Algebraic Isomorphism Testing Project Proposal

Euan Mendoza [14279196]

Sunday the 5th of November, 2023

Contents

1 Executive Summary

Algebraic Isomorphism Testing asks whether two objects in their respective categories are structurally equivalent. Isomorphism Testing is vital because we often treat structural equivalence as natural equivalence instead of the mathematical definition, which does not consider equality equivalent to isomorphism unless we take univalence as our foundation of mathematics.

This inherent relation between equality and isomorphism is foundational in the real world. In Computational Group Theory, this question may interest those asking whether two molecules share the exact symmetry. In quantum information and quantum cryptography, this is a fundamentally important question.

Historically speaking, the question of finding an efficient algorithm for isomorphism testing of p-groups of class 2 and exponent p has been a widely studied problem as one of the most challenging cases of group isomorphism. Xiaorui Sun showed isomorphism could be tested in time $N^{o(\log N)}$ where N denotes the group order, which is a prime power p^k. Additionally, there is a representation of p-groups of class 2 and exponent p under Baer's correspondence to Alternating Matrix Spaces, as well as Alternating Matrix Spaces being a fundamental TI-complete problem.

These relationships allow for a new project investigating potential improvements synthesised based on these classical results. This project proposes developing a new algorithm for testing p-groups of class 2 and exponent p and using this algorithm to improve the general status quo of the TI-complete problems. At a high level, this is achievable by improving the two new techniques developed by Sun in his seminal paper. We additionally should hopefully be able to prove this result holds for the class of even p-groups of class 2 exponent p as well as being able to extend our results to the other TI-complete problems in the same vein that Grochow and Qiao have successfully managed to do in the recent past.

2 Introduction

This report proposes a new improvement to *Algebraic and Combinatorial Isomorphism Testing*. *Isomorphism Testing* asks whether two structures in their respective (mathematical) categories are *essentially* and *structurally* equivalent. In practice, we find that very few structures are mathematically equal. Working with objects with the same *structure* but not necessarily the same *composition of elements* is more straightforward in practice.

Abstractly dealing only with the structure of objects is far easier than dealing with strictly equal objects. However, finding out if two structures are equivalent is much more difficult. The project's primary goal is to uncover the algorithmic complexity of the problem for the case of p-groups of (nilpotent) class 2 and exponent p. We also want to know how improvements can propagate to related problems.

Historically, Graph Isomorphism has presented itself as the most widely studied isomorphism testing problem. Graph Isomorphism was one of the first open questions in the development of computer science, pointedly with the question asking whether Graph Isomorphism is P or NP-complete [Kar72]. However, while *Graph Isomorphism* is a rich field of research, the isomorphism testing of other algebraic structures is a relatively prosperous and unexplored area presenting exciting gaps in the current knowledge of computational complexity and theoretical computer science.

The new development of an algorithm for testing p-groups of class 2 and exponent p in time $N^{O((\log n)^{5/6})}$ by Xiaorui Sun [Sun23] presents an opportunity to improve the current best known worst-case bounds of all the TI-complete isomorphism problems [GQ23a].

2.1 Isomorphism Testing Uses in Industry

Isomorphism Testing has many valuable applications, specifically in Post-Quantum Cryptography and Quantum Information. The leading group primarily interested in the complexity of isomorphism testing is the UTS QSI Centre of Quantum Science and Information under grant LP220100332 and NIST ((American) National Institute of Standards and Technology).

In *Post-Quantum Cryptography,* Isomorphism Testing is used as a theoretical basis for ALTEQ, which is a current candidate for a post-quantum cryptography scheme based on the trilinear forms equivalence problem, which is a TI-complete problem [Tan+22].

Isomorphism Testing is also essential to Quantum Information, Machine Learning and Computational Group Theory. The applications are described in detail later on in the report.

2.2 Preliminary Definitions

The following notation and definitions are essential to the content of the report. The following definitions can be found in the reference text [Sip12].

This report distinguishes the notion of an *algorithm* from the definition typically (mis)-used in literature. We can informally define an algorithm as a set of instructions on a Turing-complete system that always terminates on the *correct* solution. When we move over to the world of heuristics and practical algorithms, we give up on a proof of correctness or a guarantee of termination. Heuristics are usually distinguishable in literature since they utilise benchmarks and real-world performance as a metric, where here, we analyse algorithms by counting the maximum number of steps until they terminate. Here, we distinctly distinguish algorithms that yield worst-case analysis as our classical algorithms and practical and AI algorithms as our heuristics.

In *computational complexity,* we classify algorithms based on their respective worst-case running times in *time complexity* and worst-case space usage in *space complexity.* Classically, we can take P as the class of algorithms that terminate after a polynomial number of steps on a deterministic Turing machine. We can also understand NP as the class of algorithms that terminate in a polynomial amount of steps in a non-deterministic Turing machine. The notion of NP-complete is also vaguely useful in the isomorphism testing problem. NP-complete defines the class of (decision) problems such that for a given problem if it is in NP and every problem in NP is polynomial time (Karp) reducible to that problem, it is said to be NP-complete.

A reduction from a problem A to a problem B means that we write an algorithm that takes the inputs of A and modifies them to be the inputs of B. If A is reducible to B, then we can use B to solve A by changing the inputs to B and using an algorithm that solves B to solve A. In a sense, the principle of reductions is why it is not a *broad problem* to test all TI-complete problems due to the property that if we solve a single TI-complete problem, we can solve the rest in the complexity class by using the algorithm obtained to solve the single instance.

For the case of this paper, we refer to Algebraic Isomorphism Testing as the testing of TI-complete structures where TI-completeness refers to the complexity class defined by Grochow and Qiao [GQ23a].

2.3 Overview of the Report Structure

The report presents the goals of the proposed project first, introducing the project aims and objectives. The report presents a brief yet detailed overview of the history of the algebraic isomorphism testing problem. Which we can use to describe, based on the *status quo*, how significant the research is and what are the potential implications of completing the project. We finally provide an overview of the *methodology* used to accomplish our objectives.

3 Research Aims & Objectives

At a high level, this research aims to improve the current state-of-the-art complexity of algebraic and combinatorial isomorphism testing problems. Improving the current state of the art can be done by accomplishing the following tasks.

In the project, a significant component is correctly *understanding* and *improving* upon Sun's algorithm for p-group of class 2 exponent p [Sun23]. That is to develop a faster algorithm yielding worst-case analysis for isomorphism testing of p-groups of class 2 and exponent p.

In the case that we develop a new algorithm for p groups of class 2 exponent p, we know that there is a reduction from p-groups of class 2 exponent p to all other TI-complete isomorphism problems[GQ23a; GQ23b]. As such, it is vital to know how the result potentially *improves* and *extends* to the TI-complete problems, including 3-Tensor Isomorphism, Alternating Matrix Space Isometry and the testing of classes of Lie Algebras.

In his paper on p-groups of class 2 exponent p, Sun introduces two new techniques for isomorphism testing of (multi) linear structures, specifically the techniques of *high-rank matrix space individualisation refinement* and *low-rank matrix characterisation*. Another project goal is to apply these techniques to many other related problems. Notably, these techniques are related to alternating matrix space isometry testing more closely than to p-group of class 2 exponent p isomorphism testing. Similar techniques may apply to matrix space isometry problems broader than alternating matrix spaces.

Another significant objective of this project is to develop the so-called linear algebraic analogues of the Weisfeiler-Leman technique. In the research background section, the report describes how the technique has been used to powerfully compute isomorphisms on combinatorial structures. However, so far, linear algebraic models have succeeded in the average case, but there are gaps in literature for the development or contribution of analogues in the worst-case complexity.

4 Background

4.1 Graph Isomorphism and the Relationship to Algebraic Isomorphism Testing

In the initial investigation of the classic problem P vs NP, Karp asked whether Graph Isomorphism was in P or NP-complete in 1972 [Kar72]. Since then, there has been rapid development in the isomorphism testing of Graphs. The impressive results in graph isomorphism can be directly attributed to the success of the *naive colour refinement technique* [BBG17; CC82]. The k-dimensional Weisfeiler-Leman Algorithm generalised the results from the Colour Refinement technique and has proved to be an incredibly powerful foundation for Graph Isomorphism Testing [WL68; CFI92].

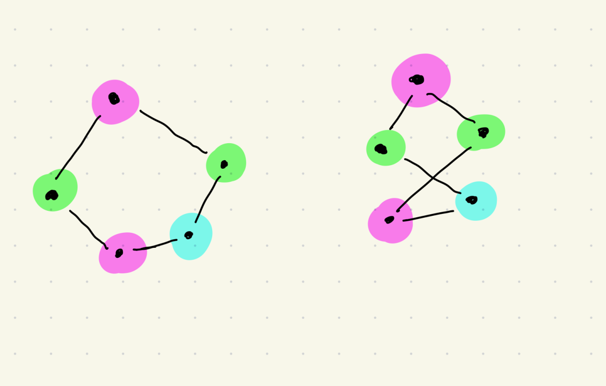

Figure 1: Naive Colour Refinement

The Weisfeiler-Leman Algorithm is a powerful technique that appears in some form in every practical and average case algorithm for Graph Isomorphism. Most notably, graph isomorphism was shown to be linear time-bounded in the average case [BES80]. Graph Isomorphism was also shown to be efficient in practice [McK81; MP14].

These results all gave strong evidence that Graph Isomorphism is likely in the complexity class P instead of NP-complete, which are the hardest problems in NP. It is known that Graph Isomorphism (and group isomorphism) lie somewhere in the complexity class NP ∩ co-AM. It is also a classic result that Graph Isomorphism being NP-complete implies the collapse of the polynomial-time hierarchy to the second level [Sch88].

Using a different group-theoretic formulation of the Graph Isomorphism Problem, Babai, in a landmark breakthrough, showed that Graph Isomorphism was quasipolynomial time-bounded [Bab16]. In his seminal paper, Babai posed the question of *how hard is Graph Isomorphism*. In his paper, he referenced Group Isomorphism as a potential roadblock to putting Graph Isomorphism in the Complexity Class P. Babai also specifically noted that p-groups of class 2 and exponent p seemed to be a particularly hard case of graph isomorphism.

Grochow and Qiao also noted in the seminal paper on Tensor Isomorphism completeness that Tensor Isomorphism is a roadblock to p-group isomorphism of class 2 exponent p groups [GQ23a].

4.2 Algebraic Isomorphism in Connection to TI-complete problems

While Graph Isomorphism forms an interesting problem, it has effectively hit a roadblock. Graph Isomorphism is seen as a problem that is *effectively* solved even though the question *is Graph Isomorphism in P* is still an open question. However, the algebraic isomorphism testing of other algebraic structures are in their own right, fascinating problems.

While Graph Isomorphism and the Isomorphism Testing of algebraic structures are fundamentally intertwined, historically, they have followed very different paths through literature. It should be noted that Graph Isomorphism was studied for roughly 50 years before the quasipolynomial time breakthrough. Even still, the quasipolynomial time breakthrough was irrespective of the fact that very early on, Graph Isomorphism had a practically efficient algorithm.

When compared to the history of Group Isomorphism, Group isomorphism was known very early on to have a worst-case time bound of $N^{O(\log N)}$ where N denotes the group order, which was initially attributed to Tarjan [Mil78]. In 40 years, the best-known algorithm for group isomorphism cannot improve this result even to the marginal improvement of $N^{o(\log N)}$ [Ros13]. In particular, an especially hard case of the *Isomorphism Problem for Groups* was the case of p-groups of class 2 exponent p.

The development of the complexity class TI and the notion of TI-complete with a definition mirroring the NP-complete complexity class by Grochow and Qiao provided a solid foundation to study this inherent difficulty [GQ23a]. Importantly noting the shift from making *improvements* to understanding *what makes Algebraic Isomorphism Testing hard*. Notably, TI closely resembles work done by Cook and Levin in the seminal result of proving SAT is NP-complete and the corollary that 3-SAT is NP-complete. With the counterparts that Tensor Isomorphism is TI-complete, and 3-Tensor Isomorphism is TI-complete.

Isomorphism Testing can be viewed as a problem of given two elements of a set X and a group acting on the set G, decide if the two elements are in the same G-orbit. Under this framework, we can view Graph Isomorphism Testing as asking, given the set of graphs given by their adjacency lists, are two graphs in the same orbit of the permutation group acting on the graph. The seemingly much more difficult instance of this problem is asking whether tensors given by three linear basis and the general linear group acting on each basis are two tensors in the same orbit.

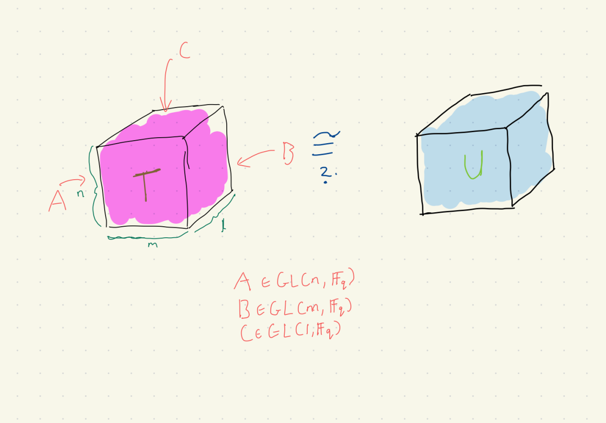

Figure 2: Pictoral View of Group Actions on a Tensor

Tensors can be constructed from Alternating Matrix Spaces, which are linear representations of p-groups of class 2 exponent p given by Baers Correspondence [Bae38]. Some breakthroughs were made in algebraic isomorphism testing using Baer's correspondence and linear representations. Notably, based on the success of the Weisfeiler-Leman algorithm, efficient average case linear analogues were developed[LQ17; Bro+19].

Using ideas taken from utilising linear analogues of the Weisfeiler-Leman algorithm, the first significant breakthrough in p-groups class 2 exponent p testing was made by Xiaorui Sun by introducing two new techniques for dealing with the aforementioned Alternating Matrix Space Isometry Problem, namely *high-rank individualisation refinement* and *low-rank matrix characterisation* [Sun23]. With low-rank matrix characterisation being developed from the work of Flanders [Fla62]. Using these new techniques, Grochow and Qiao showed that his results extended to all the other TI-complete problems [GQ23b].

5 Research Significance & Innovation

5.1 Significance of the Research

As per the history of the algebraic isomorphism testing problem, there are two avenues to explore when understanding the significance of algebraic isomorphism testing.

From the perspective of Graph Isomorphism, algebraic isomorphism testing is significant due to the properties exhibited by the Graph Isomorphism Problem. Whether Graph Isomorphism is in P has been an open question since the inception of Computer Science and Computational Complexity, with the results showing that Graph Isomorphism is an easy problem in both the practical case and the average case [BES80; McK81], it is surprising that showing Graph Isomorphism is in P has been such a difficult task. This is evidence that there is a particularly hard case of Graph Isomorphism.

Since Graph Isomorphism is known to be *easy* in practice, more work has been done to understand what makes finding an efficient algorithm in the worst-case for Graph Isomorphism so tricky. An investigation into Graph Isomorphism with parameterised complexity has been done to investigate which specific instances of Graph Isomorphism are difficult. Specifically, Graph Isomorphism has parameterised algorithms bounded by Treewidth, Graph Minors, Graph Euler Genus and maximum degree [GN21; GNW23]. However, it is essential to note the dichotomy of practically efficient algorithms using combinatorial techniques to solve Graph Isomorphism, while the best-known worst-case solutions utilise techniques from Group Theory.

It is believed that there must be a particularly hard case of Graph Isomorphism, which forms a roadblock to placing Graph Isomorphism in P. The connection between Graph Isomorphism and Group Theory, especially within efficient worst-case methods of solving Graph Isomorphism has long been thought to be a clue in this apparent difficulty. Here, Group Isomorphism is classically reducible to Graph Isomorphism [KST93]. However, the significant lack of development in the group isomorphism problem, especially the case of p-groups of class 2 and exponent p is the predominant reason that experts believe 'Graph Isomorphism cannot be solved until we solve Group Isomorphism' [Bab16].

As a side note, another perspective on why Algebraic Isomorphism Problems are so attractive compared to the Graph Isomorphism Problem is that Graph Isomorphism forms a zero-knowledge proof protocol [GMW91]. However, since Graph Isomorphism is easy to calculate in practice, it is a fundamentally insecure protocol. However, the algebraic isomorphism problems tend to be much harder to calculate. As such, understanding the complexity of algebraic isomorphism testing is essential to establish how effective a cryptographic protocol based on algebraic isomorphism testing is [Tan+22].

From the perspective of Algebraic Isomorphism Testing as a stand-alone problem. (Nilpotent) p-groups of class 2 exponent p have long stood as a hard case of the group isomorphism problem. Sun's algorithm is a significant breakthrough as it opens a 40-year-long block in the development of algorithms for Group Isomorphism [Sun23]. We now have new techniques at our disposal that have the potential to improve further isomorphism testing algorithms for all of the known TI-complete algorithms. Work has been done to show that Sun's result extends to the other TI-complete problems [GQ23b]. However, there is room for improvement in developing new and more efficient algorithms than the last.

5.2 Potential Benefits of Understanding the Complexity of Isomorphism Testing

Isomorphism testing has numerous practical applications, all in need of faster algorithms. Complexity gives a sense of what particular aspects of a problem are hard and may allow further development in various fields.

Understanding the Complexity of TI-complete problems is now more critical than ever. It is becoming increasingly common knowledge that Shor's algorithm and Quantum Computing potentially threaten information security [AA23]. However, the current NIST call for Post Quantum Cryptography Schemes all rely on lattice-based cryptography standards. This means lattice-based schemes could potentially suffer the same fate as factorisation-based algorithms, which are weak to Shor's algorithm. Essentially, we need to diversify the landscape of cryptographic protocols in order to ensure security. A cryptographic protocol based on Alternating Trilinear Forms, a known TI-complete problem, was proposed to accomplish this goal [Tan+22]. Understanding the difficulty within the TI-complexity class gives us clues as to whether TI-complete problems can stand the test of time as a secure Cryptographic Protocol.

In *Quantum Information,* UTS QSI maintains an interest in this area of research. Quantum Information is the area of study trying to understand information-theoretic problems through the lens of non-classical quantum physics. It is crucial to many industries, such as finance, for its potential use in efficiently solving challenging optimisation problems. However, this is still a field in the early stages of development. Quantum Information, by being *Quantum* mathematically, is modelled as Tensor Products within Hilbert Spaces, and a classic question asks if there is a relation of quantum states under *stochastic local operations and classical communications* (SLOCC) [Ben+01]. However, this can be precisely modelled as a problem of Tensor Isomorphism[DVC00].

In *Computational Group Theory,* the problem of TI-completeness and p-group isomorphism for class 2 and exponent p groups is fundamentally essential to developing more efficient algorithms within Computational Algebra Software such as MAGMA and GAP. These tools are used industry-wide by researchers in domains such as Chemistry, where they ask if two chemical molecular structures are equivalent under symmetry (equivalent to a group acting on a structure sharing the same orbit).

In *Machine Learning,* there are two domains in which isomorphism problems are fundamentally important. In *feature extraction,* we can use tensor isomorphism to extract the *signature tensor* from a machine-learning model [PSS19; Che57]. Feature extraction is used in *cancer cell detection. As* such, cancer researchers are primary stakeholders to feature extraction improvements. Additionally, Graph Neural Networks proliferate in computer vision through object detection and motion-tracking applications. The basis of these networks has been shown to be equivalent to the famous Weisfeiler-Leman technique described in the history section [Xu+19].

5.3 Innovation within the Proposed Project

In completing this research, we would have improved upon a 40-year-long bottleneck in showing that Group Isomorphism Testing can be done in $N^{o(\log N)}$ time.

We hope to set the status quo based on Sun's techniques. We do not believe our current algorithms are the fastest they can be, and given new techniques, we think we can improve these algorithms further.

The innovation is not singly in creating faster and more efficient algorithms. The most significant potential contribution to this project would be showing that the 2-groups of class 2 and exponent p are solvable in time $N^{o(\log N)}$. The even groups are thought to compose most p-groups of class 2 and exponent p despite p representing a prime power. This is a big feat and would allow us to show that all cases of p-groups of class 2 and exponent p are little-o quasipolynomial time bounded.

Solving all p-groups is essential in understanding the complexity of isomorphism testing problems. It has the potential to propagate through every isomorphism problem and improve our current understanding of each problem so that we may develop new techniques for optimising problems in machine learning and quantum information. As well as understanding new potential threats to cryptosystems based on alternating trilinear form equivalence.

6 Research Methods

6.1 Research Methods Related to Pure Mathematics

This research is within the space of the categorisation and complexity analysis of intractable problems. Here, we only care about the worst case.

In undertaking the research, we attempt to prove mathematically certain properties of algorithms. As such, we borrow numerous methodologies from the research of computational complexity.

In *undertaking literature reviews,* we seek to understand what makes techniques proposed in papers so powerful. This is important to gain a *conceptual* understanding of the problem and *verify* the accuracy of the information. Here, we will try to understand new techniques proposed and find potential ways to build upon and improve upon such techniques.

In *developing new mathematical methods,* we seek to identify *mathematical* areas in which we can introduce new results. Each *new* theorem or *lemma* must be verified with *proof* showing that the assumption is true based on *formal logic.* An expert, such as a fellow researcher in the same domain or a supervisor, should verify each proof. Methods of presenting new proofs could be presentations and written reports with accompanying proofs.

In *optimising mathematical results,* we attempt to find flaws in current known mathematical results and add improvements. The methodology is the same as *developing a new method* however, it is based on prior knowledge where *new methods* are original results.

In developing results, we will use mainly techniques taken from *linear* and *abstract algebra,* which is the study of *linear* and *abstract* algebraic structures. Here, we concern ourselves with *finite* structures. As such, we borrow knowledge from *representation theory,* a developed theory that asks how abstract structures can be *represented as linear structures.* Any new knowledge that *contributes* to the field of *representation theory* is considered progress. As such, we can measure progress by describing new lemmas and theorems produced while also accounting for their *importance* within the current literature to which they apply.

In developing results, we also heavily utilise the *probabilistic method,* which is a non-constructive proof technique that shows that objects exist bound by specific structure given that there is a non-zero constant probability of them existing within a set. In general, *probabilistic proofs* yield a range of potential improvements, such as *optimising the bounds* (which means we find a better probability of something existing). This works well with the above group and linear theoretic techniques and allows us to prove with certainty that structures may exist.

6.2 Research Methods to Algorithm Analysis and Computational Complexity

In *Computational Complexity,* we utilise *asymptotic analysis* for the worst-case by asking the question, how many steps does this algorithm take asymptotically on a deterministic Turing machine with respect to a given input? Here, we try to find *lower* asymptotic bounds. We need to provide both a *proof of correctness,* which says that for every input string *w,* the Turing machine will *halt* on the correct solution to the problem. We also need a *proof of time-bounds,* which is the analysis of how many *steps* it takes to compute the answer to the problem on a *deterministic single-tape Turing machine.* Our criteria for success is if the algorithm has a *lower asymptotic running time in the worst case* than the last.

It is also important to show that specific problems are in a particular *complexity class.* As such, it is essential to use the *appropriate* reduction for the complexity class. For example, for a reduction to a TI-complete problem, we must show that a given problem is polynomial time Turing reducible to Tensor Isomorphism. Here, we have specific *criteria* in order to constitute a *successful* reduction. The reduction most often needs to be a *computable function,* which is a function that runs on a Turing Machine and halts on the image of the function for every pre-image.

In most cases, the reduction will need to query an *Oracle Turing machine*, but the amount of queries defines the difference between Karp and Turing reductions. We also say that for standard reductions, we want $\forall w \in L \Leftrightarrow f(w) \in L'$, or our function is surjective. Other criteria usually depend on the *type* of reduction. Such as FPT reductions for the FPT complexity class or polynomial time reductions to show an algorithm is in P or NP-complete. A reduction is a critical research methodology as it *classifies* the difficulty of a problem. The introduction of new *appropriate* reductions verified by a *proof of correctness* is considered good progress in research in computational complexity.

6.3 On the Collection of Data and Evaluation Metrics

It should be noted that usually, we cannot simply classify research in Computational Complexity as *qualitative* or *quantitative.* Qualitative implies the collection of experimental and statistical data. In contrast, Qualitative describes the collection of data that is up to interpretation and evaluated based on non-numerical and subjective measures.

The results obtained within the project have the property that, once verified, they *should* not be up to interpretation. They should be *verified* formally. Of course, there is *potential for mistakes.* However, the results are *not experimental.* In the same vein, in contrast to qualitative data, we do not want our data to be *up to interpretation.* With this understanding, the data collected from Computational Complexity research is an equal mix of qualitative and quantitative metrics. In quantitative, we want to evaluate a result based on a numerical answer without interpretation. Our qualitative aspect is evaluating formal arguments in logic and making connections between an abstract representation and broader concepts.

The *type* of data collected will be a repository of lemmas and corresponding *proofs* utilising the techniques mentioned previously. Each *proof* can be verified as correct or incorrect and may be compared based on select criteria. Such as does the proof introduce new original knowledge to the current landscape. Does the proof obtain tighter bounds than a previous result, or does the proof generalise more objects than a previous result?

Specifically, we hope to obtain a *faster* algorithm in *deterministic worst-case* for the class of TI-complete problems, which we can *compare* with the current status quo.

6.4 The Proposed Research Structure

In undertaking our research, we want a fixed research design to improve *the algorithm for testing isomorphism in p-groups of class 2 exponent p.* However, we may want a more flexible research design in which we can *explore* the *implications* to other TI-complete problems.

In doing so, we need to *understand* the techniques proposed in the algorithm by *conducting literature reviews* and *undertaking presentation-style research activities.* We must also *create a body of Lemmas, Theorems and accompanying proofs.* Synthesising a faster algorithm for p-groups of class 2 exponent p is feasible within the project period.

However, developing new techniques based on the Weisfeiler-Leman Algorithm, a significant component of Sun's paper is a broad and flexible research goal. After developing a faster algorithm for the case of p groups of class 2 exponent p, exploring the implications, either through directly applying new techniques or through a method of TI-complete reductions and analysis, is the more exciting aspect of the project contained within the project proposal.

7 Conclusion

Algebraic Isomorphism Testing is arguably at the forefront of mathematical and theoretical computer science. It has developed into one of the most intriguing areas that puzzle mathematicians and computer scientists alike.

Establishing faster deterministic worst-case algorithms for testing TI-complete problems gives us new information on how to develop algorithms in the practical sense. TI-complete algorithms have classically been a challenging class of problems to solve.

This report describes the TI-complete problems as significant for broadening the potential post-quantum cryptography schemes available to us in a world dominated by lattice-based schemes. It also mentions the importance of the result as a widely studied theoretical problem.

This report describes the very long and significant historical connection and correlation between the isomorphism testing of (multi)linear structures and the isomorphism testing of graphs. The graph-based formulation of the problem hopes to utilise results obtained in understanding the complexity of general algebraic isomorphism described as group actions to improve results within its research domain.

In understanding the overall depiction of isomorphism testing as a problem and how it can be understood as a single open question in research. The report proposes a new project in which we attempt to improve the known worst-case time complexity status quo for isomorphism testing. We describe the methodology and also describe how, when understanding TI-complete problems as a homogeneous class of problems given by polynomial-time Turing reductions, we can understand that any faster result obtained for p-group of class 2 exponent p isomorphism testing can be extended to the other isomorphism testing problems. This is a result demonstrated in the following paper [GQ23a]. As such, it is not unreasonable or infeasible to think of this project's scope as both significant and reasonable within a year.

A Appendix

References

[AA23] ASD and ACSC. *Planning for Post-Quantum Cryptography | Cyber.Gov.Au.* 2023. URL: https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography (visited on 11/05/2023).

[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. URL: https://doi.org/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.

[BBG17] Christoph Berkholz, Paul S. Bonsma, and Martin Grohe. "Tight Lower and Upper Bounds for the Complexity of Canonical Colour Refinement." In: *Theory Comput. Syst.* 60.4 (2017), pp. 581–614. DOI: 10.1007/S00224-016-9686-0. URL: https://doi.org/10.1007/s00224-016-9686-0.

[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. URL: https://doi.org/10.1137/0209047.

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

[CC82] A. Cardon and Maxime Crochemore. "Partitioning a Graph in O(|A| Log2 |V|)." In: *Theor. Comput. Sci.* 19 (1982), pp. 85–98. DOI: 10.1016/0304-3975(82)90016-0. URL: https://doi.org/10.1016/0304-3975(82)90016-0.

[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. URL: https://doi.org/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. URL: https://www.jstor.org/stable/1969671?origin=crossref (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.

[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. URL: https://doi.org/10.1145/116825.116852.

[GN21] Martin Grohe and Daniel Neuen. "Recent Advances on the Graph Isomorphism Problem." In: *Surveys in Combinatorics, 2021: Invited Lectures from the 28th British Combinatorial Conference, Durham, UK, July 5-9, 2021.* 2021, pp. 187–234. DOI: 10.1017/9781009036214.006. URL: https://doi.org/10.1017/9781009036214.006.

[GNW23] Martin Grohe, Daniel Neuen, and Daniel Wiebking. "Isomorphism Testing for Graphs Excluding Small Minors." In: *SIAM J. Comput.* 52.1 (Feb. 2023), pp. 238–272. DOI: 10.1137/21M1401930. URL: https://doi.org/10.1137/21m1401930.

[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. URL: https://doi.org/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. URL: https://doi.org/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. URL: https://doi.org/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. URL: https://doi.org/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. URL: https://doi.org/10.1109/FOCS.2017.49.

[McK81] Brendan D McKay. “Practical Graph Isomorphism”. In: *Congressus Numerantium* 30 (1981), pp. 45–87. URL: https://users.cecs.anu.edu.au/~bdm/nauty/PGI/.

[Mil78] Gary L. Miller. “On the Nlog 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. URL: https://doi.org/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. URL: https://doi.org/10.1016/j.jsc.2013.09.003.

[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. URL: https://epubs.siam.org/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). URL: http://arxiv.org/abs/1304.3935.

[Sch88] Uwe Schöning. “Graph Isomorphism Is in the Low Hierarchy.” In: *J. Comput. Syst. Sci.* 37.3 (1988), pp. 312–323. DOI: 10.1016/0022-0000(88)90010-4. URL: https://doi.org/10.1016/0022-0000(88)90010-4.

[Sip12] Michael Sipser. *Introduction to the Theory of Computation*. Mason, OH, UNITED STATES: Cengage, 2012. ISBN: 978-1-285-40106-5.

[Sun23] Xiaorui Sun. “Faster Isomorphism for p-Groups of Class 2 and Exponent p.” In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing, STOC 2023, Orlando, FL, USA, June 20-23, 2023*. 2023, pp. 433–440. DOI: 10.1145/3564246.3585250. URL: https://doi.org/10.1145/3564246.3585250.

[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. URL: https://doi.org/10.1007/978-3-031-07082-2_21.

[WL68] Boris Weisfeiler and Andrei Leman. “The Reduction of a Graph to Canonical Form and the Algebra Which Appears Therein”. In: *nti, Series* 2.9 (1968), pp. 12–16.

[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. URL: https://openreview.net/forum?id=ryGs6iA5Km.