by permuting indices, viz. $\mathtt{A}'(i,j,k) = \mathtt{A}(i,k,j)$. The second is about dual vector spaces. Although a vector space V and its dual V^* are technically different, and the group action differs by an inverse transpose, we can choose bases in V and V^* so that there is a linear isomorphism $V \to V^*$ which induces a bijection between orbits; for example, the orbits of the action $g \cdot A = gAg^t$ are the same as the orbits of the action $g \cdot A = g^{-t}Ag^{-1}$, even though technically the former corresponds to $V \otimes V$ and the latter to $V^* \otimes V^*$. This means that if we are considering the isomorphism problem in a tensor space such as $V \otimes V \otimes W$, we can dualize each of the vector spaces V, W separately, so long as when we do so, we dualize all instances of that vector space. For example, the isomorphism problem in $V \otimes V \otimes W$ is trivially equivalent to that in $V^* \otimes V^* \otimes W$, but is not obviously equivalent to that in $V \otimes V^* \otimes W$ (though we will show such a reduction in this paper). As a consequence, when the action on all three directions comes from the same group, there are only two choices: $V \otimes V \otimes V$ and $V \otimes V \otimes V^*$; the remaining choices are trivially equivalent to one of these two. Using these, we see that the Table 2 in fact covers all possibilities up to these trivial equivalences.

2.3. On the type of reduction. As these problems arise from several different fields, there are various properties one might hope for in the notion of reduction. Most of our reductions satisfy all of the following properties; see Remark 2.5 below for details. The details of this section are not really needed for the rest of the paper; we include it as we have not found these issues discussed in quite this depth, nor something like Definition 2.4 proposed, elsewhere.

Kernel reductions: there is a function r from objects of one type to objects of the other such that $A \sim_1 B$ if and only if $r(A) \sim_2 r(B)$. See [40, 41] for some discussion on the relation between kernel reductions and more general reductions.

Efficiently computable: the function r as above is computable in polynomial time. In fact, we believe, though have not checked fully, that all of our reductions are computable by uniform constant-depth (algebraic) circuits; over finite fields and algebraic number fields, we believe they are in uniform TC^0 (the threshold gates are needed to do some simple arithmetic on the indices). That is, there is a small circuit which, given A, i, j, k as input will output the (i, j, k) entry of the output.

Polynomial-size projections ("p-projections") [101]: each coordinate of the output is either one of the input variables or a constant, and the dimension of the output is polynomially bounded by the dimension of the input. (In fact, in many cases, the dimension of the output is only linearly larger than that of the input.)

Functorial: For each type of tensor there is naturally a category of such tensors (see [74] for generalities on categories). For example, for 3TI, $U \otimes V \otimes W$, the objects of the category are three-tensors, and a morphism between $\mathtt{A} \in U \otimes V \otimes W$ and $\mathtt{B} \in U' \otimes V' \otimes W'$ is given by linear maps $P : U \to U'$, $Q \colon V \to V'$, and $R \colon W \to W'$ such that $(P, Q, R) \cdot \mathtt{A} = \mathtt{B}$. Isomorphism of 3-tensors is the special case when all three of P, Q, R are invertible. Analogous categories can be defined for the other problems we consider, such as $V \otimes V^* \otimes W$. A *functor* between two categories $\mathcal{C}, \mathcal{D}$ is a pair of maps $(r, \overline{r})$ such that (1) r maps objects of $\mathcal{C}$ to objects of $\mathcal{D}$, (2) if $f \colon A \to B$ is a morphism in $\mathcal{C}$, then $\overline{r}(f) \colon r(A) \to r(B)$ is a morphism in $\mathcal{D}$, (3) for any $A \in \mathcal{C}$, $\overline{r}(\mathrm{id}_A) = \mathrm{id}_{r(A)}$, and (4) if $f \colon A \to B$ and $g \colon B \to C$ are morphisms in $\mathcal{C}$, then $\overline{r}(g \circ f) = \overline{r}(g) \circ \overline{r}(f)$.

All our reductions are functorial on the categories in which we only consider isomorphisms; it is interesting to ask whether they are also functorial on the entire categories (that is, including non-invertible homomorphisms). Furthermore, all our reductions yield another map $\overline{s}$ such that for any isomorphism $f' \colon r(A) \to r(B)$, $\overline{s}(f)$ is an isomorphism $A \to B$, and $\overline{s}(\overline{r}(f)) = f$ for any isomorphism $f \colon A \to B$. If we only consider isomorphisms (and not other homomorphisms), nearly all known reductions between isomorphism problems have this form, cf. [5]; an interesting example where this isn't the case is the reduction from 1-Block Conjugacy of shifts of finite type to k-Block Conjugacy [92, Thm. 18].

Containment, in the sense used in the literature on wildness: Briefly speaking, wildness in mathematics aims to understand the "complexity"—in a generalized, geometric sense, not necessarily computational—of classifying orbits under group actions. For example, matrices under the conjugation action over algebraically closed fields are classified according to their Jordan normal forms (this problem is formally said to be tame), while classifying pairs of matrices under the simultaneous conjugation action is known to be complex (e. g., [97]), and classifying tensors up to isomorphism even more complicated still [11]. Wildness is then a notion of completeness or universality for a certain kind of classification problem in this theory, under a kind of reduction or morphism called *containment*. It turns out that classifying pairs of matrices problem is wild or "complete" for a certain widely occurring kind of classification problem. That is, it captures many classification problems for other group actions, or in other words, many classification problems reduce to ("are contained in") this problem.

There are several definitions of containment in the literature which typically are equivalent when restricted to so-called matrix problems. For a few such definitions, see, e. g., [42, Def. 1.2], [97], or [99, Def. XIX.1.3]. For those problems in this paper to which the preceding definitions could apply, our reductions have the defined property. However, since we are working in a slightly more general setting, we would like to suggest the following natural generalization of these notions.

Definition 2.4. *Let $\rho\colon G \to \mathrm{Aut}(V)$ be a rational action of an algebraic group G on an algebraic variety V, and $\sigma\colon H \to \mathrm{Aut}(W)$ another such. We say (G, V) (or the action of G on V, or the classification problem for G-orbits on V) is* algebraically contained in (H, W) *if there is a polynomial morphism $r\colon V \to W$ (each coordinate of the output is given by a polynomial in the coordinates of the input) that is also a kernel reduction, that is, $v, v' \in V$ are in the same G-orbit if and only if $r(v), r(v') \in W$ are in the same H-orbit.*

In our case, all our spaces V, W are affine space $\mathbb{F}^n$ for some n, and our maps r are in fact of degree 1. (It might be interesting to consider whether using higher degree allows for more efficient reductions.) We may also require it to be "functorial" or "equivariant," in the sense that there is a homomorphism of algebraic groups $\overline{r}\colon G \to H$ (simultaneously an algebraic map and a group homomorphism) such that

$$\overline{r}(g) \cdot r(v) = r(g \cdot v).$$

and a section $\overline{s}\colon H \dashrightarrow G$, such that $\overline{s} \circ \overline{r} = \mathrm{id}_G$ and

$$h \cdot r(v) = r(v') \Longrightarrow \overline{s}(h) \circ v = v',$$

where the dashed arrow above indicates that $\overline{s}$ need only be defined on a subset of H, namely, those $h \in H$ such that there exist $v, v' \in V$ with $h \cdot r(v) = r(v')$ (but on this subset it should still act like a homomorphism, in the sense that $\overline{s}(hh') = \overline{s}(h)\overline{s}(h')$).

Remark 2.5. *We believe all of our reductions satisfy all of the above properties, with the possible exceptions that Prop. 5.1 and Prop. 6.1 are only projections and algebraic containments on the set of* non-degenerate *3-tensors. These reductions still satisfy the other three properties on the set of all tensors: They are kernel reductions by construction; non-degeneracy presents no obstacle to polynomial-time computation (Observation 2.2); and two tensors are isomorphic iff their non-degenerate parts are isomorphic, so they are still functorial. The obstacle to being projections or algebraic containments on the set of all 3-tensors here is closely related to the fact that the map sending a matrix to its row echelon form (or even just zero-ing out a number of rows so that the remaining non-zero rows are linearly independent) is neither a projection nor an algebraic map. We would find it interesting if there were reductions for these results satisfying all of the above properties for all 3-tensors.*

3. Full statement of main results.

THEOREM A. *For any fixed $d \geq 1$, d-*TENSOR ISOMORPHISM *reduces to* ALGEBRA ISOMORPHISM.

Combined with the results of [42], this immediately gives:

COROLLARY A. *For any fixed $d \geq 1$, d-*TENSOR ISOMORPHISM *reduces to* 3-TENSOR ISOMORPHISM.

Given the viewpoint of Section 2.2 on the problems from Section 1.1, to show that they are equivalent, it is enough to show that the isomorphism problems for 3-way arrays corresponding to the five group actions are equivalent, where 3-way arrays may also need to satisfy certain structural constraints (e.g., the frontal slices are symmetric or skew-symmetric). This is the content of our second main result.

THEOREM B. 3-TENSOR ISOMORPHISM *reduces to each of the following problems in polynomial time.*

1. GROUP ISOMORPHISM *for p-groups exponent p ($g^p = 1$ for all g) and class 2 ($G/Z(G)$ is abelian) given by generating matrices over $\mathbb{F}_{p^e}$. Here we consider only $\mathsf{3TI}_{\mathbb{F}_{p^e}}$ where p is an odd prime.*
2. MATRIX SPACE ISOMETRY, *even for alternating or symmetric matrix spaces.*
3. MATRIX SPACE CONJUGACY, *and even the special cases:*
   (a) MATRIX LIE ALGEBRA CONJUGACY, *for solvable Lie algebras L of derived length 2.*[8]
   (b) ASSOCIATIVE MATRIX ALGEBRA CONJUGACY.[9]
4. ALGEBRA ISOMORPHISM, *and even the special cases:*
   (a) ASSOCIATIVE ALGEBRA ISOMORPHISM, *for algebras that are commutative and unital, or for algebras that are commutative and 3-nilpotent ($abc = 0$ for all $a, b, c, \in A$)*
   (b) LIE ALGEBRA ISOMORPHISM, *for 2-step nilpotent Lie algebras ($[u, [v, w]] = 0 \ \forall u, v, w$)*
5. CUBIC FORM EQUIVALENCE *and* TRILINEAR FORM EQUIVALENCE.

The algebras in (3) are given by a set of matrices which linearly span the algebra, while in (4) they are given by structure constants (see "Algebras" in Sec. 2.2).

Since the main result of [42] reduces the problems in Theorem B to 3-TENSOR ISOMORPHISM (cf. [42, Rmk. 1.1]), we have:

COROLLARY B. *Each of the problems listed in Theorem B is TI-complete.*[10]

REMARK 3.1. *Here is a brief summary of what is known about the complexity of some of these problems. Over a finite field $\mathbb{F}_q$, these problems are in $\mathsf{NP} \cap \mathsf{coAM}$. For $\ell \times n \times m$ 3-way arrays, the brute-force algorithms run in time $q^{O(\ell^2+n^2+m^2)}$, as $\mathrm{GL}(n, \mathbb{F}_q)$ can be enumerated in time $q^{\Theta(n^2)}$. Note that polynomial-time in the input size here would be $\mathrm{poly}(\ell, n, m, \log q)$. Over any field $\mathbb{F}$, these problems are in $\mathsf{NP}_{\mathbb{F}}$ in the Blum–Shub–Smale model. When the input arrays are over $\mathbb{Q}$ and we ask for isomorphism over $\mathbb{C}$ or $\mathbb{R}$, these problems are in PSPACE using quantifier elimination. By Koiran's celebrated result on Hilbert's Nullstellensatz, for equivalence over $\mathbb{C}$ they are in AM assuming the Generalized Riemann Hypothesis [65]. When the input is over $\mathbb{Q}$ and we ask for equivalence over $\mathbb{Q}$, it is unknown whether these problems are even decidable; classically this is studied under* ALGEBRA ISOMORPHISM *for associative, unital algebras over $\mathbb{Q}$ (see, e. g., [2, 87]), but by Cor. B, the question of decidability is open for all of these problems.*

[8] And even further, where $L/[L, L] \cong \mathbb{F}$.

[9] Even for algebras A whose Jacobson radical $R(A)$ squares to zero and $A/R(A) \cong \mathbb{F}$.

[10] For CUBIC FORM EQUIVALENCE, we only show that it is in $\mathsf{TI}_{\mathbb{F}}$ when $\mathrm{char}\,\mathbb{F} > 3$ or $\mathrm{char}\,\mathbb{F} = 0$.

Over finite fields, several of these problems can be solved efficiently when one of the side lengths of the array is small. For d-dimensional spaces of $n \times n$ matrices, Matrix Space Conjugacy *and* Isometry *can be solved in $q^{O(n^2)} \cdot \mathrm{poly}(d, n, \log q)$ time: once we fix an element of $\mathrm{GL}(n, \mathbb{F}_q)$, the isomorphism problem reduces to solving linear systems of equations. Less trivially,* Matrix Space Conjugacy *can be solved in time $q^{O(d^2)} \cdot \mathrm{poly}(d, n, \log q)$ and* 3TI *for $n \times m \times d$ tensors in time $q^{O(d^2)} \cdot \mathrm{poly}(d, n, m, \log q)$, since once we fix an element of $\mathrm{GL}(d, \mathbb{F}_q)$, the isomorphism problem either becomes an instance of, or reduces to [57],* Module Isomorphism, *which admits several polynomial-time algorithms [23, 31, 56, 97]. Finally, one can solve* Matrix Space Isometry *in time $q^{O(d^2)} \cdot \mathrm{poly}(d, n, \log q)$: once one fixes an element of $\mathrm{GL}(d, \mathbb{F}_q)$, there is a rather involved algorithm [57], which uses the $*$-algebra technique originated from the study of computing with p-groups [25, 104].*

Figure 2 below summarizes where the various parts of Thm. B are proven.

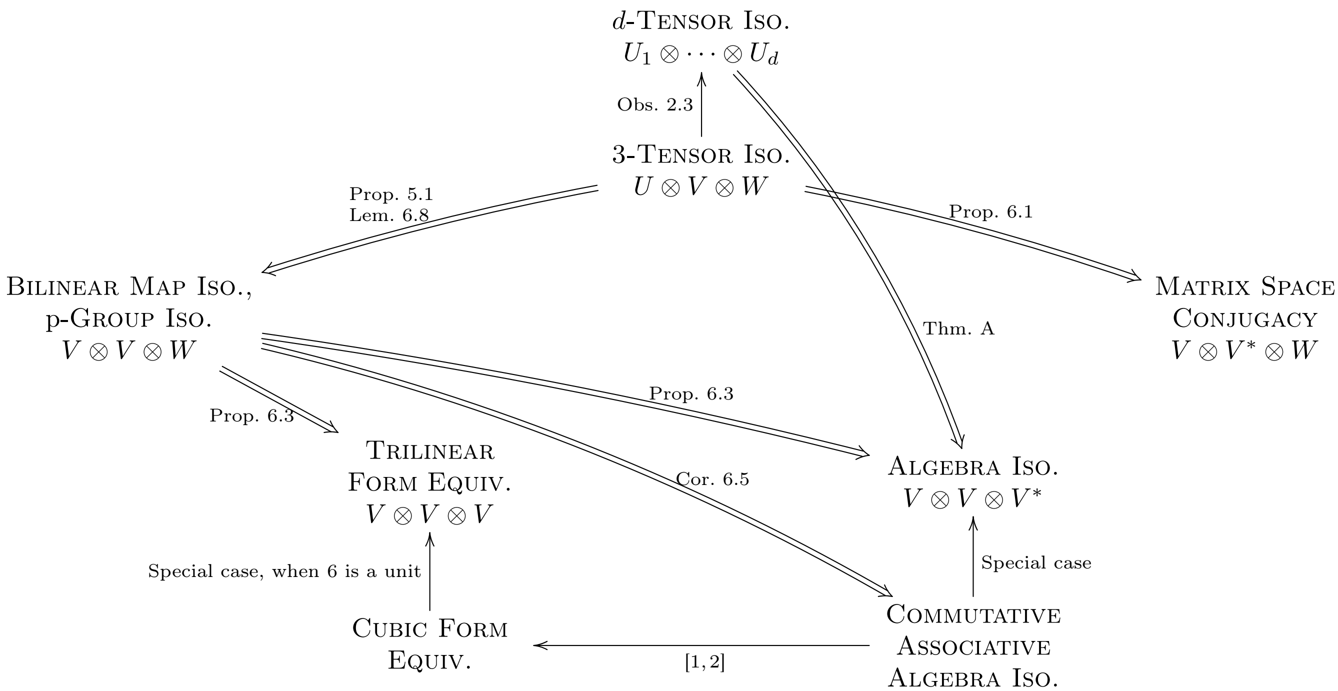


Fig. 2. *Reductions for Thm. B. An arrow $A \to B$ indicates that A reduces to B, i.e., $A \leq_m^p B$; $A \Rightarrow B$ indicates such a reduction that is a new result. For Cor. B, the five tensor problems in the center circle all reduce to* 3TI *via [42]. For the "$V \otimes V \otimes W$" notation, see Sec. 2.2. The results of [1, 2] are only used to show* 3TI*-hardness of* Cubic Form Equivalence, *in combination with Prop. 5.1 and Cor. 6.5.*

In a follow-up work [50] we give a more economical reduction from 3TI to Alternating Matrix Space Isometry, using a new gadget with only linear instead of quadratic blow-up in dimension. This improvement is important for applications to GpI in the Cayley table model, where quadratic blow-up in dimension corresponds to increasing the size of the group to $|G|^{\Theta(\log |G|)}$.

4. Main Theorem A: Reducing d-Tensor Isomorphism to 3-Tensor Isomorphism.

Theorem A. d-Tensor Isomorphism *reduces to* Algebra Isomorphism. *If the input tensor has size* $n_1 \times n_2 \times \cdots \times n_d$, *then the output algebra has dimension* $O(d^2 n^{d-1})$ *where* $n = \max\{n_i\}$.

Remark 4.1. *One cannot do too much better in terms of size of the output, as the following argument suggests. Over finite fields, we may count the number of orbits, which provides a rigorous lower bound on the size blow-up of any kernel reduction (see, e. g., [41, Sec. 4.2.4]). Over infinite fields, if we consider algebraic reductions, they must preserve dimension, so we can make a similar (albeit more heuristic) argument by considering the "dimension" of the set of orbits. Here we have put "dimension" in quotes because the set of orbits is not a well-behaved topological space (it is typically not even* T_1*), but even in this case the same argument should essentially hold. The space of* $n \times n \times \cdots \times n$ *d-tensors has dimension* n^d, *and the group* $\mathrm{GL}_n \times \cdots \times \mathrm{GL}_n$ *has dimension* dn^2, *so the "dimension" of the set of orbits is at least* $n^d - dn^2 \sim n^d$ $(d \geq 3)$*; over* $\mathbb{F}_q$, *the number of orbits is at least* $q^{n^d - dn^2}$. *For algebras of dimension* N, *the space of such algebras is* $\leq N^3$*-dimensional, so the "dimension" of the set of orbits is at most* N^3*; over* $\mathbb{F}_q$, *the number of orbits is at most* q^{N^3}. *Thus we need* $N^3 \gtrsim n^d$, *whence* $N \gtrsim n^{d/3}$. *In particular this implies that there is no kernel reduction from* dTI *to* $3TI$ *that is fixed-parameter tractable with parameter* d.

Proof idea. The idea here is similar to the reduction from 3TI to Algebra Isomorphism (see Proposition 6.3): we want to create an algebra $\mathcal{A}$ in which all products eventually land in an ideal, and multiplication of algebra elements by elements in the ideal is described by the tensor we started with. For a 3-tensor this is very natural, as the structure constants of any algebra form a 3-tensor. In that case, we use the 3-tensor to specify how to write the product of 2 elements as a linear combination (the third factor of the tensor) of basis elements. With a d-tensor for $d \geq 3$, we now want to use it to describe how to write the product of $d-1$ elements as a linear combination of basis elements. The tricky part here is that in an algebra we must still describe the product of any *two* elements. The idea is to create a set of generators, let them freely generate monomials up to degree $d-2$, and then when we get a product of $d-1$ generators, rewrite it as a linear combination of generators according to the given tensor. This idea almost provides one direction of the reduction: if two d-tensors $\mathtt{A}, \mathtt{B}$ are isomorphic, then the corresponding algebras $\mathcal{A}, \mathcal{B}$ are isomorphic. However, there is an issue with implementing this, namely that monomials (in a polynomial ring, or a quotient thereof) are commutative, but our tensors $\mathtt{A}, \mathtt{B}$ need not be symmetric, and moreover, they need not even be "square" (have all side lengths equal). In [1, Thm. 5] they reduce Degree-d Form Equivalence to Commutative Algebra Isomorphism along similar lines, but there the starting objects are themselves commutative, so this was not an issue. In our case, we will get around this using a certain noncommutative algebra where the only nonzero products are those which come "in the right order."

Another potentially tricky aspect of the reduction is the converse: suppose we build our algebras $\mathcal{A}, \mathcal{B}$ as above from two d-tensors, and $\mathcal{A}, \mathcal{B}$ are isomorphic; how can we guarantee that $\mathtt{A}$ and $\mathtt{B}$ are isomorphic? For this, we would like to be able to identify certain subsets of the algebras as characteristic (invariant under any automorphism), so that those characteristic subsets force the isomorphism to take a particular form, which we can then massage into an isomorphism between the tensors $\mathtt{A}, \mathtt{B}$. Our way of doing this is to encode the "degree" structure into the path algebra of a graph, as described in the next section. If the graph has no automorphisms, then the path algebra has the advantage that for any two vertices i, j, the subset of $\mathcal{A}$ spanned by the paths from i to j is nearly characteristic in a way we make precise below. ∎

4.1. Preliminaries for Theorem A. To make the above proof idea precise, we will need a little background on path algebras (a.k.a. quiver algebras) and their quotients. For a textbook reference on these algebras, see [4, Ch. II], and for a textbook treatment of Wedderburn–Artin theory and the Jacobson radical, see [67]. Aside from the definition of path algebra, most of this section will end up being used as a black box; we include it mostly for ease of reference.

We start with some important, classical results on the structure of associative algebras. The *Jacobson radical* of an associative algebra A, here denoted $R(A)$, is the intersection of all maximal right ideals. Equivalently, $R(A) = \{x \in A : \text{every element of } 1 + AxA \text{ is invertible}\}$. A unital algebra A over a field $\mathbb{F}$ is *semisimple* if $R(A) = 0$; in this case, by Wedderburn's Theorem (see below), A is isomorphic to a direct sum of matrix algebras over finite-degree division rings extending $\mathbb{F}$. An algebra A is called *separable* if it is semisimple over every field extending $\mathbb{F}$, that is, $A \otimes_{\mathbb{F}} \mathbb{K}$ is semisimple for all fields $\mathbb{K}$ extending $\mathbb{F}$. Equivalently, A is separable if it is isomorphic to $\bigoplus_{i=1}^{d} \mathrm{M}(d_i, \mathbb{F}_i)$, where each $\mathbb{F}_i$ is a division ring extending $\mathbb{F}$ such that the center $Z(\mathbb{F}_i)$ is a separable field extension of $\mathbb{F}$. Recall that a field extension $\mathbb{F} \subseteq \mathbb{K}$ is *separable* if for every $\alpha \in \mathbb{K}$, the minimal polynomials of α over $\mathbb{F}$ has no repeated roots in the algebraic closure $\overline{\mathbb{F}}$. A field $\mathbb{F}$ is perfect if all its algebraic extensions are separable; examples of perfect fields include characteristic-0 fields and finite fields. In the proof of Theorem A in Section 4.2, there will be a subalgebra for which we need separability, and this holds because it is simply a direct sum of copies of $\mathbb{F}$.

An element $a \in A$ is *idempotent* if $a^2 = a$. Two idempotents e, f are *orthogonal* if $ef = fe = 0$. An idempotent e is *primitive* if it cannot be written as the sum of two nonzero orthogonal idempotents. A *complete set of primitive orthogonal idempotents* of A is a set $\{e_1, \ldots, e_n\}$ of primitive idempotents which are pairwise orthogonal, and such that the set is maximal subject to this condition.

Theorem 4.2 (Wedderburn–Mal'cev, see, e. g., [38]). *Let A be an finite-dimensional, associative, unital algebra over a field $\mathbb{F}$. Then*

1. $A/R(A) \cong \bigoplus_{i=1}^{d} \mathrm{M}(d_i, \mathbb{F}_i)$ *(as algebras), where each $\mathbb{F}_i$ is a division ring of finite degree over $\mathbb{F}$.*
2. *If $A/R(A)$ is separable, then there exists a subalgebra $S \subseteq A$ such that $A = S \oplus R(A)$ (as $\mathbb{F}$-vector spaces).*
3. *If $T \subseteq A$ is any separable subalgebra, then there exists $r \in R(A)$ such that $(1+r)T(1+r)^{-1} \subseteq S$.*

The last part of the preceding theorem is what we will use to show that the set of paths $i \to j$ in our graph is "nearly characteristic;" that is, it is not characteristic, but it is characteristic up to conjugacy (=inner automorphisms).

Definition 4.3 (Path algebras). *Given a directed multigraph G (possibly with parallel edges and self-loops, a.k.a. quiver), its* path algebra *$Path(G)$ is the algebra of paths in G, where multiplication is given by concatenation of paths when this is well-defined, and zero otherwise. That is, $Path(G)$ is generated by $\{e_v : v \in V(G)\} \cup \{x_a : a \in E(G)\}$, where the generators e_v are thought of as the "path of length 0" at vertex v. The defining relations in $Path(G)$ are that the product of two paths is their concatenation if the end of the first equals the start of the second, and zero otherwise.*

More formally, the relations are:

$$e_v e_w = \delta_{v,w} e_v$$
$$e_v x_a = \delta_{v,start(a)} x_a$$
$$x_a e_v = \delta_{v,end(a)} x_a$$
$$x_a x_b = 0 \text{ if } start(b) \neq end(a),$$

where $\delta_{x,y}$ is the Kronecker delta: it is 1 if $x = y$ and 0 otherwise.

Note that we are allowed to take formal linear combinations of paths in this algebra, as it is an $\mathbb{F}$-algebra (so in particular, it is an $\mathbb{F}$-vector space). The *arrow ideal* of $\mathrm{Path}(G)$ is the two-sided ideal generated by the arrows, and has a basis consisting of all paths of length ≥ 1; it is denoted R_G. Note that the set $e_i \mathcal{A} e_j$ is linearly spanned by the paths $i \to j$ in G.

LEMMA 4.4 (See [4, Cor. II.1.11]). *If G is finite, connected, and acyclic, then $R(Path(G))$ is the arrow ideal R_G, and has a basis consisting of all paths of length ≥ 1, and the set $\{e_v : v \in V(G)\}$ is a complete set of primitive orthogonal idempotents.*

COROLLARY 4.5. *Let G be a finite, connected, acyclic graph, and I an ideal of $Path(G)$ contained in R_G; let $A = Path(G)/I$. Then (1) $R(A) = R_G/I$, (2) $A/R(A) \cong \mathbb{F}^{\oplus|V(G)|}$, whence $A/R(A)$ is separable, and (3) $\{\overline{e}_v : v \in V(G)\}$ is a complete set of primitive orthogonal idempotents, where $\overline{e}_v$ is the image of e_v under the quotient map $Path(G) \to Path(G)/I = A$.*

Proof. (1) This holds for any ideal contained in the radical of any finite-dimensional associative unital algebra [67, Prop. 4.6].

(2) It is clear that as vector spaces, $\mathrm{Path}(G) = \langle e_1, \ldots, e_n \rangle \oplus R_G$ (where $n = |V(G)|$), and the span of the e_i is easily seen to be an algebra isomorphic to $\mathbb{F}^n$, where the i-th copy of $\mathbb{F}$ is spanned by $\pi(e_i)$, where $\pi \colon \mathrm{Path}(G) \to \mathrm{Path}(G)/R_G$ is the natural projection. Thus $\mathrm{Path}(G)/R_G \cong \mathbb{F}^n$. Since $R(A) = R_G/I$, we have $A/R(A) = (\mathrm{Path}(G)/I)/(R_G/I) \cong \mathrm{Path}(G)/R_G \cong \mathbb{F}^n$. As a semisimple algebra, we thus have that $A/R(A) \cong \bigoplus \mathrm{M}(1, \mathbb{F})$, and as $\mathbb{F}$ is always a separable extension over itself, $A/R(A)$ is separable.

(3) The property of being a set of primitive orthogonal idempotents is preserved by homomorphisms, so there are only two things to check here: first, that none of the $\overline{e}_v$ is zero modulo I, and second, that there are no additional primitive idempotents in A that are mutually orthogonal with every $\overline{e}_v$. To see that none of the $\overline{e}_v$ are zero, note that $\pi \colon \mathrm{Path}(G) \to \mathrm{Path}(G)/R_G$ factors through A; then since $\pi(e_v) \neq 0$ for any v (from the previous paragraph), it must be the case that $\overline{e}_v \neq 0$ as well. Finally, we must show this is a complete set of primitive orthogonal idempotents. Suppose not; that is, suppose there is some $e \notin \{\overline{e}_v : v \in V(G)\}$ such that e is a primitive idempotent that is orthogonal in A to every $\overline{e}_v$. First, we claim that $e \notin R(A) = R_G/I$. For, since G is a finite acyclic graph, its arrow ideal R_G is nilpotent: there are no paths longer than $n - 1 = |V(G)| - 1$, so we must have $R_G^n = 0$, whence R_G cannot contain any idempotents. Since R_G is nilpotent, the same must be true of R_G/I, whence $R(A) = R_G/I$ cannot contain any idempotents, so e cannot be in $R(A)$. But then the image of e in $A/R(A)$ is nonzero (since $e \notin R(A)$), so e is another primitive idempotent orthogonal to every $\pi(e_v)$ in $\mathrm{Path}(G)/R_G = A/R(A)$. But this is a contradiction, since $\{\pi(e_v)\}$ is already a complete set of primitive orthogonal idempotents for $A/R(A)$. ∎

Finally, in the course of the proof, we will use the following construction of Grigoriev:

THEOREM 4.6 (Grigoriev [47, Theorem 1]). GRAPH ISOMORPHISM *is equivalent to* ALGEBRA ISOMORPHISM *for algebras A such that the radical squares to zero and $A/R(A)$ is abelian.*

In our proof, all we will need aside from Grigoriev's result is to see the construction itself, which we recall here in language consistent with ours.

Construction [47]. Given a graph G, construct an algebra $\mathcal{A}_G$ as follows: it is generated by $\{e_i : i \in V(G)\} \cup \{e_{ij} : (i,j) \in E(G)\}$ subject to the following relations: $e_i e_j = \delta_{ij} e_i$, $e_i e_{kj} = \delta_{ik} e_{kj}$, $e_{kj} e_i = \delta_{ij} e_{kj}$, $e_{ij} e_{kl} = 0$ when $j \neq k$, $R(\mathcal{A}_G)$ is generated by $\{e_{ij}\}$, and the radical squares to zero. It is immediate that this is just $\text{Path}(G)/R_G^2$. From any such algebra $\mathcal{A}$, Grigoriev recovers a corresponding weighted graph, where the weight on (i,j) is $\dim e_i \mathcal{A} e_j$. In our setting we use multiple parallel edges rather than weight, but the proof goes through *mutatis mutandis.* ∎

4.2. Proof of Theorem A.

Proof. Let $\mathtt{A}$ be an $n_1 \times n_2 \times \cdots \times n_d$ d-tensor. Let G be the following directed multigraph (see Figure 3): it has d vertices, labeled $1, \ldots, d$, and for $i = 1, \ldots, d-1$, it has n_i parallel arrows from vertex i to vertex $i+1$, and n_d parallel arrows from 1 to d.

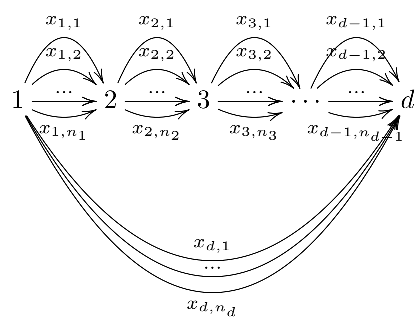


FIG. 3. *The graph G whose path algebra we take a quotient of to construct the reduction for Theorem A.*

Because of the structure of this graph, we can index the generators of $\text{Path}(G)$ a little more mnemonically than in the preliminaries above: let the generators corresponding to the n_i arrows from $i \to (i+1)$ be $x_{i,a}$ for $a = 1, \ldots, n_i$, and let the generators corresponding to the n_d arrows $1 \to d$ be $x_{d,a}$ for $a = 1, \ldots, n_d$. Let $\mathcal{A}$ be the quotient of $\text{Path}(G)$ by the relations[11]

$$x_{1,i_1} x_{2,i_2} \cdots x_{d-1,i_{d-1}} = \sum_{j=1}^{n_d} \mathtt{A}(i_1, i_2, \ldots, i_{d-1}, j) x_{d,j} \tag{4.1}$$

At the moment, we only have $\mathcal{A}$ in terms of generators and relations; however, it will be easy to turn it into its basis representation. The key is to bound its dimension, which we do now. Except for paths of length $d-1$ (because of the nontrivial relations (4.1)), this is just counting the number of paths in the graph described above. The only nonzero monomials of degree $k+1$ are those of the form $x_{i,a_i} x_{i+1,a_{i+1}} x_{i+2,a_{i+2}} \cdots x_{i+k,a_{i+k}}$. For a given choice of $i \in \{1, \ldots, d-1-k\}$, there are

[11]For those familiar with quiver algebras, we note that this ideal is *not* admissible, as it is not contained in R_G^2. It can probably be made admissible by inserting new vertices in the middle of each edge $1 \to d$. However, when we tried to do that in a naive way, we ran into problems verifying the reduction, as what should be a linear transformation either ends up being incorrect or ends up being quadratic, either of which caused issues.

exactly $n_i n_{i+1} \cdots n_{i+k}$ such monomials, so we have

$$\begin{aligned}
\dim \mathcal{A} &= \#\{e_i\} + n_d + \sum_{k<d-1} \sum_{i=1}^{d-1-k} \#\{\text{paths } i \to (i+k)\} \\
&= d + n_d + \sum_{k=0}^{d-2} \sum_{i=1}^{d-1-k} \prod_{j=i}^{i+k} n_j \\
&\leq 2n + \sum_{k=0}^{d-2} \sum_{i=1}^{d-1-k} n^{k+1} \\
&\leq O(d^2 n^{d-1}).
\end{aligned}$$

Note that in the first line we can exactly specify $\dim \mathcal{A}$, independent of $\mathtt{A}$ itself (depending only on its dimensions). For any fixed d, this dimension is polynomial in n. By the linear-algebraic analogue of breadth-first search, we may thus list a basis for $\mathcal{A}$ and its structure constants with respect to that basis.

We claim that the map $\mathtt{A} \mapsto \mathcal{A}$ is a reduction. Suppose $\mathtt{B}$ is another tensor of the same dimension, and let $\mathcal{B}$ be the associated algebra as above. We claim that $\mathtt{A} \cong \mathtt{B}$ as d-tensors if and only if $\mathcal{A} \cong \mathcal{B}$ as algebras.

For the only if direction, suppose $\mathtt{A} \cong \mathtt{B}$ via $(P_1, P_2, \ldots, P_d) \in \mathrm{GL}(n_1, \mathbb{F}) \times \cdots \times \mathrm{GL}(n_d, \mathbb{F})$, that is

$$\mathtt{A}(i_1, \ldots, i_d) = \sum_{j_1, \ldots, j_d} (P_1)_{i_1, j_1} \cdots (P_d)_{i_d, j_d} \mathtt{B}(j_1, \ldots, j_d) \tag{4.2}$$

for all $i_1, \ldots, i_d$. Then we claim that the block-diagonal matrix $P = \mathrm{diag}(P_1, P_2, \ldots, P_{d-1}, P_d^{-t}) \in \mathrm{GL}(n, \mathbb{F})$ (where $n = \sum_{i=1}^d n_i$), together with mapping e_i to e_i, induces an isomorphism from $\mathcal{A}$ to $\mathcal{B}$. Note that P itself is not an isomorphism, as $\dim \mathcal{A} \approx n^d$, but P specifies a linear map on the generators of $\mathcal{A}$, which we may then extend to all of $\mathcal{A}$.

First let us see that P indeed gives a well-defined homomorphism $\mathcal{A} \to \mathcal{B}$. Since P is only defined on the generators and is, by definition, extended by distributivity, the only thing to check here is that P sends the relations of $\mathcal{A}$ into the relations of $\mathcal{B}$. Let $y_{1,1}, \ldots, y_{1,n_1}, \ldots, y_{d,n_d}, e_1, \ldots, e_d$ denote the basis of $\mathcal{B}$ as a path algebra (recall Definition 4.3). The map P is defined by $P(e_i) = e_i$,

$$P(x_{i,a}) = \sum_{a'=1}^{n_i} (P_i)_{aa'} y_{i,a'} \qquad \text{for } i = 1, \ldots, d-1$$

and

$$P(x_{d,a}) = \sum_{a'=1}^{n_d} (P_d^{-t})_{aa'} y_{d,a'}.$$

By left multiplying by P_d^t, we may rewrite this last equation as

$$y_{d,a} = \sum_{a'=1}^{n_d} (P_d)_{a',a} P(x_{d,a'}),$$

note the transpose.

To check the relations, let us write out the path algebra relations explicitly for our graph, in our notation. The generators of $\mathcal{A}$ are $x_{1,1}, x_{1,2}, \dots, x_{1,n_1}, x_{2,1}, x_{2,2}, \dots, x_{2,n_2}, \dots, x_{d,n_d}, e_1, \dots, e_d$, and the relations are (4.1) and the quiver relations:

$$\begin{aligned}
e_i e_j &= \delta_{i,j} e_i \\
e_i x_{j,a} &= (\delta_{i,j} + \delta_{i,1}\delta_{j,d}) x_{j,a} \\
x_{j,a} e_i &= (\delta_{j+1,i} + \delta_{j,d}\delta_{i,d}) x_{j,a} \\
x_{i,a} x_{d,b} &= 0 \\
x_{d,b} x_{i,a} &= 0 \quad (i < d) \\
x_{i,a} x_{j,b} &= 0 \quad \text{ if } j \neq i+1
\end{aligned}$$

The relations involving the e_i are easy to verify, since they only depend on the first subscript of $x_{i,a}$ (resp., $y_{j,b}$), and P does not alter this subscript.

For relation $x_{i,a}x_{d,b} = 0$, we have:

$$\begin{aligned}
P(x_{i,a}x_{d,b}) &= P(x_{i,a})P(x_{d,b}) \\
&= \left(\sum_{a'=1}^{n_i} (P_i)_{aa'} y_{i,a'}\right)\left(\sum_{b'=1}^{n_d} (P_d^{-t})_{bb'} y_{d,b'}\right) \\
&= \sum_{a'=1}^{n_i}\sum_{b'=1}^{n_d} (P_i)_{aa'}(P_d^{-t})_{bb'} y_{i,a'} y_{d,b'} = 0,
\end{aligned}$$

where the final inequality comes from the defining relations $y_{i,a'}y_{d,b'} = 0$ in $\mathcal{B}$.

The verification for remaining quiver relations is similar, since P does not alter the start and end vertices of any arrow (though it may send a single arrow $i \to j$ in $\mathcal{A}$ to a linear combination of arrows $i \to j$ in $\mathcal{B}$).

We now verify the relation (4.1). The idea is that the expression (4.1) is block-multilinear, in that it is linear in each set of variables $\{x_{k,i} : 1 \leq i \leq n_k\}$, so the action of P on the monomial on the left-hand side of (4.1) turns into the multilinear action of the P_i's, each occuring once, and this lets us then apply the assumed isomorphism (4.2). In symbols and more formally, we have

$$\begin{aligned}
&P(x_{1,i_1}x_{2,i_2}\cdots x_{d-1,i_{d-1}}) \\
&= \sum_{j_1=1}^{n_1}\sum_{j_2=1}^{n_2}\cdots\sum_{j_{d-1}=1}^{n_{d-1}} (P_1)_{i_1,j_1}(P_2)_{i_2,j_2}\cdots(P_{d-1})_{i_{d-1},j_{d-1}} y_{1,j_1}y_{2,j_2}\cdots y_{d-1,j_{d-1}} \\
&= \sum_{j_1,j_2,\cdots,j_{d-1}} (P_1)_{i_1,j_1}(P_2)_{i_2,j_2}\cdots(P_{d-1})_{i_{d-1},j_{d-1}} \sum_{j_d=1}^{n_d} \mathtt{B}(j_1,j_2,\dots,j_d) y_{d,j_d} \\
&= \sum_{j_1,\cdots,j_{d-1}} (P_1)_{i_1,j_1}(P_2)_{i_2,j_2}\cdots(P_{d-1})_{i_{d-1},j_{d-1}} \sum_{j_d=1}^{n_d} \mathtt{B}(j_1,j_2,\dots,j_d) \sum_{i_d=1}^{n_d} (P_d)_{i_d,j_d} P(x_{d,i_d}) \\
&= \sum_{i_d=1}^{n_d}\left(\sum_{j_1,\cdots,j_{d-1},j_d} (P_1)_{i_1,j_1}\cdots(P_d)_{i_d,j_d}\mathtt{B}(j_1,\dots,j_d)\right) P(x_{d,i_d}) \\
&= \sum_{i_d=1}^{n_d} \mathtt{A}(i_1,\dots,i_d) P(x_{d,i_d}),
\end{aligned}$$

as desired. Thus the map $\mathcal{A} \to \mathcal{B}$ induced by P is an algebra homomorphism.

Next, since P is an isomorphism of $(d+n)$-dimensional vector spaces, the map it induces $\mathcal{A} \to \mathcal{B}$ is surjective on the generators of $\mathcal{B}$, whence it is surjective onto all of $\mathcal{B}$. Finally, since $\dim \mathcal{A} = \dim \mathcal{B} < \infty$, any linear surjective map $\mathcal{A} \to \mathcal{B}$ is automatically bijective, so this map is indeed an isomorphism of algebras.

For the if direction, suppose that $f\colon \mathcal{A} \to \mathcal{B}$ is an isomorphism of algebras. Since the Jacobson radical is characteristic, we have $f(R(\mathcal{A})) = R(\mathcal{B})$. Then $\{f(e_v) : v \in V\}$ is a set of primitive orthogonal idempotents in $\mathcal{B}$, and their span $T = \langle f(e_v) : v \in V\rangle$ is a separable subalgebra (isomorphic to $\mathbb{F}^n$) such that $\mathcal{B} = T \oplus R(\mathcal{B})$. By the Wedderburn–Mal'cev Theorem (Theorem 4.2(3)), there is some $r \in R(\mathcal{B})$ such that $(1+r)T(1+r)^{-1} = \langle e_1, \ldots, e_n\rangle =: S$. Since the e_i are the only primitive idempotents in S, we must have that $(1+r)f(e_i)(1+r)^{-1} = e_{\pi(i)}$ for all i and some permutation $\pi \in S_n$.

Next we will show that this permutation is in fact the identity, so that $(1+r)f(e_i)(1+r)^{-1} = e_i$ for all i. For this, consider $\mathcal{A}' = \mathcal{A}/R(\mathcal{A})^2$ and similarly $\mathcal{B}'$. These are precisely the algebras considered by Grigoriev [47] (reproduced as Theorem 4.6 above). Since $R(\mathcal{A})$ is characteristic, so is its square, and thus f induces an isomorphism $\mathcal{A}' \overset{\cong}{\to} \mathcal{B}'$. By Theorem 1 of Grigoriev [47], any isomorphism $\mathcal{A}' \to \mathcal{B}'$ induces an isomorphism of the corresponding graphs, so this isomorphism must map e_i to e_i for each i (since our graph G has no automorphisms). Thus π must be the identity, and $(1+r)f(e_i)(1+r)^{-1} = e_i$ for all i.

Since conjugation is an automorphism, let $f'\colon \mathcal{A} \to \mathcal{B}$ be $c_{1+r} \circ f$, where $c_{1+r}(b) = (1+r)b(1+r)^{-1}$. By the above, $f'(e_i) = e_i$ for all i. Thus $f'(e_i \mathcal{A} e_j) = e_i \mathcal{B} e_j$. (Recall that the set $e_i\mathcal{A}e_j$ is linearly spanned by the paths $i \to j$ in this graph.) In particular, define P_i to be the restriction of f' to $e_i\mathcal{A}e_{i+1}$ for $i = 1, \ldots, d-1$ and P_d to be the restriction of f' to $e_1\mathcal{A}e_d$. Then we have that P_i is a linear bijection from the span of $x_{i,1}, \ldots, x_{i,n_i}$ to the span of $y_{i,1}, \ldots, y_{i,n_i}$ for all i. Let us also use P_i to denote the matrix corresponding to the linear map P_i in the bases $\{x_{i,j}\}$ and $\{y_{i,j}\}$. We claim that $P = (P_1, \ldots, P_{d-1}, P_d^{-t})$ is a tensor isomorphism $\mathtt{A} \to \mathtt{B}$, that is,

$$\mathtt{A}(i_1, \ldots, i_d) = \sum_{j_1, \ldots, j_d} (P_1)_{i_1,j_1} \cdots (P_d^{-t})_{i_d,j_d} \mathtt{B}(j_1, \ldots, j_d).$$

From the fact that f' is an isomorphism, we have

$$\sum_{i_d=1}^{n_d} \mathtt{A}(i_1, \ldots, i_d) f'(x_{d,i_d}) = f'(x_{1,i_1} x_{2,i_2} \cdots x_{d-1,i_{d-1}})$$

$$\begin{aligned}\sum_{i_d=1}^{n_d} \mathtt{A}(i_1, \ldots, i_d) \sum_{j_d=1}^{n_d} (P_d)_{i_d,j_d} y_{d,j_d} &= f'(x_{1,i_1}) f'(x_{2,i_2}) \cdots f'(x_{d-1,i_{d-1}}) \\ &= \sum_{j_1,\ldots,j_{d-1}} (P_1)_{i_1,j_1}(P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} y_{1,j_1} y_{2,j_2} \cdots y_{d-1,j_{d-1}} \\ &= \sum_{j_1,\ldots,j_{d-1}} (P_1)_{i_1,j_1}(P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} \sum_{j_d=1}^{n_d} \mathtt{B}(j_1, \ldots, j_d) y_{d,j_d}\end{aligned}$$

For each $j_d \in \{1, \ldots, n_d\}$, equating the coefficient of y_{d,j_d} gives

$$\sum_{i_d=1}^{n_d} \mathtt{A}(i_1, \ldots, i_d)(P_d)_{i_d,j_d} = \sum_{j_1,\ldots,j_{d-1}} (P_1)_{i_1,j_1}(P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} \mathtt{B}(j_1, \ldots, j_d)$$

Let $\mathtt{A}(i_1, \dots, i_{d-1}, -)$ be the natural row vector of length n_d, and similarly for $\mathtt{B}(j_1, \dots, j_{d-1}, -)$. Then we may rewrite the preceding set of n_d equations (one for each choice of j_d) in matrix notation as

$$\mathtt{A}(i_1, \dots, i_{d-1}, -) \cdot P_d = \sum_{j_1,\dots,j_{d-1}} (P_1)_{i_1,j_1} (P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} \mathtt{B}(j_1, \dots, j_{d-1}, -)$$

Right multiplying by P_d^{-1}, we then get

$$\mathtt{A}(i_1, \dots, i_{d-1}, -) = \sum_{j_1,\dots,j_{d-1}} (P_1)_{i_1,j_1} (P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} \mathtt{B}(j_1, \dots, -) P_d^{-1}$$

$$\mathtt{A}(i_1, \dots, i_d) = \sum_{j_1,\dots,j_{d-1},j_d} (P_1)_{i_1,j_1} (P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} \mathtt{B}(j_1, \dots, j_d) (P_d^{-1})_{j_d,i_d}$$

$$= \sum_{j_1,\dots,j_d} (P_1)_{i_1,j_1} (P_2)_{i_2,j_2} \cdots (P_{d-1})_{i_{d-1},j_{d-1}} (P_d^{-t})_{i_d,j_d} \mathtt{B}(j_1, \dots, j_d),$$

as claimed. ∎

5. From 3-Tensor Isomorphism **to** Matrix Space Isometry**.** We present a reduction from 3-Tensor Isomorphism to Matrix Space Isometry using the gadgets from [42]. While we use the gadget construction from [42], the proof for correctness is different as we apply that gadget in a setting different from that in [42].

The use of gadgets from [42] results in quadratic blow-up in dimension, which is problematic when we want to apply it to groups in the Cayley table model, since then the resulting groups after the reduction have size $|G|^{\Theta(\log |G|)}$. In a follow-up paper [50], we develop a new more economical gadget that gives us linear blow-up in dimension, which corresponds to the output groups having size $|G|^{O(1)}$.

Proposition 5.1. 3-Tensor Isomorphism *reduces to* Alternating Matrix Space Isometry*. Symbolically, isomorphism in $U \otimes V \otimes W$ reduces to isomorphism in $V' \otimes V' \otimes W'$ (or even to $\bigwedge^2 V' \otimes W$), where $\ell = \dim U \leq n = \dim V$ and $m = \dim W$, $\dim V' = \ell + 7n + 3$ and $\dim W' = m + \ell(2n+1) + n(4n+2)$.*

Proof. We will exhibit a function r from 3-way arrays to matrix tuples such that two 3-way arrays $\mathtt{A}, \mathtt{B} \in T(\ell \times n \times m, \mathbb{F})$ which are non-degenerate as 3-tensors, are isomorphic as 3-tensors if and only if the matrix spaces $\langle r(\mathtt{A})\rangle, \langle r(\mathtt{B})\rangle$ are isometric. Note that we can assume our input tensors are non-degenerate by Observation 2.2. The construction is a bit involved, so we will first describe the construction in detail, and then prove the desired statement.

The gadget construction.. Given a 3-way array $\mathtt{A} \in T(\ell \times n \times m, \mathbb{F})$, let $\mathbf{A}$ denote the corresponding m-tuple of matrices, $\mathbf{A} \in M(\ell \times n)^m$. The first step is to construct $s(\mathtt{A}) \in \Lambda(\ell + n, \mathbb{F})^m$, defined by $s(\mathtt{A}) = (A_1^\Lambda, \dots, A_m^\Lambda)$ where $A_i^\Lambda = \begin{bmatrix} \mathbf{0} & A_i \\ -A_i^t & \mathbf{0} \end{bmatrix}$. Already, note that if $\mathtt{A} \cong \mathtt{B}$, then $s(\mathtt{A})$ and $s(\mathtt{B})$ are pseudo-isometric matrix tuples (equivalently, $\langle s(\mathtt{A})\rangle$ and $\langle s(\mathtt{B})\rangle$ are isometric matrix spaces).

However, it is not clear whether the converse should hold. Indeed, suppose $Ps(\mathtt{A})P^T = s(\mathtt{B})^Q$ for some $P \in \mathrm{GL}(\ell + n, \mathbb{F}), Q \in \mathrm{GL}(m, \mathbb{F})$. If we write P as a block matrix $\begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix}$, where $P_{11} \in M(\ell, \mathbb{F})$ and $P_{22} \in M(n, \mathbb{F})$, then by considering the (1,2) block we get that $P_{11} A_i P_{22}^t - P_{21}^t A_i^t P_{12} = \sum_{j=1}^m q_{ij} B_j$ for all $i = 1, \dots, m$, whereas what we would want is the same equation but without the $P_{21}^t A_i^t P_{12}$ term. To remedy this, it would suffice if we could extend the tuple $s(\mathtt{A})$ to $r(\mathtt{A})$ so that any pseudo-isometry (P, Q) between $r(\mathtt{A})$ and $r(\mathtt{B})$ will have $P_{21} = 0$.

To achieve this, we start from $s(\mathtt{A}) = \mathbf{A}^\Lambda \in \Lambda(n+\ell, \mathbb{F})^m$, and construct $r(\mathtt{A}) \in \Lambda(\ell + 7n + 3, \mathbb{F})^{m+\ell(2n+1)+n(4n+2)}$ as follows. Here we write it out symbolically, on the next page is the same thing in matrix format, and in Figure 4 is a picture of the construction. Let $s = m + \ell(2n+1) + n(4n+2)$. Write $r(\mathtt{A}) = (\tilde{A}_1, \ldots, \tilde{A}_s)$, where $\tilde{A}_i \in \Lambda(\ell + 7n + 3, \mathbb{F})$ are defined as follows:

- For $1 \le i \le m$, $\tilde{A}_i = \begin{bmatrix} A_i^\Lambda & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. Recall that $A_i^\Lambda \in \Lambda(\ell + n, \mathbb{F})$.
- For the next $\ell(2n+1)$ slices, that is, $m+1 \le i \le m+\ell(2n+1)$, we can naturally represent $i - m$ by (p, q) where $p \in [\ell]$, $q \in [2n+1]$. We then let $\tilde{A}_i$ be the elementary alternating matrix $E_{p,\ell+n+q} - E_{\ell+n+q,p}$.
- For the next $n(4n+2)$ slices, that is $m + \ell(2n+1) + 1 \le i \le m + \ell(n+1) + n(4n+2)$, we can naturally represent $i - m - \ell(n+1)$ by (p, q) where $p \in [n]$, $q \in [4n+2]$. We then let $\tilde{A}_i$ be the elementary alternating matrix $E_{\ell+p,n+\ell+2n+1+q} - E_{n+\ell+2n+1+q,\ell+p}$.

We may view the above construction is as follows. Write the frontal view of $\mathtt{A}$ as

$$\mathtt{A} = \begin{bmatrix} a'_{1,1} & \cdots & a'_{1,n} \\ \vdots & \ddots & \vdots \\ a'_{\ell,1} & \cdots & a'_{\ell,n} \end{bmatrix},$$

where $a'_{i,j} \in \mathbb{F}^m$, which we think of as a column vector, but when place in the above array, we think of it as coming out of the page.

Let $\tilde{\mathtt{A}}$ be the 3-way array whose frontal slices are $\tilde{A}_i$, so $\tilde{\mathtt{A}} \in \mathrm{T}((\ell + 7n + 3) \times (\ell + 7n + 3) \times (m + \ell(2n+1) + n(4n+2)), \mathbb{F})$. Then the frontal view of $\tilde{\mathtt{A}}$ is

$$\tilde{\mathtt{A}} = \left[\begin{array}{ccc:ccc:ccc:ccc}
\mathbf{0} & \cdots & \mathbf{0} & a_{1,1} & \cdots & a_{1,n} & e_{1,1} & \cdots & e_{2n+1,1} & \mathbf{0} & \cdots & \mathbf{0} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\mathbf{0} & \cdots & \mathbf{0} & a_{\ell,1} & \cdots & a_{\ell,n} & e_{1,\ell} & \cdots & e_{2n+1,\ell} & \mathbf{0} & \cdots & \mathbf{0} \\ \hdashline
-a_{1,1} & \cdots & -a_{\ell,1} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & f_{1,1} & \cdots & f_{4n+2,1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
-a_{1,n} & \cdots & -a_{\ell,n} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & f_{1,n} & \cdots & f_{4n+2,n} \\ \hdashline
-e_{1,1} & \cdots & -e_{1,\ell} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
-e_{2n+1,1} & \cdots & -e_{2n+1,\ell} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \hdashline
\mathbf{0} & \cdots & \mathbf{0} & -f_{1,1} & \cdots & -f_{1,n} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
\mathbf{0} & \cdots & \mathbf{0} & -f_{4n+2,1} & \cdots & -f_{4n+2,n} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0}
\end{array}\right],$$

where $a_{i,j} = \begin{bmatrix} a'_{i,j} \\ \mathbf{0} \end{bmatrix} \in \mathbb{F}^{m+\ell(2n+1)+n(4n+2)}$, $e_{i,j} = \vec{e}_{m+(j-1)(2n+1)+i}$, and $f_{i,j} = \vec{e}_{m+\ell(2n+1)+(j-1)(4n+2)+i}$.

We now examine the ranks of the lateral slices L_i of $\tilde{\mathtt{A}}$. We claim:

For i...						rk(L_i)			
1	$\le$	i	$\le$	ℓ	$2n+1$	$\le$	$\mathrm{rk}(L_i)$	$\le$	$3n+1$
$\ell+1$	$\le$	i	$\le$	$\ell+n$	$4n+2$	$\le$	$\mathrm{rk}(L_i)$	$\le$	$5n+2$
$\ell+n+1$	$\le$	i	$\le$	$\ell+n+6n+3$			$\mathrm{rk}(L_i)$	$\le$	n

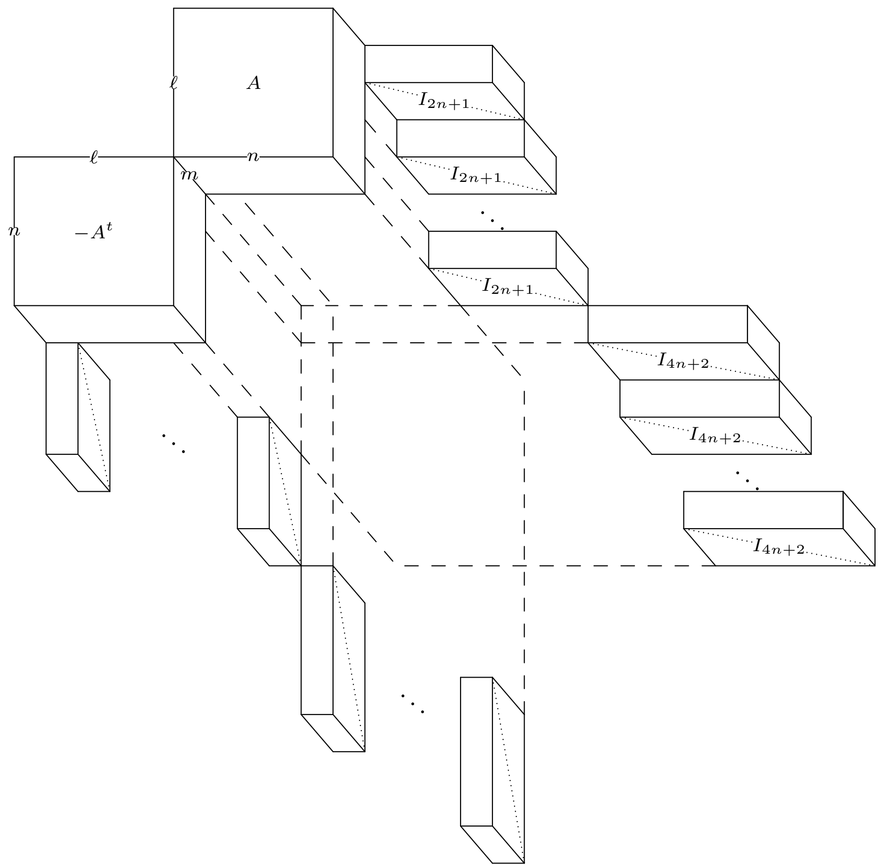


Fig. 4. *Pictorial representation of the reduction for Proposition 5.1.*

To see why these hold:

- For $1 \leq i \leq \ell$, the ith lateral slice L_i is block-diagonal with two non-zero blocks. One block is of size $n \times m$, and the other is $-I_{2n+1}$. Therefore $2n+1 \leq \mathrm{rk}(L_i) \leq 3n+1$.
- For $\ell+1 \leq i \leq \ell+n$, the ith lateral slice L_i is also block-diagonal with two non-zero blocks. One block is of size $\ell \times m$, and the other is $-I_{4n+2}$. Therefore $4n+2 \leq \mathrm{rk}(L_i) \leq 5n+2$. (Recall that we have assumed $\ell \leq n$.)
- For $\ell+n+1 \leq i \leq \ell+n+6n+3$, after rearranging the columns, the ith lateral slice L_i has one non-zero block which is is I_ℓ for the first $2n+1$ slices, and I_n for the next $4n+2$ slices. Therefore $\mathrm{rk}(L_i) = \ell$ or n, and since we have assumed $\ell \leq n$, in either case we have $\mathrm{rk}(L_i) \leq n$.

We then consider the ranks of the linear combinations of the lateral slices.

- As long as the linear combination involves L_i for $\ell+1 \leq i \leq \ell+n$, then the resulting matrix has rank at least $4n+2$, because of the matrix $-I_{4n+2}$ in the last $4n+2$ rows.

- If the linear combination does not involve L_i for $\ell+1 \le i \le \ell+n$, then the resulting matrix has rank at most $4n+1$, because in this case, there are at most $\ell+n+2n+1 \le 4n+1$ non-zero rows.
- If the linear combination involves L_i for $1 \le i \le \ell$, then the resulting matrix has rank at least $2n+1$, because of the matrix $-I_{2n+1}$ in the $(\ell+n+1)$th to the $(\ell+3n+1)$th rows.

We then prove that $\mathtt{A}$ and $\mathtt{B}$ are isomorphic as 3-tensors if and only if $\langle r(\mathtt{A})\rangle$ and $\langle r(\mathtt{B})\rangle$ are isometric as matrix spaces. At first glance, the only if direction seems the easy one, as one expects to extend a 3-tensor isomorphism between $\mathtt{A}$ to $\mathtt{B}$ to an isometry between $\langle r(\mathtt{A})\rangle$ and $\langle r(\mathtt{B})\rangle$ easily. However, it turns out that this direction becomes somewhat technical because of the gadget introduced. This is handled in the following.

For the if direction, suppose $P^t\tilde{\mathtt{A}}P = \tilde{\mathtt{B}}^Q$, for some $P \in \mathrm{GL}(\ell+7n+3,\mathbb{F})$ and $Q \in \mathrm{GL}(m+\ell(2n+1)+n(4n+2),\mathbb{F})$. Write P as $\begin{bmatrix} P_{1,1} & P_{1,2} & P_{1,3} \\ P_{2,1} & P_{2,2} & P_{2,3} \\ P_{3,1} & P_{3,2} & P_{3,3}\end{bmatrix}$, where $P_{1,1}$ is of size $\ell\times\ell$, $P_{2,2}$ is of size $n\times n$, and $P_{3,3}$ is of size $(6n+3)\times(6n+3)$. By the discussion on the ranks of the linear combinations of the lateral slices, we have $P_{2,1}=\mathbf{0}$, $P_{1,2}=\mathbf{0}$, $P_{1,3}=\mathbf{0}$, and $P_{2,3}=\mathbf{0}$. So $P = \begin{bmatrix} P_{1,1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & P_{2,2} & \mathbf{0} \\ P_{3,1} & P_{3,2} & P_{3,3}\end{bmatrix}$, where $P_{1,1}$, $P_{2,2}$, $P_{3,3}$ are invertible. Then consider the action of such P on the first m frontal slices of $\tilde{\mathtt{A}}$. The first m frontal slices of $\tilde{\mathtt{A}}$ are of the form $\begin{bmatrix} \mathbf{0} & A_i & \mathbf{0} \\ -A_i^t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0}\end{bmatrix}$, where A_i is of size $\ell\times n$. Then we have

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

From the fact that Q is invertible and $P^t\tilde{\mathtt{A}}P = \tilde{\mathtt{B}}^Q$, by considering the $(1,2)$ block, we find that every frontal slice of $P_{11}^t\mathtt{A}P_{22}$ lies in $\langle\mathbf{B}\rangle$ (since the gadget does not affect the block-(1,2) position), which gives an isomorphism of tensors, as desired.

For the only if direction, suppose $\mathtt{A}$ and $\mathtt{B}$ are isomorphic as 3-tensors, that is, $P^t\mathtt{A}Q = \mathtt{B}^R$, for some $P \in \mathrm{GL}(\ell,\mathbb{F})$, $Q \in \mathrm{GL}(n,\mathbb{F})$, and $R \in \mathrm{GL}(m,\mathbb{F})$.

We show that there exist $U \in \mathrm{GL}(6n+3,\mathbb{F})$ and $V \in \mathrm{GL}(\ell(2n+1)+n(4n+2),\mathbb{F})$ such that setting

$$\begin{array}{rcccl} \tilde{Q} & = & \mathrm{diag}(P,Q,U) & \in & \mathrm{GL}(\ell+7n+3,\mathbb{F}) \\ \tilde{R} & = & \mathrm{diag}(R,V) & \in & \mathrm{GL}(m+\ell(2n+1)+n(4n+2),\mathbb{F}), \end{array}$$

we have

$$\tilde{Q}^t r(\mathtt{A})\tilde{Q} = r(\mathtt{B})^{\tilde{R}},$$

which will demonstrate that $r(\mathtt{A})$ and $r(\mathtt{B})$ are pseudo-isometric.

Since we are claiming that $\tilde{R} = \mathrm{diag}(R,V) \in \mathrm{GL}(m,\mathbb{F})\times\mathrm{GL}(\ell(2n+1)+n(4n+2),\mathbb{F})$ works, and $\tilde{R}$ is block-diagonal, it suffices to consider the first m frontal slices separately from the remaining slices. For the first m frontal slices, we have:

$$\tilde{Q}^t\tilde{A}_i\tilde{Q} = \begin{bmatrix} P^t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & Q^t & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & U^t\end{bmatrix}\begin{bmatrix} \mathbf{0} & A_i & \mathbf{0} \\ -A_i^t & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0}\end{bmatrix}\begin{bmatrix} P & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & Q & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & U\end{bmatrix} = \begin{bmatrix} \mathbf{0} & P^tA_iQ & \mathbf{0} \\ -Q^tA_i^tP & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0}\end{bmatrix}.$$

It follows from the fact that $P^t \mathtt{A} Q = \mathtt{B}^R$ that the first m frontal slices of $\tilde{Q}^t r(\mathtt{A})\tilde{Q}$ and of $r(\mathtt{B})^{\tilde{R}}$ are the same.

We now consider the remaining frontal slices separately. Towards that end, let $\tilde{\mathtt{A}}' \in \mathrm{T}((\ell + 7n+3) \times (\ell + 7n+3) \times (\ell(2n+1) + n(4n+2)), \mathbb{F})$ be the 3-way array obtained by removing the first m frontal slices from $\tilde{\mathtt{A}}$. That is, the ith frontal slice of $\tilde{\mathtt{A}}'$ is the $(m+i)$th frontal slice of $\tilde{\mathtt{A}}$. Similarly construct $\tilde{\mathtt{B}}'$ from $\tilde{\mathtt{B}}$. We are left to show that $\tilde{\mathtt{A}}'$ and $\tilde{\mathtt{B}}'$ are pseudo-isometric under some $\tilde{Q} = \mathrm{diag}(P, Q, U)$ and V. Note that P and Q are from the isomorphism between $\mathtt{A}$ and $\mathtt{B}$, while U and V are what we still need to design.

We first note that both $\tilde{\mathtt{A}}'$ and $\tilde{\mathtt{B}}'$ can be viewed as a block 3-way array of size $4 \times 4 \times 2$, whose two frontal slices are the block matrices

$$\begin{bmatrix} \mathtt{0} & \mathtt{0} & \mathtt{E} & \mathtt{0} \\ \mathtt{0} & \mathtt{0} & \mathtt{0} & \mathtt{0} \\ -\mathtt{E} & \mathtt{0} & \mathtt{0} & \mathtt{0} \\ \mathtt{0} & \mathtt{0} & \mathtt{0} & \mathtt{0} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \mathtt{0} & \mathtt{0} & \mathtt{0} & \mathtt{0} \\ \mathtt{0} & \mathtt{0} & \mathtt{0} & \mathtt{F} \\ \mathtt{0} & \mathtt{0} & \mathtt{0} & \mathtt{0} \\ \mathtt{0} & -\mathtt{F} & \mathtt{0} & \mathtt{0} \end{bmatrix},$$

where $\mathtt{E}$ is of size $\ell \times (2n+1) \times \ell(2n+1)$, and $\mathtt{F}$ is of size $n \times (4n+2) \times n(4n+2)$. Although these are already identical in $\mathtt{A}', \mathtt{B}'$, the issue here is that P and Q may alter the slices of $\tilde{\mathtt{A}}'$ when they act on $\mathtt{A}$, so we need a way to "undo" this action to bring it back to the same slices in $\mathtt{B}'$.

We now claim that we may further handle these two block slices—the "E" slices and the "F"-slices—separately, that is, that we may take $U = \mathrm{diag}(U_1, U_2)$ and $V = \mathrm{diag}(V_1, V_2)$ where $U_1 \in \mathrm{GL}(2n+1, \mathbb{F})$, $U_2 \in \mathrm{GL}(4n+2, \mathbb{F})$, $V_1 \in \mathrm{GL}(\ell(2n+1), \mathbb{F})$, and $V_2 \in \mathrm{GL}(n(4n+2), \mathbb{F})$.

To handle $\mathtt{E}$, first note that we have

$$\begin{bmatrix} P^t & & & \\ & R^t & & \\ & & U_1^t & \\ & & & U_2^t \end{bmatrix} \begin{bmatrix} \mathbf{0} & \mathbf{0} & E & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -E^t & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P & & & \\ & R & & \\ & & U_1 & \\ & & & U_2 \end{bmatrix} = \begin{bmatrix} \mathbf{0} & \mathbf{0} & P^t E U_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ -U_1^t E^t P & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix},$$

where $E \in M(\ell \times (2n+1), \mathbb{F})$.

Now we examine the lateral slices of $\mathtt{E}$. The ith lateral slice of $\mathtt{E}$ (up to a suitable permutation) is

$$L_i = \begin{bmatrix} \mathbf{0} & \dots & \mathbf{0} & I_\ell & \mathbf{0} & \dots & \mathbf{0} \end{bmatrix},$$

where each $\mathbf{0}$ is of size $\ell \times \ell$, I_ℓ is the ith block, and there are $2n+1$ block matrices in total. The action of P on L_i is by left multiplication. So it sends L_i to $P^t L_i = \begin{bmatrix} \mathbf{0} & \dots & \mathbf{0} & P^t & \mathbf{0} & \dots & \mathbf{0} \end{bmatrix}$. If we set U_1 to be the identity and $V_1 = \mathrm{diag}(P^t, \dots, P^t)$, where there are $(2n+1)$ copies of P^t on the diagonal, then we have $L_i V_1 = P^t L_i$, and thus $P^t \mathtt{E} U_1 = \mathtt{E}^{V_1}$.

It is easy to check that $\mathtt{F}$ can be handled in the same way, where now R, U_2, V_2 play the roles that P, U_1, V_1 played before, respectively. This produces the desired U_1, U_2, V_1, and V_2, and concludes the proof. ∎

COROLLARY 5.2. 3-TENSOR ISOMORPHISM *reduces to* SYMMETRIC MATRIX SPACE ISOMETRY.

Proof. In the proof of Proposition 5.1, we can easily replace A_i^Λ with $A_i^s = \begin{bmatrix} \mathbf{0} & A_i \\ A_i^t & \mathbf{0} \end{bmatrix}$, and the elementary alternating matrices with the elementary symmetric matrices, and the resulting proof goes through *mutatis mutandis.* ∎

6. Other reductions for the Main Theorem B.

In this section, we present other reductions to finish the proof of Theorem B. The reductions here are based on the constructions which may be summarized as "putting the given 3-way array to an appropriate corner of a larger 3-way array." Such an idea is quite classical in the context of matrix problems and wildness [43]; here we use the same idea for problems on 3-way arrays.

6.1. From 3-Tensor Isomorphism to Matrix Space Conjugacy.

Proposition 6.1. 3-Tensor Isomorphism *reduces to* Matrix Space Conjugacy. *Symbolically,* $U \otimes V \otimes W$ *reduces to* $V' \otimes V'^* \otimes W$*, where* $\dim V' = \dim U + \dim V$*.*

Proof. **The construction.** For a 3-way array $\mathtt{A} \in \mathrm{T}(\ell \times n \times m, \mathbb{F})$, let $\mathbf{A} = (A_1, \ldots, A_m) \in \mathrm{M}(\ell \times n, \mathbb{F})^m$ be the matrix tuple consisting of frontal slices of $\mathtt{A}$. Construct $\tilde{\mathbf{A}} = (\tilde{A}_1, \ldots, \tilde{A}_m) \in \mathrm{M}(\ell + n, \mathbb{F})^m$ from $\mathbf{A}$, where $\tilde{A}_i = \begin{bmatrix} \mathbf{0} & A_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. See Figure 5.

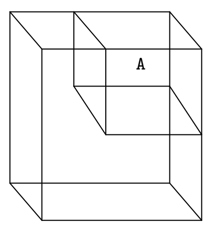
$\tilde{\mathtt{A}} =$ 

Fig. 5. *Pictorial representation of the reduction for Proposition 6.1.*

Given two non-degenerate 3-way arrays $\mathtt{A}, \mathtt{B}$ which we wish to test for isomorphism (we can assume non-degeneracy without loss of generality, see Observation 2.2), we claim that $\mathtt{A} \cong \mathtt{B}$ as 3-tensors if and only if the matrix spaces $\langle \tilde{\mathbf{A}} \rangle$ and $\langle \tilde{\mathbf{B}} \rangle$ are conjugate.

For the only if direction, since $\mathtt{A}$ and $\mathtt{B}$ are isomorphic as 3-tensors, there exist $P \in \mathrm{GL}(\ell, \mathbb{F})$, $Q \in \mathrm{GL}(n, \mathbb{F})$, and $R \in \mathrm{GL}(m, \mathbb{F})$, such that $P\mathbf{A}Q = \mathbf{B}^R = (B'_1, \ldots, B'_m) \in \mathrm{M}(\ell \times n, \mathbb{F})^m$. Let $\tilde{P} = \begin{bmatrix} P^{-1} & \mathbf{0} \\ \mathbf{0} & Q \end{bmatrix}$. Then $\tilde{P}^{-1}\tilde{A}_i\tilde{P} = \begin{bmatrix} P & \mathbf{0} \\ \mathbf{0} & Q^{-1} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{0} & A_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \cdot \begin{bmatrix} P^{-1} & \mathbf{0} \\ \mathbf{0} & Q \end{bmatrix} = \begin{bmatrix} \mathbf{0} & PA_iQ \\ \mathbf{0} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & B'_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. It follows that, $\tilde{P}^{-1}\tilde{\mathbf{A}}\tilde{P} = \tilde{\mathbf{B}}^R$, which just says that $\tilde{P}^{-1}\langle \tilde{\mathbf{A}} \rangle \tilde{P} = \langle \tilde{\mathbf{B}} \rangle$.

For the if direction, since $\langle \tilde{\mathbf{A}} \rangle$ and $\langle \tilde{\mathbf{B}} \rangle$ are conjugate, there exist $\tilde{P} \in \mathrm{GL}(\ell + n, \mathbb{F})$, and $\tilde{R} \in \mathrm{GL}(m, \mathbb{F})$, such that $\tilde{P}^{-1}\tilde{\mathbf{A}}\tilde{P} = \tilde{\mathbf{B}}^{\tilde{R}}$. Write $\tilde{\mathbf{B}}^{\tilde{R}} := \tilde{\mathbf{B}}' = (\tilde{B}'_1, \ldots, \tilde{B}'_m)$, where $\tilde{B}'_i = \begin{bmatrix} \mathbf{0} & B'_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$, $B'_i \in \mathrm{M}(\ell \times n, \mathbb{F})$. Let $\tilde{P} = \begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix}$, where $P_{1,1} \in \mathrm{M}(\ell, \mathbb{F})$. Then as $\tilde{\mathbf{A}}\tilde{P} = \tilde{P}\tilde{\mathbf{B}}'$, we have for every $i \in [m]$,

$$\begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix} \begin{bmatrix} \mathbf{0} & A_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & P_{1,1}A_i \\ \mathbf{0} & P_{2,1}A_i \end{bmatrix} = \begin{bmatrix} B'_iP_{2,1} & B'_iP_{2,2} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & B'_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix}. \tag{6.1}$$

This in particular implies that for every $i \in [m]$, $P_{2,1}A_i = \mathbf{0}$. In other words, every row of $P_{2,1}$ lies in the common left kernel of A_i with $i \in [m]$. Since $\mathbf{A}$ is non-degenerate, $P_{2,1}$ must be the zero matrix. It follows that $\tilde{P} = \begin{bmatrix} P_{1,1} & P_{1,2} \\ \mathbf{0} & P_{2,2} \end{bmatrix} \in \mathrm{GL}(\ell+n, \mathbb{F})$, so $P_{1,1}$ and $P_{2,2}$ are both invertible matrices. By Equation 6.1, we have $P_{1,1}\mathbf{A} = \mathbf{B}^{\tilde{R}} P_{2,2}$, where $P_{1,1} \in \mathrm{GL}(\ell, \mathbb{F})$, $P_{2,2} \in \mathrm{GL}(n, \mathbb{F})$, and $\tilde{R} \in \mathrm{GL}(m, \mathbb{F})$, which just says that `A` and `B` are isomorphic as 3-tensors. □

COROLLARY 6.2. 3-TENSOR ISOMORPHISM *reduces to*
1. MATRIX LIE ALGEBRA CONJUGACY, *where L is commutative;*
2. ASSOCIATIVE MATRIX ALGEBRA CONJUGACY, *where A is commutative (and in fact has the property that $ab = 0$ for all $a, b \in A$; note that A is not unital);*
3. MATRIX LIE ALGEBRA CONJUGACY, *where L is solvable of derived length 2, and $L/[L, L] \cong \mathbb{F}$; and,*
4. ASSOCIATIVE MATRIX ALGEBRA CONJUGACY, *where the Jacobson radical $R(A)$ squares to zero, and $A/R(A) \cong \mathbb{F}$.*

Proof. We use the notation from the proof of Proposition 6.1. Note that the matrix spaces constructed there, e. g., $\tilde{\mathbf{A}}$, are all subspaces of the $(\ell+n)\times(\ell+n)$ matrix space $\mathcal{U} := \begin{bmatrix} \mathbf{0} & M(\ell \times n, \mathbb{F}) \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$.

For (1) and (2), observe that for any two matrices $A, A' \in \mathcal{U}$, we have $AA' = 0$, and thus $[A, A'] = AA' - A'A = 0$ as well. Thus any matrix subspace of $\mathcal{U}$ is both a commutative matrix Lie algebra and a commutative associative matrix algebra with zero product.

For (3) and (4), we note that we can alter the construction of Proposition 6.1 by including the matrix $M_0 = \begin{bmatrix} I_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$ in both matrix spaces $\tilde{\mathcal{A}}$ and $\tilde{\mathcal{B}}$ without disrupting the reduction. Indeed, for the forward direction we have that (again, following notation as above)

$$\tilde{P}^{-1} \begin{bmatrix} I_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \tilde{P} = \begin{bmatrix} P & \mathbf{0} \\ \mathbf{0} & Q^{-1} \end{bmatrix} \begin{bmatrix} I_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P^{-1} & \mathbf{0} \\ \mathbf{0} & Q \end{bmatrix} = \begin{bmatrix} I_\ell & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}.$$

For the reverse direction, we then have that for $\tilde{\mathbf{B}}' = \tilde{\mathbf{B}}^{\tilde{R}}$, we have $\tilde{B}'_i = \begin{bmatrix} \alpha I_d & B'_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. Let $\tilde{P} = \begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix}$, where $P_{1,1} \in \mathrm{M}(\ell, \mathbb{F})$. Then as $\tilde{\mathbf{A}}\tilde{P} = \tilde{P}\tilde{\mathbf{B}}'$, we have for every $i \in [m]$,

(6.2)
$$\begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix} \begin{bmatrix} \mathbf{0} & A_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{0} & P_{1,1}A_i \\ \mathbf{0} & P_{2,1}A_i \end{bmatrix} = \begin{bmatrix} \alpha P_{1,1} + B'_i P_{2,1} & B'_i P_{2,2} \\ \alpha P_{2,1} & \mathbf{0} \end{bmatrix} = \begin{bmatrix} \alpha I_d & B'_i \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P_{1,1} & P_{1,2} \\ P_{2,1} & P_{2,2} \end{bmatrix}.$$

Considering the (2,1) block of this equation, we find that if $\alpha \neq 0$, then immediately $P_{2,1} = \mathbf{0}$. But even if $\alpha = 0$, then we are back to the same argument as in Proposition 6.1, namely that by the non-degeneracy of $\mathbf{A}$, we still get $P_{2,1} = \mathbf{0}$ by considering the (2,2) block. The remainder of the argument only depended on the (1,2) block of the preceding equation, which is the same as before.

Finally, to see the structure of the corresponding algebras, we must consider how our new element M_0 interacts with the others. Easy calculations reveal:

$$M_0^2 = M_0 \qquad M_0\tilde{A}_i = \tilde{A}_i \qquad \tilde{A}_i M_0 = \mathbf{0} \qquad [M_0, \tilde{A}_i] = M_0\tilde{A}_i - \tilde{A}_i M_0 = \tilde{A}_i$$

(3) For the structure of the Lie algebra, we have from the above equations that any commutator is either 0 or lands in $\mathcal{U}$. And since $[M_0, \tilde{A}_i] = \tilde{A}_i$, we have that $[L, L]$ is the subspace of $\mathcal{U}$ that we started with before including M_0. Since everything in that subspace commutes, we get that

$[[L, L], [L, L]] = 0$, and thus the Lie algebra is solvable of derived length 2. Moreover, $L/[L, L]$ is spanned by the image of M_0, whence it is isomorphic to $\mathbb{F}$.

(4) Recall that for rings without an identity, the Jacobson radical can be characterized as $R(A) = \{a \in A | (\forall b \in A)(\exists c \in A)[c + ba = cba]\}$ [67, p. 63]. Note that the only nontrivial cases to check are those for which $b = M_0$, since otherwise $ba = 0$ and then we may take $c = 0$ as well. So we have $R(A) = \{a \in A | (\exists c \in A)[c + M_0 a = cM_0 a]\}$. But since M_0 is a left identity, this latter equation is just $c + a = ca$. For any $a \in \mathcal{U}$, we may take $c = -a$, since then both sides of the equation are zero, and thus $R(A)$ includes all the matrices in the original space from Proposition 6.1. However, $M_0 \notin R(A)$, for there is no c such that $c + M_0 = cM_0$: any element of A can be written $\alpha M_0 + u$ for some $u \in \mathcal{U}$. Writing c this way, we are trying to solve the equation $\alpha M_0 + u + M_0 = (\alpha M_0 + u)M_0 = \alpha M_0$. Thus we conclude $u = 0$, and then we get that $\alpha + 1 = \alpha$, a contradiction. So $M_0 \notin R(A)$, and thus $A/R(A)$ is spanned by the image of M_0, whence it is isomorphic to $\mathbb{F}$. ∎

6.2. From Matrix Space Isometry to Algebra Isomorphism and Trilinear Form Equivalence.

Proposition 6.3. Matrix Space Isometry *reduces to* Algebra Isomorphism *and* Trilinear Form Equivalence. *Symbolically, $V \otimes V \otimes W$ reduces to $V' \otimes V' \otimes V'^*$ and to $V' \otimes V' \otimes V'$, where $\dim V' = \dim V + \dim W$.*

Proof. **The construction.** Given a matrix space $\mathcal{A}$ by an ordered linear basis $\mathbf{A} = (A_1, \ldots, A_m)$, construct the 3-way array $\mathtt{A}' \in T((n+m) \times (n+m) \times (n+m), \mathbb{F})$ whose frontal slices are:

$$A'_i = \mathbf{0} \quad (\text{for } i \in [n]) \qquad A'_{n+i} = \begin{bmatrix} A_i & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \quad (\text{for } i \in [m]).$$

Let $\mathrm{Alg}(\mathtt{A}')$ denote the algebra whose structure constants are defined by $\mathtt{A}'$, and let $f_{\mathtt{A}'}$ denote the trilinear form whose coefficients are given by $\mathtt{A}'$.

Given two matrix spaces $\mathcal{A}, \mathcal{B}$, we claim that $\mathcal{A}$ and $\mathcal{B}$ are isometric if and only if $\mathrm{Alg}(\mathtt{A}') \cong \mathrm{Alg}(\mathtt{B}')$ (isomorphism of algebras) if and only if $f_{\mathtt{A}'}$ and $f_{\mathtt{A}'}$ are equivalent as trilinear forms. The proofs are broken into the following two lemmas, which then complete the proof of the proposition. ∎

Lemma 6.4. *Let notation be as above. The matrix spaces $\mathcal{A}, \mathcal{B}$ are isometric if and only if $Alg(\mathtt{A}')$ and $Alg(\mathtt{B}')$ are isomorphic.*

Proof. Let $\mathbf{A}, \mathbf{B}$ be the ordered bases of $\mathcal{A}, \mathcal{B}$, respectively. Recall that $\mathcal{A}, \mathcal{B}$ are isometric if and only if there exist $(P, R) \in \mathrm{GL}(n, \mathbb{F}) \times \mathrm{GL}(m, \mathbb{F})$ such that $P^t \mathbf{A} P = \mathbf{B}^R$. Also recall that $\mathrm{Alg}(\mathtt{A}')$ and $\mathrm{Alg}(\mathtt{B}')$ are isomorphic as algebras if and only if there exists $\tilde{P} \in \mathrm{GL}(n+m, \mathbb{F})$ such that $\tilde{P}^t \mathbf{A}' \tilde{P} = \mathbf{B}'^{\tilde{P}}$. Since A_i (resp. B_i) form a linear basis of $\mathcal{A}$ (resp. $\mathcal{B}$), we have that A_i (resp. B_i) are linearly independent.

The only if direction is easy to verify. Given an isometry (P, R) between $\mathcal{A}$ and $\mathcal{B}$, let $\tilde{P} = \begin{bmatrix} P & \mathbf{0} \\ \mathbf{0} & R \end{bmatrix}$. Let $\tilde{P}^t \mathbf{A}' \tilde{P} = (A''_1, \ldots, A''_{n+m})$. Then for $i \in [n]$, $A''_i = \mathbf{0}$. For $n+1 \le i \le n+m$, $A''_i = \begin{bmatrix} P^t A_i P & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$. Let $\mathbf{B}'^{\tilde{P}} = (B''_1, \ldots, B''_{n+m})$. Then for $i \in [n]$, $B''_i = \mathbf{0}$. For $n+1 \le i \le n+m$, B''_i is the $(i-n)$th matrix in $\mathbf{B}^R$, which in turn equals $P^t A_i P$ by the assumption on P and R. This proves the only if direction.

For the if direction, let $\tilde{P} = \begin{bmatrix} P & X \\ Y & R \end{bmatrix} \in \mathrm{GL}(n+m, \mathbb{F})$ be an algebra isomorphism, where

P is of size $n \times n$. Let $\tilde{P}\mathbf{A}'\tilde{P}^t = (A''_1, \dots, A''_{n+m})$, and $\mathbf{B}'^{\tilde{P}} = (B''_1, \dots, B''_{n+m})$. Since for $i \in [n]$, $A'_i = \mathbf{0}$, we have $A''_i = \mathbf{0} = B''_i$. Therefore Y has to be $\mathbf{0}$, because B_i's are linearly independent. It follows that $\tilde{P} = \begin{bmatrix} P & X \\ \mathbf{0} & R \end{bmatrix}$, where P and R are invertible. So for $1 \leq i \leq m$, we have $\tilde{P}^t A'_{i+n} \tilde{P} = \begin{bmatrix} P^t & \mathbf{0} \\ X^t & R^t \end{bmatrix} \begin{bmatrix} A_i & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \begin{bmatrix} P & X \\ \mathbf{0} & R \end{bmatrix} = \begin{bmatrix} P^t A_i P & P^t A_i X \\ X^t A_i P & X^t A_i X \end{bmatrix}$. Also the last m matrices in $\mathbf{B}'^{\tilde{P}}$ are $\begin{bmatrix} B''_i & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix}$, where B''_i is the ith matrix in $\mathbf{B}^R$. This implies that $P \in \mathrm{GL}(n, \mathbb{F})$ and $R \in \mathrm{GL}(m, \mathbb{F})$ together form an isometry between $\mathcal{A}$ and $\mathcal{B}$. ∎

Corollary 6.5. Matrix Space Isometry *reduces to*

1. Associative Algebra Isomorphism, *for algebras that are commutative and unital;*
2. Associative Algebra Isomorphism, *for algebras that are commutative and 3-nilpotent ($abc = 0$ for all $a, b, c \in A$); and,*
3. Lie Algebra Isomorphism, *for Lie algebras that are 2-step nilpotent ($[u, [v, w]] = 0$ for all $u, v, w \in L$).*

Proof. We follow the notation from the proof of Lemma 6.4. We begin by observing that $\mathrm{Alg}(\mathtt{A}')$ is a 3-nilpotent algebra, and therefore is automatically associative. Let $V' = V \oplus W$, where $\dim V = n$, $\dim W = m$, and, as a subspace of $V' \cong \mathbb{F}^{n+m}$, V has a basis given by $e_1, \dots, e_n$ and W has a basis given by $e_{n+1}, \dots, e_{n+m}$. Let $\circ$ denote the product in $\mathrm{Alg}(\mathtt{A}')$, so that $x_i \circ x_j = \sum_k \mathtt{A}'(i, j, k) x_k$. Note that because the lower m rows and the rightmost m columns of each frontal slice of $\mathtt{A}'$ are zero, we have that $w \circ x = x \circ w = 0$ for any $w \in W$ and any $x \in V'$. Thus only way to get a nonzero product is of the form $v \circ v'$ where $v, v' \in V$, and here the product ends up in W, since the only nonzero frontal slices are $n+1, \dots, n+m$. Since any nonzero product ends up in W, and anything in W times anything at all is zero, we have that $abc = 0$ for all $a, b, c \in \mathrm{Alg}(\mathtt{A}')$, that is, $\mathrm{Alg}(\mathtt{A}')$ is 3-nilpotent. Any 3-nilpotent algebra is automatically associative, since the associativity condition only depends on products of three elements.

(1) As is standard, from the algebra $A = \mathrm{Alg}(\mathtt{A}')$, we may adjoin a unit by considering $A' = A[e]/(e \circ x = x \circ e = x | x \in A')$. In terms of vector spaces, we have $A' \cong A \oplus \mathbb{F}$, where the new $\mathbb{F}$ summand is spanned by the identity e. This standard algebraic construction has the property that two such algebras A, B are isomorphic if and only if their corresponding unit-adjoined algebras A', B' are (see, e. g., [35, 103]).

(2) If instead of general Matrix Space Isometry, we start from Symmetric Matrix Space Isometry (which is also 3TI-complete by Corollary 5.2), then we see that the algebra is commutative, for we then have $\mathtt{A}'(i, j, k) = \mathtt{A}'(j, i, k)$, which corresponds to $x_i \circ x_j = x_j \circ x_i$.

(3) By starting from an alternating matrix space $\mathcal{A}$ (and noting that Alternating Matrix Space Isometry is still 3TI-complete, by Corollary 5.2), we get that $\mathrm{Alg}(\mathtt{A}')$ is alternating, that is, $v \circ v = 0$. Since we still have that it is 3-nilpotent, $a \circ b \circ c = 0$, we find that $\circ$ automatically satisfies the Jacobi identity. An alternating product satisfying the Jacobi identity is, by definition, a Lie bracket (that is, we can define $[v, w] := v \circ w$), and thus we get a Lie algebra with structure constants $\mathtt{A}'$. Translating the 3-nilpotency condition $a \circ b \circ c = 0$ into the Lie bracket notation, we get $[a, [b, c]] = 0$, or in other words that the Lie algebra is nilpotent of class 2. ∎

Corollary 6.6. 3-Tensor Isomorphism *reduces to* Cubic Form Equivalence.

Proof. Agrawal and Saxena [2] show that Commutative Algebra Isomorphism reduces to Cubic Form Equivalence. Combine with Corollary 6.5(1). ∎

The reduction from $V \otimes V \otimes W$ to $V' \otimes V' \otimes V'$ is achieved by the same construction.

LEMMA 6.7. *Let* $\mathbf{A}, \mathbf{B}, \mathbf{A}'$, *and* $\mathbf{B}'$ *be as above. Then* $\mathbf{A}$ *and* $\mathbf{B}$ *are pseudo-isometric if and only if* $\mathbf{A}'$ *and* $\mathbf{B}'$ *are isomorphic as trilinear forms.*

Proof. Recall that $\mathbf{A}$ and $\mathbf{B}$ are pseudo-isometric if there exist $P \in \mathrm{GL}(n, \mathbb{F}), R \in \mathrm{GL}(m, \mathbb{F})$ such that $P^t \mathbf{A} P = \mathbf{B}^R$. Also recall that $\mathbf{A}'$ and $\mathbf{B}'$ are equivalent as trilinear forms if there exists $\tilde{P} \in \mathrm{GL}(n+m, \mathbb{F})$ such that $\tilde{P}^t \mathbf{A}'^{\tilde{P}} \tilde{P} = \mathbf{B}'$. Since A_i (resp. B_i) form a linear basis of $\mathcal{A}$, we have that A_i (resp. B_i) are linearly independent.

The only if direction is easy to verify. Given an pseudo-isometry P, R between $\mathbf{A}$ and $\mathbf{B}$, let $\tilde{P} = \begin{bmatrix} P & \mathbf{0} \\ \mathbf{0} & R^{-1} \end{bmatrix}$. Then it can be verified easily that $\tilde{P}$ is a trilinear form equivalence between $\mathbf{A}'$ and $\mathbf{B}'$, following the same approach in the proof of Lemma 6.4.

For the if direction, write $\tilde{P} = \begin{bmatrix} P & X \\ Y & R \end{bmatrix} \in \mathrm{GL}(n+m, \mathbb{F})$ be a trilinear form equivalence between $\mathbf{A}'$ and $\mathbf{B}'$. We first observe that the last m matrices in $\tilde{P}^t \mathbf{A}' \tilde{P}$ are still linearly independent. Then, because of the first n matrices in $\mathbf{B}'$ are all zero matrices, Y has to be the zero matrix. It follows that $\tilde{P} = \begin{bmatrix} P & X \\ \mathbf{0} & R \end{bmatrix}$, where P and R are invertible. Then it can be verified easily that P and R^{-1} form an pseudo-isometry between $\mathbf{A}$ and $\mathbf{B}$, following the same approach in the proof of Lemma 6.4. ∎

Finally, to show the connection between ALTERNATING MATRIX SPACE ISOMETRY and isomorphism testing of p-groups of class 2 and exponent p, we need a lemma which can be viewed as a constructive version of Baer's correspondence, communicated to us by James B. Wilson, with origins in the work of Brahana [20] and Baer [10] (see [107, Sec. 3]). A proof of this lemma can be found in [51].

LEMMA 6.8 (Constructive version of Baer's correspondence for matrix groups). *Let p be an odd prime. Over the finite field $\mathbb{F} = \mathbb{F}_{p^e}$,* ALTERNATING MATRIX SPACE ISOMETRY *is equivalent to* GROUP ISOMORPHISM *for matrix groups over $\mathbb{F}$ that are p-groups of class* 2 *and exponent p. More precisely, there are functions computable in time* $\mathrm{poly}(n, m, \log|\mathbb{F}|)$*:*

- $G\colon \Lambda(n, \mathbb{F})^m \to \mathrm{M}(n+m+1, \mathbb{F})^{n+m}$ *and*
- $Alt\colon \mathrm{M}(n, \mathbb{F})^m \to \Lambda(m, \mathbb{F})^{O(m^2)}$

such that: (1) for an alternating bilinear map $\mathbf{A}$*, the group generated by* $G(\mathbf{A})$ *is the Baer group corresponding to* $\mathbf{A}$*, (2) G and Alt are mutually inverse, in the sense that the group generated by* $G(Alt(M_1, \dots, M_m))$ *is isomorphic to the group generated by* $M_1, \dots, M_m$*, and conversely* $Alt(G(\mathbf{A}))$ *is pseudo-isometric to* $\mathbf{A}$*.*

7. Outlook: universality and open questions.

7.1. Towards universality for basis-explicit linear structures. A classic result is that GI is complete for isomorphism problems of explicitly given structures (see, e. g., [109, Section 15]). Here we formally state the linear-algebraic analogue of this result, and observe trivially that the results of [42] already show that 3-TENSOR ISOMORPHISM is universal among what we call "basis-explicit" (multi)linear structures of degree 2.

First let us recall the statement of the result for GI, so we can develop the appropriate analogue for TENSOR ISOMORPHISM. A *first-order signature* is a list of positive integers $(r_1, r_2, \dots, r_k; f_1, \dots, f_\ell)$; a *model* of this signature consists of a set V (colloquially referred to as "vertices"), k relations $R_i \subseteq V^{r_i}$, and ℓ functions $F_i\colon V^{f_i} \to V$. The numbers r_i are thus the arities of the relations

R_i, and the f_i are the arities of the functions F_i.[12] Two such models $(V; R_1, \ldots, R_k; F_1, \ldots, F_\ell)$ and $(V'; R'_1, \ldots, R'_k; F'_1, \ldots, F'_\ell)$ are isomorphic if there is a bijection $\varphi\colon V \to V'$ that sends R_i to R'_i for all i and F_i to F'_i for all i. In symbols, φ is an isomorphism if $(v_1, \ldots, v_{r_i}) \in R_i \Leftrightarrow (\varphi(v_1), \ldots, \varphi(v_{r_i})) \in R'_i$ for all i and all $v_* \in V$, and similarly if $\varphi(F_i(v_1, \ldots, v_{f_i})) = F'_i(\varphi(v_1), \ldots, \varphi(v_{f_i}))$ for all i and all $v_* \in V$. By an "explicitly given structure" or "explicit model" we mean a model where each relation R_i is given by a list of its elements and each function is given by listing all of its input-output pairs. Fixing a signature, the isomorphism problem for that signature is to decide, given two explicit models of that signature, whether they are isomorphic. This isomorphism problem is directly encoded into the isomorphism problem for edge-colored hypergraphs, which can then be reduced to GI using standard gadgets.

For example, the signature for directed graphs (possibly with self-loops) is simply $\sigma = (2;)$—its models are simply binary relations. If one wants to consider graphs without self-loops, this is a special case of the isomorphism problem for the signature σ, namely, those explicit models in which $(v, v) \notin R_1$ for any v. Note that a graph without self-loops is never isomorphic to a graph with self-loops, and two directed graphs without self-loops are isomorphic as directed graphs if and only if they are isomorphic as models of the signature σ. In other words, the isomorphism problem for simple directed graphs really is just a special case. The same holds for undirected graphs without self-loops, which are simply models of the signature σ in which $(v, v) \notin R_1$ and R_1 is symmetric. As another example, the signature for finite groups is $\gamma = (1; 1, 2)$: the first relation R_1 will be a singleton, indicating which element is the identity, the function F_1 is the inverse function $F_1(g) = g^{-1}$, and the second function F_2 is the group multiplication $F_2(g, h) = gh$. Of course, models of the signature γ can include many non-groups as well, but, as was the case with directed graphs, a group will never be isomorphic to a non-group, and two groups are isomorphic as models of γ iff they are isomorphic as groups.

A natural linear-algebraic analogue of the above is as follows. One additional feature we add here for purposes of generality is that we need to account for dual vector spaces. A *linear signature* is then a list of pairs of nonnegative integers $((r_1, r_1^*), \ldots, (r_k, r_k^*); (f_1, f_1^*), \ldots, (f_\ell, f_\ell^*))$ with the property that $r_i + r_i^* > 0$ and $f_i + f_i^* > 0$ for all i. By the arity of the i-th relation (resp., function) we mean the sum $r_i + r_i^*$ (resp., $f_i + f_i^*$).

Definition 7.1 (Linear signature, basis-explicit). *Given a linear signature*

$$\sigma = ((r_1, r_1^*), \ldots, (r_k, r_k^*); (f_1, f_1^*), \ldots, (f_\ell, f_\ell^*)),$$

a linear model *for σ over a field $\mathbb{F}$ consists of an $\mathbb{F}$-vector space V, and linear subspaces $R_i \leq V^{\otimes r_i} \otimes (V^*)^{\otimes r_i^*}$ for $1 \leq i \leq k$ and linear maps $F_i\colon V^{\otimes f_i} \otimes (V^*)^{\otimes f_i^*} \to V$ for $1 \leq i \leq \ell$. Two such linear models $(V; R_1, \ldots, R_k; F_1, \ldots, F_\ell), (V'; R'_1, \ldots, R'_k; F'_1, \ldots, F'_\ell)$ are* isomorphic *if there is a linear bijection $\varphi\colon V \to V'$ that sends R_i to R'_i for all i and F_i to F'_i for all i (details below).*

A basis-explicit linear model *is given by a basis for each R_i, and, for each element of a basis of the domain of F_i, the value of F_i on that element. Vectors here are written out in their usual dense coordinate representation.*

In particular, this means that an element of $V^{\otimes r}$—say, a basis element of R_1—is written out as a vector of length $(\dim V)^r$. We will only be concerned with finite-dimensional linear models.

[12]Sometimes one also includes constants in the definition, but these can be handled as relations of arity 1. While we could have done the same for functions, treating a function of arity f as its graph, which is a relation of arity $f + 1$, distinguishing between relations and functions will be useful when we come to our linear-algebraic analogue.

Given $\varphi\colon V \to V'$, let $\varphi^{\otimes r_i \otimes r_i^*}$ denote the linear map $\varphi^{\otimes r_i \otimes r_i^*}\colon V^{\otimes r_i} \otimes (V^*)^{\otimes r_i^*} \to V'^{\otimes r_i} \otimes (V'^*)^{\otimes r_i^*}$ which is defined on basis vectors factor-wise: $\varphi^{\otimes r_i \otimes r_i^*}(v_1 \otimes \cdots \otimes v_{r_i} \otimes \ell_1 \otimes \cdots \otimes \ell_{r_i^*}) = \varphi(v_1) \otimes \cdots \otimes \varphi(v_{r_i}) \otimes \varphi^*(\ell_1) \otimes \cdots \otimes \varphi^*(\ell_{r_i^*})$, and then extended to the whole space by linearity. (Recall that $V^* = \mathrm{Hom}(V, \mathbb{F})$, so elements of V^* are linear maps $\ell\colon V \to \mathbb{F}$, and thus $\varphi^*(\ell) := \ell \circ \varphi^{-1}$ is a map from $V' \to V \to \mathbb{F}$, i. e., an element of V'^*, as desired). Similarly, when we say that φ sends F_i to F_i', we mean that $\varphi(F_i(v_1 \otimes \cdots \otimes v_{f_i} \otimes \ell_1 \otimes \cdots \otimes \ell_{f_i^*})) = F_i'(\varphi^{\otimes f_i \otimes f_i^*}(v_1 \otimes \cdots \otimes v_{f_i} \otimes \ell_1 \otimes \cdots \otimes \ell_{f_i^*}))$.

REMARK 7.2. *We use the term "basis-explicit" rather than just "explicit," because over a* finite *field, one may also consider a linear model of σ as an explicit model of a different signature (where the different signature additionally encodes the structure of a vector space on V, namely, the addition and scalar multiplication), and then one may talk of a single mathematical object having explicit representations—where everything is listed out—and basis-explicit representations—where things are described in terms of bases. An example of this distinction arises when considering isomorphism of p-groups of class 2: the "explicit" version is when they are given by their full multiplication table (which reduces to* GI*), while the "basis-explicit" version is when they are given by a generating set of matrices or a polycyclic presentation (which* GI *reduces* to*).*

THEOREM 7.3 (Futorny–Grochow–Sergeichuk [42]). *Given any linear signature σ where all relationship arities are at most 3 and all function arities are at most 2, the isomorphism problem for finite-dimensional basis-explicit linear models of σ reduces to* 3-TENSOR ISOMORPHISM *in polynomial time.*

Because of the equivalence between d-TENSOR ISOMORPHISM and 3-TENSOR ISOMORPHISM (Theorem A + [42]), we expect the analogous result to hold for arbitrary d. Thus an analogue of the results of [42] for d-tensors would yield the full analogue of the universality result for GI.

OPEN QUESTION 7.4. *Is d-*TENSOR ISOMORPHISM *universal for isomorphism problems on d-way arrays? That is, prove the analogue of the results of [42] for d-way arrays for all $d \geq 3$.*

7.2. Other open questions. We start by highlighting two questions about the type of reductions used. First, we wonder whether all the reductions in this paper can be made into p-projections on the set of all tensors, rather than only on the set of non-degenerate tensors; see Remark 2.5. Second, we ask about functoriality, as this has potential connections to the theory of asymptotic spectra [100, 102]:

OPEN QUESTION 7.5. *Which reductions in this paper can be made functorial on the relevant categories with all homomorphisms, not just isomorphisms? Which categories admit a theory of asymptotic spectra, and do these reductions provide morphisms between the asymptotic spectra?*

Most of our results hold for arbitrary fields, or arbitrary fields with minor restrictions. However, in all of our reductions, we reduce one problem over $\mathbb{F}$ to another problem over the same field $\mathbb{F}$.

OPEN QUESTION 7.6. *What is the relationship between* TI *over different fields? In particular, what is the relationship between* $\mathsf{TI}_{\mathbb{F}_p}$ *and* $\mathsf{TI}_{\mathbb{F}_{p^e}}$*, between* $\mathsf{TI}_{\mathbb{F}_p}$ *and* $\mathsf{TI}_{\mathbb{F}_q}$ *for coprime p, q, or between* $\mathsf{TI}_{\mathbb{F}_p}$ *and* $\mathsf{TI}_{\mathbb{Q}}$*?*

We note that even the relationship between $\mathsf{TI}_{\mathbb{F}_p}$ and $\mathsf{TI}_{\mathbb{F}_{p^e}}$ is not particularly clear. For matrix *tuples* (rather than spaces; equivalently, representations of finitely generated algebras) it is the case that for any extension field $\mathbb{K} \supseteq \mathbb{F}$, two matrix tuples over $\mathbb{F}$ are $\mathbb{F}$-equivalent (resp., conjugate) if and only if they are $\mathbb{K}$-equivalent [63] (see [34] for a simplified proof). However, for equivalence of tensors this need not be the case. This is closely related to the so-called "problem of forms" for various algebras, namely the existence of algebras that are not isomorphic over $\mathbb{F}$, but which become isomorphic over an extension field. The problem of forms is why $\mathbb{Q}$-isomorphism of $\mathbb{Q}$-algebras is not known to be decidable, even though $\mathbb{C}$-isomorphism of $\mathbb{Q}$-algebras is in PSPACE.

Example 7.7 (Non-isomorphic tensors isomorphic over an extension field). *Over $\mathbb{R}$, let $M_1 = I_2$ and let $M_2 = \mathrm{diag}(1,-1)$. Since these two matrices have different signatures, they are not isometric over $\mathbb{R}$; since they have the same rank, they* are *isometric over $\mathbb{C}$. To turn this into an example of 3-tensors, first we consider the corresponding instance of* Matrix Space Isometry *given by $\mathcal{M}_1 = \langle M_1 \rangle$ and $\mathcal{M}_2 = \langle M_2 \rangle$. Note that $\mathcal{M}_1 = \{\lambda I_2 : \lambda \in \mathbb{R}\}$, so the signatures of all matrices in $\mathcal{M}_1$ are $(2,0)$, $(0,0)$, or $(0,2)$. Similarly, the signatures appearing in $\mathcal{M}_2$ are $(1,1)$ and $(0,0)$, so these two matrix spaces are not isometric over $\mathbb{R}$, though they are isometric over $\mathbb{C}$ since M_1 and M_2 are. Finally, apply the reduction from* Matrix Space Isometry *to* 3TI *[42] to get two 3-tensors $\mathtt{A}_1, \mathtt{A}_2$. Since the reduction itself is independent of field, if we consider it over $\mathbb{R}$ we find that $\mathtt{A}_1$ and $\mathtt{A}_2$ must not be isomorphic 3-tensors over $\mathbb{R}$, but if we consider the reduction over $\mathbb{C}$ we find that they are isomorphic as 3-tensors over $\mathbb{C}$.*

Similar examples can be constructed over finite fields $\mathbb{F}$ of odd characteristic, taking $M_1 = I_2$ and $M_2 = \mathrm{diag}(1,\alpha)$ where α is a non-square in $\mathbb{F}$ (and replacing the role of $\mathbb{C}$ with that of $\mathbb{K} = \mathbb{F}[x]/(x^2-\alpha)$). Instead of signature, isometry types of matrices over $\mathbb{F}$ are characterized by their rank and whether their determinant is a square or not. In this case, since our matrices are even-dimensional diagonal matrices, scaling them multiplies their determinant by a square. Thus every matrix in $\mathcal{M}_1$ will have its determinant being a square in $\mathbb{F}$, and every nonzero matrix in $\mathcal{M}_2$ will not, but in $\mathbb{K}$ they are all squares.

It would also be interesting to study the complexity of other group actions on tensors and how they relate to the problems here. For example, the action of unitary groups $U(\mathbb{C}^{n_1}) \times \cdots \times U(\mathbb{C}^{n_d})$ on $\mathbb{C}^{n_1} \otimes \cdots \otimes \mathbb{C}^{n_d}$ classifies pure quantum states up to "local unitary operations" (e. g., [32,44,79]). Isomorphism of m-dimensional lattices in n-dimensional space can be seen as the natural action of $O_n(\mathbb{R}) \times \mathrm{GL}_m(\mathbb{Z})$ by left and right multiplication on $n \times m$ real matrices. As another example, orbits for several of the natural actions of $\mathrm{GL}_n(\mathbb{Z}) \times \mathrm{GL}_m(\mathbb{Z}) \times \mathrm{GL}_r(\mathbb{Z})$ on 3-tensors over $\mathbb{Z}$, even for small values of n, m, r, are the fundamental objects in Bhargava's groundbreaking work on higher composition laws [15–18]. In analogy with Hilbert's Tenth Problem, we might expect this problem to be undecidable. We note that while the orthogonal group $O(V)$ is the stabilizer of a 2-form on V (that is, an element of $V \otimes V$) and $\mathrm{SL}(V)$ is the stabilizer of the induced action on $\bigwedge^{\dim V} V$ (by the determinant)—so gadgets similar to those in this paper might be useful—$\mathrm{GL}_n(\mathbb{Z})$ is not the stabilizer of any such structure.

In Remark 4.1 we observed that any reduction (in the sense of Sec. 2.3) from dTI to 3TI must have a blow-up in dimension which is asymptotically at least $n^{d/3}$, while our construction uses dimension $O(d^2 n^{d-1})$. Using the quiver from Fig. 6 below instead of that in Fig. 3 we can reduce this to $O(d^2 n^{\lfloor d/2 \rfloor})$ for $d \geq 5$:

Open Question 7.8. *Is there a reduction from dTI to 3TI (as in Sec. 2.3) such that the dimension of the output is $\mathrm{poly}(d) \cdot n^{d/3(1+o(1))}$?*

Finally, in terms of practical algorithms, we wonder how well modern SAT solvers would do on instances of 3-Tensor Isomorphism over $\mathbb{F}_2$ (or over other finite fields, encoded into bit-strings).

Acknowledgments. The authors would like to thank James B. Wilson for related discussions, and Uriya First, Lek-Heng Lim, and J. M. Landsberg for help searching for references asking whether dTI could reduce to 3TI. They also thank Nengkun Yu, Yinan Li, and Graeme Smith for explaining the notion of SLOCC, and Ryan Williams for pointing out the problem of distinguishing between

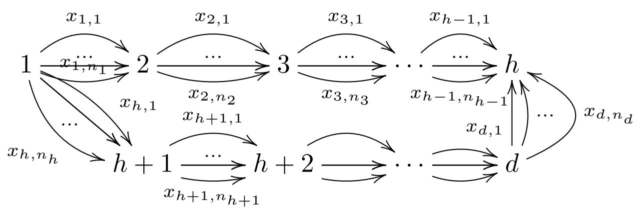


Fig. 6. *An alternative graph G whose path algebra we take a quotient of to construct a more efficient reduction than that of Theorem A. Here $h = \lfloor d/2 \rfloor + 2$; the reason to add 2 rather than 1 is to avoid introducing any nontrivial graph automorphisms. Given an $n_1 \times n_2 \times \cdots \times n_d$ d-tensor $\mathtt{A}$, we quotient by the relation $x_{1,i_1} x_{2,i_2} \cdots x_{h-1,i_{h-1}} = \sum_{i_h=1}^{n_h} \sum_{i_{h+1}=1}^{n_{h+1}} \cdots \sum_{i_d=1}^{n_d} \mathtt{A}(i_1, i_2, \ldots, i_{h-1}, i_h, i_{h+1}, \cdots, i_d) x_{h,i_h} x_{h+1,i_{h+1}} \cdots x_{d,i_d}$.*

ETH and #ETH. The authors would like to thank the anonymous reviewers for their careful reading and valuable suggestions. Ideas leading to this work originated from the 2015 workshop "Wildness in computer science, physics, and mathematics" at the Santa Fe Institute.

Appendix A. Reducing Cubic Form Equivalence to Degree-d Form Equivalence.

Proposition A.1. Cubic Form Equivalence *reduces to* Degree-d Form Equivalence*, for any $d \geq 3$.*

We suspect that the map $f \mapsto z^{d-d'} f$ would give a reduction from Degree-d' Form Equivalence to Degree-d Form Equivalence for any $d' < d$, but our argument relies on a case analysis that is somewhat specific to $d' = 3$. For $d > 2d'$ our same argument works. Our argument might be adaptable to any fixed value of d' the prover desires for all $d \geq d'$, with a consequently more complicated case analysis, but to prove it for all d' simultaneously seems to require a different argument.

Proof. The reduction itself is quite simple: $f \mapsto z^{d-3} f$, where z is a new variable not appearing in f. If A is an equivalence between f and g—that is, $f(x) = g(Ax)$—then $\mathrm{diag}(A, 1_z)$ is an equivalence from $z^{d-3} f$ to $z^{d-3} g$. Conversely, suppose $\tilde{f} = z^{d-3} f$ is equivalent to $\tilde{g} = z^{d-3} g$ via $\tilde{f}(x) = \tilde{g}(Bx)$. We split the proof into several cases.

If $d = 3$, then z is not present so we already have that f and g are equivalent.

If f is not divisible by ℓ^{d-3} for any linear form ℓ, then z^{d-3} is the unique factor in both $z^{d-3} f$ and $z^{d-3} g$ which is raised do the $d-3$ power. Thus any equivalence B between these two must map z to itself, hence has the form

$$B = \left(\begin{array}{ccc|c} * & \ldots & * & 0 \\ \vdots & \ddots & \vdots & \vdots \\ * & \ldots & * & 0 \\ \hline * & \ldots & * & 1 \end{array} \right),$$

(if we put z last in our basis, and think of the matrix as acting on the left of the column vectors corresponding to the variables). However, since both f and g do not depend on z, it must be the case that whatever contributions z makes to $g(Bx)$, they all cancel. More precisely, all monomials involving z in $g(Bx)$ must cancel, so if we alter B into $\tilde{B}$ that $\tilde{B} x_i$ never includes z (that is, if we make the stars in the last row above all zero), then $g(\tilde{B}x) = g(Bx)$, hence $f(x) = g(\tilde{B}x)$, so f and g are equivalent.

The preceding case always applies when $d > 6$, for then $d - 3 > 3$, but $\deg f = 3$.

If f is divisible by ℓ^{d-3} for some linear form ℓ, then we are left to the following cases:

1. $d \leq 6$ and f is a product of linear forms;
2. $d = 4$, f is a product of a linear form and an irreducible quadratic form.

Case 1: $d \leq 6$ and f is a product of linear forms. Let us define $\mathrm{rk}(f)$ as the number of linearly independent linear forms appearing in the factorization of f. Since we have supposed $z^{d-3}f \sim z^{d-3}g$, by uniqueness of factorization g must be a product of linear forms of the same rank as f. We will use several times the fact that GL_n acts transitively on k-tuples of linearly independent vectors for all $k \leq n$, and and in order to have $\mathrm{rk}(f)$ linearly independent forms, we must have $n \geq \mathrm{rk}(f)$. (Note that when $d = 6$ we must have $\mathrm{rk}(f) = 1$, since we've assumed some ℓ^{d-3} divides f, and similarly when $d = 5$ we must have $f = \ell_1^2\ell_2$.) Let B denote an equivalence such that $z^{d-3}f = (Bz)^{d-3}g(Bx)$.

- If $\mathrm{rk}(f) = 1$, then $f = \alpha\ell^3$ for some $\alpha \in \mathbb{F}$. Since we have assumed $z^{d-3}f \sim z^{d-3}g$, we get that $\mathrm{rk}(g) = 1$, so g also has the form $\beta\ell'^3$. If B does not send z to a scalar multiple of itself, then as B sends $z^{d-3}f$ to $z^{d-3}g$, B needs to sent z to ℓ' and ℓ to z up to scalar multiples. That is, $d = 6$, $B \cdot z = \gamma\ell$, and $B \cdot \ell' = \eta z$, for some nonzero $\gamma, \eta \in \mathbb{F}$. Then we have $z^3\alpha\ell^3 = B \cdot (z^{d-3}g) = \beta(\gamma\eta)^3 z^3\ell^3$. By transitivity of GL_n, there is a matrix $B' \in \mathrm{GL}_n$ such that $B \cdot \ell' = \ell$, and we have that $(\gamma\eta)B'$ is an equivalence sending g to f, and thus $f \sim g$.
  If B sends z to a scalar multiple of itself, then $B \cdot \ell' = \eta\ell$, and we get $B \cdot (z^{d-3}g) = \beta\eta^3\ell$. Letting B' be as above, we find that $\eta B'$ is an equivalence sending g to f. In either case, we thus that $z^{d-3}f \sim z^{d-3}g \Leftrightarrow f \sim g$.
- If $\mathrm{rk}(f) = 2$, then f can either be written $\ell_1^2\ell_2$ or $\ell_1\ell_2\ell_3$ such that there are nonzero α_i with $\alpha_1\ell_1 + \alpha_2\ell_2 + \alpha_3\ell_3 = 0$.
  If $f = \ell_1^2\ell_2$, then since $z^{d-3}f \sim z^{d-3}g$, we also have $g = \ell_1'^2\ell_2'$ by uniqueness of factorization, and since GL_n acts transitively on linearly independent pairs, there is always an element sending $\ell_1 \mapsto \ell_1'$ and $\ell_2 \mapsto \ell_2'$, and thus $f \sim g$. (Note that, unlike the rank-1 case, there is no issue with scalars, since scalars can be absorbed into ℓ_2.)
  If $f = \ell_1\ell_2\ell_3$ satisfying $\alpha_1\ell_1 + \alpha_2\ell_2 + \alpha_3\ell_3 = 0$ with all $\alpha_i \neq 0$, then we must have $d = 4$, for we have assumed that f is divisible by some linear form to the $d - 3$ power. By uniqueness of factorization, $g = \ell_1'\ell_2'\ell_3'$. Let B be an equivalence sending zg to zf. Since z is linearly independent from ℓ_1, ℓ_2, ℓ_3, but ℓ_1, ℓ_2, ℓ_3 satisfy a linear relation with all nonzero coefficients, we must have that $B \cdot \mathit{Span}\{\ell_1', \ell_2', \ell_3'\} = \mathit{Span}\{\ell_1, \ell_2, \ell_3\}$. In particular, B must send the x-variables that occur in the ℓ_i' to the x-variables (not involving z), so B restricts to a map $B' \colon \mathit{Span}\{x_i\} \to \mathit{Span}\{x_i\}$ such that $B' \cdot g = f$. Thus $f \sim g$.
- If $\mathrm{rk}(f) = 3$, then $f = \ell_1\ell_2\ell_3$ with all ℓ_i linearly independent. If $z^{d-3}f \sim z^{d-3}g$, then $\mathrm{rk}(g) = \mathrm{rk}(f) = 3$, so g must have the form $\ell_1'\ell_2'\ell_3'$ with all ℓ_i' linearly independent. Since GL_n acts transitively on 3-tuples of linearly independent vectors, we thus have $f \sim g$.

In all the above cases, we thus get $z^{d-3}f \sim z^{d-3}g$ iff $f \sim g$, as desired.

Case 2: $d = 4$ and $f = \ell\varphi$ where ℓ is linear and φ is an irreducible quadratic. Then to understand the situation we begin by first doing a change of basis on f to put φ into a form in which its kernel is evident. Note that none of these simplifications are part of the reduction, but rather they are to help us prove that the reduction works. Thinking of φ as given by its matrix M_φ

such that $\varphi(x) = x^t M_\varphi x$, we can always change basis to get M_φ into the form

$$\begin{bmatrix} M' & 0 \\ 0 & 0_{n-r} \end{bmatrix}$$

where $r = \mathrm{rk}(M_\varphi) = \mathrm{rk}(M')$. Since φ does not depend on z, if we think of φ as a quadratic form on $\{x_1, \ldots, x_n, z\}$, then the matrices are the same, but larger by one additional zero row and column.

Next we will try to simplify ℓ as much as possible while maintaining the (new) form of $M_\varphi = \mathrm{diag}(M', \mathbf{0})$. For this we first compute the stabilizer of the new form of M_φ. We can compute the stabilizer as the set of invertible matrices A such that:

$$\begin{bmatrix} A_{11}^t & A_{21}^t \\ A_{12}^t & A_{22}^t \end{bmatrix} \begin{bmatrix} M' & 0 \\ 0 & 0_{n-r+1} \end{bmatrix} \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} = \begin{bmatrix} M' & 0 \\ 0 & 0_{n-r+1} \end{bmatrix}.$$

This turns into the following equations on the blocks of X:

$$\begin{array}{rclcrcl} A_{11}^t M' A_{11} & = & M' & \qquad & A_{12}^t M' A_{11} & = & 0 \\ A_{12}^t M' A_{12} & = & 0 & & A_{11}^t M' A_{12} & = & 0 \end{array}$$

From the first equation and the fact that M' is full rank, we find that A_{11} must be an invertible $r \times r$ matrix. From the next equation and the fact that both M and A_{11} are full rank, we then find that $A_{12} = 0$. Thus the stabilizer of M_φ is:

$$S := \left\{ \begin{bmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{bmatrix} : A_{11}^t M' A_{11} = M' \text{ and } A_{22} \text{ is invertible} \right\}.$$

Now we simplify ℓ. Note that S acts on ℓ as a column vector. Consider $\ell = \sum_{i=1}^n \ell_i x_i$, with $\ell_i \in \mathbb{F}$; we will say "ℓ contains x_i" if and only if $\ell_i \neq 0$. If ℓ contains some x_{r+k} with $k \geq 1$, then by setting $A_{11} = I_r$ and $A_{21} = 0$, we may choose A_{22} to be any invertible matrix which sends $(\ell_{r+1}, \ldots, \ell_n, \ell_{n+1})$ (recall the trailing ℓ_{n+1} for the z coordinate) to $(1, 0, \ldots, 0)$, and thus without loss of generality we may assume that ℓ only contains x_i with $1 \leq i \leq r+1$.

Next, note that if ℓ contains some x_i for $1 \leq i \leq r$ *and* x_{r+1}, then we may use the action of S to eliminate the x_{r+1}. Namely, by taking $A_{11} = I_r$, $A_{22} = I_{n+1}$, and $A_{21} = (-\ell_{r+1}/\ell_i)E_{1i}$. This makes $\ell_i x_i$ in ℓ contribute $-\ell_{r+1}$ to the x_{r+1} coordinate, eliminating x_{r+1}. Thus, under the action of S, we need only consider two cases for linear forms under the action of S: a linear form is equivalent to either

a. one which contains some x_i with $1 \leq i \leq r$, in which case we can bring it to a form in which it contains *no* x_{r+j} with $j \geq 1$ (and no z), *or*
b. it contains no x_i with $1 \leq i \leq r$, in which case we can use the action of S to bring it to the form $\ell = x_{r+1}$.

Let us call the corresponding linear forms "type (a)" and "type (b)." Note that the linear form z is of type (b).

Now, write $f = \ell\varphi$ and $g = \ell'\varphi'$, and assume that we have applied the preceding change of basis to bring f to the form specified above. Recall that we are assuming $\tilde{f} \sim \tilde{g}$, and need to show that $f \sim g$. If, after applying the same change of basis to g, we do not have $M_{\varphi'} = M_\varphi$, then $f \not\sim g$ and also $\tilde{f} \not\sim \tilde{g}$—contrary to our assumption—since φ (resp., φ') is the unique irreducible quadratic factor of $\tilde{f}$ (resp., $\tilde{g}$). So we may assume that, after this change of basis, $\varphi = \varphi'$, both of which have $M_\varphi = \mathrm{diag}(M', 0_{n-r+1})$ with $r = \mathrm{rank}(M_\varphi)$.

Next, since we are assuming $\tilde{f} \sim \tilde{g}$, and z itself is of type (b), so it must be the case that the types of ℓ, ℓ' are the same. Thus we have two cases to consider: either they are both of type (a), or both of type (b).

Suppose both ℓ, ℓ' are of type (a). In this case, the equivalence between $\tilde{f}$ and $\tilde{g}$ cannot send z to ℓ' and ℓ to z, for both ℓ, ℓ' are of type (a), whereas z is of type (b). Thus the equivalence between $\tilde{f}$ and $\tilde{g}$ must restrict to an equivalence between f and g (when we ignore z, or set its contribution to the other variables to zero, as in the above case where f was not divisible by ℓ^{d-3}).

Suppose both ℓ, ℓ' are of type (b). In this case, it is possible that the equivalence from $\tilde{f}$ to $\tilde{g}$ *could* send z to ℓ' and ℓ to z (since all three of ℓ, ℓ', z are in case (b)); however, we will see that in this case, even such a situation will not cause an issue. Without loss of generality, by the change of bases described above, we have $\tilde{f} = zx_{r+1}\varphi$ and $\tilde{g} = z\ell'\varphi$ (the same φ), where ℓ' contains no x_i with $1 \leq i \leq r$. Using elements of S with $A_{11} = I_r$, and $A_{21} = 0$, we then get an action of GL_{n-r+1} (via A_{22}) on linear forms in the variables $x_{r+1}, \dots, x_n, z$. Since ℓ' is linearly independent from z (in particular, it does not contain z) and the action of GL is transitive on pairs of linearly independent vectors, we may use S to fix φ and z, and send x_{r+1} to ℓ', giving the desired equivalence $f \sim g$. ∎

Appendix B. Relations with Graph Isomorphism and Code Equivalence.

We observe then Graph Isomorphism and Code Equivalence reduce to 3-Tensor Isomorphism. In particular, the class TI contains the classical graph isomorphism class GI.

Recall Code Equivalence asks to decide whether two linear codes are the same up to a linear transformation preserving the Hamming weights of codes. Here the linear codes are just subspaces of $\mathbb{F}_q^n$ of dimension d, represented by linear bases. Linear transformations preserving the Hamming weights include permutations and monomial transformations. Recall that the latter consists of matrices where every row and every column has exactly one non-zero entry. Indeed, over many fields this is without loss of generality, as Hamming-weight-preserving linear maps are always induced by monomial transformations (first proved over finite fields [75], and more recently over much more general algebraic objects, e. g., [46]). CodeEq has long been studied in the coding theory community; see e.g. [85, 93].

For Code Equivalence, we observe that previous results already combine to give:

Observation B.1. Code Equivalence *(under permutations) reduces to* 3-Tensor Isomorphism*.*

Proof. Code Equivalence reduces to Matrix Lie Algebra Conjugacy [48], a special case of Matrix Space Conjugacy, which in turn reduces to 3TI [42]. ∎

Since Graph Isomorphism reduces to Code Equivalence [71] (see [80]) and [85] (even over arbitrary fields [48]), by Obs. B.1 and Thm. B, we have the following.

Corollary B.2. Graph Isomorphism *reduces to* Alternating Matrix Space Isometry*.*

Using similar gadgets, in a follow-up paper we in fact show that the more general problem Monomial Code Equivalence—which is perhaps more natural from the viewpoint of coding theory and Hamming distance, see above—also reduces to 3TI.

Proposition B.3 (G. & Q., [51, Prop. 7]). Monomial Code Equivalence *reduces to* 3-Tensor Isomorphism*.*

REFERENCES

[1] M. Agrawal and N. Saxena, *Automorphisms of finite rings and applications to complexity of problems*, in STACS 2005, 22nd Annual Symposium on Theoretical Aspects of Computer Science, Proceedings, 2005, pp. 1–17, https://doi.org/10.1007/978-3-540-31856-9_1.

[2] M. Agrawal and N. Saxena, *Equivalence of $\mathbb{F}$-algebras and cubic forms*, in STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science, Proceedings, 2006, pp. 115–126, https://doi.org/10.1007/11672142_8.

[3] E. Allender and B. Das, *Zero knowledge and circuit minimization*, Inf. Comput., 256 (2017), pp. 2–8, https://doi.org/10.1016/j.ic.2017.04.004.

[4] I. Assem, D. Simson, and A. Skowroński, *Elements of the representation theory of associative algebras. Vol. 1*, vol. 65 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 2006, https://doi.org/10.1017/CBO9780511614309. Techniques of representation theory.

[5] L. Babai, *On the automorphism groups of strongly regular graphs I*, in Proceedings of the 5th Conference on Innovations in Theoretical Computer Science, ITCS '14, 2014, pp. 359–368, https://doi.org/10.1145/2554797.2554830.

[6] L. Babai, *Graph isomorphism in quasipolynomial time [extended abstract]*, in Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, 2016, pp. 684–697, https://doi.org/10.1145/2897518.2897542. arXiv:1512.03547 [cs.DS] version 2.

[7] L. Babai, R. Beals, and Á. Seress, *Polynomial-time theory of matrix groups*, in Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, 2009, pp. 55–64, https://doi.org/10.1145/1536414.1536425.

[8] L. Babai, P. Codenotti, J. A. Grochow, and Y. Qiao, *Code equivalence and group isomorphism*, in Proceedings of the Twenty-Second Annual ACM–SIAM Symposium on Discrete Algorithms (SODA11), Philadelphia, PA, 2011, SIAM, pp. 1395–1408, https://doi.org/10.1137/1.9781611973082.107.

[9] L. Babai, P. Erdős, and S. M. Selkow, *Random graph isomorphism*, SIAM J. Comput., 9 (1980), pp. 628–635, https://doi.org/10.1137/0209047.

[10] R. Baer, *Groups with abelian central quotient group*, Trans. AMS, 44 (1938), pp. 357–386, https://doi.org/10.1090/S0002-9947-1938-1501972-1.

[11] G. R. Belitskii and V. V. Sergeichuk, *Complexity of matrix problems*, Lin. Algebra Appl., 361 (2003), pp. 203–222, https://doi.org/10.1016/S0024-3795(02)00391-9. Ninth Conference of the International Linear Algebra Society (Haifa, 2001).

[12] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, *Exact and asymptotic measures of multipartite pure-state entanglement*, Physical Review A, 63 (2000), p. 012307, https://doi.org/10.1103/PhysRevA.63.012307.

[13] J. Berthomieu, J. Faugère, and L. Perret, *Polynomial-time algorithms for quadratic isomorphism of polynomials: The regular case*, J. Complexity, 31 (2015), pp. 590–616, https://doi.org/10.1016/j.jco.2015.04.001.

[14] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-correcting linear codes: Classification by isometry and applications*, vol. 18, Springer Science and Business Media, 2006.

[15] M. Bhargava, *Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations*, Ann. of Math. (2), 159 (2004), pp. 217–250, https://doi.org/10.4007/annals.2004.159.217.

[16] M. Bhargava, *Higher composition laws. II. On cubic analogues of Gauss composition*, Ann. of Math. (2), 159 (2004), pp. 865–886, https://doi.org/10.4007/annals.2004.159.865.

[17] M. Bhargava, *Higher composition laws. III. The parametrization of quartic rings*, Ann. of Math. (2), 159 (2004), pp. 1329–1360, https://doi.org/10.4007/annals.2004.159.1329.

[18] M. Bhargava, *Higher composition laws. IV. The parametrization of quintic rings*, Ann. of Math. (2), 167 (2008), pp. 53–94, https://doi.org/10.4007/annals.2008.167.53.

[19] W. Bosma, J. J. Cannon, and C. Playoust, *The Magma algebra system I: the user language.*, J. Symb. Comput., (1997), pp. 235–265, https://doi.org/10.1006/jsco.1996.0125.

[20] H. R. Brahana, *Metabelian groups and trilinear forms*, Duke Math. J., 1 (1935), pp. 185–197, https://doi.org/10.1215/S0012-7094-35-00117-X.

[21] P. Brooksbank, E. O'Brien, and J. Wilson, *Testing isomorphism of graded algebras*, Trans. Amer. Math. Soc., 372 (2019), pp. 8067–8090, https://doi.org/10.1090/tran/7884.

[22] P. A. Brooksbank, J. A. Grochow, Y. Li, Y. Qiao, and J. B. Wilson, *Incorporating Weisfeiler–Leman into algorithms for group isomorphism.* arXiv:1905.02518 [cs.CC], 2019.

[23] P. A. Brooksbank and E. M. Luks, *Testing isomorphism of modules*, J. Algebra, 320 (2008), pp. 4020 – 4029, https://doi.org/10.1016/j.jalgebra.2008.07.014.

[24] P. A. Brooksbank, J. Maglione, and J. B. Wilson, *Thetensor.space.* https://github.com/

thetensor-space/, 2019.

[25] P. A. Brooksbank and J. B. Wilson, *Computing isometry groups of Hermitian maps*, Trans. Amer. Math. Soc., 364 (2012), pp. 1975–1996, https://doi.org/10.1090/S0002-9947-2011-05388-2.

[26] P. A. Brooksbank and J. B. Wilson, *The module isomorphism problem reconsidered*, J. Algebra, 421 (2015), pp. 541–559, https://doi.org/10.1016/j.jalgebra.2014.09.004.

[27] P. Bürgisser, M. L. Doğan, V. Makam, M. Walter, and A. Wigderson, *Polynomial time algorithms in invariant theory for torus actions*, in 36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference), V. Kabanets, ed., vol. 200 of LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, pp. 32:1–32:30, https://doi.org/10.4230/LIPIcs.CCC.2021.32.

[28] J. Cannon and D. F. Holt, *Automorphism group computation and isomorphism testing in finite groups*, J. Symb. Comput., 35 (2003), pp. 241–267, https://doi.org/10.1016/S0747-7171(02)00133-5.

[29] K.-T. Chen, *Integration of paths, geometric invariants and a generalized baker-hausdorff formula*, Ann. Math., (1957), pp. 163–178, https://doi.org/10.2307/1969671.

[30] I. Chevyrev and A. Kormilitzin, *A primer on the signature method in machine learning*. arXiv:1603.03788 [stat.ML], 2016.

[31] A. Chistov, G. Ivanyos, and M. Karpinski, *Polynomial time algorithms for modules over finite dimensional algebras*, in Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, ISSAC '97, ACM, 1997, pp. 68–74, https://doi.org/10.1145/258726.258751.

[32] O. Chterental and D. v. Đoković, *Normal forms and tensor ranks of pure states of four qubits*, in Linear Algebra Research Advances, G. D. Ling, ed., Nova Science Publishers, New York, 2007, ch. 4, pp. 133–167. arXiv:quant-ph/0612184 .

[33] W. de Graaf, *Lie Algebras: Theory and Algorithms*, vol. 56 of North-Holland Mathematical Library, Elsevier Science, 2000.

[34] C. de Seguins Pazzis, *Invariance of simultaneous similarity and equivalence of matrices under extension of the ground field*, Linear Algebra Appl., 433 (2010), pp. 618–624, https://doi.org/10.1016/j.laa.2010.03.022.

[35] J. Dorroh, *Concerning adjunctions to algebras*, Bull. AMS, 38 (1932), pp. 85–88, https://doi.org/10.1090/S0002-9904-1932-05333-2.

[36] W. Dür, G. Vidal, and J. I. Cirac, *Three qubits can be entangled in two inequivalent ways*, Physical Review A, 62 (2000), p. 062314, https://doi.org/10.1103/PhysRevA.62.062314.

[37] W. Eberly and M. Giesbrecht, *Efficient decomposition of associative algebras over finite fields*, J. Symb. Comput., 29 (2000), pp. 441–458, https://doi.org/10.1006/jsco.1999.0308.

[38] R. Farnsteiner, *The theorem of Wedderburn–Malcev: $H^2(A, N)$ and extensions*. Lecture at BIREP: Representations of Finite Dimensional Algebras and Quantum Groups at Bielefield, 2005, https://www.math.uni-bielefeld.de/~sek/select/RF6.pdf.

[39] V. Felsch and J. Neubüser, *On a programme for the determination of the automorphism group of a finite group.*, in Computational Problems in Abstract Algebra (Proceedings of a Conference on Computational Problems in Algebra, Oxford, 1967), P. J. Leech, ed., Oxford, 1970, pp. 59–60.

[40] J. Finkelstein and B. Hescott, *Polynomial-time kernel reductions*. arXiv:1604.08558 [cs.CC], 2016.

[41] L. Fortnow and J. A. Grochow, *Complexity classes of equivalence problems revisited*, Inform. and Comput., 209 (2011), pp. 748–763, https://doi.org/10.1016/j.ic.2011.01.006. Also available as arXiv:0907.4775 [cs.CC].

[42] V. Futorny, J. A. Grochow, and V. V. Sergeichuk, *Wildness for tensors*, Lin. Algebra Appl., 566 (2019), pp. 212–244, https://doi.org/10.1016/j.laa.2018.12.022.

[43] I. M. Gelfand and V. A. Ponomarev, *Remarks on the classification of a pair of commuting linear transformations in a finite-dimensional space*, Functional Anal. Appl., 3 (1969), pp. 325–326, https://doi.org/10.1007/BF01076321.

[44] G. Gour and N. R. Wallach, *Classification of multipartite entanglement of all finite dimensionality*, Phys. Rev. Lett., 111 (2013), p. 060502, https://doi.org/10.1103/PhysRevLett.111.060502. arXiv:1304.7259 [quant-ph].

[45] D. R. Grayson and M. E. Stillman, *Macaulay2, a software system for research in algebraic geometry.* Available at https://faculty.math.illinois.edu/Macaulay2/.

[46] M. Greferath, A. Nechaev, and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl., 3 (2004), pp. 247–272, https://doi.org/10.1142/S0219498804000873.

[47] D. J. Grigoriev, *Complexity of "wild" matrix problems and of the isomorphism of algebras and graphs*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), 105 (1981), pp. 10–17, 198, https://doi.org/10.1007/BF01084390. Theoretical applications of the methods of mathematical logic, III.

[48] J. A. Grochow, *Matrix Lie algebra isomorphism*, in IEEE Conference on Computational Complexity

(CCC12), 2012, pp. 203–213, https://doi.org/10.1109/CCC.2012.34. Also available as arXiv:1112.2012 [cs.CC] and ECCC Technical Report TR11-168.

[49] J. A. Grochow and Y. Qiao, *Algorithms for group isomorphism via group extensions and cohomology*, SIAM J. Comput., 46 (2017), pp. 1153–1216, https://doi.org/10.1137/15M1009767. Preliminary version in IEEE Conference on Computational Complexity (CCC) 2014 (DOI:10.1109/CCC.2014.19). Also available as arXiv:1309.1776 [cs.DS] and ECCC Technical Report TR13-123.

[50] J. A. Grochow and Y. Qiao, *On isomorphism problems for tensors, groups, and polynomials III: reductions with linear blow-up, with applications*, 2021. Under preparation.

[51] J. A. Grochow and Y. Qiao, *On p-Group Isomorphism: Search-to-decision, counting-to-decision, and nilpotency class reductions via tensors*, in 36th Computational Complexity Conference (CCC 2021), V. Kabanets, ed., vol. 200 of Leibniz International Proceedings in Informatics (LIPIcs), Dagstuhl, Germany, 2021, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, pp. 16:1–16:38, https://doi.org/10.4230/LIPIcs.CCC.2021.16.

[52] J. A. Grochow and Y. Qiao, *On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness*, in 12th Innovations in Theoretical Computer Science Conference, ITCS 2021, January 6-8, 2021, Virtual Conference, J. R. Lee, ed., vol. 185 of LIPIcs, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, pp. 31:1–31:19, https://doi.org/10.4230/LIPIcs.ITCS.2021.31, https://doi.org/10.4230/LIPIcs.ITCS.2021.31.

[53] H. A. Helfgott, J. Bajpai, and D. Dona, *Graph isomorphisms in quasi-polynomial time.* arXiv:1710.04574 [math.GR], 2017.

[54] G. Higman, *Enumerating p-groups. I. Inequalities*, Proc. London Math. Soc. (3), 10 (1960), pp. 24–30, https://doi.org/10.1112/plms/s3-10.1.24.

[55] G. Ivanyos, *Fast randomized algorithms for the structure of matrix algebras over finite fields*, in Proceedings of the 2000 international symposium on Symbolic and algebraic computation, ACM, 2000, pp. 175–183, https://doi.org/10.1145/345542.345620.

[56] G. Ivanyos, M. Karpinski, and N. Saxena, *Deterministic polynomial time algorithms for matrix completion problems*, SIAM J. Comput., 39 (2010), pp. 3736–3751, https://doi.org/10.1137/090781231.

[57] G. Ivanyos and Y. Qiao, *Algorithms based on *-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing*, SIAM J. Comput., 48 (2019), pp. 926–963, https://doi.org/10.1137/18M1165682, https://doi.org/10.1137/18M1165682.

[58] G. Ivanyos and L. Rónyai, *Computations in associative and Lie algebras*, in Some tapas of computer algebra, Springer, 1999, pp. 91–120, https://doi.org/10.1007/978-3-662-03891-8_5.

[59] Z. Ji, Y. Qiao, F. Song, and A. 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, D. Hofheinz and A. Rosen, eds., vol. 11891 of Lecture Notes in Computer Science, Springer, 2019, pp. 251–281, https://doi.org/10.1007/978-3-030-36030-6_11. Preprint arXiv:1906.04330 [cs.CR].

[60] N. Kayal, *Efficient algorithms for some special cases of the polynomial equivalence problem*, in Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011, 2011, pp. 1409–1421, https://doi.org/10.1137/1.9781611973082.108.

[61] N. Kayal, *Affine projections of polynomials: extended abstract*, in Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012, 2012, pp. 643–662, https://doi.org/10.1145/2213977.2214036.

[62] N. Kayal and N. Saxena, *Complexity of ring morphism problems*, Computational Complexity, 15 (2006), pp. 342–390, https://doi.org/10.1007/s00037-007-0219-8.

[63] L. Klingler and L. S. Levy, *Sweeping-similarity of matrices*, Linear Algebra Appl., 75 (1986), pp. 67–104, https://doi.org/10.1016/0024-3795(86)90182-5.

[64] J. Köbler, U. Schöning, and J. Torán, *The graph isomorphism problem: its structural complexity*, Birkhauser Verlag, Basel, Switzerland, Switzerland, 1993, https://doi.org/10.1007/978-1-4612-0333-9.

[65] P. Koiran, *Hilbert's Nullstellensatz is in the polynomial hierarchy*, J. Complexity, 12 (1996), pp. 273–286, https://doi.org/10.1006/jcom.1996.0019.

[66] T. G. Kolda and B. W. Bader, *Tensor decompositions and applications*, SIAM Review, 51 (2009), pp. 455–500, https://doi.org/10.1137/07070111X.

[67] T. Y. Lam, *A first course in noncommutative rings*, vol. 131 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1991, https://doi.org/10.1007/978-1-4684-0406-7.

[68] J. Landsberg, *Tensors: Geometry and Applications*, vol. 128 of Graduate studies in mathematics, American Mathematical Soc., 2012, https://doi.org/10.1090/gsm/128.

[69] Y. Li and Y. Qiao, *Linear algebraic analogues of the graph isomorphism problem and the Erdős–Rényi model*, in 58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, C. Umans, ed., IEEE Computer Society, 2017, pp. 463–474, https://doi.org/10.1109/FOCS.2017.49.

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

[71] E. M. Luks, *Permutation groups and polynomial-time computation*, in Groups and computation (New Brunswick, NJ, 1991), vol. 11 of DIMACS Ser. Discrete Math. Theoret. Comput. Sci., Amer. Math. Soc., Providence, RI, 1993, pp. 139–175.

[72] T. J. Lyons, *Rough paths, signatures and the modelling of functions on streams*, in Proc. International Congress of Mathematicians, Kyung Moon Publishers, 2014, pp. 163–184.

[73] T. J. Lyons and W. Xu, *Inverting the signature of a path*, J. Eur. Math. Soc.(JEMS), 20 (2018), pp. 1655–1687, https://doi.org/10.4171/JEMS/796.

[74] S. MacLane, *Categories for the working mathematician*, Springer-Verlag, New York-Berlin, 1971, https://doi.org/10.1007/978-1-4757-4721-8. Graduate Texts in Mathematics, Vol. 5.

[75] F. J. MacWilliams, *Combinatorial problems of elementary abelian groups*, PhD thesis, Radcliffe College, 1962.

[76] B. D. McKay, *Practical graph isomorphism*, Congr. Numer., (1980), pp. 45–87.

[77] B. D. McKay and A. Piperno, *Practical graph isomorphism, II*, Journal of Symbolic Computation, 60 (2014), pp. 94 – 112, https://doi.org/10.1016/j.jsc.2013.09.003.

[78] G. L. Miller, *On the $n^{\log n}$ isomorphism technique (a preliminary report)*, in STOC, ACM, 1978, pp. 51–58, https://doi.org/10.1145/800133.804331.

[79] A. Miyake, *Multipartite entanglement under stochastic local operations and classical communication*, Int. J. Quant. Info., (2004), pp. 65–77, https://doi.org/10.1142/S0219749904000080. arXiv:quant-ph/0401023 .

[80] T. Miyazaki, *Luks's reduction of graph isomorphism to code equivalence.* Comment to E. W. Clark, https://groups.google.com/forum/#!msg/sci.math.research/puZxGj9HXKI/CeyH2yyyNFUJ, 1996.

[81] P. J. Moore, T. J. Lyons, and J. Gallacher, *Using path signatures to predict a diagnosis of Alzheimer's disease*, PLOS ONE, 14 (2019), https://doi.org/10.1371/journal.pone.0222212.

[82] E. A. O'Brien, *Isomorphism testing for p-groups*, J. Symb. Comput., 17 (1994), pp. 133–147, https://doi.org/10.1006/jsco.1994.1007.

[83] R. Oldenburger, *Non-singular multilinear forms and certain p-way matrix factorizations*, Trans. Amer. Math. Soc., 39 (1936), pp. 422–455, https://doi.org/10.2307/1989760.

[84] J. 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, 1996, pp. 33–48, https://doi.org/10.1007/3-540-68339-9_4.

[85] E. Petrank and R. M. Roth, *Is code equivalence easy to decide?*, IEEE Trans. Inf. Theory, 43 (1997), pp. 1602–1604, https://doi.org/10.1109/18.623157.

[86] M. Pfeffer, A. Seigal, and B. Sturmfels, *Learning paths from signature tensors*, SIAM Journal on Matrix Analysis and Applications, 40 (2019), pp. 394–416, https://doi.org/10.1137/18M1212331. arXiv:1809.01588.

[87] B. Poonen, *Undecidable problems: a sampler*, in Interpreting Gödel, Cambridge Univ. Press, Cambridge, 2014, pp. 211–241. arXiv:1204.0299 [math.LO].

[88] L. Rónyai, *Zero divisors in quaternion algebras*, J. Algorithms, 9 (1988), pp. 494–506, https://doi.org/10.1016/0196-6774(88)90014-4.

[89] D. J. Rosenbaum, *Bidirectional collision detection and faster deterministic isomorphism testing.* arXiv preprint arXiv:1304.3935 [cs.DS], 2013.

[90] D. J. Rosenbaum, *Breaking the $n^{\log n}$ barrier for solvable-group isomorphism*, in Proceedings of the Twenty-Fourth Annual ACM-SIAM Symposium on Discrete Algorithms, SIAM, 2013, pp. 1054–1073, https://doi.org/10.1137/1.9781611973105.76. Preprint arXiv:1205.0642 [cs.DS].

[91] N. Saxena, *Morphisms of rings and applications to complexity*, PhD thesis, Indian Institute of Technology, Kanpur, 5 2006, https://www.cse.iitk.ac.in/users/nitin/papers/thesis.pdf.

[92] T. Schrock and R. Frongillo, *Computational complexity of k-block conjugacy*, Theoret. Comp. Sci., (2021), pp. 21–40, https://doi.org/10.1016/j.tcs.2020.12.009.

[93] N. Sendrier, *Finding the permutation between equivalent linear codes: The support splitting algorithm*, IEEE Trans. Information Theory, 46 (2000), pp. 1193–1203, https://doi.org/10.1109/18.850662.

[94] N. Sendrier and D. E. Simos, *The hardness of code equivalence over $\mathbb{F}_q$ and its application to code-based cryptography*, in International Workshop on Post-Quantum Cryptography, Springer, 2013, pp. 203–216.

[95] Á. Seress, *Permutation group algorithms*, vol. 152, Cambridge University Press, 2003, https://doi.org/10.

1017/CBO9780511546549.

[96] V. V. Sergeichuk, *The classification of metabelian p-groups*, in Matrix problems (Russian), Akad. Nauk Ukrain. SSR Inst. Mat., Kiev, 1977, pp. 150–161.

[97] V. V. Sergeichuk, *Canonical matrices for linear matrix problems*, Linear Algebra Appl., 317 (2000), pp. 53–102, https://doi.org/10.1016/S0024-3795(00)00150-6.

[98] C. C. Sims, *Some group-theoretic algorithms*, in Topics in algebra, Springer, 1978, pp. 108–124, https://doi.org/10.1007/BFb0103126.

[99] D. Simson and A. Skowroński, *Elements of the representation theory of associative algebras. Vol. 3*, vol. 72 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 2007. Representation-infinite tilted algebras.

[100] V. Strassen, *The asymptotic spectrum of tensors*, J. Reine Angew. Math., 384 (1988), pp. 102–152, https://doi.org/10.1515/crll.1988.384.102.

[101] L. G. Valiant, *An algebraic approach to computational complexity*, in Proceedings of the International Congress of Mathematicians, Vol. 2 (Warsaw, 1983), PWN, Warsaw, 1984, pp. 1637–1643, https://www.mathunion.org/fileadmin/ICM/Proceedings/ICM1983.2/ICM1983.2.ocr.pdf.

[102] A. Wigderson and J. Zuiddam, *Asymptotic spectra: theory, applications, and extensions.* https://staff.fnwi.uva.nl/j.zuiddam/papers/convexity.pdf, 2022.

[103] Wikipedia contributors, *Rng (algebra): adjoining an identity element — Wikipedia, the free encyclopedia*, 2019, https://en.wikipedia.org/wiki/Rng_(algebra)#Adjoining_an_identity_element. [Online; accessed 19-Feb-2019].

[104] J. B. Wilson, *Decomposing p-groups via Jordan algebras*, J. Algebra, 322 (2009), pp. 2642–2679, https://doi.org/10.1016/j.jalgebra.2009.07.029.

[105] J. B. Wilson, *2014 conference on* Groups, Computation, and Geometry *at Colorado State University, co-organized by P. Brooksbank, A. Hulpke, T. Penttila, J. Wilson, and W. Kantor*. Personal communication, 2014.

[106] J. B. Wilson, *Surviving in the wilderness.* Talk presented at the Sante Fe Institute Workshop on Wildness in Computer Science, Physics, and Mathematics, 2015.

[107] J. B. Wilson, *The threshold for subgroup profiles to agree is logarithmic*, Theory Comput., 15 (2019), https://doi.org/10.4086/toc.2019.v015a019.

[108] S. Zangi, J.-L. Li, and C.-F. Qiao, *Quantum state concentration and classification of multipartite entanglement*, Physical Review A, 97 (2018), p. 012301, https://doi.org/10.1103/PhysRevA.97.012301.

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