Review of Literature on Algebraic Isomorphism Testing

Euan Mendoza

November 8, 2023

Abstract

Graph Isomorphism has become a foundational problem to computational complexity and has led to many developments in computer vision and machine learning. However, the worst-case deterministic complexity of this isomorphism problem is not well understood. In order to provide a path for improvement we develop a class called the TI-complete problems and discuss how they impact the complexity of Graph Isomorphism. We attempt to solve many long standing open questions in mathematics and theoretical computer science and push the bounds of the status quo. We discuss new techniques and methodolgies which have had success in improving the complexity of isomorphism problems and the current status quo of isomorphism testing. In doing this we hope to further develop the field of quantum computing, computational group theory and machine learning.

Contents

1 Introduction

Isomorphism Testing of Algebraic and Combinatorial Structures asks to decide whether two objects are *isomorphic*. Understanding the complexity is to try and improve the worst-case asymtoptic time-complexity on a deterministic turing machine. An isomorphism ($\cong$) is an equivalence relation that is less strict than an equality. This is important to all fields of mathematics and science since very rarely real world objects are strictly equivalent (for example trying to match objects given by a image representation, or match molecules given their graphs).

The *Isomorphism Testing Problem* for algebras and combinatorial structures is a widely studied problem in theoretical computer science [GQ23b; GQ21; GQ23a]. It has a variety of applications in quantum information, post-quantum cryptography and machine learning, with the most widely studied problem being that of Graph Isomorphism.

Isomorphism problems are studied heavily in the field of computational complexity. Graph Isomorphism was one of the first problems described in Karp's seminal paper describing the 21 NP-complete problem [Kar72]. In which Karp listed Graph Isomorphism as an open question whether Graph Isomorphism is in P or is NP-complete. Graph Isomorphism is the most studied Isomorphism Problem, however only recently graph isomorphism was shown to be quasi-polynomial time [Bab16]. While theoretically graph isomorphism seems like a difficult problem, in practice it is quite easy, for example Babai, Erdos and Selkow showed Graph Isomorphism has a linear time average case running time [BES80]. Graph Isomorphism is seen as effectively solved in practice, see [McK81; MP14].

Graph Isomorphism is important as many objects can be generalised as graphs, however showing that graph isomorphism can be solved efficiently for all graphs (this is equivalent to showing graph isomorphism is in P). It is thought by experts in the field that we first need to improve group isomorphism [Bab16].

Compared to Graph Isomorphism Problem, the isomorphism problems for general algebraic structures such as tensors, and polynomials are much more difficult to solve. Like Graph Isomorphism they also exhibit the property that it is unknown whether they are in P or are NP-complete. Compared to Graph Isomorphism which took many years to develop a quasi-polynomial time algorithm. The *Group Isomorphism Problem* is an interesting case. It has been quasi-polynomial time bounded since its initial investigation, with time $N^{O(\log N)}$ where N denotes the group order, originally attributed to Tarjan, [Mil78]. With the best known improvement not improving Group Isomorphism testing to even $N^{o(\log N)}$, [Ros13]. The *group isomorphism* problem asks to decide whether two finite groups given by their cayley tables are isomorphic. This is at least as hard as graph isomorphism since group isomorphism can be cast as a graph isomorphism problem, [KST93]. However, there has been relatively little progress in improving the worst-case bound for Group Isomorphism compared to Graph Isomorphism.

A particularly interesting and hard case of group isomorphism testing is the isomorphism testing problem of p-groups of (nilpotent) class 2 and exponent p. Historically this class proved difficult to show an improvement over the current status quo of group isomorphism with running time $N^{O(\log N)}$, until Sun showed p-groups of class 2 and exponent p could be tested in time $N^{o(\log N)}$, [Sun23].

1.1 The Practical Applications of Isomorphism Testing

The isomorphism testing of algebraic structures, specifically of polynomials, tensors and groups has been widely studied for applications in machine learning, quantum information, and post-quantum cryptography.

Computational Group Theory is a branch of applied mathematics concerned with developing efficient algorithms relating to group theory, see ([O'B94]). A notoriously difficult case of groups for computation is p-groups of class 2 and exponent p. Currently little improvement has been made over the previous results however the representation of p-groups as linear spaces of matrices presents new avenues to explore within computational group theory, [LQ17].

In *Post-Quantum Cryptography*, Graph Isomorphism had been explored as a potential avenue as a protocol for zero-knowledge proofs, see [GMW91]. However due to Graph Isomorphism being easily solvable in practice [BES80], Graph Isomorphism did not provide a solid foundation as a Cryptography Scheme. In contrast with Graph Isomorphism, the Tensor Isomorphism Problem seems much more difficult, difficult enough practically to yield a plausible cryptography scheme, see [Tan+22].

In *Quantum Information* an important question asking if two quantum states are interconvertible by SLOCC (local operation and classical communication statistically). This can be cast as a tensor isomorphism testing problem, [DVC00; Ben+01].

Within *Data Science and Machine Learning* in feature extraction a method would be to utilise a *signature tensor* and reconstruct the path of the tensor, see [Che57]. This can be seen as a tensor congruence problem, see [PSS19].

2 Literature Review

The isomorphism testing problem for algebraic structures given by a group acting on a set are closely related problems which can be described by what the underlying set is. A group acting on combinatorial structures (graphs) have been heavily explored and researched. Trivially yielding the successful Weisfeiler-Leman algorithm and colour refinement [BES80]. However it is also important to consider a group acting on a linear structure. Finite groups can be represented as matrix spaces and lie algebras, and polynomials can also trivially be represented as (multi)linear structures. This is the main motivation of the complexity class TI.

2.1 Preliminary Definitions and Notation

First we describe some basic definitions and notation.

Sylow p-groups and Nilpotent Groups. A *commutator* of a group G is defined as $[a, b] = a^{-1}b^{-1}ab$, if A, B are subgroups of G than the *commutator subgroup* is defined as $[A, B]$ is the group generated by $[a, b]$ where $a \in A, b \in B$. The *lower central series* of a group G is defined as $\gamma_1 = G, \gamma_{k+1}(G) = [\gamma_k(G), G]$. A group is defined to be *nilpotent* if there is a c such that $\gamma_{c+1}(G) = 1$. So c denotes the class of the group. A classic result in finite group theory is that for a finite group, the group is nilpotent if and only if it is the product of it's Sylow subgroups. So the groups of prime power order p^r are nilpotent.

Linear spaces. $\mathbb{F}_q$ denotes a finite field of order q. Sometimes written as $\mathbb{F}_p$ depending on the context. The corresponding linear space of dimension n over the field is denoted as $\mathbb{F}_q^n$.

Matrices and Matrix spaces. The space of $n\times n$ matrices over the field $\mathbb{F}_q$ is denoted $M(n, \mathbb{F}_q)$ and the space of $n\times m$ matrices over $\mathbb{F}_q$ is similarly denoted $M(n\times m, \mathbb{F}_q)$. Given a matrix $A \in M(n\times m, \mathbb{F}_q)$, the transpose of A is denoted $A^\top$. A matrix $A \in M(n\times m, \mathbb{F}_q)$ is said to be *symmetric* if $A = A^\top$ and *skew-symmetric* or *alternating* if $A = -A^\top$. The space of alternating matrices is denoted $\Lambda(n, \mathbb{F}_p)$.

Linear Groups. $GL(n, \mathbb{F}_q)$ denotes the general linear group or the set of $n\times n$ invertible matrices over the field $\mathbb{F}_q$.

Font	Object	Corresponding space
$A, B, \ldots$	matrix	$M(n, \mathbb{F}_q)$ or $M(n \times m, \mathbb{F}_q)$
$\mathcal{A}, \mathcal{B}, \ldots$	matrix spaces	The subspaces of $M(n, \mathbb{F}_q)$ or $M(n\times m, \mathbb{F}_q)$
$\mathfrak{A}, \mathfrak{B}, \ldots$	matrix spaces	The subspaces of $M(n, \mathbb{F}_q)$ or $M(n\times m, \mathbb{F}_q)$ corresponding to a tensor slice
$\mathtt{A}, \mathtt{B}, \ldots$	tensors	$T(n\times m\times l, \mathbb{F}_q)$

Description of notation and corresponding objects.

Here we give a general definition, that extends to all (algebraic & combinatorial) structures.

Definition 2.1. The Isomorphism Testing Decision Problem for Algebraic Structures can be generalised as Given a group G acting on a set X, decide if two set elements $x, y \in X$ are in the same G-orbit.

An important distinction between the isomorphism testing of graphs and the isomorphism testing of algebraic structures. In the testing of graphs the underlying set that the group acts on is a combinatorial structure (implying the use of combinatorial techniques to solve graph isomorphism). While the group acting on an algebra is generally linear, and the underlying set being a (multi)-linear structure (implying the use of linear algebraic techniques).

Tensors can be understood as multidimensional arrays, and 3-Tensors which denote 3-dimensional arrays can be understood as matrix spaces when slicing them. This leads to important definitions of actions on matrix spaces.

Definition 2.2. Two matrix spaces $\mathcal{A}, \mathcal{B} \subseteq M(n\times m, \mathbb{F}_p)$ are said to be *equivalent* if (and only if) there exists matrices $P \in GL(m, \mathbb{F}_p)$ and $Q \in GL(n, \mathbb{F}_p)$ such that $P\mathcal{A}Q = \mathcal{B}$, and $P\mathcal{A}Q$ denotes the space $\{PAQ \mid A \in \mathcal{A}\}$. Similarly two matrix spaces $A, B \subseteq M(n, \mathbb{F}_p)$ are said to be *conjugate* if there exists a $P \in GL(n, \mathbb{F}_p)$ such that $P\mathcal{A}P^{-1} = \mathcal{B}$. Finally the matrix spaces are said to be *isometric* if and only if $P\mathcal{A}P^\top = \mathcal{B}$.

2.2 Tensor Isomorphism and Tensor Isomorphism Completeness

Given that algebraic isomorphism problems seem harder to improve at least in literature compared to that of graph isomorphism, it is important to understand the *theoretical complexity* of algebraic isomorphism problems. Algebraic Isomorphism Problems can trivially be understood in the complexity class GI which is explored by Kobler in his book on Graph Isomorphism Complexity ([KST93]). However, this approach has limitations since while Graph Isomorphism is easy in practice, algebraic isomorphism problems are thought to be intractable ([GQ23a]). It is unknown whether algebraic isomorphism problems are P or NP-complete either so the usual framework for dealing with intractability is not very useful. That is to say, we need to come up with a way of understanding the complexity of algebraic isomorphism problems that properly encapsulates the difficulty of them.

This is the primary motivation for the development of the complexity class TI and the definition of TI-complete which is the hardest problems in TI.

Recall definition 2.1. This can be extended to the d-Tensor Isomorphism Problem where the general linear group acts on the sides of the tensor.

Definition 2.3. For vector spaces $V_i \in \mathbb{F}_q^{n_i}$ over a field $\mathbb{F}_q$. A d-Tensor $\mathtt{T} = V_1 \otimes V_2 \otimes \ldots \otimes V_d$ and $\mathtt{S} = U_1 \otimes U_2 \otimes \ldots \otimes U_d$. The d-Tensor Isomorphism Problem asks to decide whether there exists matrices $A_i \in GL(n_i, \mathbb{F}_q)$ such that for a tensor $\mathtt{T}$, A_i acting on V_i produces $\mathtt{S}$. Trivially the 3-Tensor Isomorphism Problem is equivalent with three vector spaces U, V, W and the tensors $U \otimes V \otimes W$.

This leads us to the related notion of the complexity class TI and TI-completeness. Like graph isomorphism, the class TI gives a notion of which problems exhibit similar properties, such as being somewhere between NP-complete and P. Showing that a variety of problems were in TI including isomorphism for algebras over a finite field was a classic result, see [FGS19]. However, showing that problems in TI exhibit the same property of intractability required introducing the notion of TI-complete problems, this is the major result of Grochow and Qiao [GQ23a].

Definition 2.4 ([GQ23a]). TI or TI$\mathbb{F}_q$ is the class of problems polynomial-time turing (Cook) reducible to the d-tensor isomorphism problem for a fixed d over a field $\mathbb{F}_q$. A problem is said to be *TI-hard* iff for any d, d-Tensor Isomorphism reduces to the problem in polynomial time (turing). Finally a problem is said to be *TI-complete* iff it is both TI-hard and in TI. Note that TI-completeness denotes the hardest problems in TI.

The significance of this cannot be understated. Showing that problems are TI-complete is fundamental to understanding the complexity of problems such as group isomorphism (for which the hardest cases are TI-complete) and as evidence for showing that Graph Isomorphism is in P. That is to say if we show any problem that is TI-complete can be solved efficiently, we improve the bounds for all TI-complete problems, the problem of p-groups is specifically of interest due to Babai [Bab16] describing them as a roadblock to showing GI is in P. This leads to an important theorem in the testing of algebraic isomorphism problems.

Theorem 1 ([GQ23a]). *The following problems are TI-complete.*

1. ***3-Tensor Isomorphism*** *(over a field $\mathbb{F}_q$)*
2. ***Group Isomorphism*** *for the case of p-groups of (nilpotent) class 2 (reduces to TI$\mathbb{F}_{p^c}$ for the special case of tensors over the field $\mathbb{F}_{p^c}$).*
3. ***Matrix Space Isometry***
4. ***Matrix Space Conjugacy***
5. ***Algebra Isomorphism*** *including the cases:*
   (a) ***Associative Algebra Isomorphism*** *for algebras that commutative and unital, or for algebras that are commutative and 3-nilpotent.*
   (b) ***Lie Algebra Isomorphism*** *for 2-step nilpotent Lie Algebras*
6. ***Cubic Form Equivalence*** *and* ***Trilinear Form Equivalence****.*

2.3 Isomorphism Testing for p-Groups of Class 2 and Exponent p

Graph Isomorphism has been incredibly important to the field of machine learning [**zotero-62**]. Interestingly, while Graph Isomorphism is not known to be in P, Graph Isomorphism is efficiently solvable in practice due to the successful weisfeiler-leman and colour refinement techniques, see [CFI92]. In fact this algorithm forms the basis of graph neural networks and is shown to be as powerful as graph isomorphism networks, see [Xu+19].

Tensors and linear structures are much easier for a computer to represent however, it has long been known that it is much more difficult to efficiently compute TI-complete problems (specifically that of p-groups class 2 exponent p) in practice. Colour refinement and weisfeiler-leman (colour refinement is a special case of weisfeiler-leman) have been successful in the average case analysis of graph isomorphism, see [BES80]. This leads to the question of applying a refinement technique in the context of linear group actions. This lead to the linear analogues as a technique for the average case complexity analysis of tensor isomorphism, see [LQ17; Bro+19].

However in the context of worst-case analysis it is important to understand the complexity of p-group of class 2 exponent p isomorphism since as per the introduction it is the most well-known TI-complete problem in literature. Importantly p-group of class 2 exponent p under Baer's correspondence can be represented as alternating matrix spaces, and again represented as a 3-tensor by combining the matrix spaces to form 3-dimensional arrays.

Lemma 2.1 ([Bae38])**.** *Let G, H be two p-groups of class 2 and exponent p, with group order p^c. There is a bijection between G and H and corresponding alternating bilinear maps $G/Z(G) \times G/Z(G) \to [G, G]$ where $Z(G)$ denotes the center of the group. Since bilinear maps can be represented as alternating matrix spaces $\mathcal{G}, \mathcal{H} \subseteq \Lambda(n, \mathbb{F}_p)$. The isomorphism problem for p-groups of class 2 exponent p is equivalent to the matrix space isometry problem over the field $\mathbb{F}_p$. Which is decide if there exists a matrix $P \in GL(n, \mathbb{F}_p)$ such that $P\mathcal{A}P^\top = \mathcal{B}$.*

Now we can ask what is the worst case complexity of p-groups of class 2 exponent p given a brute force algorithm.

Lemma 2.2. *There exists a brute-force algorithm for testing p-groups of class 2 and exponent p in time $N^{O(\log N)}$ where $N = p^c$ denotes the group order.*

Proof. Consider the algorithm.

Algorithm 1 Brute-Force Algorithm for p-group of class 2 exponent p

.

Input

$\mathcal{A}$	A matrix spaces in $\Lambda(n, \mathbb{F}_p)$ which is a representations of p-groups of class 2 exponent p
$\mathcal{B}$	A matrix spaces in $\Lambda(n, \mathbb{F}_p)$ which is a representations of p-groups of class 2 exponent p

Output

YES	Is isomorphic
NO	Not isomorphic

Algorithm

```
1. For each matrix in $P \in GL(n, \mathbb{F}_p)$, if $P\mathcal{A}P^\top = \mathcal{B}$, return YES.
2. Return NO.
```

Since their are p^{n^2} possible entries for a matrix in $M(n, \mathbb{F}_p)$ the running time of Alg 1. $\leq p^{n^2} \cdot \text{poly}(n, \log p)$. So clearly the algorithm is in time $N^{O(\log N)}$. ■

The point of this shows that even a naive brute force algorithm is quasi-polynomial time bounded. As described before, linear analogues to colour refinement and weisfeiler-leman have been successful in average case analysis of this problem [LQ17; Bro+19]. Inspired by this Sun introduces two techniques inspired by colour refinement approaches called *matrix space indvidualisation refinement* and *low-rank matrix characterisation*, [Sun23]. In matrix space individualisation refinement, Sun presents a proof that we can find a left and right multiplication matrix with a resulting image of matrices of smaller size, such that given a suitably high rank, they produce a non-zero matrix. However, while the left and right matrices are small enough to enumerate with little cost to the algorithm runtime, it does not deal with small rank matrices. Based on the work of Flanders, Atkinson and Lloyd, Sun introduces a method called *low rank matrix characterisation* for producing smaller matrices from low rank matrices [Fla62; AL81].

Theorem 2 ([Sun23])**.** *Let $\mathcal{A}$ and $\mathcal{B}$ be two $n \times n$ skew-symmetric matrix spaces, both of dimension m, over $\mathbb{F}_p$ for some prime number $p > 2$ and positive m, n. There is an algorithm with running time $p^{O((n+m)^{1.8} \cdot \log p)}$, which determines whether there exists a matrix $S \in GL(n, \mathbb{F}_p)$ such that $S\mathcal{A}S^\top = \mathcal{B}$.*

This presents the secondary result from Sun which shows that skew-symmetric matrix space isometry testing can be improved upon.

Theorem 3 ([Sun23])**.** *Let G and H be two p-groups of class 2 exponent p for an odd prime power p (where the group order is p^c), there is an algorithm with running time $N^{O((\log N)^{5/6})}$ to determine whether G and H are isomorphic, where N denotes the group order.*

This is Sun's main result, it shows clearly that p-groups of class 2 and exponent p are testable in time $N^{o(\log N)}$. Using new techniques he improves a long standing bound in isomorphism testing.

2.4 Future Work and Review

We have new tools for testing matrix space isometry. However, there is still an important class of p-groups which Sun explicitly did not test for, that of 2-groups. Additionally, whether his lower bounds are optimal is still a open question to experts. It is currently under investigation whether his bounds can be improved.

The big question also remains about what his breakthrough means for all TI-complete problems. That is a question first answered by Grochow and Qiao in their recent paper [GQ23a]. However, given the potential improvements of the bounds of p-group isomorphism, very soon the bounds of all TI-complete problem may once again require investigation.

3 Conclusion

The important problem of the isomorphism testing of TI-complete problems has the potential to revolutionalise many industries. As described it could potentially introduce new powerful techniques of machine learning [Xu+19].

Recently the cryptography scheme based on alternating trilinear form equivalence was proposed as a NIST submission for the post-quantum cryptography standardisation process (ALTEQ), see appendix ALTEQ. Understanding the computational complexity of the TI-complete problems is fundamentally important to the success of the submission.

In conclusion the TI-complete problems are still not well understood, there is still much discovery to be made about how much they can be improved. Understanding the complexity of such problems can lead to new techniques and improvement to long standing questions in mathematics that have formed the foundation of techniques prevalent to those in machine learning. As quantum computing and machine learning become ever prevalent in industry understanding how complex these problems are become ever important to pushing the bounds of the future of computing.

A Appendix

A.1 ALTEQ

`https://pqcalteq.github.io/`

References

[AL81] MD Atkinson and S Lloyd. “Primitive Spaces of Matrices of Bounded Rank”. In: *Journal of the Australian Mathematical Society* 30.4 (1981), pp. 473–482. ISSN: 1446-8107.

[Bab16] László Babai. “Graph Isomorphism in Quasipolynomial Time [Extended Abstract].” In: *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016.* 2016, pp. 684–697. DOI: 10.1145/2897518.2897542.

[Bae38] Reinhold Baer. “Groups with Preassigned Central and Central Quotient Group”. In: *Transactions of the American Mathematical Society* 44.3 (1938), pp. 387–412. ISSN: 0002-9947.

[Ben+01] Charles H. Bennett et al. “Exact and Asymptotic Measures of Multipartite Pure-State Entanglement”. In: *Physical review. A, Atomic, molecular, and optical physics* 63.1 (2001). ISSN: 1050-2947. DOI: 10.1103/PhysRevA.63.012307.

[BES80] László Babai, Paul Erdös, and Stanley M. Selkow. “Random Graph Isomorphism.” In: *SIAM J. Comput.* 9.3 (1980), pp. 628–635. DOI: 10.1137/0209047.

[Bro+19] Peter A. Brooksbank et al. “Incorporating Weisfeiler-Leman into Algorithms for Group Isomorphism.” In: *CoRR* abs/1905.02518 (2019).

[CFI92] Jin-yi Cai, Martin Fürer, and Neil Immerman. “An Optimal Lower Bound on the Number of Variables for Graph Identification.” In: *Comb.* 12.4 (1992), pp. 389–410. DOI: 10.1007/BF01305232.

[Che57] Kuo-Tsai Chen. “Integration of Paths, Geometric Invariants and a Generalized Baker- Hausdorff Formula”. In: *The Annals of Mathematics* 65.1 (Jan. 1957), p. 163. ISSN: 0003486X. DOI: 10.2307/1969671. JSTOR: 1969671. (Visited on 09/20/2023).

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. “Three Qubits Can Be Entangled in Two Inequivalent Ways”. In: *Physical review. A, Atomic, molecular, and optical physics* 62.6 (2000). ISSN: 1050-2947. DOI: 10.1103/PhysRevA.62.062314.

[FGS19] Vyacheslav Futorny, Joshua A. Grochow, and Vladimir V. Sergeichuk. “Wildness for Tensors”. In: *Linear Algebra and its Applications* 566 (Apr. 2019), pp. 212–244. ISSN: 0024-3795. DOI: 10.1016/j.laa.2018.12.022. (Visited on 09/23/2023).

[Fla62] H. Flanders. “On Spaces of Linear Transformations with Bounded Rank”. In: *Journal of the London Mathematical Society* s1-37.1 (1962), pp. 10–16. ISSN: 0024-6107. DOI: 10.1112/jlms/s1-37.1.10.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. “Proofs That Yield Nothing But Their Validity for All Languages in NP Have Zero-Knowledge Proof Systems.” In: *J. ACM* 38.3 (1991), pp. 691–729. DOI: 10.1145/116825.116852.

[GQ21] Joshua A. Grochow and Youming Qiao. “On p-Group Isomorphism: Search-To-Decision, Counting-To-Decision, and Nilpotency Class Reductions via Tensors.” In: *36th Computational Complexity Conference, CCC 2021, July 20-23, 2021, Toronto, Ontario, Canada (Virtual Conference).* 2021, 16:1–16:38. DOI: 10.4230/LIPIcs.CCC.2021.16.

[GQ23a] Joshua A. Grochow and Youming Qiao. “On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials I: Tensor Isomorphism-Completeness.” In: *SIAM J. Comput.* 52.2 (Apr. 2023), pp. 568–617. DOI: 10.1137/21m1441110.

[GQ23b] Joshua A. Grochow and Youming Qiao. “On the Complexity of Isomorphism Problems for Tensors, Groups, and Polynomials IV: Linear-Length Reductions and Their Applications.” In: *CoRR* abs/2306.16317 (2023). DOI: 10.48550/arXiv.2306.16317.

[Kar72] Richard M. Karp. “Reducibility Among Combinatorial Problems.” In: *Proceedings of a Symposium on the Complexity of Computer Computations, Held March 20-22, 1972, at the IBM Thomas J. Watson Research Center, Yorktown Heights, New York, USA.* 1972, pp. 85–103. DOI: 10.1007/978-1-4684-2001-2_9.

[KST93] Johannes Köbler, Uwe Schöning, and Jacobo Torán. “Decision Problems, Search Problems, and Counting Problems”. In: *The Graph Isomorphism Problem: Its Structural Complexity.* Ed. by Johannes Köbler, Uwe Schöning, and Jacobo Torán. Progress in Theoretical Computer Science. Boston, MA: Birkhäuser, 1993, pp. 11–50. ISBN: 978-1-4612-0333-9. DOI: 10.1007/978-1-4612-0333-9_3. (Visited on 09/23/2023).

[LQ17] Yinan Li and Youming Qiao. “Linear Algebraic Analogues of the Graph Isomorphism Problem and the Erdős-Rényi Model.” In: *58th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2017, Berkeley, CA, USA, October 15-17, 2017.* 2017, pp. 463–474. DOI: 10.1109/FOCS.2017.49.

[McK81] Brendan D McKay. "Practical Graph Isomorphism". In: *Congressus Numerantium* 30 (1981), pp. 45–87.

[Mil78] Gary L. Miller. "On the N̄log n Isomorphism Technique: A Preliminary Report". In: *Proceedings of the 10th Annual ACM Symposium on Theory of Computing, May 1-3, 1978, San Diego, California, USA.* 1978, pp. 51–58. DOI: 10.1145/800133.804331.

[MP14] Brendan D. McKay and Adolfo Piperno. "Practical Graph Isomorphism, II." In: *Journal of Symbolic Computation* 60 (2014), pp. 94–112. DOI: 10.1016/j.jsc.2013.09.003.

[O'B94] E. A. O'Brien. "Isomorphism Testing for P-Groups." In: *J. Symb. Comput.* 17.2 (1994), pp. 133–147. DOI: 10.1006/jsco.1994.1007.

[PSS19] Max Pfeffer, Anna Seigal, and Bernd Sturmfels. "Learning Paths from Signature Tensors". In: *SIAM Journal on Matrix Analysis and Applications* 40.2 (Jan. 2019), pp. 394–416. ISSN: 0895-4798, 1095-7162. DOI: 10.1137/18M1212331. (Visited on 09/20/2023).

[Ros13] David J. Rosenbaum. "Bidirectional Collision Detection and Faster Deterministic Isomorphism Testing". In: *CoRR* abs/1304.3935 (2013).

[Sun23] Xiaorui Sun. *Faster Isomorphism for p-Groups of Class 2 and Exponent p.* 2023. DOI: 10.48550/arXiv.2303.15412.

[Tan+22] Gang Tang et al. "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.* 2022, pp. 582–612. DOI: 10.1007/978-3-031-07082-2_21.

[Xu+19] Keyulu Xu et al. "How Powerful Are Graph Neural Networks?" In: *7th International Conference on Learning Representations, ICLR 2019, New Orleans, LA, USA, May 6-9, 2019.* 2019.