On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness

Joshua A. Grochow
Departments of Computer Science and Mathematics, University of Colorado, Boulder, CO, USA
jgrochow@colorado.edu

Youming Qiao
Centre for Quantum Software and Information, University of Technology Sydney, Australia
youming.qiao@uts.edu.au

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).

2012 ACM Subject Classification Theory of computation → Complexity classes; Computing methodologies → Linear algebra algorithms; Hardware → Quantum communication and cryptography

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

Digital Object Identifier 10.4230/LIPIcs.ITCS.2021.31

Related Version A full version of the paper is available at `https://arxiv.org/abs/1907.00309`.

Funding *Joshua A. Grochow*: Partially supported by NSF grants DMS-1750319 and DMS-1622390. *Youming Qiao*: Partially supported by the Australian Research Council DP200100950.

Acknowledgements We would like to thanks 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 $3TI$. We 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 ETH and #ETH.

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 [51, 52], and Babai's recent quasi-polynomial-time breakthrough is one of the theoretical gems of the last several decades [5].

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 [39, 57] – and in theory: the best known worst-case upper bounds are barely improved from brute force (e. g., [46, 63]). 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).

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 [26], 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, 42] 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, 42] Here we greatly expand these and show a much wider class of problems are equivalent (see Thm. 4=Thm. B and Fig. 1).

In a follow-up paper [33], we study search and counting to decision reductions, apply these these results 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 [43]. 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 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.

Organization. Due to page constraints and the nature of this work, we are only able to present the main results and the related implications and discussions. For detailed proofs, we refer the reader to the full version [32]. In the remainder of this paper, we first present the origins of those isomorphism problems we consider (Sec. 2). We then state our main results in Sec. 3, and briefly indicate the main techniques in Sec. 4. In Sec. 5, we present formal statements of the various problems involved and a detailed statement of one main result. Finally in Sec. 6 we present the implication to quantum information and discuss on some further related works and the outlook of this research direction.

2 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 $\mathrm{M}(n, q)$, respectively.

Multivariate cryptography. In 1996, Patarin [57] 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 $\vec{f} = (f_1, \ldots, f_m)$ and $\vec{g} = (g_1, \ldots, g_m)$ be two m-tuples of homogeneous quadratic polynomials, where $f_i, g_j \in \mathbb{F}[x_1, \ldots, x_n]$. 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 [11, 38] 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 [20] 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 [21, 49, 54] and references therein. The algorithmic problem of reconstructing the path from the signature tensor is of considerable interest; see e.g. [50, 59]. In this context, the following problem was recently studied by Pfeffer, Seigal, and Sturmfels [59], 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 [10, 23]. It is well-known by [23] that ρ and τ are interconvertible via SLOCC, if and only if there exist $T_i \in \mathrm{GL}(\mathcal{H}_i)$, such that $(T_1 \otimes \ldots T_m)|\phi\rangle = |\psi\rangle$. 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).

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., [55]). Here, the groups are represented succinctly, e. g., by generating sets of permutations or matrices over finite fields. Testing isomorphism of p-groups is considered to be a bottleneck to testing isomorphism of general groups [7, 19, 31]. Even for p-groups of class 2 and exponent p, current methods are still limited to instances of quite small size.

Theoretical computer science. As already mentioned, Agrawal, Kayal, and Saxena studied isomorphism and automorphism problems of rings, algebras, and polynomials [1, 2, 42], 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 [40, 41] (see also [30]). 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 [51, 52]. Indeed, the problems we consider have been proposed to be difficult enough for cryptographic purposes [39, 57]. 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 [59, arXiv version 1], computations on special cases of the Tensor Congruence problem were performed in Macaulay2 [28], 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 [45].

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 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 $\mathbb{F}$.

3 Main results

3.1 Defining the Tensor Isomorphism complexity class

Given the diversity of the isomorphism problems from Sec. 2, 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. 2 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 [43].

[1] We thank James B. Wilson, who maintains a suite of algorithms for p-group isomorphism testing [16], 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.

▶ **Definition 1** (The d-Tensor Isomorphism problem). *d-Tensor Isomorphism over a field $\mathbb{F}$ is the problem: given two d-way arrays $\mathtt{A} = (a_{i_1,\ldots,i_d})$ and $\mathtt{B} = (b_{i_1,\ldots,i_d})$, where $i_k \in [n_k]$ for $k \in [d]$, and $a_{i_1,\ldots,i_d}, b_{i_1,\ldots,i_d} \in \mathbb{F}$, decide whether there are $P_k \in \mathrm{GL}(n_k, \mathbb{F})$ for $k \in [d]$, such that for all $i_1, \ldots, i_d$,*

$$a_{i_1,\ldots,i_d} = \sum_{j_1,\ldots,j_d} b_{j_1,\ldots,j_d} (P_1)_{i_1,j_1} (P_2)_{i_2,j_2} \cdots (P_d)_{i_d,j_d}. \tag{1}$$

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

▶ **Theorem 2** (=Cor. A). *d-Tensor Isomorphism reduces to 3-Tensor Isomorphism in time $O(n^d)$.*

Thm. 2 is also key to the application to quantum information in Sec. 6.1.

Thus, while the 2TI problem is easy (it's just matrix rank), 3TI already captures the complexity of dTI for any 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 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 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. 2, we may take $d = 3$ without loss of generality. When we write TI without mentioning the field, the result holds for any field.

3.2 TI-complete problems

Our second main result shows the wide applicability and robustness of the TI class.

▶ **Theorem 4** (Informal statement of part of Theorem B). *All the problems mentioned in Sec. 2 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 [26], we conclude that they are in fact TI-complete.

▶ Remark 5. Our results allow us to mostly answer a question from Saxena's thesis [64, 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 [26], we get a new such reduction – very different from the previous one [1] – which works over any field of characteristic not 2 or 3.

[2] We asked several experts who knew of the question, but we were unable to find a written reference. Interestingly, Oldenburger [56] 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.

Here, we would also like to point out that some of the polynomial-time equivalences in Thm. 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 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" [25]; cf. functorial reductions [4]). 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, one of our results is that for *linear spaces* of matrices (one form of 3-way arrays; see Sec. 5.1), conjugacy testing and equivalence testing are polynomial-time equivalent. 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.

3.3 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 [26, 30, 34, 48, 58], Graph Isomorphism and Permutational Code Equivalence reduce to 3-Tensor Isomorphism. For the inverse direction, we have the following connection.

▶ **Corollary 6.** *Let* A *and* 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* A *and* 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 [5] (see [35] 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.

4 An overview of proof strategies and techniques

4.1 The main new technique

Our main new technique, used to show the reduction from dTI to 3TI (Thm. 2=Thm. A), is a simultaneous generalization of our reduction from 3TI to Algebra Isomorphism and the technique Grigoriev used [29] 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 $x_1, \ldots, x_n$ 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 [29] to show that GI was equivalent Algebra Isomorphism for a certain restricted class of algebras (see Sec. 6 for a comparison).

4.2 The proof strategy for Theorem 4=B

Let us now explain briefly on the proof of Thm. B=Thm. 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. 5. 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 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. 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. 5.1 for detailed explanations. [3]

The first step only provides the context for proving Thm. 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 [26], and the "embedding" technique from [27]. To implement these ideas, however, usually involves detailed and complicated computations.

For example, in the proof of Theorem 4, we use a gadget construction from [26] for the reduction from Tensor Isomorphism to IP2S. To show that this gadget works in our setting, we need a proof strategy that is different from that in [26]. Furthermore, the gadget from [26] introduces a quadratic blow-up in the input parameters. We then devise a new gadget, which achieves the same function with only linear blow-up, and enables Corollary 6. Having only linear blow-up is important in applications, e. g., to Group Isomorphism in the Cayley table model (see [33]).

5 More details and more results on TI-completeness

5.1 Five group actions on 3-way arrays and the corresponding mathematical objects

In Section 3, we briefly defined five group actions on 3-way arrays with the help of Equation 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 2. To connect the interpretations with the formulas themselves, one technical tool is very useful, namely, given a 3-way array $\mathtt{A}(i,j,k)$, we define its *frontal slices* to be the matrices A_k defined by $A_k(i,j) := \mathtt{A}(i,j,k)$; that is, we think of the box of $\mathtt{A}$ as arranged so that the i and j axes lie in the page, while the k-axis is perpendicular to the page. Similarly, its *lateral slices* (viewing the 3D box of $\mathtt{A}$ "from the side") are defined by $L_j(i,k) := \mathtt{A}(i,j,k)$. An $\ell \times n \times m$ 3-way array thus has m frontal slices and n lateral slices.

A natural action on arrays of size $\ell \times n \times m$ is that of $\mathrm{GL}(\ell,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F}) \times \mathrm{GL}(m,\mathbb{F})$ by change of basis in each of the 3 directions, namely

$$((P,Q,R)\cdot \mathtt{A})(i',j',k') = \sum_{i,j,k} \mathtt{A}(i,j,k) P_{ii'} Q_{jj'} R_{kk'}.$$

We will see several interpretations of this action below.

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 $\sum_{i,j,k} \mathtt{A}(i,j,k) \vec{e_i} \otimes \vec{e_j} \otimes \vec{e_k}$

[3] While problems in Thm. 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 [18], Matrix Lie Algebra Conjugacy from [30], and Bilinear Map Isotopism from [13]; see Sec. 5.1 and Sec. 6.

in $\mathbb{F}^\ell \otimes \mathbb{F}^n \otimes \mathbb{F}^m$. The natural action by $\mathrm{GL}(\ell,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F}) \times \mathrm{GL}(m,\mathbb{F})$ above 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.[4] This problem has been studied as far back as the 1930s [56].

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 [59] (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, $\mathcal{A} = \langle A_1, \ldots, A_m \rangle$, 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 $A_1, \ldots, A_d$, are Matrix Space Equivalence, Matrix Space Conjugacy, and Matrix Space Isometry, respectively.

Isomorphism of quadratic polynomials with 2 secrets. For a tuple of homogeneous quadratic polynomials (over a field of characteristic not 2) $\vec{f} = (f_1, \ldots, f_m)$, we may encode f_i by a symmetric matrix F_i in the usual way – where $f_i(x) = x^t F_i x$ – and thus obtain a tuple of (symmetric) matrices $(F_1, \ldots, F_m)$. Since, in the IP2S problem, we are also allowed to take linear combinations of the f_i themselves, we see that the IP2S problem is equivalent to the Matrix Space Isometry problem for $\langle F_1, \ldots, F_m \rangle$. Equivalently, the action of $(P,Q) \in \mathrm{GL}(m,\mathbb{F}) \times \mathrm{GL}(n,\mathbb{F})$ is by $F_i \mapsto \sum_j P_{ij} Q^t F_j Q$.

Finite p-groups. If we consider the quadratic polynomials f_i as defining a (symmetric) bilinear map $\mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^m$, we may generalize to see that (not necessarily symmetric) bilinear maps arise naturally in other areas, notably in group theory. For matrices A_k over $\mathbb{F}_p$, p an odd prime, we may consider Matrix Space Isometry for the matrix space $\langle A_1, \ldots, A_m \rangle$. Two bilinear maps that are essentially the same up to such basis changes are sometimes called pseudo-isometric [17].

[4] 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.

When the A_k are skew-symmetric, Baer's correspondence [9] 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 $[G, G] \leq Z(G)$, 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.

Bilinear maps. If we generalize even further to bilinear maps $U \times V \to W$, we find that from an $\ell \times n \times m$ 3-way array $\mathtt{A}$, we can construct such 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 $(u^t A_1 v, \ldots, u^t A_m v)^t$, 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 [13], in the context of testing isomorphism of graded algebras.

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 $x_1, \ldots, x_n$, 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 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.

Summary. 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); see the full version [32] for a detailed discussion.

5.2 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 [26], this immediately gives:

▶ **Corollary A.** *For any fixed $d \geq 1$, d-*Tensor Isomorphism *reduces to* 3-Tensor Isomorphism.

Given the viewpoint of Section 5.1 on the problems from Section 2, 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.*[5]
   b. Associative Matrix Algebra Conjugacy.[6]
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. 5.1).

Since the main result of [26] reduces the problems in Theorem B to 3-Tensor Isomorphism (cf. [26, Rmk. 1.1]), we have:

▶ **Corollary B.** *Each of the problems listed in Theorem B is* TI*-complete.*[7]

▶ Remark 7. 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 [44]. 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, 60]), but by Cor. B, the question of decidability is open for all of these problems.

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 [38], Module Isomorphism, which admits several polynomial-time algorithms [15, 22, 37, 67]. 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 [38], which uses the $*$-algebra technique originated from the study of computing with p-groups [17, 69].

[5] And even further, where $L/[L, L] \cong \mathbb{F}$.
[6] Even for algebras A whose Jacobson radical $J(A)$ squares to zero and $A/J(A) \cong \mathbb{F}$.
[7] For Cubic Form Equivalence, we only show that it is in $\mathsf{TI}_{\mathbb{F}}$ when $\mathrm{char}\,\mathbb{F} > 3$ or $\mathrm{char}\,\mathbb{F} = 0$.

6 Implications, more related works, and further discussions

6.1 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) [10, 23]. 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 $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \cdots \times \mathrm{GL}(V_k)$ [23].[8] 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 [72], 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.

6.2 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 [26]. 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 [26]. Thm. A considers d-tensors for any $d \geq 3$, which were not considered in [26].

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

[8] 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.

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 [26] and our main Theorem B, 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 [29] 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.

Brooksbank and Wilson [18] showed a reduction from Associative Algebra Isomorphism (when given by structure constants) to Matrix Algebra Conjugacy. Grochow [30], among other things, showed that GI and CodeEq reduce to Matrix Lie Algebra Conjugacy, which is a special case of Matrix Space Conjugacy.

In [42], 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 $\mathsf{NP} \cap \mathsf{coAM}$ [42, Thm. 4.1], reduce GI to this problem [42, Thm. 4.4], and prove that counting the number of ring automorphism (#RA) is in $\mathsf{FP}^{\mathsf{AM} \cap \mathsf{coAM}}$ [42, 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.

6.3 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 [5], 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 [68] (see, e. g., [65] 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 [6]. 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 [46] adapted the individualisation and refinement technique, as used by Babai, Erdős and Selkow [8], to tackle Alternating

Matrix Space Isometry over $\mathbb{F}_q$. This algorithm was recently shown [14] to practically improve over the default algorithms in Magma [12]. 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.

6.4 Outlook

In light of Babai's breakthrough on GI [5], it is natural to consider "what's next?" for isomorphism problems. That is, what isomorphism problems stand as crucial bottlenecks 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 [5, 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 [5] that Group Isomorphism (GpI) in the Cayley table model is a key bottleneck[9] 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., [9, 36, 66, 71]). Third, by Baer's correspondence [9], isomorphism for such groups is equivalent[10] to Alternating Matrix Space Isometry (see Section 5.1). 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. 6.

This theory for TI is far from complete, and many questions remain, largely inspired by the study of GI. In the full version [32, Section 10.1], we discuss a possible theory of universality for basis-explicit linear structures, in analogy with the universality of GI for explicit combinatorial structures [73, 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.

---

[9] Indeed, the current-best upper bounds on these two problems are now quite close: $n^{O(\log n)}$ for GpI (originally due to [24, 53] – Miller attributes this to Tarjan – with improved constants [62, 63, 70]), and $n^{O(\log^2 n)}$ for GI [5] (see [35] for calculation of the exponent).

[10] 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.

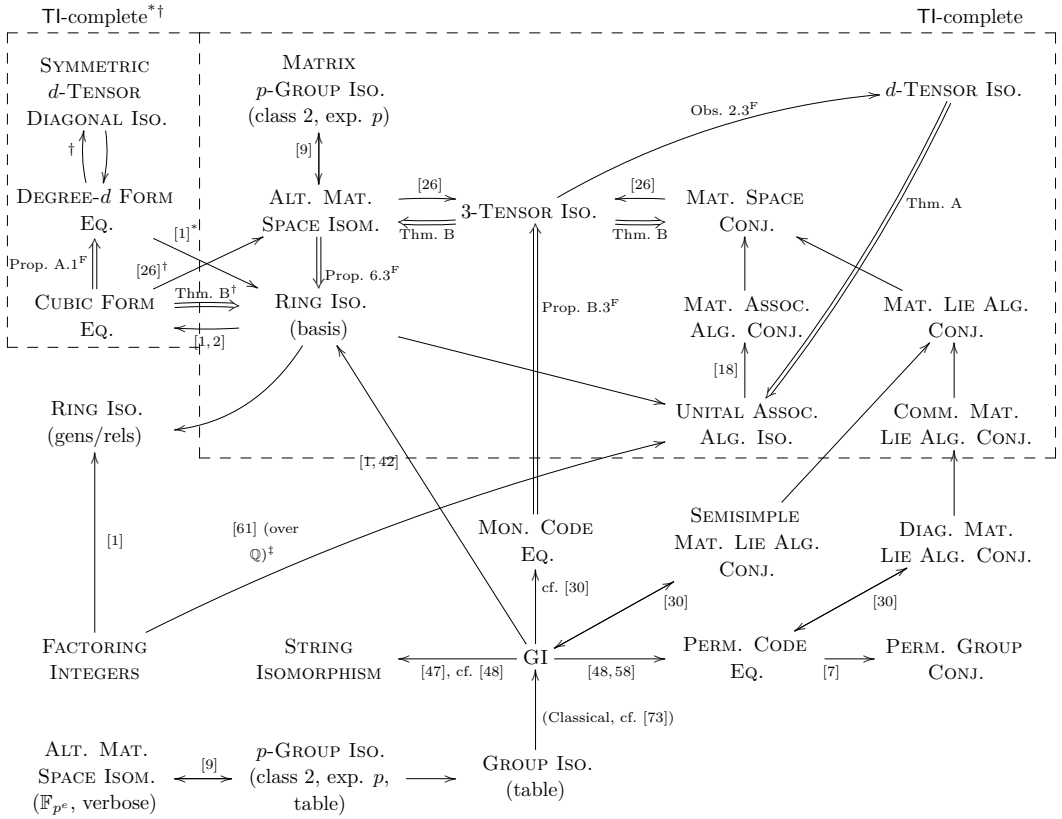

Figure 1 Summary of key isomorphism problems. $A \to B$ indicates that A reduces to B, i. e., $A \leq_m^p B$. $A \Rightarrow B$ indicates a new result. Unattributed arrows indicate A is clearly a special case of B. Note that the definition of ring used in [1] is commutative, finite, and unital; by "algebra" 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 [61] 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.

F Refers to numbers in the full version [32].

References

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

2 Manindra Agrawal and Nitin Saxena. Equivalence of $\mathbb{F}$-algebras and cubic forms. In *STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science, Proceedings*, pages 115–126, 2006. doi:10.1007/11672142_8.

3 Eric Allender and Bireswar Das. Zero knowledge and circuit minimization. *Inf. Comput.*, 256:2–8, 2017. doi:10.1016/j.ic.2017.04.004.

4 László Babai. On the automorphism groups of strongly regular graphs I. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 359–368, 2014. doi:10.1145/2554797.2554830.

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

6 László Babai, Robert Beals, and Ákos Seress. Polynomial-time theory of matrix groups. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009*, pages 55–64, 2009. doi:10.1145/1536414.1536425.

7 László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *Proceedings of the Twenty-Second Annual ACM–SIAM Symposium on Discrete Algorithms (SODA11)*, pages 1395–1408, Philadelphia, PA, 2011. SIAM. doi:10.1137/1.9781611973082.107.

8 László Babai, Paul Erdős, and Stanley M. Selkow. Random graph isomorphism. *SIAM J. Comput.*, 9(3):628–635, 1980. doi:10.1137/0209047.

9 Reinhold Baer. Groups with abelian central quotient group. *Trans. AMS*, 44(3):357–386, 1938. doi:10.1090/S0002-9947-1938-1501972-1.

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

11 Jérémy Berthomieu, Jean-Charles Faugère, and Ludovic Perret. Polynomial-time algorithms for quadratic isomorphism of polynomials: The regular case. *J. Complexity*, 31(4):590–616, 2015. doi:10.1016/j.jco.2015.04.001.

12 W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system I: the user language. *J. Symb. Comput.*, pages 235–265, 1997. doi:10.1006/jsco.1996.0125.

13 Peter Brooksbank, E O'Brien, and James Wilson. Testing isomorphism of graded algebras. *Trans. Amer. Math. Soc.*, 372:8067–8090, 2019. doi:10.1090/tran/7884.

14 Peter A. Brooksbank, Joshua A. Grochow, Yinan Li, Youming Qiao, and James B. Wilson. Incorporating Weisfeiler–Leman into algorithms for group isomorphism. arXiv:1905.02518 [cs.CC], 2019.

15 Peter A. Brooksbank and Eugene M. Luks. Testing isomorphism of modules. *J. Algebra*, 320(11):4020–4029, 2008. doi:10.1016/j.jalgebra.2008.07.014.

16 Peter A. Brooksbank, Joshua Maglione, and James B. Wilson. Thetensor.space. https://github.com/thetensor-space/, 2019.

17 Peter A. Brooksbank and James B. Wilson. Computing isometry groups of Hermitian maps. *Trans. Amer. Math. Soc.*, 364:1975–1996, 2012. doi:10.1090/S0002-9947-2011-05388-2.

18 Peter A Brooksbank and James B Wilson. The module isomorphism problem reconsidered. *Journal of Algebra*, 421:541–559, 2015. doi:10.1016/j.jalgebra.2014.09.004.

19 John Cannon and Derek F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symbolic Comput.*, 35(3):241–267, 2003. doi:10.1016/S0747-7171(02)00133-5.

20 Kuo-Tsai Chen. Integration of paths, geometric invariants and a generalized baker-hausdorff formula. *Annals of Mathematics*, pages 163–178, 1957. doi:10.2307/1969671.

21 Ilya Chevyrev and Andrey Kormilitzin. A primer on the signature method in machine learning, 2016. arXiv:1603.03788.

22 Alexander Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC '97, pages 68–74. ACM, 1997. doi:10.1145/258726.258751.

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

24 V. Felsch and J. Neubüser. On a programme for the determination of the automorphism group of a finite group. In Pergamon J. Leech, editor, *Computational Problems in Abstract Algebra (Proceedings of a Conference on Computational Problems in Algebra, Oxford, 1967)*, pages 59–60, Oxford, 1970.

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

26 Vyacheslav Futorny, Joshua A. Grochow, and Vladimir V. Sergeichuk. Wildness for tensors. *Lin. Alg. Appl.*, 566:212–244, 2019. doi:10.1016/j.laa.2018.12.022.

27 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.*, 3:325–326, 1969. doi:10.1007/BF01076321.

28 Daniel R. Grayson and Michael E. Stillman. Macaulay2, a software system for research in algebraic geometry. Available at https://faculty.math.illinois.edu/Macaulay2/.

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

30 Joshua A. Grochow. Matrix Lie algebra isomorphism. In *IEEE Conference on Computational Complexity (CCC12)*, pages 203–213, 2012. Also available as arXiv:1112.2012 [cs.CC] and ECCC Technical Report TR11-168. doi:10.1109/CCC.2012.34.

31 Joshua A. Grochow and Youming Qiao. Algorithms for group isomorphism via group extensions and cohomology. *SIAM J. Comput.*, 46(4):1153–1216, 2017. 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. doi:10.1137/15M1009767.

32 Joshua A. Grochow and Youming Qiao. Isomorphism problems for tensors, groups, and cubic forms: completeness and reductions. *CoRR*, abs/1907.00309, 2019. arXiv:1907.00309.

33 Joshua A. Grochow and Youming Qiao. On isomorphism problems for tensors, groups, and polynomials II: search and counting to decision reductions, and applications to group isomorphism, 2020. Under preparation.

34 Xiaoyu He and Youming Qiao. On the Baer–Lovász–Tutte construction of groups from graphs: isomorphism types and homomorphism notions, 2020. arXiv:2003.07200 [math.CO].

35 Harald Andrés Helfgott, Jitendra Bajpai, and Daniele Dona. Graph isomorphisms in quasi-polynomial time. arXiv:1710.04574 [math.GR], 2017.

36 Graham Higman. Enumerating p-groups. I. Inequalities. *Proc. London Math. Soc. (3)*, 10:24–30, 1960. doi:10.1112/plms/s3-10.1.24.

37 Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010. doi:10.1137/090781231.

38 Gábor Ivanyos and Youming 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(3):926–963, 2019. doi:10.1137/18M1165682.

39 Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. General linear group action on tensors: A candidate for post-quantum cryptography. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I*, volume 11891 of *Lecture Notes in Computer Science*, pages 251–281. Springer, 2019. Preprint `arXiv:1906.04330` [cs.CR]. `doi:10.1007/978-3-030-36030-6_11`.

40 Neeraj 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*, pages 1409–1421, 2011. `doi:10.1137/1.9781611973082.108`.

41 Neeraj 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*, pages 643–662, 2012. `doi:10.1145/2213977.2214036`.

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

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

44 Pascal Koiran. Hilbert's Nullstellensatz is in the polynomial hierarchy. *J. Complexity*, 12(4):273–286, 1996. `doi:10.1006/jcom.1996.0019`.

45 J.M. Landsberg. *Tensors: Geometry and Applications*, volume 128 of *Graduate studies in mathematics*. American Mathematical Soc., 2012. `doi:10.1090/gsm/128`.

46 Yinan Li and Youming Qiao. Linear algebraic analogues of the graph isomorphism problem and the Erdős–Rényi model. In Chris Umans, editor, *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017*, pages 463–474. IEEE Computer Society, 2017. `doi:10.1109/FOCS.2017.49`.

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

48 Eugene M. Luks. Permutation groups and polynomial-time computation. In *Groups and computation (New Brunswick, NJ, 1991)*, volume 11 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 139–175. Amer. Math. Soc., Providence, RI, 1993.

49 T. J. Lyons. Rough paths, signatures and the modelling of functions on streams. In *Proc. International Congress of Mathematicians*, pages 163–184. Kyung Moon Publishers, 2014.

50 Terry J. Lyons and Weijun Xu. Inverting the signature of a path. *J. Eur. Math. Soc.(JEMS)*, 20(7):1655–1687, 2018. `doi:10.4171/JEMS/796`.

51 Brendan D. McKay. Practical graph isomorphism. *Congr. Numer.*, pages 45–87, 1980.

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

53 Gary L. Miller. On the $n^{\log n}$ isomorphism technique (a preliminary report). In *STOC*, pages 51–58. ACM, 1978. `doi:10.1145/800133.804331`.

54 P. J. Moore, T. J. Lyons, and J. Gallacher. Using path signatures to predict a diagnosis of alzheimer's disease. *PLoS ONE*, 14(9), 2019. `doi:10.1371/journal.pone.0222212`.

55 Eamonn A O'Brien. Isomorphism testing for p-groups. *Journal of Symbolic Computation*, 17(2):133–147, 1994. `doi:10.1006/jsco.1994.1007`.

56 Rufus Oldenburger. Non-singular multilinear forms and certain p-way matrix factorizations. *Trans. Amer. Math. Soc.*, 39(3):422–455, 1936. `doi:10.2307/1989760`.

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

58 Erez Petrank and Ron M. Roth. Is code equivalence easy to decide? *IEEE Trans. Inf. Theory*, 43(5):1602–1604, 1997. `doi:10.1109/18.623157`.

59 Max Pfeffer, Anna Seigal, and Bernd Sturmfels. Learning paths from signature tensors. *SIAM Journal on Matrix Analysis and Applications*, 40(2):394–416, 2019. arXiv:1809.01588. doi:10.1137/18M1212331.

60 Bjorn Poonen. Undecidable problems: a sampler. In *Interpreting Gödel*, pages 211–241. Cambridge Univ. Press, Cambridge, 2014. arXiv:1204.0299 [math.LO].

61 Lajos Rónyai. Zero divisors in quaternion algebras. *J. Algorithms*, 9(4):494–506, 1988. doi:10.1016/0196-6774(88)90014-4.

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

63 David 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*, pages 1054–1073. SIAM, 2013. Preprint arXiv:1205.0642 [cs.DS].

64 Nitin Saxena. *Morphisms of rings and applications to complexity*. PhD thesis, Indian Institute of Technology, Kanpur, May 2006. URL: https://www.cse.iitk.ac.in/users/nitin/papers/thesis.pdf.

65 Ákos Seress. *Permutation group algorithms*, volume 152. Cambridge University Press, 2003. doi:10.1017/CBO9780511546549.

66 V. V. Sergeichuk. The classification of metabelian p-groups. In *Matrix problems (Russian)*, pages 150–161. Akad. Nauk Ukrain. SSR Inst. Mat., Kiev, 1977.

67 Vladimir V. Sergeichuk. Canonical matrices for linear matrix problems. *Linear Algebra Appl.*, 317(1-3):53–102, 2000. doi:10.1016/S0024-3795(00)00150-6.

68 Charles C Sims. Some group-theoretic algorithms. In *Topics in algebra*, pages 108–124. Springer, 1978. doi:10.1007/BFb0103126.

69 James B. Wilson. Decomposing p-groups via Jordan algebras. *J. Algebra*, 322:2642–2679, 2009. doi:10.1016/j.jalgebra.2009.07.029.

70 James 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.

71 James B. Wilson. Surviving in the wilderness. Talk presented at the Sante Fe Institute Workshop on Wildness in Computer Science, Physics, and Mathematics, 2015.

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

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