On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials IV: Linear-Length Reductions and Their Applications

Joshua A. Grochow
University of Colorado Boulder
Boulder, USA
Joshua.Grochow@colorado.edu

Youming Qiao
University of Technology Sydney
Sydney, Australia
youming.qiao@uts.edu.au

Abstract

By giving new reductions, we show the following algorithmic results and relations between various isomorphism problems

If Graph Isomorphism is in P, then testing equivalence of cubic forms in n variables over a finite field $\mathbb{F}_q$, and testing isomorphism of n-dimensional algebras over $\mathbb{F}_q$, can both be solved in time $q^{O(n)}$, improving from the brute-force upper bound $q^{O(n^2)}$ for both of these.

Polynomial-time search- and counting-to-decision reduction for testing isomorphism of p-groups of class 2 and exponent p in the Cayley table model. This answers questions of Arvind and Torán (*Bull. EATCS*, 2005) for this group class, thought to be one of the hardest cases of Group Isomorphism.

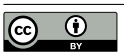
Combined with the $|G|^{O((\log |G|)^{1/2})}$-time isomorphism test for p-groups of Frattini class 2 (Ivanyos, Mendoza, Qiao, Sun, & Zhang, *FOCS* '24), our reductions extend this runtime to p-groups of exponent p and class $c < p$.

Our reductions show that several other Tensor Isomorphism-complete problems over a finite prime field $\mathbb{F}_q$ can be solved in time $q^{\tilde{O}(n^{3/2})}$, where n is the side length. This improves the previous state of the art bound, which was the brute force $q^{O(n^2)}$, for the isomorphism problems for cubic forms, algebras, tensors, and more.

The key to our reductions is to give new gadgets that improve the parameters of previous reductions around Tensor Isomorphism (Grochow & Qiao, *ITCS* '21; *SIAM J. Comp.*, '23). In particular, several of these previous reductions incurred a quadratic increase in the length of the tensors involved. When the tensors represent p-groups, this corresponds to an increase in the order of the group of the form $|G|^{\Theta(\log |G|)}$, negating any asymptotic gains in the Cayley table model. We remedy this by presenting a new kind of tensor gadget that allows us to replace those quadratic-length reductions with linear-length ones, yielding the above consequences.

CCS Concepts

• **Theory of computation → Complexity classes**; **Problems, reductions and completeness**; *Algebraic complexity theory*.



STOC '25, Prague, Czechia

ACM ISBN 979-8-4007-1510-5/25/06
https://doi.org/10.1145/3717823.3718282

Keywords

tensor isomorphism, graph isomorphism, completeness, algebra isomorphism, polynomial isomorphism

ACM Reference Format:
Joshua A. Grochow and Youming Qiao. 2025. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials IV: Linear-Length Reductions and Their Applications. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing (STOC '25), June 23–27, 2025, Prague, Czechia.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3717823.3718282

1 Introduction

Given two combinatorial or algebraic structures, the isomorphism problem asks whether they are essentially the same. The most well-known such problem is Graph Isomorphism (GI for short), which has received considerable attention since the birth of computational complexity (see [2, Sec. 1]). As many isomorphism problems of combinatorial structures reduce to GI in polynomial time, the complexity class GI was introduced, consisting of problems polynomial-time reducible to GI [32].

The study of isomorphism problems of algebraic structures, such as groups, rings, and polynomials, appears naturally in theoretical computer science [1, 3, 18, 30], cryptography [39, 41], computer algebra [12], quantum information [7], and machine learning [40]. Partly motivated by developing a complexity class capturing those problems, the complexity class TI was recently introduced in [20], consisting of problems polynomial-time reducible to Tensor Isomorphism (TI for short).

Problem 1.1. Let $\mathtt{A} = (a_{i,j,k}), \mathtt{A}' = (a'_{i,j,k})$ be two 3-way arrays, with $i \in \{1,\dots,n\}$, $j \in \{1,\dots,m\}$, and $k \in \{1,\dots,\ell\}$, and entries $a_{i,j,k}, a'_{i,j,k}$ from some field $\mathbb{F}$. Are there invertible matrices P, Q, R such that for all i, j, k, we have

$$a'_{i',j',k'} = \sum_{i,j,k} P_{i'i} Q_{j'j} R_{k'k} a_{ijk}. \tag{1}$$

Tensor Isomorphism is a natural generalisation of the matrix equivalence problem, which asks whether two $n \times m$ matrices A and A' are the same up to left and right multiplications of invertible matrices. As GI reduces to TI in polynomial time [20], GI ⊆ TI.

In [20], it was shown that many isomorphism problems studied in different research areas mentioned above are TI-complete. (Other problems have subsequently been shown to be TI-complete as well, e.g., [14, 24].) This theory was developed further to tackle search- and counting-to-decision reductions for group isomorphism [22], and was used to guide the study of group action based cryptography [24, 29, 43], as well as to deduce consequences in quantum

information [13, 20]. A generalisation to over commutative rings leads several connections to number theory, geometry, and computability [23]. Therefore, despite being only recently developed, the complexity theory of TI has shown to be useful in unifying isomorphism problems for algebraic structures, with applications to quantum information and cryptography.

A starting point of this theory is a gadget design that originated in [16], which plays the role of the graph coloring gadget in the study of GI. One serious limitation of this gadget design is that it blows up the dimensions of the resulting tensors by a quadratic factor, which makes several desirable applications unattainable.

In this paper, we provide a new gadget design that achieves only a linear blow-up of the dimensions. This allows us to deduce several interesting consequences, as we will explain in Section 1.2. For now, let us mention one application. Recently, Xiaorui Sun [42] showed that testing isomorphism of p-groups of class 2 and exponent p of order n can be solved in time $n^{O((\log n)^{5/6})}$. This breakthrough is the first $n^{o(\log n)}$-time algorithm for a widely-regarded difficult case of Group Isomorphism [5, 38]. This was subsequently improved to $n^{\tilde{O}((\log n)^{1/2})}$ in [27]. Combining that result with our new gadget design, we can go beyond class-2 p-groups, that is, we can use Sun's algorithm and our reductions to get an $n^{\tilde{O}((\log n)^{1/2})}$-time algorithm to test isomorphism of p-groups of class c and exponent p for any $c < p$. Similarly, for several TI-complete problems over $\mathbb{F}_p$ such as isomorphism problems for tensors, algebras, and cubic forms [1, 16, 20, 22, 24], our linear-size reductions show that Sun's algorithm improves the runtime from $p^{\Theta(n^2)}$ to $p^{\tilde{O}(n^{1.5})}$.

In this extended abstract, we will report our results and give an instance of the application of the new gadget design. The full version can be found at [21].

1.1 Motivation for Improving from Quadratic to Linear Blow-ups

For an $n \times m \times \ell$ 3-way array, we refer to the sum of its side lengths, $n + m + \ell$, as its *length*. Many of the key gadgets designed and used in [16, 20, 22, 24] have quadratic blow-ups in the lengths of 3-way arrays. Such quadratic blow-ups prohibit several important applications, which are enabled by the linear-length reductions we develop here. Here we briefly discuss some motivations here, and refer the readers to Section 1.2 for more details of these applications.

3-way arrays from group isomorphism. The following problem will be useful to discuss the motivations. We use $\mathrm{M}(n, \mathbb{F})$ to denote the linear space of $n \times n$ matrices over $\mathbb{F}$, and $\Lambda(n, \mathbb{F})$ for the linear space of $n \times n$ alternating[1] matrices over $\mathbb{F}$.

Definition 1.2. The Alternating Matrix Space Isometry (AMSI for short) problem asks the following: given $\mathsf{A} = (A_1, \ldots, A_m), \mathsf{B} = (B_1, \ldots, B_m) \in \Lambda(n, \mathbb{F})^m$, decide if there exist $P \in \mathrm{GL}(n, \mathbb{F})$ and $R = (r_{i,j}) \in \mathrm{GL}(m, \mathbb{F})$, such that for any $i \in [m]$, $PA_iP^t = \sum_{j\in[m]} r_{i,j}B_j$.

Note that by naturally viewing matrix tuples as 3-way arrays, the input to AMSI consists of two 3-way arrays. It differs from TI in that there is one matrix $P \in \mathrm{GL}(n, \mathbb{F})$ acting simultaneously on two directions.

[1] An $n \times n$ matrix A is alternating, if for any $u \in \mathbb{F}^n$, $u^t Au = 0$. When the characteristic of $\mathbb{F}$ is not 2, alternating is the same as skew-symmetric (i.e. $A = -A^t$).

Remark 1.3. To see the reason for different actions on 3-way arrays, it is instructive to realise that there are three natural actions on matrices (2-way arrays). By viewing matrices as encoding different kinds of objects: bilinear forms are considered isomorphic if the corresponding matrices are congruent PXP^t, linear maps $V \to V$ are considered isomorphic if they are conjugate PXP^{-1}, and linear maps $V \to W$ are considered isomorphic if they are equivalent under the action $(P, Q) \cdot X = PXQ^t$. Similarly, 3-way arrays can be naturally endowed with five actions of (direct products of) general linear groups, corresponding to representing five different kinds of algebraic or geometric objects. We refer the reader to Definition 1.9 for more details.

Alternating Matrix Space Isometry is closely related to the finite Group Isomorphism problem (GpI for short). When Cayley (multiplication) tables are given, GpI admits an $N^{\log N + O(1)}$-time algorithm by Tarjan (cf. [38]) and Felsch & Neubüser [15] for groups of order N, but to get it down to polynomial time turns out to be difficult. It is long regarded that p-groups of class 2 and exponent p form a bottleneck for further progress on Group Isomorphism (cf. e.g. [5, 17]). By Baer's correspondence [6], testing isomorphism of such groups is equivalent to AMSI over $\mathbb{F}_p$, where $|G| \sim p^{n+m}$ for m-dimensional spaces of $n \times n$ alternating matrices.

The intriguing significance of moderately exponential time. For isomorphism of $n \times m \times \ell$ tensors over $\mathbb{F}_q$—we denote the space of such tensors by $\mathrm{T}(n \times m \times \ell, \mathbb{F}_q)$—and AMSI with inputs from $\mathrm{T}(n \times n \times m, \mathbb{F}_q)$, a "true" polynomial runtime would be $\mathrm{poly}(n, m, \ell, \log(q))$, and $\mathrm{poly}(n, m, \log(q))$, respectively, while the brute-force algorithms run in time $q^{n^2} \cdot \mathrm{poly}(n, m, \ell, \log(q))$ and $q^{n^2} \cdot \mathrm{poly}(n, m, \log(q))$ respectively. It turns out that for these problems, moderately exponential times, namely $q^{O(n+m+\ell)}$ and $q^{O(n+m)}$, are surprisingly significant.

To start with, recall that GpI—when the groups are given by their multiplication (a.k.a. Cayley) tables—reduces to GI [32], and testing isomorphism of p-groups of class 2 and exponent p of order p^ℓ can be reduced to Alternating Matrix Space Isometry for $(A_1, \ldots, A_m) \in \Lambda(n, p)^m$ where $n + m = \ell$ (via Baer's correspondence [6], cf. [35]). So if GI is in P, then AMSI can be solved in time $p^{O(n+m)}$. Slightly extending Babai's suggestion of GpI as a bottleneck for putting GI in P [4], we can also say that a $p^{O(n+m)}$-time algorithm for AMSI stands as a bottleneck to putting GI in P.

Let us then examine the current status of testing isomorphism of p-groups of class 2 and exponent p. Indeed, recent progress on that problem heavily relies on examining AMSI over finite fields [27, 28, 34, 35, 42]. For the purpose of a polynomial-time algorithm for GpI, it suffices to solve this problem in time $p^{O(n+m)}$. This turns out to be difficult: despite much attention from theoretical computer science and computational group theory, only recently was any $p^{o(n+m)^2}$ progress made, in that Sun's breakthrough [42] solves the problem in time $p^{O((n+m)^{1.8}\cdot\log_2(p))}$, and the later improvement to $p^{\tilde{O}((n+m)^{1.5})}$ time [27]. An average-case $p^{O(n+m)}$-time algorithm is also known [10, 35].

Motivation 1: moderately exponential-time equivalence, and bottlenecks for GI.. From the above, we see that moderately exponential time is an important criterion for AMSI due to the connections with

GI and GpI, as well as the current algorithm status. It is therefore of interest to ask whether a $q^{O(n+m+\ell)}$-time algorithm for TI implies a $q^{O(n+m)}$-time algorithm for AMSI and vice versa. Such a moderately exponential-time equivalence cannot be achieved via gadgets causing quadratic blow-ups. These moderately exponential-time equivalences would imply that, if GI in P, then many TI-complete problems, such as TI, Algebra Isomorphism, and Cubic Form Equivalence, admit moderately exponential-time algorithms. This would give us a family of problems that could be viewed as bottlenecks of putting GI in P.

Motivation 2: going beyond class-2 for p-group isomorphism. By the discussion above, obtaining a moderately exponential-time algorithm AMSI can be cast as a special instance of GpI. By the $N^{\tilde{O}((\log N)^{1/2})}$-time algorithm for p-groups of class 2 and exponent p [27], and the widely-held belief that such groups are a bottleneck to general group isomorphism, it is natural to ask if this would lead to a similar result for wider classes of groups, such as p-groups of class 3 and exponent p. Actually, p-groups of class c and exponent p where $c < p$ (such as $c = 3$ and $p = 5$) can be incorporated into TI framework via the Lazard correspondence [22, 33]. However, in the Cayley table model this is not possible with quadratic length increases, as that would yield groups of quasi-polynomial orders.

Motivation 3: search- and counting-to-decision reductions. Arvind and Torán asked whether there exist polynomial-time search- and counting-to-decision reductions for GpI [3]. Moderately-exponential-time reductions are known for p-groups of class 2 and exponent p in the matrix group model, thanks to gadgets restricting to monomial and diagonal groups [22]. The quadratic blow-up was known as a key issue for obtaining any meaningful such reductions for the Cayley table model.

1.2 Our Results: Applications to Isomorphism of Groups, Tensors, and Graphs

Our main technical results are to achieve length-length reductions between several isomorphism problems for 3-way arrays. These allow us to address some questions in Section 1.1 as follows.

Testing isomorphism of p-groups of class c and exponent p, $c < p$. For convenience, let $\mathcal{G}rp(p, c, N)$ be the class of p-groups of class c and exponent p of order N.

Recently, a breakthrough on isomorphism of groups in $\mathcal{G}rp(p, 2, N)$ was achieved by Sun [42], with further improvement in [27].

Theorem 1.4 ([27, Theorem 1.2])**.** *Given the Cayley tables of two groups G and H from $\mathcal{G}rp(p, 2, N)$, there is an $N^{\tilde{O}((\log N)^{1/2})}$-time algorithm testing whether G and H are isomorphic.*

After this result, it is natural to ask the extension of this result to $\mathcal{G}rp(p, c, N)$ with $c > 2$. From prior work this seems plausible, because of a reduction from testing isomorphism of $\mathcal{G}rp(p, c, N)$, $c < p$ to that of $\mathcal{G}rp(p, 2, N)$ in [22], which built on the classical Lazard's correspondence [33]. Alas, that reduction was for matrix groups over finite fields, and the quadratic blow-up in lengths there negates any gains from results in Theorem 1.4. But now with the help of our main technical Theorem 1.10, we get the following corollary of Theorem 1.4.

Corollary 1.5. *Given the Cayley tables of two groups G and H from $\mathcal{G}rp(p, c, N)$, $c < p$, there is an $N^{\tilde{O}((\log N)^{1/2})}$-time algorithm testing whether G and H are isomorphic.*

Improved runtime for other TI*-complete problems.* We also get a related improvement in the runtime of succinctly given 3-tensor problems (in terms of bases, rather than lists or tables). The prior state of the art runtime for the TI-complete problems covered by the following corollary was the nearly-trivial $p^{O(n^2)}$.

Corollary 1.6. *Any problem that reduces to* Tensor Isomorphism *over $\mathbb{F}_q$ by linear-length reductions that are computable in time $q^{O(n)}$ can be solved in time $q^{\tilde{O}(n^{3/2})}$.*[2] *In particular, this holds for* TI, Cubic Form Equivalence *(commutative or noncommutative),* Algebra Isomorphism *(when given by a basis and structure coefficients), and* Isomorphism of Quadratic Maps.

Combined with our linear-length gadgets, this covers all "3-ary" TI-complete problems we are aware of at the time of writing (see [20, Sec. 7.1] for discussion of the notion of 3-ary tensor isomorphism problems).

More bottlenecks for Graph Isomorphism *to be in* P. Combining the reduction from Graph Isomorphism to Group Isomorphism and the Baer's correspondence, we see that $GI \in \mathsf{P}$ implies that AMSI over $\mathbb{F}_p$ can be solved in time $p^{O(L)}$ where L is the length of the input 3-way arrays. By Theorem 1.10, we have the following result.

Corollary 1.7. *Let $\mathbb{F}_p$ be a field of order p, p a prime. If* Graph Isomorphism *is in* P*, then*

(1) For $p > 3$, Cubic Form Equivalence *over $\mathbb{F}_p$ on n-variables can be solved in $p^{O(n)}$ time.*
(2) Algebra Isomorphism *for (associative or Lie) for algebras over $\mathbb{F}_p^n$ can be solved in $p^{O(n)}$ time.*

For Corollary 1.7 (1), we need the classical transformations between symmetric trilinear forms and cubic forms over fields of characteristic not 2 or 3 (cf. [1, 20]). Corollary 1.7 (2) is immediate from Theorem 1.10 (3).

Babai suggested that GpI is bottleneck for putting GI in P [4]. By the wide belief that $\mathcal{G}rp(p, 2, N)$ is a bottleneck case of GpI,[3] solving AMSI over $\mathbb{F}_p$ in time $p^{O(L)}$ is also one. Corollary 1.7 can be viewed as including Polynomial Equivalence and Algebra Isomorphism as further bottleneck problems for putting GI in P, but here the bottleneck is to even get moderately-exponential-time algorithms for these problems (rather than polynomial).

[2] In fact, we could allow the reductions to run in time $q^{\tilde{O}(n^{3/2})}$ as well and get the same result. We state it this way for two reasons: first, all the reductions we are aware of work in this more efficient time bound, and second, should further improvements be found to the exponent in the algorithm in [27], those improvements will apply to this corollary as is.

[3] There are several indications for $\mathcal{G}rp(p, 2, N)$ as a bottleneck case of GpI. First, from the enumeration viewpoint, $\mathcal{G}rp(p, 2, N)$ is an abundant family of groups, namely the number of groups in $\mathcal{G}rp(p, 2, N)$ (up to isomorphism) is (somewhat) comparable to the number of all groups [8]. Second, from the empirical viewpoint, isomorphism testing for many other group classes can be improved considerably [5, 12], while isomorphism testing of $\mathcal{G}rp(p, 2, N)$ has seen relatively little progress until some recent works [27, 35, 42].

Search- and counting-to-decision reductions for $\mathcal{G}rp(p,2,N)$. In complexity theory, polynomial-time search- and counting-to-decision reductions for GI are classical results [32, 37]. Arvind and Torán asked such reductions for GpI [3]. Moderately-exponential time reductions were devised for $\mathcal{G}rp(p,2,N)$ in [22] in the matrix group model. Our linear-length gadgets for restricting to monomial and diagonal groups allow us to deduce the following.

Theorem 1.8. *There are polynomial-time search- and counting-to-decision for isomorphism of groups from $\mathcal{G}rp(p,2,N)$ when Cayley tables are given.*

1.3 Main Technical Results

We now state our main technical results that enable the applications in Section 1.2. To state the results, we review the five actions on 3-way arrays.

Five actions on 3-way arrays. In Remark 1.3, we mentioned that there are three natural actions on matrices (2-way arrays). For 3-way arrays, there are five natural actions as follows.

Definition 1.9. Let $\mathrm{T}(n\times m\times \ell,\mathbb{F})$ be the linear space of 3-way arrays of size $n\times m\times \ell$ over a field $\mathbb{F}$. Let $\mathrm{GL}(n,\mathbb{F})$ be the general linear group of degree n over $\mathbb{F}$.

(1) Given $\mathsf{A}\in \mathrm{T}(n\times m\times \ell,\mathbb{F})$, $(R,S,T)\in \mathrm{GL}(n,\mathbb{F})\times \mathrm{GL}(m,\mathbb{F})\times \mathrm{GL}(\ell,\mathbb{F})$ sends $\mathsf{A}=(a_{i,j,k})$ to $\mathsf{A}'=(a'_{i,j,k})$ as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U)\times \mathrm{GL}(V)\times \mathrm{GL}(W)$ on $U\otimes V\otimes W$.
(2) Given $\mathsf{A}\in \mathrm{T}(n\times n\times \ell,\mathbb{F})$, $(R,T)\in \mathrm{GL}(n,\mathbb{F})\times \mathrm{GL}(\ell,\mathbb{F})$ sends A to A' by (R,R,T) on A as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U)\times \mathrm{GL}(W)$ on $U\otimes U\otimes W$.
(3) Given $\mathsf{A}\in \mathrm{T}(n\times n\times \ell,\mathbb{F})$, $(R,T)\in \mathrm{GL}(n,\mathbb{F})\times \mathrm{GL}(\ell,\mathbb{F})$ sends A to A' by (R,R^{-t},T) on A as defined in Equation 1. Here R^{-t} denotes the transpose inverse of R. This corresponds to the natural action of $\mathrm{GL}(U)\times \mathrm{GL}(W)$ on $U\otimes U^*\otimes W$, where U^* denotes the dual space of U.
(4) Given $\mathsf{A}\in \mathrm{T}(n\times n\times n,\mathbb{F})$, $R\in \mathrm{GL}(n,\mathbb{F})$ sends A to A' by (R,R,R) on A as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U)$ on $U\otimes U\otimes U$.
(5) Given $\mathsf{A}\in \mathrm{T}(n\times n\times n,\mathbb{F})$, $R\in \mathrm{GL}(n,\mathbb{F})$ sends A to A' by (R,R,R^{-t}) on A as defined in Equation 1. This corresponds to the natural action of $\mathrm{GL}(U)$ on $U\otimes U\otimes U^*$. Note that in this case A can be viewed as recording the structure constants of some (possibly non-associative) algebra.

We also need the following notions for 3-way arrays. Let $\mathsf{A}\in \mathrm{T}(n\times m\times \ell,\mathbb{F})$. The frontal slices of A are $\{A_1,\dots,A_\ell\}\in \mathrm{M}(n\times m,\mathbb{F})$, where $A_k(i,j)=a_{i,j,k}$. Let $\mathsf{A}\in \mathrm{T}(n\times n\times n,\mathbb{F})$. Then A is *symmetric* if for any $\sigma\in \mathrm{S}_3$, $\mathsf{A}(i,j,k)=\mathsf{A}(\sigma(i),\sigma(j),\sigma(k))$, and A is anti-symmetric if for any $\sigma\in \mathrm{S}_3$, $\mathsf{A}(i,j,k)=\mathrm{sgn}(\sigma)\mathsf{A}(\sigma(i),\sigma(j),\sigma(k))$.

Linear-length reductions between five actions. Given a group G acting on a set S, the orbit problem for this group action asks, given $s,t\in S$, whether there exists $g\in G$ that sends s to t. Isomorphism problems for graphs, groups, and tensors can all be cast as orbit problems for certain group actions. Our main technical result is a reduction between the orbit problems associated with the five actions in Definition 1.9.

Theorem 1.10. *For $i,j\in[5]$, $i\neq j$, let A and B two 3-way arrays of total length L whose sizes admit the ith action defined in Definition 1.9. Then there exists a polynomial-time computable function f that takes A and B and outputs 3-way arrays $f(\mathsf{A})$ and $f(\mathsf{B})$, such that (1) the lengths of $f(\mathsf{A})$ and $f(\mathsf{B})$ are upper bounded by $O(L)$, and (2) A and B are in the same orbit under the ith action if and only if $f(\mathsf{A})$ and $f(\mathsf{B})$ are in the same orbit under the jth action.*

Furthermore, the above holds even with the following additional structural restrictions:

(1) For $j=2$, i.e. the action of $\mathrm{GL}(U)\times\mathrm{GL}(W)$ on $U\otimes U\otimes W$, the frontal slices of $f(\mathsf{A})$ and $f(\mathsf{B})$ are symmetric (or skew-symmetric).
(2) For $j=4$, i.e. the action of $\mathrm{GL}(U)$ on $U\otimes U\otimes U$, $f(\mathsf{A})$ and $f(\mathsf{B})$ are symmetric (or anti-symmetric) 3-way arrays.
(3) For $j=5$, i.e. the action of $\mathrm{GL}(U)$ on $U\otimes U\otimes U^*$, $f(\mathsf{A})$ and $f(\mathsf{B})$ record the structure constants of associative or Lie algebras.

When $\mathbb{F}=\mathbb{F}_q$, these problems are equivalent under $q^{O(L)}$-time reductions.

Previously in [20], a version of Theorem 1.10 was proved but with the lengths of $f(\mathsf{A})$ and $f(\mathsf{B})$ upper bounded by $O(L^2)$, instead of $O(L)$ as here.

A framework for restricting to isomorphisms by matrix groups and instantiations. Let $G\leq \mathrm{GL}(n,\mathbb{F})$. Suppose we wish to test whether $\mathsf{A},\mathsf{B}\in \mathrm{T}(n\times m\times \ell,\mathbb{F})$ are in the same orbit under the action of $G\times \mathrm{GL}(m,\mathbb{F})\times \mathrm{GL}(\ell,\mathbb{F})$, and our goal is to reduce such an isomorphism to the plain TI problem. The cases for G being monomial groups and diagonal groups are key to the search- and counting-to-decision reductions as in [22]. There, this was achieved with quadratic blow-ups, and some restrictions on the field orders in the diagonal case. The two gadgets designs were achieved in a somewhat ad hoc fashion.

In this work, we develop a framework for restricting to any subgroups of $G\leq \mathrm{GL}(n,\mathbb{F})$, provided that G appears as the first component of the automorphism group of some tensor $\mathsf{A}_G\in \mathrm{T}(n\times m'\times \ell',\mathbb{F})$. This framework makes it easier to work with such problems. We demonstrate the uses of this framework by restricting to G being monomial and diagonal groups. For diagonal groups, we can get rid of the conditions on the order of the field from the prior work [22]. More specifically, we have the following.

Theorem 1.11. *Let $G=\mathrm{Mon}(n,\mathbb{F})\leq \mathrm{GL}(n,\mathbb{F})$ be the monomial subgroup. There exists a polynomial-time computable function $f:\mathrm{T}(n\times m\times \ell,\mathbb{F})\to \mathrm{T}(n'\times m'\times \ell',\mathbb{F})$, such that $\mathsf{A},\mathsf{B}\in \mathrm{T}(n\times m\times \ell,\mathbb{F})$ are isomorphic under $G\times \mathrm{GL}(m,\mathbb{F})\times \mathrm{GL}(\ell,q)$ if and only if $f(\mathsf{A})$ and $f(\mathsf{B})$ are isomorphic as plain tensors. In particular, n',m',ℓ' are upper bounded by $O(n+m+\ell)$.*

The above also holds for $G=\mathrm{diag}(n,\mathbb{F})$ when f is a Las-Vegas randomised polynomial-time computable function.

The proof for the diagonal subgroup relies on connections between graphs and matrix spaces [36] and random regular graphs [45].

1.4 Idea of the New Gadgets

A gadget for partitioned tensor isomorphism with linear-size blow-up. One of the crucial steps in the development of the complexity

class TI is to reduce *partitioned* tensor isomorphism to ordinary TI [16]; this is the tensor analogue of a classical reduction from *colored* GI to ordinary GI (e.g., [32]. It is also one of the places where a quadratic length increase is incurred. As this reduction was then used in several other reductions around TI, they all inherited its quadratic length increase, which we will remedy in this paper. In this section we recall that gadget, and we use two different gadgets from GI as an analogy to explain our new linear-length gadget in the setting of tensors.

Gadgets reducing colored GI *to ordinary* GI.. Colored Graph Isomorphism (color-GI for short) is the problem of deciding whether tow vertex-colored graphs are isomorphic, where we only allow isomorphisms respecting the colors. One way of reducing color-GI to GI is to introduce "star gadgets". For simplicity, let us assume there are no vertices of degree 1 (if there are, we may remove them and use a Weisfeiler–Leman-style coloring to re-color their neighbors according to the multiset of colors of removed vertices, and then iterate this process until no degree-1 vertices are left). Then, if there are c colors, say $1, \dots, c$, then to each vertex of color i, we attach $n + i$ new vertices, which are not attached to any other vertices. Thus each vertex from the original graph, together with this new gadget, forms a star graph. By simple degree considerations of the size of these stars, any isomorphism of the new uncolored graphs must respect the coloring of the original graphs.

Although the star gadgets increase the number of vertices of the graph quadratically, a more economical reduction is to introduce a "color palette." This consists of a path of length c, with a star of size $n+1$ attached to one end (the path and star give an ordering to the vertices in this gadget); then every vertex of color i is attached to the i-th vertex in this path. This gives a linear-size reduction from color-GI to GI. The analogy we pursue in the rest of this section is that our gadget is to priori quadratic-length gadgets [16] as the color palette is to the star gadgets.

The quadratic-length gadget to reduce Partitioned TI *to* TI*: the Futorny–Grochow–Sergeichuk (FGS) gadget.* Let us first define Partitioned TI formally.

Definition 1.12. Given $\mathsf{A}, \mathsf{B} \in \mathrm{T}(n \times m \times \ell, \mathbb{F})$, and a partition of $[\ell] = D_1 \cup D_2 \cup \cdots \cup D_L$, the Partitioned Tensor Isomorphism (part-TI) problem asks whether there exists (P, Q, R) that sends A to B via the action defined in Equation 1, where $P \in \mathrm{GL}(n, \mathbb{F})$, $Q \in \mathrm{GL}(m, \mathbb{F})$, and $R \in \mathrm{GL}(\ell_1, \mathbb{F}) \times \cdots \times \mathrm{GL}(\ell_L, \mathbb{F})$ viewed as a subgroup of block-diagonal matrices in $\mathrm{GL}(\ell, \mathbb{F})$ respecting the partition.

One can of course consider partitions in all three directions, but for clarity of exposition we focus just on one direction in this section. In [16], they show that many tensor problems reduce to Partitioned Tensor Isomorphism, and that the latter reduces to ordinary TI, albeit with quadratic length increase.

Reducing part-TI to TI was done using a gadget designed in [16], which we call the *Futorny–Grochow–Sergeichuk gadget*, or FGS gadget for short. This gadget can be naturally viewed as corresponding to the star graph gadget, which we now explain (see also the discussion in [22, Sec. 3]).

To see how the FGS gadget works, consider the following simplified scenario. By slicing along the third index, a 3-way array $\mathsf{A} \in \mathrm{T}(n \times m \times 6, \mathbb{F})$ can be represented as a tuple of six matrices $\mathbf{A} = (A_1, \dots, A_6)$. Suppose $\ell = 6$ and $L = 3$, $n \le m$, with $[6]$ partitioned into $D_1 = \{1, 2\}, D_2 = \{3, 4\}, D_3 = \{5, 6\}$. To reduce this part-TI to TI, we construct

$$\tilde{A}_1 = \begin{bmatrix} A_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I_n & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{A}_2 = \begin{bmatrix} A_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I_n & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{A}_3 = \begin{bmatrix} A_3 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{2n} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{A}_4 = \begin{bmatrix} A_4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I_{2n} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$\tilde{A}_5 = \begin{bmatrix} A_5 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I_{4n} & 0 \end{bmatrix},$$

$$\tilde{A}_6 = \begin{bmatrix} A_6 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I_{4n} \end{bmatrix}.$$

Let $\tilde{\mathbf{A}} = (\tilde{A}_1, \dots, \tilde{A}_6)$. By [16, Lemma 2.2], A and B in $\mathrm{M}(n \times m, \mathbb{F})^6$ are partitioned isomorphic if and only if $\tilde{\mathsf{A}}$ and $\tilde{\mathsf{B}}$ are isomorphic.

To see how this gadget compares to the star graph gadget, first note that ranks can be viewed as corresponding to degrees, which are isomorphism invariants. Then note that those I_s, I_{2s}, and I_{4s} ensure that the partition is respected, analogous to adding stars of different sizes. (Here, rather than the stars increasing linearly in size, the ranks seem to need to double each time.) For example, if a linear combination involves $\tilde{A}_3, \dots, \tilde{A}_6$, then it will yield a matrix of rank larger than $\mathrm{rank}(\tilde{A}_1)$ or $\mathrm{rank}(\tilde{A}_2)$.

While such a comparison gives a first clue as to why the FGS gadget works, a rigorous proof is more complicated than the graph setting; for example, the Krull–Schmidt theorem for quiver representations needs to be used [16].

A key issue with the FGS gadget is that the sizes of $\tilde{A}_i$ are quadratic in the sizes of A_i. This is not evident in the example above, but the reader can easily see that if $[\ell]$ is partitioned into $[\ell - 1]$ and $\{\ell\}$, then I_s needs to be repeated $\ell - 1$ times, so the sizes of $\tilde{A}_i$ would be of $(n + n + 2n) \times (m + (\ell - 1)n + 2n)$. More formally, the FGS gadget gives us the following.

Theorem 1.13 ([16, Theorem 2.1]). *Fix a partition $[\ell] = D_1 \cup \cdots \cup D_L$, and suppose $n \le m$. There exists a function $f : \mathrm{T}(n \times m \times \ell, \mathbb{F}) \to \mathrm{T}(n' \times m' \times \ell', \mathbb{F})$, such that $\mathsf{A}, \mathsf{B} \in \mathrm{T}(n \times m \times \ell, \mathbb{F})$ are isomorphic as partitioned tensors if and only if $f(\mathsf{A})$ and $f(\mathsf{B})$ are isomorphic as plain tensors. In particular, n', m', ℓ', and the time needed to compute f, are upper bounded by $2^{O(L)} \cdot (n \cdot \ell + m)$.*

Our linear-length gadgets. Instead of adding one identity matrix *per slice* (corresponding to one star per vertex in the graph setting), in our new gadget, we only add one new slice *per partition* (corresponding to one new vertex in the color palette in the graph setting). We still use the ranks of these slices to keep them separate, similar to the single star used at one end of the color palette, but the key gain comes from only having one gadget slice per part rather than one gadget slice per original slice. (The exponential dependence on the number of parts, 2^L, remains; however, in all our uses of PART-TI, our partitions will only need $L = O(1)$ parts. The latter is convenient, because we still do not know whether it is possible to remove this exponential dependence.)

One difficulty that arises in using so few new additional slices is the following. Whereas in previous gadgets, the structure of the gadget enforced that no linear combination of the frontal slices that was part of an isomorphism could alter the gadgets themselves, our gadgets do not have this property. Indeed, there almost always *will be* isomorphisms in which the linear combinations of the frontal slices change the newly added gadget slices. One of our innovations here is that the gadgets also have some additional structure which then allows them to *cancel* these modifications, in a way that leaves the rest of the tensor essentially unchanged. An example of this can be seen in Lemma 2.4, and is formalized for re-use in our definition of "gadget cancellation property".

As a result of the new gadget, we obtain the following reduction from PART-TI to TI with only linear-size blow-ups in the lengths. The reader may want to compare this with Theorem 1.13.

Theorem 1.14. *Fix a partition $[\ell] = D_1 \cup \cdots \cup D_L$, and suppose $n \le m$. There exists a function $g : \mathrm{T}(n\times m\times \ell, \mathbb{F}) \to \mathrm{T}(n'\times m'\times \ell', \mathbb{F})$, such that $\mathsf{A}, \mathsf{B} \in \mathrm{T}(n\times m\times \ell, \mathbb{F})$ are isomorphic as partitioned tensors if and only if $g(\mathsf{A})$ and $g(\mathsf{B})$ are isomorphic as plain tensors. In particular, n', m', ℓ', and the time needed to compute g, are upper bounded by $2^{O(L)} \cdot O(n + \ell + m)$.*

Gadgets for restricting to monomial and diagonal subgroups. As mentioned in Section 1.3, we also develop linear-length gadgets for restricting various groups to consist of monomial or diagonal matrices, and these are crucial in our search- and counting-to-decision reductions. Here we briefly remark on how to view partition tensor isomorphism and these problems from a single viewpoint.

We can formulate colored graph isomorphism and partitioned tensor isomorphism using group-theoretic languages as follows. For colored graph isomorphism, we are interested in permutations of vertices that come from some *Young subgroup* of the symmetric group.[4] Analogously, for partitioned tensor isomorphism, the invertible matrices of interest are from some *Levi subgroup* of the general linear group.[5]

In [22], several questions were studied, including reductions from graph isomorphism to monomial code equivalence, search- and counting-to-decision reductions for tensor isomorphism, and nilpotency-class reduction for group isomorphism. For these reductions, it is of interest to study isomorphism problems of tensors where we restrict the invertible matrices to be from other subgroups of $\mathrm{GL}(n, \mathbb{F})$, such as *monomial subgroups* (consisting of invertible matrices where each row and each column has exactly one nonzero entry) and *diagonal subgroups* (consisting of diagonal matrices). Note that the FGS gadget cannot be used for restricting to diagonal subgroups, because of the exponential dependence on the number of parts.

[4] Given a partition of $[n] = S_1 \cup \cdots \cup S_d$, the Young subgroup corresponding to this partition is the set of permutations π that respect this partition, i.e. $\forall i \in [d]$, $\pi(S_i) = S_i$; see [31].

[5] Given a direct sum decomposition $\mathbb{F}^n = U_1 \oplus \cdots \oplus U_d$, the Levi subgroup corresponding to this decomposition consists of invertible matrices T that preserve this decomposition, i.e. $\forall i \in [d]$, $T(U_i) = U_i$; see [9].

1.5 Some Recent Developments and Outlooks

Recent development. After this work appeared on arXiv, the results and techniques have been used in two recent works.

In [27], Sun's $N^{O((\log N)^{5/6})}$-time algorithm for p-groups of class 2 and exponent p [42] was improved to $N^{\tilde{O}((\log N)^{1/2})}$-time algorithm for p-groups of Frattini class 2. The linear-length reduction from AMSI to TI allows for working with TI instead of AMSI, which helps to simplify parts of the algorithm in [42]. The upgrade from p-groups of class 2 and exponent p to p-groups of Frattini class 2 was also made possible because of the gadgets in this paper.

In [23], the techniques in this paper was further developed to study isomorphism of tensors over commutative rings. These allow for making further progress on p-groups of class 2 (without exponent constraints), and showing polynomial-time equivalence of some problems considered by Grunewald and Segal [25], as well as a problem underlying the classification of Calabi–Yau threefolds via Wall's criterion [44], a geometric object of significance in string theory [11, 26].

Open question: k-TI for $k > 3$. While Corollary 1.6 covers 3-ary TI problems, it does not seem to cover k-TI for $k \ge 4$. (Though it can still yield nontrivial improvements in some unbalanced cases, for example, 4-tensors of format $n^{12/13} \times n^{1/39} \times n^{1/39} \times n^{1/39}$.) Indeed, [20, Remark 4.1] argues that any reduction from k-TI to 3-TI must take k-tensors of side length n to 3-tensors of side length $\gtrsim n^{k/3}$, and the best reduction we are currently aware of only produces 3-tensors of side length $\Theta(n^{\lfloor k/2 \rfloor})$ for $k \ge 5$. If one is looking for goalposts prior to achieving $p^{O(n)}$ (corresponding to isomorphism for the corresponding groups being in P), one might ask for (a) a reduction from 4-TI to 3-TI with side length blowup only $n^{4/3}$ along with devising an algorithm for AMSI in time $p^{O(n^{3/2-\varepsilon})}$—this would reduce the runtime for 4-TI to $p^{O(n^{2-\varepsilon'})}$—or (b) a reduction from 5-TI to 3-TI with side length $n^{5/3}$ along with devising an algorithm for AMSI in time $p^{O(n^{6/5-\varepsilon})}$—which would reduce the runtime for 5-TI to $p^{O(n^{2-\varepsilon''})}$. We note that already for 6-TI, this strategy cannot work to improve the runtime below the trivial $p^{\Theta(n^2)}$ without solving 3-TI in time $p^{O(n)}$, for the side length blowup from 6-TI to 3-TI must be at least n^2. It is thus also an interesting question whether Sun's techniques [27, 42] can be directly extended to k-TI for $k > 3$.

2 From TI to Alternating Matrix Space Isometry

In this section we prove Theorem 2.3. For this we need the following lemmas.

Lemma 2.1 (Individualizing by rank). *Let $r \ge 0$. Let $T_1, \ldots, T_N$ be matrices such that $\mathrm{rk}(T_I) = r2^{I-1}$ for each $i = 1, \ldots, N$.*

Let A be a 3-way array with the following frontal slices:

- $A_1, \ldots, A_\ell$ *are of the form:*

$$\left[\begin{array}{cc:c:ccc:c} *_{n\times m} & * & * & * & \cdots & * \\ * & 0 & 0 & 0 & \cdots & 0 \\ \hdashline * & 0 & 0 & & & \\ * & 0 & & 0 & & \\ \vdots & \vdots & & & \ddots & \\ * & 0 & & & & 0 \end{array}\right],$$

  where each entry represents a block, $*$'s represent arbitrary blocks (one of whose sizes is indicated), $n+m<r$, and 0 or blank represents a block of zeroes;
- *For $I = 1, \ldots, N$, the $\ell + I$-th slice $A_{\ell+I}$ is of the form*

$$\left[\begin{array}{cc:c:ccc:c} * & * & * & \cdots & * & \cdots & * \\ * & 0 & 0 & \cdots & 0 & \cdots & 0 \\ \hdashline * & 0 & 0 & & & & \\ \vdots & \vdots & & \ddots & & & \\ * & 0 & & & T_I & & \\ \vdots & \vdots & & & & \ddots & \\ * & 0 & & & & & 0 \end{array}\right],$$

  (where the block sizes are the same as those in the first form, where T_i appears on the $(2+I)$-th diagonal block).

Let $\mathtt{A}'$ be another 3-way array with the same description as above (but possibly different values filled in for the $*$ blocks).

If $(P,Q,R)\cdot \mathtt{A} = \mathtt{A}'$, then R must have the form $R = \begin{bmatrix} R_{11} & 0 \\ R_{21} & R_{22} \end{bmatrix}$ where R_{11} is $\ell \times \ell$, and R_{22} is $N \times N$ and diagonal.

Proof. First, we show that the upper-right block of R must be zero. To see this, note that that block being nonzero means adding some multiples of $\tilde{A}_{\ell+I}$ with $I \geq 1$ to (some of) the first ℓ frontal slices. But because the T_i's in the lower-right block appear in positions that are zero in the first ℓ slices, such a linear combination would have rank at least $\min\{\mathrm{rk}(T_1), \ldots, \mathrm{rk}(T_N)\} = \mathrm{rk}(T_1) = r$. But this is strictly greater than $n+m$ by assumption, which in turn is an upper bound on the rank of any of the first ℓ slices of $\mathtt{A}'$ because they are supported on a union of n rows and m columns. Thus the upper-right block of R must be zero.

Next, we show that R_{22} is diagonal. The effect of R_{22} is to take linear combinations of $\{A_{\ell+1}, \ldots, A_{\ell+N}\}$. Now consider

$$\hat{A}_{\ell+I} := \sum_{i=1}^{\ell} (R_{21})_{I,i} A_i + \sum_{I'=1}^{N} (R_{22})_{II'} A_{\ell+I'}.$$

Since (P,Q,R) was an isomorphism, and the actions of P, Q, and R commute with one another, we have $P\hat{A}_{\ell+I}Q^t = A'_{\ell+I}$, and therefore $\mathrm{rk}\hat{A}_{\ell+I} = \mathrm{rk}A'_{\ell+I}$. Because the first block-row has height n and the first block-column has width m, we have that $\mathrm{rk}A'_{\ell+I}$ must be in the range

$$[\mathrm{rk}(T_I), \mathrm{rk}(T_I) + n + m]. \tag{2}$$

Let $S = \{I' \in [N] : (R_{22})_{II'} \neq 0\}$ be the support of the I-th row of R_{22}. Then we have that $\mathrm{rk}(\hat{A}_{\ell+I})$ lies in the range

$$\left[\sum_{I'\in S} \mathrm{rk}(T_{I'}),\ n+m+\sum_{I'\in S} \mathrm{rk}(T_{I'})\right]. \tag{3}$$

For $\mathrm{rk}(\hat{A}_{\ell+I})$ to equal $\mathrm{rk}(A'_{\ell+I})$, the range (3) must thus overlap with the range (2).

Since $\mathrm{rk}(T_{I'}) \geq 2\mathrm{rk}(T_I) > n+m+\mathrm{rk}(T_I)$ for $I' > I$, we must have $S \subseteq [I]$ (that is, R_{22} is lower triangular).

Next, if S includes I itself, it cannot include any other indices without going over the allowed range (2), since even the smallest $\mathrm{rk}(T_1)$ is strictly larger than $n+m$. In this case, we would be done (for $S = \{I\}$ would mean that R_{22} is diagonal).

The only remaining possibility is if S is a subset of $[I-1]$. But even if it were all of $[I-1]$, we would then have that the rank is at most

$$\begin{aligned} n+m+\sum_{I'=1}^{I-1} \mathrm{rk}(T_{I'}) &= n+m+\sum_{I'=1}^{I-1} r2^{I'-1} \\ &< r+\sum_{I'=1}^{I-1} r2^{I'-1} \\ &= r2^I = \mathrm{rk}(T_I). \end{aligned}$$

Because of the strict inequality on the second line, we conclude that no subset of strictly earlier slices can have the ranks add up to the necessary rank. Thus we must have $S = \{I\}$, and hence R_{22} is diagonal. This completes the proof of the lemma. □

Lemma 2.2. *Suppose A, A' are full-rank $a \times a$ matrices. The set of pairs $(P,Q) \in \mathrm{GL}_{a+b}(\mathbb{F}) \times \mathrm{GL}_{a+c}(\mathbb{F})$ such that*

$$P\begin{bmatrix} A & 0 \\ 0 & 0_{b\times c} \end{bmatrix} Q^t = \begin{bmatrix} A' & 0 \\ 0 & 0_{b\times c} \end{bmatrix}$$

are precisely those of the form

$$P = \begin{bmatrix} P_{11} & P_{12} \\ 0 & P_{22} \end{bmatrix} \qquad Q = \begin{bmatrix} Q_{11} & Q_{12} \\ 0 & Q_{22} \end{bmatrix}$$

where $P_{11}AQ_{11}^t = A'$, $P_{22} \in \mathrm{GL}_b(\mathbb{F})$, $Q_{22} \in \mathrm{GL}_c(\mathbb{F})$, and P_{12}, Q_{12} are arbitrary.

Proof. Note that

$$\begin{bmatrix} P_{11} & P_{12} \\ P_{21} & P_{22} \end{bmatrix} \begin{bmatrix} A & 0 \\ 0 & 0_{b\times c} \end{bmatrix} \begin{bmatrix} Q_{11}^t & Q_{21}^t \\ Q_{12}^t & Q_{22}^t \end{bmatrix}$$

$$= \begin{bmatrix} P_{11}AQ_{11}^t & P_{11}AQ_{21}^t \\ P_{21}AQ_{11}^t & P_{21}AQ_{21}^t \end{bmatrix} = \begin{bmatrix} A' & 0 \\ 0 & 0_{b\times c} \end{bmatrix}.$$

From the (1,1) entry, we find that $P_{11}AQ_{11}^t = A'$, which is full rank; hence, both Q_{11} and P_{11} have full rank. Next, from the fact that AQ_{11}^t is full rank, by examining the (2,1) position, we find that $P_{21} = 0$. Similarly, the fact that $P_{11}A$ is full rank, by examining the (1,2) position, we find that $Q_{21} = 0$. Finally, we get the invertibility of P_{22} and Q_{22} from the fact that P and Q are block-triangular invertible matrices, so each of their diagonal blocks must be invertible. Lastly, note that $P_{12}, Q_{12}, P_{22}, Q_{22}$ do not occur in the above equations, so they can otherwise be arbitrary. □

Theorem 2.3. 3TI *reduces to* Alternating Matrix Space Isometry *with linear blow-up. In particular, for $n \times m \times \ell$ tensors, the output is an $(\ell+1)$-dimensional space of matrices of size at most $3n+2m+2$.*

Proof. Suppose A is $n \times m \times \ell$, and let the frontal slices of A be $A_1, \ldots, A_\ell$, each of which is an $n \times m$ matrix. We will use parameters r and s which we will set later. Let $\mathcal{A}$ be the matrix space spanned by the following slices:

- For $i = 1, \ldots, \ell$,
$$\tilde{A}_i = \begin{bmatrix} 0_n & A_i & 0_{n\times n} & 0_{n\times 2r} \\ -A_i^t & 0_m & & \\ & & 0_n & \\ & & & 0_{2r} \end{bmatrix}.$$
- A standard alternating slice of rank $2r + 2n$, connected to the first n rows by an I_n in the appropriate place:
$$\tilde{A}_{\ell+1} = \begin{bmatrix} 0_n & 0_{n\times m} & I_n & 0_{n\times 2r} \\ 0_{m\times n} & 0_m & & \\ -I_n & & 0_n & \\ & & & \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix} \end{bmatrix}.$$

Now, note that the rank of any linear combinations of the first ℓ slices is at most $n + m$. The condition on r that we need is

$$2r > n + m.$$

This will enforce that we cannot add $\tilde{A}_{\ell+1}$ to any of the first ℓ slices, as this would make their ranks strictly larger than $n + m$. (Note that the I_n in $\tilde{A}_{\ell+1}$ might not contribute n to the rank of $\tilde{A}_i + \tilde{A}_{\ell+1}$, since it occurs in the same rows as A_i.) This condition is easily satisfied, for example by setting $r = \lfloor (n + m)/2 \rfloor + 1$.

We claim that the map $\mathsf{A} \mapsto \mathcal{A} = \langle \tilde{A}_1, \ldots, \tilde{A}_{\ell+1} \rangle$ is a reduction from 3TI to Alternating Matrix Space Isometry, that is, that $\mathsf{A} \cong \mathsf{B}$ as 3-tensors if and only if $\mathcal{A}$ and $\mathcal{B}$ are isometric matrix spaces.

Note that the matrix tuple which is a basis for $\mathcal{A}$ has dimensions $(2n+m+2r) \times (2n+m+2r) \times (\ell+1)$, and that $2n+m+2r < 3n+2m+2$, so the dimensions of $\mathcal{A}$ are linear in those of A.

($\Rightarrow$) Suppose $\mathsf{A} \cong \mathsf{B}$, via (P, Q, R), that is, $(P\mathsf{A}Q^t)^R = \mathsf{B}$, or in coordinates

$$\mathsf{B}(i, j, k) = \sum_{i'j'k'} P_{ii'} Q_{jj'} R_{kk'} \mathsf{A}(i', j', k').$$

Let $\tilde{P} = \mathrm{diag}(P, Q, P^{-t}, I_{2r})$, $\tilde{R} = \begin{bmatrix} R & 0 \\ 0 & 1 \end{bmatrix}$; we claim that $(\tilde{P}, \tilde{R})$ is a pseudo-isometry of the matrix tuples $(\tilde{A}_1, \ldots, \tilde{A}_{\ell+1})$ and $(\tilde{B}_1, \ldots, \tilde{B}_{\ell+1})$.

First let us consider the last slice. Since R is 1 in its lower-right corner, the last slice is unchanged by $\tilde{R}$. Let us see how it is affected by the isometry action of $\tilde{P}$. For the $\ell + 1$ slice we examine:

$$\begin{bmatrix} P & & & \\ & Q & & \\ & & P^{-t} & \\ & & & I_{2r} \end{bmatrix} \cdot \begin{bmatrix} 0_n & 0_{n\times m} & I_n & 0_{n\times 2r} \\ 0_{m\times n} & 0_m & & \\ -I_n & & 0_n & \\ & & & \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix} \end{bmatrix} \cdot \begin{bmatrix} P^t & & & \\ & Q^t & & \\ & & P^{-1} & \\ & & & I_{2r} \end{bmatrix}.$$

From this we see that in the 4th diagonal block, we get

$$I_{2r} \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix} I_{2r} = \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix},$$

as desired. Because $\tilde{P}$ is block diagonal, all the other zeros in $\tilde{A}_{\ell+1}$ remain zero, and all that is left to check are the (1,3) and (3,1) blocks; we check the (1,3) and the other follows by (skew-)symmetry: it is $PI_nP^{-1} = I_n$, as desired.

All that remains is to check the first ℓ slices. Because these have the form $\begin{bmatrix} 0 & A_i & \\ -A_i^t & 0 & \\ & & 0_{n+2r} \end{bmatrix}$, and $\tilde{P}$ is block-diagonal commensurate with the blocks of the $\tilde{A}_i$, we only focus on the upper 2×2 blocks. For these, we have

$$\begin{bmatrix} P & \\ & Q \end{bmatrix} \begin{bmatrix} 0 & A_i \\ -A_i^t & 0 \end{bmatrix} \begin{bmatrix} P^t & \\ & Q^t \end{bmatrix} = \begin{bmatrix} 0 & PA_iQ^t \\ -QA_i^tP^t & 0 \end{bmatrix}$$

Since $\tilde{R}$ acts on the first ℓ slices the same as R, after applying $\tilde{R}$ we find in the (1,2) block $\sum_{i'} R_{ii'} PA_{i'}Q^t = B_i$, as desired. Thus $(\tilde{P}, \tilde{R})$ is a pseudo-isometry of the corresponding matrix tuples, and thus $\tilde{A}$ and $\tilde{B}$ are isometric matrix spaces, as claimed.

($\Leftarrow$) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are isometric matrix spaces, via (P, R), that is, $\sum_{i'} R_{ii'} P\tilde{A}_{i'}P^t = B_i$ for $i = 1, \ldots, \ell + 1$. Let us write R in block form commensurate with (some of) the blocks of the construction:

$$R = \begin{bmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{bmatrix}$$

where R_{11} is $\ell \times \ell$ and R_{22} is 1×1.

From Lemma 2.1 with (following the notation of the lemma) $N = 1$ and $T_1 := \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix}$, we get that $R_{12} = 0$. (Note that our I_n blocks here occur in the $*$ blocks of Lemma 2.1.)

Now, let $(\tilde{A}'_1, \ldots, \tilde{A}'_{\ell+1}) = (\tilde{A}_1, \ldots, \tilde{A}_{\ell+1})^R$. Since the actions of P and R commute with one another, we have $P\tilde{A}'_iP^t = \tilde{B}_i$ for all $i = 1, \ldots, \ell + 1$.

We have

$$\tilde{A}'_{\ell+1} = \begin{bmatrix} 0 & X & \sigma I & 0 \\ -X^t & 0 & 0 & 0 \\ -\sigma I & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma J_r \end{bmatrix},$$

where $X = \sum_{i=1}^{\ell} (R_{21})_{1i} A_i$, $J_r = \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix}$, σ is the nonzero entry of R_{22}, and the block sizes are $n, m, n, 2r$ (in order).

Lemma 2.4. *For any $n \times m$ matrix X and any nonzero scalar σ, there is a matrix P_0 of the form $P_0 = \begin{bmatrix} I_{n+m} & * \\ 0 & * \end{bmatrix}$ such that*

$$P_0 \begin{bmatrix} 0 & X & \sigma I & 0 \\ -X^t & 0 & 0 & 0 \\ -\sigma I & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma J_r \end{bmatrix} P_0^t = \begin{bmatrix} 0 & 0 & \sigma I & 0 \\ 0 & 0 & 0 & 0 \\ -\sigma I & 0 & 0 & 0 \\ 0 & 0 & 0 & \sigma J_r \end{bmatrix}.$$

Proof. Let

$$P_0 := \begin{bmatrix} I_n & & & \\ & I_m & -X^t/\sigma & \\ & 0 & I_n & \\ & & & I_{2r} \end{bmatrix}.$$

Then

$$\begin{bmatrix} I & 0 & 0 & \\ 0 & I & -X^t/\sigma & \\ 0 & 0 & I & \\ & & & I_{2r} \end{bmatrix} \begin{bmatrix} 0 & X & \sigma I & \\ -X^t & 0 & 0 & \\ -\sigma I & 0 & 0 & \\ & & & \sigma J_{2r} \end{bmatrix} \begin{bmatrix} I & 0 & 0 & \\ 0 & I & 0 & \\ 0 & -X/\sigma & I & \\ & & & I_{2r} \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & \sigma I & \\ 0 & 0 & 0 & \\ -\sigma I & 0 & 0 & \\ & & & \sigma J_{2r} \end{bmatrix},$$

as claimed. □

Remark 2.5. This is in fact one of the novelties of our technique: whereas previous gadgets enforced that such "errors" (like the $\begin{bmatrix} 0 & X \\ -X^t & 0 \end{bmatrix}$ in the upper left) could simply not occur, in our gadgets we no longer enforce that, but the gadgets themselves allow us to *cancel* such errors, without disturbing the rest of the 3-way array.

Let P_0 be as in Lemma 2.4. Now, because P_0 is the identity in its upper-left $(n+m) \times (n+m)$ block, and that is precisely the block where the slices $\tilde{A}'_i$ are supported for $i = 1, \ldots, \ell$, the isometry action of P_0 does not change those slices. Combined with Lemma 2.4, we thus have $P_0(\tilde{A}'_1, \ldots, \tilde{A}'_{\ell+1})P_0^t = (\tilde{A}'_1, \ldots, \tilde{A}'_\ell, \sigma\tilde{A}_{\ell+1})$. Let $\mathcal{A}'' = \langle \tilde{A}'_1, \ldots, \tilde{A}'_\ell, \sigma\tilde{A}_{\ell+1} \rangle$. Since we already have $P\mathcal{A}'P^t = \mathcal{B}$ and $\mathcal{A}'' = P_0\mathcal{A}'P_0^t$, we get

$$(PP_0^{-1})\mathcal{A}''(P_0^{-t}P^t) = \mathcal{B}.$$

Let $P' = PP_0^{-1}$, and let us see what we can learn about P'.

Since we have used the action of R, we have $P'\sigma\tilde{A}_{\ell+1}(P')^t = \tilde{B}_{\ell+1}$. Let us see what constraints this puts on P'. The following lemma is a direct application of Lemma 2.2, but we list it here in a form more directly applicable to the current setting.

Lemma 2.6. *Let $n, m, r, t \geq 0$. Suppose a matrix*

$$P' = \begin{bmatrix} P_{11} & \cdots & P_{16} \\ \vdots & \ddots & \vdots \\ P_{61} & \cdots & P_{66} \end{bmatrix},$$

with diagonal block sizes n, m, n, r, r, t, is such that

$$\sigma P' \begin{bmatrix} 0_n & 0 & I_n & & & \\ 0 & 0_m & 0 & & & \\ -I_n & 0 & 0_n & & & \\ & & & 0_r & I_r & \\ & & & -I_r & 0_r & \\ & & & & & 0_t \end{bmatrix} (P')^t$$

$$= \begin{bmatrix} 0 & 0 & I_n & & & \\ 0 & 0 & 0 & & & \\ -I_n & 0 & 0 & & & \\ & & & 0 & I_r & \\ & & & -I_r & 0 & \\ & & & & & 0_t \end{bmatrix},$$

for some nonzero scalar σ. Then

$$\begin{bmatrix} P_{21} & P_{23} & P_{24} & P_{25} \\ P_{61} & P_{63} & P_{64} & P_{65} \end{bmatrix} = 0.$$

Proof. Let π be the permutation matrix that acts on the block-rows as the cycle $(2, 5, 4, 3)$ (that is, it shifts the second block-row to the fifth block-row, while leaving the order of the other block-rows unchanged). Then

$$\pi P'\pi^t = \left[\begin{array}{cccc:cc} P_{11} & P_{13} & P_{14} & P_{15} & P_{12} & P_{16} \\ P_{31} & P_{33} & P_{34} & P_{35} & P_{32} & P_{36} \\ P_{41} & P_{43} & P_{44} & P_{45} & P_{42} & P_{46} \\ P_{51} & P_{53} & P_{54} & P_{55} & P_{52} & P_{56} \\ \hdashline P_{21} & P_{23} & P_{24} & P_{25} & P_{22} & P_{26} \\ P_{61} & P_{63} & P_{64} & P_{65} & P_{62} & P_{66} \end{array}\right].$$

The equation in the assumption of the lemma is equivalent to

$$(\pi P'\pi^t) \begin{bmatrix} 0 & \sigma I_n & & & & \\ -\sigma I_n & 0 & & & & \\ & & 0_r & \sigma I_r & & \\ & & -\sigma I_r & 0_r & & \\ & & & & 0_{m+t} \end{bmatrix} (\pi P'\pi^t)^t$$

$$= \begin{bmatrix} 0 & I_n & & & & \\ -I_n & 0 & & & & \\ & & 0_r & I_r & & \\ & & -I_r & 0_r & & \\ & & & & 0_{m+t} \end{bmatrix}$$

As the upper-left $(2n+2r) \times (2n+2r)$ matrix here is full rank, by Lemma 2.2, we have that the lower-left $(m+t) \times (2n+2r)$ block of $\pi P'\pi^t$ is zero. But this lower left block is precisely the block in the conclusion of the lemma, completing the proof of Lemma 2.6. □

Now let us consider what happens within the first ℓ frontal slices. From the action of R on the original tuple $(\tilde{A}_1, \ldots, \tilde{A}_{\ell+1})$, and the fact that P_0 did not affect the first ℓ matrices, we have $\tilde{A}'_i = \sum_{i'} R_{ii'}\tilde{A}_i$ for $i = 1, \ldots, \ell$. Such a slice has the form

$$\tilde{A}'_i = \begin{bmatrix} 0 & A'_i & \\ -(A'_i)^t & 0 & \\ & & 0_{n+m+2r+2s} \end{bmatrix}$$

where all empty blocks are zero, and $A'_i = \sum_{i'} R_{ii'}A_i$. Let us see how P' affects such a slice. Since (P', R) was a pseudo-isometry from $(\tilde{A}'_1, \ldots, \tilde{A}'_\ell, \sigma\tilde{A}_{\ell+1})$ to $(\tilde{B}_1, \ldots, \tilde{B}_{\ell+1})$, it must be the case that $P'\tilde{A}'_i(P')^t = \tilde{B}_i$ for $i = 1, \ldots, \ell$. We will now focus only on the upper 2×2 blocks, grouping the remaining blocks all together:

$$\begin{bmatrix} P_{11} & P_{12} & * \\ P_{21} & P_{22} & * \\ * & * & * \end{bmatrix} \begin{bmatrix} 0 & A'_i & \\ -(A'_i)^t & 0 & \\ & & 0_{n+m+2r+2s} \end{bmatrix} \begin{bmatrix} P_{11}^t & P_{21}^t & * \\ P_{21}^t & P_{22}^t & * \\ * & * & * \end{bmatrix}$$

$$= \begin{bmatrix} -P_{12}(A'_i)^t & P_{11}A'_i & 0 \\ -P_{22}(A'_i)^t & P_{21}A'_i & 0 \\ * & * & 0 \end{bmatrix} \begin{bmatrix} P_{11}^t & P_{21}^t & * \\ P_{12}^t & P_{22}^t & * \\ * & * & * \end{bmatrix}.$$

(Because of the zeros in $\tilde{A}'_i$, the $*$ blocks play no role.) The (1,2) entry here gives us the equation

$$-P_{12}(A'_i)^t P_{21}^t + P_{11}A'_i P_{22}^t = B_i$$

However, from above we saw that $P_{21} = 0$, so we are left with

$$P_{11}A'_i P_{22}^t = B_i.$$

Recalling that $A'_i = \sum_{i'} R_{ii'}A_i$, the preceding equation, when applied for all $i = 1, \ldots, \ell$, gives us

$$(P_{11}\mathsf{A}P_{22}^t)^{R_{11}} = \mathsf{B},$$

and thus $\mathsf{A} \cong \mathsf{B}$ as tensors, as desired. □

Acknowledgments

J. A. G. was partly supported NSF CAREER award CCF-2047756.

Y. Q. is supported in part by Australian Research Council DP200100950 and LP220100332. Part of this work was done while Youming was a member of the Institute for Advanced Study in Princeton supported by the Ky Fan and Yu-Fen Fan Endowment Fund.

References

[1] Manindra Agrawal and Nitin Saxena. 2006. Equivalence of $\mathbb{F}$-Algebras and Cubic Forms. In *STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science, Proceedings*. 115–126. doi:10.1007/11672142_8

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

[3] Vikraman Arvind and Jacobo Torán. 2005. Isomorphism Testing: Perspective and Open Problems. *Bulletin of the EATCS* 86 (2005), 66–84.

[4] László Babai. 2016. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, Daniel Wichs and Yishay Mansour (Eds.). ACM, 684–697. doi:10.1145/2897518.2897542

[5] László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. 2011. Code Equivalence and Group Isomorphism. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2011, San Francisco, California, USA, January 23-25, 2011*. 1395–1408.

[6] Reinhold Baer. 1938. Groups with abelian central quotient group. *Trans. Amer. Math. Soc.* 44, 3 (1938), 357–386.

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

[8] Simon R. Blackburn, Peter M. Neumann, and Geetha Venkataraman. 2007. *Enumeration of finite groups*. Cambridge Univ. Press.

[9] Armand Borel. 2012. *Linear algebraic groups*. Vol. 126. Springer Science & Business Media.

[10] Peter A. Brooksbank, Yinan Li, Youming Qiao, and James B. Wilson. 2020. Improved Algorithms for Alternating Matrix Space Isometry: From Theory to Practice. In *28th Annual European Symposium on Algorithms, ESA 2020, September 7-9, 2020, Pisa, Italy (Virtual Conference) (LIPIcs, Vol. 173)*, Fabrizio Grandoni, Grzegorz Herman, and Peter Sanders (Eds.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 26:1–26:15. doi:10.4230/LIPIcs.ESA.2020.26

[11] Philip Candelas, Gary T Horowitz, Andrew Strominger, and Edward Witten. 1985. Vacuum configurations for superstrings. *Nuclear Physics B* 258 (1985), 46–74.

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

[13] Zhili Chen, Joshua A. Grochow, Youming Qiao, Gang Tang, and Chuanqi Zhang. 2024. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials III: Actions by Classical Groups. In *15th Innovations in Theoretical Computer Science Conference, ITCS 2024, January 30 to February 2, 2024, Berkeley, CA, USA (LIPIcs, Vol. 287)*, Venkatesan Guruswami (Ed.). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 31:1–31:23. doi:10.4230/LIPICS.ITCS.2024.31

[14] Giuseppe D'Alconzo. 2023. Monomial Isomorphism for Tensors and Applications to Code Equivalence Problems. Cryptology ePrint Archive, Paper 2023/396. https://eprint.iacr.org/2023/396

[15] V. Felsch and J. Neubüser. 1970. On a programme for the determination of the automorphism group of a finite group. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*. „ 59–60.

[16] Vyacheslav Futorny, Joshua A. Grochow, and Vladimir V. Sergeichuk. 2019. Wildness for tensors. *Lin. Algebra Appl.* 566 (2019), 212–244. doi:10.1016/j.laa.2018.12.022

[17] Joshua A. Grochow. 2019. Answer to "What is the hardest instance for the group isomorphism problem?" on cstheory.stackexchange.com. https://cstheory.stackexchange.com/a/42551/129.

[18] Joshua A. Grochow and Youming Qiao. 2017. Algorithms for group isomorphism via group extensions and cohomology. *SIAM J. Comput.* 46, 4 (2017), 1153–1216. doi: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..

[19] Joshua A. Grochow and Youming Qiao. 2019. Isomorphism problems for tensors, groups, and cubic forms: completeness and reductions. arXiv:1907.00309 [cs.CC].

[20] Joshua A. Grochow and Youming Qiao. 2023. On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness. *SIAM J. Comput.* 52 (2023), 568–617. Issue 2. doi:10.1137/21M1441110 Part of the preprint [19]. Preliminary version appeared at ITCS '21, DOI:10.4230/LIPIcs.ITCS.2021.31.

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

[22] Joshua A. Grochow and Youming Qiao. 2024. On p-Group Isomorphism: Search-to-Decision, Counting-to-Decision, and Nilpotency Class Reductions via Tensors. Vol. 16. 2:1–2:39. doi:10.1145/3625308 Part of the preprint [19]. Preliminary version in CCC 2021..

[23] Joshua A. Grochow, Youming Qiao, Katherine E. Stange, and Xiaorui Sun. 2025. On the complexity of isomorphism problems for tensors, groups, and polynomials V: over commutative rings. In *Proceedings of the 57th ACM Symposium on Theory of Computing, STOC 2025*. to appear.

[24] Joshua A. Grochow, Youming Qiao, and Gang Tang. 2022. Average-case algorithms for testing isomorphism of polynomials, algebras, and multilinear forms. *J. Groups Complex. Cryptol.* 14, 1 (2022), [Paper No. 9431], 21. doi:10.46298/jgcc.2022.14.1.9431 Extended abstract appeared in STACS '21.

[25] Fritz Grunewald and Daniel Segal. 1980. Some general algorithms. I: Arithmetic groups. *Annals of Mathematics* 112, 3 (1980), 531–583.

[26] Tristan Hubsch. 1992. *Calabi-Yau manifolds: A Bestiary for physicists*. World scientific.

[27] Gábor Ivanyos, Euan Jacob Mendoza, Youming Qiao, Xiaorui Sun, and Chuanqi Zhang. 2024. Faster Isomorphism Testing of p-Groups of Frattini Class-2. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024*. IEEE, 1408–1424.

[28] Gábor Ivanyos and Youming Qiao. 2019. 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 (2019), 926–963. doi:10.1137/18M1165682

[29] Zhengfeng Ji, Youming Qiao, Fang Song, and Aaram Yun. 2019. 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*. 251–281. doi:10.1007/978-3-030-36030-6_11

[30] Neeraj Kayal and Nitin Saxena. 2006. Complexity of Ring Morphism Problems. *Computational Complexity* 15, 4 (2006), 342–390. doi:10.1007/s00037-007-0219-8

[31] Adalbert Kerber. 2006. *Representations of Permutation Groups I: Representations of Wreath Products and Applications to the Representation Theory of Symmetric and Alternating Groups*. Vol. 240. Springer.

[32] Johannes Köbler, Uwe Schöning, and Jacobo Torán. 1993. *The graph isomorphism problem: its structural complexity*. Birkhauser Verlag, Basel, Switzerland, Switzerland.

[33] Michel Lazard. 1954. Sur les groupes nilpotents et les anneaux de Lie. *Ann. Sci. Ecole Norm. Sup. (3)* 71 (1954), 101–190. doi:0.24033/asens.1021

[34] Mark L. Lewis and James B. Wilson. 2012. Isomorphism in expanding families of indistinguishable groups. *Groups Complex. Cryptol.* 4, 1 (2012), 73–110.

[35] Yinan Li and Youming Qiao. 2017. 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, Berkeley, CA, USA, October 15-17, 2017*, Chris Umans (Ed.). IEEE Computer Society, 463–474. doi:10.1109/FOCS.2017.49

[36] Yinan Li, Youming Qiao, Avi Wigderson, Yuval Wigderson, and Chuanqi Zhang. 2022. Connections between graphs and matrix spaces. *CoRR* abs/2206.04815 (2022). doi:10.48550/arXiv.2206.04815 arXiv:2206.04815

[37] Rudolf Mathon. 1979. A note on the graph isomorphism counting problem. *Inform. Process. Lett.* 8, 3 (1979), 131–136.

[38] Gary L. Miller. 1978. On the $n^{\log n}$ isomorphism technique (A Preliminary Report). In *STOC* (San Diego, California, United States). ACM, New York, NY, USA, 51–58. doi:10.1145/800133.804331

[39] Jacques Patarin. 1996. 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*. 33–48. doi:10.1007/3-540-68339-9_4

[40] Max Pfeffer, Anna Seigal, and Bernd Sturmfels. 2019. Learning paths from signature tensors. *SIAM J. Matrix Anal. Appl.* 40, 2 (2019), 394–416. doi:10.1137/18M1212331 arXiv:1809.01588.

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

[42] Xiaorui Sun. 2023. Faster Isomorphism for p-Groups of Class 2 and Exponent p. In *STOC*. 443–440. doi:10.1145/3564246.3585250 Preprint arXiv:2303.15412.

[43] Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. 2022. Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms. In *Advances in Cryptology - EUROCRYPT*

2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III (Lecture Notes in Computer Science, Vol. 13277), Orr Dunkelman and Stefan Dziembowski (Eds.). Springer, 582–612. doi:10.1007/978-3-031-07082-2_21

[44] Charles Terence Clegg Wall. 1966. Classification problems in differential topology. V: On certain 6-manifolds. *Inventiones mathematicae* 1, 4 (1966), 355–374.

[45] Nicholas C. Wormald. 1999. Models of random regular graphs. *London Mathematical Society Lecture Note Series* (1999), 239–298.