TECHNISCHE
UNIVERSITÄT
DARMSTADT

Combinatorial approaches to the group isomorphism problem

Vom Fachbereich Mathematik
der Technischen Universität Darmstadt
zur Erlangung des akademischen Grades
Doctor rerum naturalium
(Dr. rer. nat.)
genehmigte

Dissertation

von

Jendrik Brachter
aus Erkelenz

Erstgutachter: Prof. Dr. Pascal Schweitzer
Zweitgutachter: Prof. Dr. Max Horn

Tag der Einreichung: 6. September 2023
Tag der mündlichen Prüfung: 15. November 2023

Darmstadt 2023

Combinatorial approaches to the group isomorphism problem
Doctoral thesis by Jendrik Brachter, M. Sc.
Darmstadt, Technische Universität Darmstadt, 2023, D17

Referee: Prof. Dr. Pascal Schweitzer
1st co-referee: Prof. Dr. Max Horn
Date of hand-in: September 6, 2023
Date of defense: November 15, 2023

Published by TUprints in 2023.
URN: urn:nbn:de:tuda-tuprints-263875

Abstract

The isomorphism problem of finite groups, that is, the task of deciding whether two given finite groups are isomorphic, is one of the most fundamental problems in computational group theory for which we currently do not have efficient algorithmic tools. This is equally true in practical applications, as well as in terms of computational complexity: in the general case, apart from minor improvements, we are essentially stuck with an upper bound of $n^{O(\log n)}$ (obtained from enumerating all $\log n$-sized generating sets), where n is the group order. On the other hand, there are currently no substantial lower bounds.

In this thesis, we develop new algorithmic perspectives on the group isomorphism problem. We define and analyze a series of combinatorial algorithms in the context of finite groups, and in fact arbitrary relational structures. More precisely, we study the *k-dimensional* WL-*algorithm* (k-WL) for natural numbers k, which is an essential tool for the graph isomorphism problem. It is a crucial subroutine in all state-of-the-art graph isomorphism solvers, and it forms an important building block in Babai's break-through quasi-polynomial time ($n^{O((\log n)^c)}$) algorithm for graph isomorphism. It is a combinatorial algorithm with a runtime of $n^{\mathcal{O}(k)}$, that assigns canonical colorings to graphs. It thereby serves as a non-isomorphism test, with important connections to logic, games, and graph structure theory.

Our first contribution is the generalization of the WL-algorithm from graphs to relational structures, in terms of three potentially different versions of the WL. We compare these versions, showing that they can be placed in a hierarchy of distinguishing powers. The general result that we prove is that each version is natural under a certain point of view (and can be characterized by a corresponding logic), but asymptotically, it does not matter which version of WL we work with.

In particular, we obtain an asymptotically robust notion of the *Weisfeiler-Leman dimension for relational structures*, which denotes the smallest natural number k, such that the k-dimensional WL-algorithm identifies a given structure up to isomorphism. This allows us to subsequently initiate a descriptive complexity theory of finite groups, where we propose the Weisfeiler-Leman dimension as a natural measure of complexity.

We construct a compendium of structural properties and group theoretic constructions that are detectable via a low-dimensional Weisfeiler-Leman algorithm. This includes various major building blocks of group theory, for example, we show that groups share the same multiset of composition factors if they are indistinguishable via 5-WL. We also provide a framework that allows one to easily extend and adapt our results to other group theoretic properties. We thereby uncover far-reaching connections between the WL-dimension and the structure of a finite group, and we provide an effective tool-kit to analyze the WL-algorithm on groups and related algebraic structures.

We then employ these tools to derive upper bounds on the WL-dimension of several important group classes. For instance, we show that the WL-dimension of coprime extensions of abelian groups and the WL-dimension of semisimple groups are both bounded by $\mathcal{O}(\log \log n)$. We also identify several natural group classes of bounded WL-dimension.

Finally, we discuss lower bounds in two ways: first, we provide explicit examples that certify Weisfeiler-Leman indistinguishability for small dimensions, and second, we devise combinatorial reductions that asymptotically preserve the WL-dimension. The latter provides potential sources for groups of unbounded Weisfeiler-Leman dimension.

Zusammenfassung

Das Gruppenisomorpieproblem, also die Aufgabe, zu entscheiden, ob zwei gegebene endliche Gruppen isomorph sind, ist eines der fundamentalsten Probleme in der algorithmischen Gruppentheorie, für welches uns zurzeit keine effizienten algorithmischen Methoden zur Verfügung stehen. Dies gilt sowohl für praktische Anwendungen, als auch im Sinne der Komplexitätstheorie: Abgesehen von geringfügigen Verbesserungen, bleibt die beste obere Schranke von der Form $n^{O(\log n)}$ (resultierend aus der Auflistung von Erzeugendensystemen der Mächtigkeit $\log n$), wobei n die Gruppenordnung bezeichnet.

In der vorliegenden Arbeit entwickeln wir neue algorithmische Ansätze für das Gruppenisomorphieproblem. Wir definieren und analysieren eine Reihe von kombinatorischen Algorithmen im Kontext von endlichen Gruppen, beziehungsweise allgemeiner beliebigen relationalen Strukturen. Genauer studieren wir den *k-dimensionalen Weisfeiler-Leman-Algorithmus* (k-WL) für natürliche Zahlen k, welcher ein essenzielles Werkzeug für das Graphenisomorphieproblem darstellt. Er ist eine wichtige Subroutine in allen kompetitiven Graphenisomorphie-Solvern und er formt einen wichtigen Baustein in Babais Quasipolynomialzeit-Algorithmus ($n^{O((\log n)^c)}$) für das Graphenisomorphieproblem. Es handelt sich dabei um einen kombinatorischen Algorithmus der Laufzeit $n^{\mathcal{O}(k)}$, welcher Graphen kanonische Färbungen zuweist. Dadurch fungiert der Algorithmus als Nicht-Isomorphie-Test, mit wichtigen Verbindungen zur Logik, Spieltheorie und Graphenstrukturtheorie.

Unser erster Beitrag besteht in der Verallgemeinerung des WL-Algorithmus auf relationale Strukturen in der Form von drei möglicherweise verschiedenen Versionen. Wir vergleichen diese Versionen und zeigen, dass sie bezüglich ihrer Fähigkeit relationale Strukturen zu unterscheiden in einer Hierarchie angeordnet werden können. Das Hauptresultat ist hier, dass jede Version unter einem bestimmten Gesichtspunkt natürlich ist (und durch eine entsprechende Logik charakterisiert werden kann), aber asymptotisch alle Versionen eine vergleichbare Aussagekraft besitzen.

Insbesondere erhalten wir so eine asymptotisch robuste Definition der *Weisfeiler-Leman-Dimension für relationale Strukturen*, welche die kleinste natürliche Zahl k bezeichnet, sodass der k-dimensionale WL-Algorithmus eine gegebene Struktur bis auf Isomorphie identifiziert. Dies ermöglicht es uns, im Folgenden eine deskriptive Komplexitätstheorie für endliche Gruppen zu initiieren, wobei die Weisfeiler-Leman-Dimension als natürliches Komplexitätsmaß fungiert.

Wir erstellen im Laufe dieser Arbeit ein Kompendium an gruppentheoretischen Struktureigenschaften, welche von einem niedrigdimensionalen WL-Algorithmus identifiziert werden. Dies beinhaltet verschiedene wichtige Bausteine der Gruppentheorie, zum Beispiel zeigen wir, dass Gruppen, welche nicht von 5-WL unterschieden werden, stets dieselbe Multimenge an Kompositionsfaktoren besitzen. Außerdem stellen wir ein Framework bereit, welches es leicht ermöglicht, unsere Resultate zu erweitern oder an spezielle gruppentheoretische Kontexte anzupassen. Wir etablieren so weitreichende Verbindungen zwischen der WL-Dimension und der Struktur einer endlichen Gruppe und wir liefern effektive Werkzeuge für die Analyse des WL-Algorithmus auf Gruppen und verwandten algebraischen Strukturen.

Wir verwenden diese Werkzeuge dann, um obere Schranken an die WL-Dimension verschiedener wichtiger Klassen von Gruppen herzuleiten. Unter anderem zeigen wir, dass die WL-Dimension von teilerfremden Erweiterungen abelscher Gruppen oder von halbeinfachen Gruppen durch $\mathcal{O}(\log\log n)$ beschränkt ist. Des Weiteren identifizieren wir einige natürliche Klassen von Gruppen mit beschränkter WL-Dimension.

Schließlich diskutieren wir untere Schranken auf zwei Arten: Erstens geben wir explizit Gruppen an, welche für niedrigdimensionale Versionen von WL nicht unterscheidbar sind und zweitens entwerfen wir kombinatorische Reduktionen, welche die WL-Dimension asymptotisch erhalten. Letzteres liefert potenzielle Quellen für Gruppen von unbeschränkter WL-dimension.

Acknowledgements

I am grateful to Sofia Brenner and Markus Anders for proofreading early versions of this thesis and for many interesting and motivating discussions, and to Moritz Lichter for his helpful thoughts, throughout the years and in the preparation of the thesis. Furthermore, I want to thank Irene Heinrich, Eda Kaja and Thomas Schneider for their companionship during the past years. Special thanks to Irene for always being there to listen and for always being able to provide uplifting perspectives. I thank Jan Herzog for making me feel a little bit more at home in Darmstadt.

I am grateful to Professor Schweitzer for his mentorship throughout my Ph.D. years. Lastly, I am grateful for receiving funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (EngageS: grant agreement No. 820148) and from the German Research Foundation DFG (SFB-TRR 195 "Symbolic Tools in Mathematics and their Application") in preparing this thesis.

Contents

Chapter 1

Introduction

Symmetry is central to almost all areas of the mathematical sciences, crucial to our understanding of both mathematical objects and the real world. We encounter symmetry in mathematical equations, chemical molecules, and economic systems, to name just a few examples.

On the one hand, from an algebraic point of view, symmetry can be formalized and universally modeled through the concept of a group. Groups admit an incredibly rich theory, connecting numerous branches of classical and modern day algebra, culminating in one of the biggest mathematical achievements of the 20th century: the classification of finite simple groups. A big driving force behind recent advances in group theory are computational methods, more specifically the ability to construct, analyze, and utilize groups in computer algebra systems such as GAP [43] or Magma [16]. As an example, we recall recent efforts of enumerating various classes of groups up to certain orders: the enumeration of p-groups up to order p^7 [93], the enumeration of finite solvable groups (now complete up until order 2304, see [34]), or the enumeration of perfect groups up to order $2 \cdot 10^6$ [64]. In all cases, the results are heavily backed by computational experiments and algorithmic enumeration of groups with prescribed properties. Moreover, for many orders, the groups are explicitly listed and available in GAP libraries [43].

On the other hand, from a real-world perspective, detecting and exploiting symmetries in large and complex data systems is becoming more and more important. This calls for the development of efficient computational tools for symmetry detection. This is formalized in the graph isomorphism problem, one of the biggest open problems in theoretical computer science. It is a major candidate for an NP-intermediate problem, the existence of which is guaranteed by Ladner's Theorem [77], assuming that P is not equal to NP. Here, graphs are another universal tool to model and visualize symmetries, in the sense that a graph represents the symmetries it admits via its automorphism group. This establishes a direct connection between graphs, as objects on which groups act in a natural way, and groups, modeling symmetries of graphs. Consequently, advances on the graph isomorphism problem often build on heavy group theoretic machinery, combined with complex algorithmic paradigms and a powerful combinatorial coloring procedure, known as the Weisfeiler-Leman algorithm. As graphs universally capture symmetries of combinatorial objects, the graph isomorphism problem can be understood as the prototype of isomorphism problems and symmetry computation.

Despite our deep understanding of groups and how they can be used to model symmetry, the symmetries that can be found in groups themselves remain a more mysterious topic. For instance, it is currently not known which groups are realized as automorphism groups of finite groups (it is known however, that not all groups are, see for example [84]). In the present thesis, we investigate the symmetries of finite groups, with a primary focus on the group isomorphism problem. The group isomorphism problem is one of the central unresolved problems in computational group theory. It formalizes the task of deciding, with an algorithm, if two given (finite) groups are isomorphic. The problem's research history goes back at least 70 years (see [89]), yet progress is still limited.

Taking an algorithmic point of view, the present thesis is first and foremost concerned with the *computation* of symmetries, that is automorphisms, of a given finite group. The thesis advances our understanding of the group isomorphism problem by developing new combinatorial approaches and it initiates the study of the descriptive complexity theory of finite groups. We transfer the Weisfeiler-Leman algorithm, a crucial tool in the context of graph isomorphism, to relational structures, and analyze its distinguishing power in this general setting. The main focus lies on finite groups, and we uncover far reaching connections between the structure of finite groups and the canonical colorings computed by the Weisfeiler-Leman algorithm. We leverage these connections to derive bounds on the Weisfeiler-Leman dimension of numerous important classes of groups.

The group isomorphism problem The group isomorphism problem formalizes the task of deciding, with an algorithm, if two given (finite) groups are isomorphic. Of course the isomorphism problem is also defined for infinite groups, however the questions are very different in the finite and infinite case. In the infinite case, the focus usually lies on computability as opposed to efficiency, and the isomorphism problem for arbitrary finite presentations is famously undecidable as a consequence of the Novikov-Boone theorem (see [20]). In the present thesis, we focus on finite groups and complexity theoretic aspects of their isomorphism problem. In the case of finite groups, the isomorphism problem is among the most fundamental problems in group theory for which we currently do not have efficient algorithmic tools. This statement is true, independent of whether we are interested in practical algorithms, more theoretical aspects of computational complexity, or structural group theory. If we measure complexity relative to the group order, the group isomorphism problem is not known to be polynomial-time solvable (even with respect to the group order), but it is polynomial-time reducible to graph isomorphism. In particular, it is not known to be NP-complete. As such, group isomorphism, next to graph isomorphism, is another natural candidate for an NP-intermediate problem.

Considering groups of order n, a simple approach to group isomorphism, attributed to Tarjan in [89], is based on enumerating generating sets up to a certain cardinality in a brute-force manner. For each fixed pair of (ordered) generating sets we can test in polynomial time if there is an isomorphism mapping the i-th element of one to the i-th element of the other. If d is the rank of a given group G, that is, the minimal cardinality of a generating set for G, then testing isomorphism with G can be done in time of $n^{\log d+\mathcal{O}(1)}$ through Tarjan's generator enumeration algorithm. Since every group of order n has a generating set of size at most $\log n$, this provides a general $n^{\mathcal{O}(\log n)}$-bound for group isomorphism.

Despite the considerable body of research that was dedicated towards group isomorphism since the 1950s, the bound for general groups has only seen minor improvements.

Rosenbaum and Wagner gave a bound of $n^{1/2 \log_p n + \mathcal{O}(p)}$ for p-group isomorphism [98], later slightly improving these results further. Inspired by their techniques, Luks gave a polynomial-time algorithm to solve the group isomorphism problem relative to a fixed composition series [83]. This does not asymptotically improve on the generator enumeration bound, since there exist groups with $n^{\Omega(\log n)}$ distinct but indistinguishable composition series (consider for instance elementary abelian groups). LeGall and Rosenbaum observed in [42], that combining the algorithm for composition series isomorphism with a bidirectional collision technique gives the currently best upper bound of $n^{1/4 \log n + \mathcal{O}(1)}$ for general groups.

Apart from that, progress on group isomorphism is almost exclusively limited to special classes of groups, and the bounds usually rely heavily on an in-depth analysis of the groups' structural properties. For instance, isomorphism with an abelian group can be tested in linear time [72]. Babai, Codenotti and Qiao [9] gave a polynomial-time algorithm for group isomorphism of semisimple groups, that is groups without non-trivial abelian normal subgroups, and Babai and Qiao gave a polynomial-time algorithm for groups with abelian Sylow-towers [11]. More generally, the latter reduces the computation of $\mathrm{Aut}(N \rtimes H)$ to the computation of $\mathrm{Aut}(H)$, given that the orders of N and H are coprime and that N is abelian. In this case, the techniques are largely representation theoretic, analyzing the induced action of H on elementary abelian subgroups of N. We discuss these *coprime extensions* in the context of the Weisfeiler-Leman algorithm in more detail below.

On the other hand, even very limited classes of groups seem to provide hard cases for isomorphism testing. Particularly curious is the prominent example of p-groups, or the even more restricted groups of odd, prime exponent p (respectively exponent 4) and nilpotency class 2 (i.e., groups in which all commutators are central). These groups possess a lot of extra structure, but they are difficult to distinguish in terms of their group theoretic properties, as non-isomorphic p-groups can appear very similar from an algebraic point of view. Despite a considerable body of research dedicated towards this class of groups, our understanding of the isomorphism problem, even for p-groups, is still very limited. However, during the preparation of this thesis, a new break-through result for the class of groups of exponent p and class 2 was featured at STOC 2023 [102]. In [102], Sun derives an $n^{\mathcal{O}((\log n)^{5/6})}$ bound for testing isomorphism of such groups, for the first time asymptotically beating the $n^{\mathcal{O}(\log n)}$-bound for a considerably generic class of groups. The result is based on a recent reduction from group isomorphism (for groups of exponent p and class 2) to an isometry problem for tuples of skew-symmetric matrices (see [69]), where Sun manages to effectively restrict the resulting search space through combinatorial gadget constructions.

Yet, formal reductions from the isomorphism problem of any larger group class to the case of exponent p and nilpotency class 2 (or to any similar class of groups) are currently limited to a single result by Grochow and Qiao [51], who provided a polynomial-time reduction from nilpotency class less than p to nilpotency class 2. More generally, despite the lack of efficient methods for the group isomorphism problem, effective lower-bounds of any kind are currently not known.

Another algorithmic perspective was proposed in [42], where the authors give a reduction from group isomorphism to a particular case of the string isomorphism problem in time $n^{\mathcal{O}(\log \log n)}$. The string isomorphism problem asks to decide if two strings over a fixed alphabet $\mathcal{A}$ can be mapped to each other by permuting the characters, where the permutations are be taken from a given subgroup of $\mathrm{Sym}(\mathcal{A})$. In the general case, without restrictions on the permutation group, the string isomorphism problem generalizes graph isomorphism and it admits a quasi-polynomial solution through Babai's algorithm [6]. The reduction from group isomorphism to string isomorphism given in [42] restricts the possible non-abelian composition factors of the permutation group to be projective special linear.

Lastly considering the state of practical group isomorphism solvers, many issues from the theoretical side carry over to the practical side. The current state of the art general purpose methods, for example those implemented in GAP [43], are based on Leon's backtracking search [78, 79]. Due to the quasi-polynomial worst-case scaling of these methods, they cannot really be considered practical, even for groups of relatively small orders. As before, the situation for specific group classes is better in some cases. For instance, there are specialized algorithms for solvable groups [101], or p-groups [35, 92]. Yet again, the precise methods are highly specialized in each case, sometimes depending on representations specific to group classes, such as power commutator presentations. Dietrich and Wilson report that current isomorphism tests are already infeasible in practice on some groups with orders in the thousands [30]. The overall situation is somewhat chaotic in the sense that there is no one place to look for an efficient all-purpose solver. In contrast to this, practical graph isomorphism solvers are highly optimized and typically provide solutions in almost-linear time (i.e., $n(\log n)^c$), as we discuss in more detail below.

In conclusion, while there exists a vast collection of algebraic tools and heuristics for tackling the group isomorphism problem, complexity theoretic and algorithmic aspects are less developed. This observation was the initial spark of the present thesis, and it is arguably surprising: for the related graph isomorphism problem, historically, it has been the other way around. Indeed, for graph isomorphism testing, combinatorial approaches are well-developed and often successful, yet their limits have been firmly established.

The Weisfeiler-Leman algorithm One of the most important tools in the scope of the graph isomorphism problem is the *Weisfeiler-Leman (WL) algorithm*. It is a crucial subroutine in all practical state-of-the-art graph isomorphism solvers. It also plays a key role in the currently fastest theoretical algorithm, which is due to Babai's famous breakthrough result from 2016 [6], placing graph isomorphism in quasi-polynomial time, that is $n^{(\log n)^{\mathcal{O}(1)}}$, where n is the number of vertices.

The WL-algorithm has a *dimension* parameter, given by a natural number k. The k-dimensional Weisfeiler-Leman algorithm (k-WL) iteratively classifies k-tuples of vertices of a graph in terms of how they are related to other vertices in the graph. More concretely, the algorithm operates through initially assigning isomorphism invariant colors to each k-tuple of vertices, and then iteratively refining the coloring until it stabilizes. The output of k-WL is the *stable coloring* and, being canonical, that is, automorphism invariant, it gives rise to an incomplete, but largely effective non-isomorphism test (see e.g. [108, 24]). Fixing the dimension parameter k, the stable color classes of k-WL can be computed in time $\mathcal{O}(n^{k+1}\log n)$, where n is the number of vertices (see [66, 67]). In particular, with increasing k, the running time and distinguishing power of k-WL increase, while the running time is polynomial for fixed k.

Already the 1-dimensional version of the Weisfeiler-Leman algorithm, sometimes also called *color refinement*, is surprisingly effective: it distinguishes asymptotically almost all graphs up to isomorphism [10]. Furthermore, it is very effective on graphs one typically encounters in practice, which is one of the reasons behind the large success of state of the art graph isomorphism solvers, like nauty [87, 86], traces [87, 86] or dejavu [3, 2].

Beyond distinguishing non-isomorphic graphs, the WL-algorithm more generally serves as a measure of similarity and complexity, which we can express in terms of the smallest integer k such that k-WL distinguishes two graphs. We say that the *Weisfeiler-Leman dimension* of a graph Γ is the smallest k, such that k-WL distinguishes Γ from all other non-isomorphic graphs. The WL-dimension can also be understood from the perspective of descriptive complexity, establishing deep connections between WL and the expressiveness in the first order logic with counting (i.e., the ordinary first order logic on graphs, extended by counting quantifiers). By [24], k-WL is provably universal, in the sense that it precisely captures those combinatorial properties of an input graph that can be expressed in the $(k+1)$-variable fragment of first-order logic with counting quantifiers.

Numerous classes of graphs have constant WL-dimension, and consequently, isomorphism with graphs from one such class can be decided in polynomial time, purely through the Weisfeiler-Leman algorithm. Examples include planar graphs [75], the WL-dimension of which is at most 3, or graphs of bounded tree-width, where the WL-dimension is linearly bounded in the tree-width [55]. The most general result in this vein is due to Grohe, who showed that each graph class that can be defined by excluded minors has constant WL-dimension (the constant does depend on the specific set of excluded minors), see [54].

Beyond bounding the WL-dimension, one can also investigate the structural properties that k-WL identifies in (a class of) graphs. For example, the 2-dimensional WL-algorithm implicitly decomposes a graph into its 3-connected components [74], and it recognizes vertex- and arc-transitivity for graphs of prime order [38].

Generally speaking, the WL-algorithm provides a combinatorial analysis of a graph's structure, expressed through the stable colorings it computes. Given a graph Γ, the stable coloring computed by k-WL induces a vertex coloring on Γ, that either separates vertices by assigning distinct colors to them, or certifies a certain level of regularity, by assigning the same color to vertices. In the latter case, the vertices share many combinatorial properties, a simple example being the degree. With increasing k, the degree of separation increases as well, and this can be interpreted as k-WL expressing more structural properties of the input graphs in terms of the stable colors. While small vertex color classes severely restrict possible automorphisms of the input graph, the presence of large color classes hints at a possibly high level of symmetry, ensuring that many vertices admit similar combinatorial properties.

Despite the large success of the WL-algorithm, its theoretical limits have been firmly established. Cai, Fürer and Immerman prove that the WL-dimension of graphs is unbounded, by explicitly constructing an infinite family of graphs for which the WL-dimension is linear in the number of vertices [24]. These graphs are nowadays referred to as the *CFI-graphs*.

When two worlds collide In the remainder of the introduction, we discuss the structure of the thesis and its results in greater detail. The first aim of this thesis is to transfer the Weisfeiler-Leman algorithm to the setting of groups, thus initiating a descriptive complexity theory of finite groups. Ultimately this advances our understanding of group isomorphism by providing a new algorithmic perspective that is currently not well explored. In doing so, we build a new bridge between the combinatorial algorithms that are essential for our understanding of graph isomorphism and computational group theory. In the context of group isomorphism, communication between these areas has been limited, but interconnecting them seems more than natural.

Historically, the interplay of group and graph theory sparked significant progress in the case of the graph isomorphism problem. In [82], Luks observes that for automorphism groups of graphs of bounded degree there is essentially a constant bound on the order of possible non-abelian composition factors (formally one needs to consider connected graphs with an individualized vertex). Luks goes on to devise a polynomial-time algorithm for isomorphism of bounded degree graphs based on this insight. In Babai's work the presence of large alternating composition factors in the automorphism group of a graph is identified as the only obstruction to efficient isomorphism testing via Luks' methods. This is precisely the problem that Babai's graph isomorphism algorithm solves, and Babai's results are partially based on heavy permutation group machinery, such as combinatorial recognition methods for certain O'Nan-Scott classes (see [6]).

In conclusion, the case of graphs suggests that isomorphism testing for combinatorial structures can generally be tackled through an analysis of the possible automorphism groups, a firm understanding of the structure of the input objects and a canonical coloring procedure given by a Weisfeiler-Leman-type algorithm. In the context of group isomorphism, not all of these principles have been explored in greater detail. While the former two aspects are arguably well-developed for finite groups, what is missing from the picture are effective combinatorial and algorithmic methods.

Our study of the Weisfeiler-Leman algorithm in the context of group isomorphism is roughly split into three parts. In the first part (Chapter 3), we discuss suitable definitions of the WL-algorithm in a context more general than graphs. A priori, it is not clear how to generalize the WL-algorithm beyond graphs. For instance, if we consider a tuple of elements in a group, we may or may not want to use properties of the subgroup it generates in order to distinguish it from other tuples and it is not clear how such decisions influence the distinguishing power of the resulting version of the WL-algorithm. Consequently, we investigate several generalizations of WL which fall together in the case of graphs, but not necessarily for groups and related structures.

More concretely, for each natural number k, we devise three distinct versions of the k-dimensional Weisfeiler-Leman algorithm (k-WL). We do not limit them to groups, but rather we allow arbitrary relational structures as inputs. The first version, the *explicit WL-algorithm*, formalizes the standard Weisfeiler-Leman algorithm on graphs, generalized to relational structures. The second version, the *implicit WL-algorithm* is geared towards algebraic structures, and it generalizes the Weisfeiler-Leman algorithm on groups introduced in [17]. It allows for the consideration of compressed representations, by which we mean the representation through a *generating set*, which naturally arises in the context of algebraic structures, such as groups, linear codes, or bilinear spaces. The third version, the *graph-encoded WL-algorithm*, is just the standard WL-algorithm for graphs, applied to a natural graph encoding of a relational structure. It ties our results back to the Weisfeiler-Leman algorithm on graphs. Working with general relational structures and multiple versions of the WL-algorithm enables us to formulate results and reason about various classes of combinatorial structures in a unified fashion. For instance, many aspects of our analysis of WL on groups, through our general set-up, have automatic implications for permutation groups or linear codes.

The second part (Chapter 4), is intended as a collection of standard tools and techniques we developed to analyze the WL-algorithm on groups (and other algebraic structures). We provide a compendium of structural properties and group theoretic constructions that are detectable via the Weisfeiler-Leman algorithm. This includes various major building blocks of group theory (for example, we show that groups share the same multiset of composition factors if they are indistinguishable via 5-WL), and we provide a comprehensive framework that allows to extend and adapt this catalog.

In the third part (Chapters 5 and 6), we employ this framework to derive bounds on the Weisfeiler-Leman dimension of various natural and important group classes. In the case of upper bounds, we investigate specific classes of groups (e.g. certain p-groups, abelian groups, and coprime group extensions), analyze their structure and show how the Weisfeiler-Leman algorithm can exploit these structural aspects to identify the groups in question up to isomorphism. In the case of lower bounds, either we give explicit examples that certify Weisfeiler-Leman indistinguishability for small dimensions, or we provide algorithmic reductions that preserve the Weisfeiler-Leman dimension to obtain conditional lower bounds. For example, we show that the WL-dimension of semisimple groups, that is, groups without abelian normal subgroups, is closely related to the Weisfeiler-Leman dimension of arbitrary permutation groups.

Finally, we point out that a part of the results presented in this thesis is covered in two publications by the author together with Pascal Schweitzer [17, 18]. The publications contain versions of many results presented in Chapter 3 and Chapter 4, but only for groups instead of arbitrary relational structures. Lemma 3.4.5, Section 3.4.1, and Section 3.5 have not been published before, allowing us to derive new upper and lower bounds on the WL-dimension of certain group classes in later Chapters of the thesis. Moreover, in Chapter 4, we cover many additional group theoretc properties that are not covered in [18]. The results of Chapters 5 and 6 have mostly not been published before, with the exception of the construction of groups from CFI-graphs, which is identical to [17, Sections 4–6]. We discuss the relationship of the thesis with [17] and [18] in more detail in the next Section of the introduction, and again at the beginning of each Chapter.

1.1 Detailed overview of the results

In the first part of the thesis, we begin by characterizing each version of k-WL in terms of a version of first order counting logic, thus arguing that each version is again universal in a formal sense, and natural under a certain point of view. While different versions of k-WL may define inherently different colorings, our first main result is that, at least asymptotically, their distinguishing powers are comparable. More precisely, each version subsumes the others after multiplying the dimension parameter by a constant that depends on the concrete class of input structures. In the case of finite groups, we show the following (see Theorem 3.2.25):

- $k\text{-WL}_{\text{explicit}} \preceq k\text{-WL}_{\text{implicit}} \preceq (k/2+2)\text{-WL}_{\text{graph}-\text{encoded}} \preceq (k+5)\text{-WL}_{\text{explicit}}$,
- $k\text{-WL}_{\text{implicit}} \preceq (k+1)\text{-WL}_{\text{explicit}}$,

where for two algorithms $\mathcal{A}$ and $\mathcal{B}$, the notation $\mathcal{A} \preceq \mathcal{B}$ denotes the fact that the distinguishing power of $\mathcal{B}$ is at least as high as the distinguishing power of $\mathcal{A}$. In this sense, our generalizations of the WL-algorithm are robust, and we obtain an asymptotically well-defined notion of the Weisfeiler-Leman dimension. This version of the Theorem is essentially the one that was published in [17]. Here, we derive a more general version for WL on relational structures, and apart from groups we explicitly consider graphs, permutation groups, monoids, linear codes, and bilinear spaces. The details are left to Chapter 3.

The crucial observation in the context of group isomorphism is the following: if the WL-dimension of groups turns out to be globally bounded, then we obtain a polynomial-time solution to the group isomorphism problem. Otherwise, the WL-dimension divides the class of finite groups in infinitely many similarity classes and we obtain interesting instances of non-isomorphic groups of 'arbitrary high similarity'. As for graphs, it makes sense to study group theoretic isomorphism invariants and aspects of structural group theory in terms of the Weisfeiler-Leman dimension. From this perspective, the thesis is also intended as a compendium of well-known group theoretic isomorphism invariants, parameterized by the WL-dimension.

In the second part, we focus mostly on finite groups. Additionally, we always consider the possibility of assigning a coloring to the input structure and running the WL-algorithm on the colored structure. For instance, we consider colored groups (G, γ), where $\gamma\colon G \to \mathcal{C}$ is a function that specifies a color in some color domain $\mathcal{C}$ for every groups element in G. Intuitively, these colorings can be thought of as restricting symmetries, and the automorphism group of the colored group is just the (possibly trivial) subgroup of color preserving automorphisms.

One of the key principles of our analysis of WL on groups is a compatibility of stable colorings with basic group structure. Let us say that a subset of a group is k-WL-detectable (for one of the three versions of k-WL as introduced above), if it is a union of stable color classes (the actual definition of detectability is slightly more general, see Section 3.3). We show that subgroups generated by color classes of k-WL are also k-WL-detectable, and so are centralizers, normalizers, or commutators of k-WL-detectable subsets. Crucially, stable colorings turn out to be compatible with quotient groups as well. Given a coloring $\gamma : G \to \mathcal{C}$ and a normal subgroup $N \trianglelefteq G$, we define the induced *quotient coloring* $\overline{\gamma}$ on G/N via $\overline{\gamma}(gN) := \{\{\gamma(gn) \mid n \in N\}\}$. Then, for k at least 4, we obtain the following correspondence (see Theorem 4.1.10, the result was published in [18, Theorem 4.8]).

- Consider a colored group (G, γ) with k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable subgroups U and N, where N is normal in G. Then U/N is k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable in $(G/N, \overline{\gamma})$.

- Consider colored groups (G, γ_G) and (H, γ_H) which are indistinguishable via k-$\mathrm{WL}_{\mathrm{explicit}}$. Let $\Psi : G \to H$ be a bijection that respects the stable colors. Then $M \subseteq G$ is k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable if and only if $\Psi(M) \subseteq H$ is k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable. In this case it holds $\Psi(\langle M \rangle) = \langle \Psi(M) \rangle$. In particular, if M is a subgroup then so is $\Psi(M)$ and then $(M, \gamma_G|_M)$ is indistinguishable from $(\Psi(M), \gamma_H|_{\Psi(M)})$ via k-$\mathrm{WL}_{\mathrm{explicit}}$. Additionally, M is normal if and only if $\Psi(M)$ is and if so, then it also holds that $(G/M, \overline{\gamma_G})$ is indistinguishable from $(H/\Psi(M), \overline{\gamma_H})$.

These principles allow us to build up more complicated and expressive detectable subsets in an iterative fashion: starting from the subset of group elements that share a certain property, like being a commutator, the WL-algorithm iteratively detects the subsets that can be inductively defined as the generalized commutators with an unbounded number of entries. It turns out that a large number of group theoretic properties can be re-interpreted in this fashion, and hence can be exploited by the WL-algorithm in distinguishing groups. The list of properties that can be detected/identified by a constant dimensional WL-algorithm includes the following and many more are discussed in detail in the third Chapter.

- the terms of the derived series, upper and lower central series, omega and agemo series together with the isomorphism types of the respective quotients,
- solvability & nilpotency class,
- maximal normal nilpotent/solvable/π-subgroups,
- the socle & the isomorphism types of minimal normal subgroups,
- the multiset of composition factors,
- the isomorphism type of iterated direct products of simple and abelian groups,
- the cycle type of group elements induced by conjugation on detectable subgroups.

Many of the results in Chapter 4 are contained in [18]. In comparison to [18], the present thesis additionally provides a complete discussion of the stable 2-$\mathrm{WL}_{\mathrm{explicit}}$-color classes, as well as a discussion of p-groups, verbal subgroups and group actions. Some bounds on the WL-dimension in Chapter 3 have been improved compared to [18].

Building on these results, we investigate the ability of the Weisfeiler-Leman algorithm to decompose groups. We show that for k sufficiently large, the k-dimensional WL-algorithm implicitly computes the decomposition of a group into indecomposable direct factors in the following precise sense (see Theorem 4.3.27, the result was published in [18, Theorem 6.18]).

- Let $G = G_1 \times \cdots \times G_d$ be a decomposition into indecomposable direct factors and let $k \geq 5$. If H is another group that is indistinguishable from G via k-$\mathrm{WL}_{\mathrm{implicit}}$, then there are indecomposable direct factors $H_i \leq H$ such that $H = H_1 \times \cdots \times H_d$ and G_i is indistinguishable from H_i via $(k-1)$-$\mathrm{WL}_{\mathrm{implicit}}$ for all $i \in [d]$. Moreover G and H have isomorphic maximal abelian direct factors.

As a corollary, the Weisfeiler-Leman dimension of any class of groups can be bounded by bounding the Weisfeiler-Leman dimension of the directly indecomposable groups that arise from the group class. In proving this result, we also introduce a new, canonical central decomposition for finite groups, that is detectable by the implicit 5-dimensional WL-algorithm.

The analysis of direct decompositions finishes the second part of the thesis, where we explored the expressiveness of WL on groups, and we go on to derive bounds on the WL-dimension of various important group classes.

We conduct experiments on groups of relatively small order in GAP [43], finding further support for the effectiveness of the WL-algorithm. In fact, all groups of order at most 243 are identified up to isomorphism by 3-$\mathrm{WL}_{\mathrm{implicit}}$ (we note that 2-$\mathrm{WL}_{\mathrm{implicit}}$ is somewhat special, in that this version is not able to access the full 3-ary multiplication relation, which we discuss in more detail below). Via the enumeration of p-groups (see for example [36]), we can further show that all groups of order p^5 are identified up to isomorphism by the same algorithm.

Next, we devise a construction of infinitely many pairs of groups that are highly similar (in a formally precise sense) but can be easily distinguished by 3-WL. These groups have prime exponent p, for an arbitrary odd prime p, and nilpotency class 2, and by construction, their commuting graphs (where two group elements are joined by an edge if and only if they commute) are versions of CFI-graphs. The high similarity found in pairs of CFI-graphs transfers to high similarity of the groups we construct. In particular, our construction provides new infinite families of groups with highly similar subgroup-profiles. The *k-profile* of a group is defined as the multiset of isomorphism types of its k-generated subgroups. The discussion of this isomorphism invariant was initiated by Gowers, who asked on Lipton's blog [47] whether there is an integer c such that the isomorphism class of each finite group is determined by their c-profile. Glauberman and Grabowski gave a negative answer by constructing pairs of non-isomorphic groups with the same $\Theta(\sqrt{\log n})$-profiles [44]. Subsequently, Wilson constructed many examples of exponent p and nilpotency class 2 groups which agree in various invariants, including having the same $\Theta(\log n)$-profiles [110], which is best possible. Despite the fact that the groups we construct here are highly similar from a group theoretic perspective, the WL-dimension of these groups is bounded by 3, and in this sense, the Weisfeiler-Leman algorithm provides an explanation for the non-isomorphism of groups beyond what we can currently explain with group theoretic properties. The following is a summary of the results in Section 5.3.2. The section was published in [17, Sections 4–6].

- For infinitely many n there exist pairs of groups of order n which have
  - equal $\Theta(\sqrt{\log n})$-profiles,
  - exponent p and nilpotency class 2, with isomorphic derived subgroups (which are furthermore equal to their centers),
  - the same sizes of conjugacy classes,
  - commuting graphs indistinguishable by $\Theta(\sqrt{\log n})$-$\mathrm{WL}_{\mathrm{graphs}}$.

  Yet, they have $\mathrm{WL}_{\mathrm{implicit}}$-dimension ≤ 3.

Moving on to abelian groups, we take a more detailed look at colored abelian groups, where the coloring carries specific information about the group's structure. While the isomorphism problem of colored graphs is reducible to isomorphism of uncolored graphs via standard gadget constructions, this is unclear for groups. In particular, it is not clear how to encode a colored group as an uncolored one in a way that preserves isomorphism and non-isomorphism. Nevertheless, we can use colorings on groups to restrict possible automorphisms. For example, given an abelian group A, we can encode a fixed isomorphism defined on a sub- or quotient group of A via assigning suitable colors to the elements of A. We show that the WL-dimension of such colored abelian groups is bounded in important cases (see Lemmas 5.6.19, 5.6.9).

- Let A and B be groups and let $\varphi\colon A \to B$ be a homomorphism. We say that a coloring γ of the elements of A *encodes the homomorphism* φ, if the color classes of γ are exactly the fibers of φ. We say that γ *encodes a partial isomorphism*, if there is a subgroup $A_0 \leq A$, such that $A \setminus A_0$ forms one single color class of γ and each element of A_0 is in a singleton color class.

  Then, the $\mathrm{WL}_{\mathrm{implicit}}$-dimension of any colored abelian group (A, γ), where γ encodes a homomorphism or a partial isomorphism, is bounded by 4.

In other words, the Weisfeiler-Leman algorithm efficiently decides if isomorphisms defined on sub- or quotient groups of abelian groups can be extended to global isomorphisms.

We use these results to investigate more complex group classes, by analyzing the induced actions on normal abelian subgroups. Concretely, we apply this principle to derive bounds on the WL-dimension of certain coprime extensions and certain central extensions. A group G is an *extension* of N by Q, if N is (isomorphic to) a normal subgroup of G with quotient $G/N \cong Q$. The extension is called *coprime*, if $|N|$ and $|Q|$ are coprime, and then G is a semi-direct product $N \rtimes Q$ by the Schur-Zassenhaus Theorem. In the case of an elementary abelian normal subgroup N, the isomorphism type of G is entirely encoded by representation theoretic properties of the induced action of Q on N, regarded as a linear representation in positive (coprime) characteristic. We devise combinatorial analogues of fundamental representation theoretic principles to parameterize the WL-dimension of such extensions in terms of their representation theory. Among other results, we prove the following (Corollary 5.7.22 and Corollary 5.7.24):

- Let G be an extension of an abelian group H by an abelian p-group A, where p does not divide $|H|$. If $\Omega_1(A)$ is a minimal normal subgroup of G (i.e., the representation induced by H acting on $\Omega_1(A)$ is irreducible), or if A/A^p is a minimal normal subgroup of G/A^p, then the $\mathrm{WL}_{\mathrm{implicit}}$-dimension of G is bounded by 6.
- Let G be a coprime extensions of two finite abelian groups. Then the $\mathrm{WL}_{\mathrm{implicit}}$-dimension of G is bounded by $\log\log|G|$.

In the other direction, we provide (conditional) lower bounds for the WL-dimension of certain group classes, suggesting sources of hardness in group isomorphism. As a first step, we devise lower bounds for the 2-dimensional versions of the WL-algorithm, exploiting the fact that we can still describe the color classes computed by 2-WL in fair generality, and also reporting on concrete experiments in GAP. We devise the following generic condition (see Lemma 6.2.1) on pairs of groups of exponent p and nilpotency class 2 that ensures, a priori, that they are indistinguishable by 2-WL (explicit or implicit). Here, the commuting graph $\mathrm{Com}(G)$ of a group G is the simple graph with vertex set G, and two elements $g, h \in G$ are joined via an edge, if and only if they commute.

- Let G and H be groups of exponent p and nilpotency class 2, and assume that $\mathrm{Com}(G)$ is indistinguishable from $\mathrm{Com}(H)$ via $2\text{-}\mathrm{WL}_{\mathrm{graphs}}$. Then G and H are indistinguishable via $2\text{-}\mathrm{WL}_{\mathrm{implicit}}$.

Towards conditional lower bounds for the WL-dimension of groups, we devise a collection of $\dim_{\mathrm{WL}}$-preserving reductions between different classes of algebraic structures, ultimately interconnecting their descriptive complexity. To state these correspondences, we devise the notion of *set-extended* structures. Given a relational structure $\mathfrak{X}$ over a ground set V, the set extended version of $\mathfrak{X}$ has an extended ground set, where we add a new element v_S for each subset $S \subseteq V$. We also add a new relation R_{set} that describes the subset structure, i.e., it holds $(v, v_S) \in R_{\mathrm{set}}$ if and only if $v \in V$ is contained in the subset S. The intuition is that, under certain circumstances, the new elements v_S can sometimes encode information about all the elements in S. This situation often arises in the context of groups, where for each color class computed by the WL-algorithm, we want to reason about the information encoded in products of it elements.

A group G is called semisimple, if its socle does not have abelian direct factors, that is, if $\mathrm{soc}(G)$ is a direct product of non-abelian simple groups. The permutational isomorphism type of the induced action of G on the simple direct factors of $\mathrm{Soc}(G)$ precisely captures the isomorphism type of G as an abstract group (see [9]). This observation was used in [9] to derive a polynomial-time isomorphism algorithm for semisimple groups of order n and to bound the number of possible automorphisms by $n^{\mathcal{O}(\log \log n)}$. Here, we use the structural restrictions that apply to semisimple groups to bound their WL-dimension by $\log \log n$ (Lemma 5.4.4). This result is independent of [9], reproving the $n^{\mathcal{O}(\log \log n)}$-bound on the order of the automorphism group of a semisimple group solely in terms of the WL-algorithm, without explicitly solving permutational isomorphism.

- If G is a finite semisimple group, then the $\mathrm{WL}_{\mathrm{implicit}}$-dimension of G is bounded by $\log \log |G| + \mathcal{O}(1)$.

On the other hand, we show that the WL-dimension of a semisimple group G corresponds to the WL-dimension of domain-extended permutation groups (by which we mean the permutation group together with the set-extended domain, encoded as a relational structure, see Corollary 6.3.10). Similarly, we relate the WL-dimension of groups of prime exponent and class 2 to the WL-dimension of bilinear spaces (see Lemma 6.2.9) and we show that the WL-dimension of coprime extensions, asymptotically, is at least as high as the WL-dimension of binary codes, regarded as relational structures (see Lemma 6.3.8).

- The WL-dimension of semisimple groups of the form $S^n \rtimes Q$, with S non-abelian simple and $Q \leq S_n$ permuting the copies if S, is bounded, if and only if the WL-dimension of domain-extended permutation groups is bounded.
- The WL-dimension of groups of odd, prime exponent and nilpotency class 2 is bounded, if and only if the WL-dimension of alternating biliear spaces is bounded.
- There is a class of coprime group extensions, whose WL-dimension is bounded if and only if the WL-dimension of binary codes (regarded as relational structures) is bounded.

1.2 Related work

In short, this thesis studies and develops the descriptive complexity theory of finite groups, with a particular focus on the Weisfeiler-Leman dimension. In the case of finite abelian groups, descriptive complexity has been explicitly studied in [45]. Generally speaking, the descriptive complexity theory of groups and its relation to the group isomorphism problem are not well developed. In contrast to this, the situation for graphs and the graph isomorphism problem is significantly better understood. We refer to Grohe's monograph [54] for an extensive overview on the descriptive complexity of graphs. One of the central results of [54] is that graph classes defined through forbidden minors always have constantly bounded WL-dimension. Concrete structural aspects of graphs that are identified by the Weisfeiler-Leman algorithm are investigated, for example, in [38, 40, 74]. For instance, the 2-$\mathrm{WL}_{\mathrm{graphs}}$ determines the spectrum of a graph or the number of cycles of length at most 6, and it implicitly computes the decomposition of a graph into its 3-connected components.

Despite the limited progress for more general classes of groups, the group isomorphism problem has been frequently studied in the literature. Often the results target specific group classes, aiming to turn more specific structural restrictions into more effective upper bounds for the isomorphism problem. In [9], Babai, Codenotti and Qiao provide a polynomial-time isomorphism algorithm for semisimple groups. Based on representation-theoretic methods, Babai and Qiao recently gave a polynomial-time algorithm for isomorphism of groups with abelian Sylow towers [11], that is, groups that are iterated coprime extensions with abelian groups.

Attacking the problem of p-group isomorphism, recent results often consider linearizations of the isomorphism problem for important subclasses, for example they tackle the isomorphism problem of groups of exponent p and class 2 through the isometry problem of alternating matrix spaces [22], or they consider p-groups with restrictions on the corresponding Lie-algebra from the Baer correspondence [23].

In a series of papers [50, 51, 52, 53], Grochow and Qiao investigate the relation of the group isomorphism problem to other combinatorial and algebraic equivalence problems. Among other results, they show that group isomorphism for groups of exponent p and nilpotency class $c < p$ reduces to isomorphism for groups of exponent p and class 2, and they define a class of various algorithmic problems that are polynomial-time equivalent to tensor isomorphism, including isomorphism of groups of exponent p and class 2. Moreover, they develop search-to-decision and counting-to-decision $n^{\mathcal{O}(\log\log n)}$-reductions for group isomorphism.

The connection of group isomorphism and tensor isomorphism provided by Grochow and Qiao is exploited in the recent break-through result, showing an $n^{\mathcal{O}((\log n)^{5/6})}$-time bound for isomorphism of groups of exponent p and nilpotency class 2.

Furthermore, in [49], Grochow and Qiao discuss cohomologic methods in the context of group isomorphism, providing algorithmic characterizations and efficient algorithms for the isomorphism problem of various classes of group extensions.

Dietrich and Wilson show [31], that group isomorphism can be solved in nearly-linear time for an asymptotically dense set of group orders.

Brooksbank et al. provide an overview over many state-of-the-art group isomorphism tools in [21], and they combine them all in one framework, also incorporating new strong combinatorial invariants. The combinatorial invariants they use are inspired by the Weisfeiler-Leman algorithm, in the sense that they compute an automorphism invariant hypergraph from a group and apply the Weisfeiler-Leman algorithm to the resulting hypergraph. However, this hypergraph is unlikely to encode the full isomorphism type of a group, and even when replacing the use of WL here by an isomorphism solver, the distinguishing power of the framework remains unclear. In contrast to our approach, the WL-algorithm is not directly employed on the input group, and there is no known relation to descriptive complexity and group logic.

In his PhD thesis [105], Vagnozzi investigates the WL-algorithm on groups, as defined below and provided in [17]. He shows that our construction of groups of exponent p and class 2 from graphs, applied to trees, produces only groups of low WL-dimension. Moreover, it is shown that the Weisfeiler-Leman dimension of finite groups and the Weisfeiler-Leman dimension of Latin square graphs of their Cayley tables are asymptotically equivalent. In particular, one is bounded if and only the other is.

For graphs, there is a characterization of the WL-algorithm in terms of isomorphism of Schur-rings [96], providing an algebraic interpretation of the k-dimensional version of WL for each k. In [29], Chen, Ren and Ponomarenko develop a analogous characterization for groups, defining a Schur ring over the direct powers G^m for every finite group G and every $m \in \mathbb{N}$.

Grohe and Verbitsky describe a parallel implementation of the WL-algorithm and thereby relate the WL-dimension to parallel complexity and circuit complexity [56]. Essentially, whenever the WL-dimension of a class of graphs is bounded and the WL-algorithm terminates in a logarithmic number of rounds, then this directly translates to effective parallel and circuit complexity bounds (more concretely, the isomorphism problem is placed in TC^1). The same principles apply to the versions of the WL-algorithm discussed below: combining this parallelization framework for WL with the WL-algorithm on groups, Grochow and Levet obtain new results on the parallel complexity of group isomorphism [48]. In particular, they show that our results on the WL-definability of indecomposable direct factors of a group hold with a logarithmic number of rounds in the WL-algorithm and hence can be parallelized.

In [48], the authors also consider coprime extensions with abelian normal subgroups, as well as semisimple groups. In the case of coprime extensions, they investigate the special scenario where one can fix an explicit isomorphism on the quotient groups, i.e., where the quotient group is generated by a globally constant number of group elements. It then remains to check if group elements corresponding to each other via the given isomorphism act on the abelian normal subgroup accordingly (essentially equivalence of representations), which is shown to be decidable with a constant dimensional WL-algorithm in a logarithmic number of rounds. In the present thesis, we solve a more general problem, where the quotient group is not yet fixed. This means that instead of testing representations for equivalence, we need to check for twisted-equivalence, where the representations can additionally be twisted with an automorphism of the quotient group. In this sense, the machinery we develop for coprime extensions is significantly more general.

In the case of semisimple groups, Grochow and Levet use the fact that a semisimple group has at most $\log\log n$ automorphisms to consider each possible ordering of the direct factors of the socle by hand (again realized through individualization of suitable group elements) and then apply the WL-algorithm. Again, they obtain a logarithmic bound on the round number and extract parallel complexity bounds ($\mathrm{quasiSAC}^1$). In contrast to this, we investigate the WL algorithm with $\log\log n$ total individualizations, allowing us to establish more general connections between the structure of semisimple groups and

WL-colorings. Our techniques also apply in more general contexts, such as groups with small solvable radical, as opposed to semisimple groups, having a trivial solvable radical.

1.3 Structure of the thesis

Chapter 2 contains a short introduction to groups, as well as descriptive complexity, and we present the theoretical background on group isomorphism and the Weisfeiler-Leman algorithm. In Chapter 3 we introduce three versions of the Weisfeiler-Leman algorithm (*explicit*, *implicit*, and *graph-encoded*), where the input can be an arbitrary relational structure. The main result of Chapter 3 is a comparison of these versions, and we show that, in terms of their distinguishing power, they are contained in a (possibly infinite) hierarchy, and thus, asymptotically, they define equivalent similarity measures.

In Chapter 4 we employ the technical framework from the previous chapter and apply it specifically to the class of finite groups. We develop far reaching connections between the structure of a finite group and the color classes that the Weisfeiler-Leman algorithm assigns to it. This is intended as a compendium of techniques used to analyze the WL-algorithm on groups and related structures.

Chapters 5 and 6 build on our analysis of stable color classes in finite groups to devise bounds on the Weisfeiler-Leman dimension of several important group classes. In the case of lower bounds, we also consider conditional lower bounds, where we develop algorithmic reductions that preserve the Weisfeiler-Leman dimension, at least asymptotically, for a variety of group classes, including groups of exponent p and class 2 (where we reduce to isometry problems for bilinear maps), coprime extensions (reducing to equivalence of binary codes), and semisimple groups (reducing to permutational isomorphism of permutation groups).

Finally, the appendix contains further referential information, namely parts of the GAP-code we utilized in the preparation of this thesis, including a (non-optimized) version of the 2-dimensional Weisfeiler-Leman algorithm for groups in Appendix A, as well as presentations of groups we explicitly use in the thesis. For reasons of simplicity, we only reference concrete groups in terms of their identifier in the Small Groups Library in GAP [43]. To ensure that the results presented here remain correct and comprehensible, independent of the Small Groups Library, we list presentations for all groups we explicitly reference in Appendix B.

Chapter 2

Preliminaries

2.1 Notation

General We use the convention $[n] := \{1, \ldots, n\}$, where n is an arbitrary natural number. The t-fold cartesian power of a set M is denoted by $M^t = \{(m_1, \ldots, m_t) \mid m_i \in M\}$, and if M carries additional algebraic structure, e.g., if M is a group, we also denote the t-fold direct power of M by M^t. We use $\{\!\{\cdots\}\!\}$ for multisets.

Graphs & colorings We mostly consider *simple, undirected* graphs, that is, graphs without loops or multi-edges. Given a graph Γ, we denote its vertex set by $V(\Gamma)$ and its edge set by $E(\Gamma)$. A *colored graph* is a graph together with a (vertex) coloring $\gamma\colon V(\Gamma) \to \mathcal{C}$, where $\mathcal{C}$ is a set of target colors (usually the choice of $\mathcal{C}$ is not important and we often omit to define $\mathcal{C}$ more specifically). Given another graph Γ^*, the set of graph isomorphisms between Γ and Γ^* is denoted by $\mathrm{Iso}(\Gamma, \Gamma^*)$, and we set $\mathrm{Aut}(\Gamma) := \mathrm{Iso}(\Gamma, \Gamma)$. The set of color preserving automorphisms of the colored graph (Γ, γ) is denoted by $\mathrm{Aut}(\Gamma, \gamma)$. The fibers of a coloring are called *color classes*, and they induce a natural partition of the vertex set.

Given a subset $S \subseteq V(\Gamma)$, the induced subgraph graph on S is denoted by $\Gamma[S]$. Given a tuple of graph vertices, $s = (v_1, \ldots, v_k) \in V(\Gamma)^k$ for some $k \in \mathbb{N}$, we denote the ordered induced subgraph on $\{v_1, \ldots, v_k\}$ by $\Gamma[s]$, where the order is taken from the order of the tuple (in particular, vertices are allowed to appear multiple times).

For $v \in V(\Gamma)$, let $N(v) := \{w \in V(\Gamma) \mid wv \in E(\Gamma)\}$ denote the *neighborhood* of v.

Groups The symmetric group on Ω is denoted by $\mathrm{Sym}(\Omega)$ and $\mathrm{Sym}(\{1, \ldots, n\})$ is also denoted by S_n. The general linear group in dimension n over a field F is denoted by $\mathrm{GL}_n(F)$.

Given a group G, we denote the minimal size of a generating set of G by $d(G)$. For elements $g, h \in G$, we denote the conjugate of h by g, that is, ghg^{-1}, by h^g, the inner automorphism resulting from g conjugating G by κ_g, and the commutator of g and h by $[g, h] := h^g h^{-1}$. The orbit of h under the conjugation action of G is accordingly denoted by h^G. Given group elements $g_1, \ldots, g_t \in G$, we denote their normal closure in G by $\langle\!\langle g_1, \ldots, g_t \rangle\!\rangle$ or $\langle g_1, \ldots, g_t \rangle^G$, which is the normal subgroup generated by $g_1, \ldots, g_t$.

2.2 Combinatorial aspects of graph isomorphism

In this section, we recall combinatorial aspects of the graph isomorphism problem. The main tool in this scope is the Weisfeiler-Leman algorithm, we refer to [108, 54] for further material. Apart from the algorithm itself, we cover some important connections to logic, combinatorial game theory and graph structure theory, and we present essential bounds on the Weisfeiler-Leman dimension of certain graph classes.

2.2.1 The Weisfeiler-Leman algorithm for graphs

We first recapture the conventional formulation of the Weisfeiler-Leman algorithm for graphs. Throughout the section, let Γ be a simple, undirected graph, potentially vertex-colored. For each natural number k, there is a Weisfeiler-Leman algorithm of dimension k, to which we refer as k-WL.

The k-dimensional WL-algorithm repeatedly colors each k-tuple of vertices with abstract colors that encode how each tuple is situated within the graph. The algorithm has two main phases, consisting of an initial coloring and a refinement step that is iterated until no more changes to the induced color class partition occur.

For a fixed tuple $\bar{v} := (v_1, \ldots, v_k)$, the initial coloring, denoted by $\chi^{k,0}_{\text{graphs}}(\bar{v})$ encodes the isomorphism type of the ordered graph $\Gamma[\bar{v}]$. If Γ is vertex-colored, then the initial coloring additionally encodes the color of each vertex. Formally, if $\bar{v^*} := (v^*_1, \ldots, v^*_k)$ is another vertex tuple, then it holds $\chi^{k,0}_{\text{graphs}}(\bar{v}) = \chi^{k,0}_{\text{graphs}}(\bar{v^*})$, if and only if mapping v_i to v^*_i for all i defines an isomorphism (of colored graphs) from $\Gamma[\bar{v}]$ to $\Gamma[\bar{v^*}]$.

In the subsequent refinement phase of the algorithm, the coloring is iteratively refined as follows. For a tuple $\bar{v} = (v_1, \ldots, v_k) \in V(\Gamma)^k$ and $x \in V(\Gamma)$, define $\bar{v}_{|i\leftarrow x}$ to be the tuple $(v_1, \ldots, v_{i-1}, x, v_{i+1}, \ldots, v_k)$ obtained by replacing the i-th entry with x. Then, for $k > 1$, we define the coloring $\chi_i(\bar{v}) :=$

$$\left(\chi_{i-1}(\bar{v}), \{\!\{(\chi_{i-1}(\bar{v}_{|1\leftarrow x}), \ldots, \chi_{i-1}(\bar{v}_{|k\leftarrow x})) \mid x \in V(\Gamma)\}\!\}\right).$$

Intuitively, for a fixed $x \in V(\Gamma)$, the expression

$$(\chi_{i-1}(\bar{v}_{|1\leftarrow x}), \ldots, \chi_{i-1}(\bar{v}_{|k\leftarrow x}))$$

encodes the relation of x to the tuple $\bar{v}$ with respect to those properties that are encoded in χ_{i-1}. Including the color of the previous iteration ensures that the iterated coloring is indeed a refinement of the previous one, that is, the *color class partition* induced on $V(\Gamma)^k$ by χ_i is at least as fine as the color class partition induced by χ_{i-1}. Let j be the smallest positive integer for which the partition induced by χ_{j-1} agrees with the partition induced by χ_j, then we define the *stable coloring* χ^k_{graphs} to be χ_{j-1}.

In the special case $k = 1$, we need to slightly alter the refinement step: to define $\chi_i(v_1)$, the multiset is only taken over vertices x in the neighborhood $N(v_1)$.

We summarize the algorithm in terms of the following pseudo code.

Algorithm 1 WL-algorithm of dimension k (k-$\mathrm{WL}_{\mathrm{graphs}}$)

```
Input: a colored graph $(\Gamma, \gamma)$ with vertex set $V$
Output: stable coloring $\chi^k_{\mathrm{graphs}}(\Gamma, \gamma)$          // $\mathrm{Aut}(\Gamma, \gamma)$-invariant $k$-coloring on $\mathfrak{X}$
  for $\bar{v} := (v_1, \ldots, v_k) \in V^k$ do
    set $\chi^{k,0}_{\mathrm{graphs}}(\bar{v})$ to the isomorphism type of the ordered graph $(\Gamma[\bar{v}], \gamma_{|\{v_1,\ldots,v_k\}})$
  end for
  set $i := 0$
  repeat
    $i := i + 1$
    for $\bar{v} := (v_1, \ldots, v_k) \in V^k$ do
      $\chi^{k,i}_{\mathrm{graphs}}(\bar{v}) := (\chi^{k,i-1}_{\mathrm{graphs}}(\bar{v}), \{\{(\chi^{k,i-1}_{\mathrm{graphs}}(\bar{v}_{1\leftarrow x}), \ldots, \chi^{k,i-1}_{\mathrm{graphs}}(\bar{v}_{k\leftarrow x})) \mid x \in V\}\})$
    end for
  until the color class partitions induced on $V^k$ by $\chi^{k,i}_{\mathrm{graphs}}$ and $\chi^{k,i-1}_{\mathrm{graphs}}$ agree
  return $\chi^{k,i}_{\mathrm{graphs}}$
```

The domain of each iterated coloring computed by k-WL has size $|V(\Gamma)|^k$, so the number of iterations is bounded by $|V(\Gamma)|^k$. For fixed $k \in \mathbb{N}$, it is possible to compute the color class partition of χ^k_{graphs} in polynomial time, as pointed out in the following lemma.

Lemma 2.2.1 (see [67, 66]). *Let $\chi^k_{\mathrm{graphs}}(\Gamma, \gamma)$ be the output of Algorithm 1 on a colored graph (Γ, γ) with vertex set $V := V(\Gamma)$. Then, the color class partition of $\chi^k_{\mathrm{graphs}}(\Gamma, \gamma)$ induced on V^k can be computed in time*

$$\mathcal{O}\left(|V|^{k+1} \log|V|\right).$$

Moreover, $\chi^k_{\mathrm{graphs}}(\Gamma, \gamma)$ is invariant under $\mathrm{Aut}(\Gamma, \gamma)$*, and if (Γ^*, γ^*) is another colored graph that is isomorphic to (Γ, γ) (as a colored graph), then the multisets of colors in $\chi^k_{\mathrm{graphs}}(\Gamma, \gamma)$ and $\chi^k_{\mathrm{graphs}}(\Gamma^*, \gamma^*)$ agree.*

So to *distinguish* two non-isomorphic graphs the algorithm is applied on the disjoint union. If in the stable coloring the multiset of colors appearing in one graph is different than those appearing in the other graph, then the graphs are not isomorphic. The converse does not necessarily hold, as we explain below (see Section 2.2.4). Distinguishing non-isomorphic graphs is the main purpose of the WL-algorithm, which brings us to the next definition.

Definition 2.2.2. For $k \in \mathbb{N}$, we say that a graph Γ has *Weisfeiler-Leman dimension (also WL-dimension, in symbols* $\dim_{\mathrm{WL}_{\mathrm{graphs}}}$*)* at most k, if Γ is distinguished from all other (non-isomorphic) graphs by k-$\mathrm{WL}_{\mathrm{graphs}}$. In this case, we also say that k-WL *identifies* Γ. A class of graphs has WL-dimension at most k, if all graphs in the class are identified by k-WL.

In the special case that all stable k-WL-color classes induced on $V(\Gamma)$ have size 1, we obtain a canonical ordered copy of the input graph Γ. In general, such colorings, where each color class is a singleton set, are called *discrete*.

2.2.2 First order logic with counting

There is a close connection between the Weisfeiler-Leman algorithm of dimension k and the $(k+1)$-variable fragment of first order logic on graphs with counting quantifiers [24]. To obtain this logic we endow first order logic with counting quantifiers. The formula $\exists^{\geq i} x \varphi(x)$ expresses then the fact that there are at least i distinct elements that satisfy the formula φ. For example the formula $\exists^{\geq 3} x \exists^{\geq 4} y E(x, y)$ would express that the graph contains at least 3 vertices of degree at least 4. The logic $\mathbf{C}^k$ is the fragment of said logic which allows formulas to only use k distinct variables (that can however be reused an arbitrary number of times). We refer to [66] for a more thorough introduction to these logics and a proof that two graphs can be distinguished by k-dimensional WL exactly if there is a formula in $\mathbf{C}^{k+1}$ that holds on the one graph but not on the other. Often such logics are endowed with a fixed-point operator, but since we will only apply the formulas to structures of fixed size, this will not be necessary for us (see [94] for more information).

The following definition relates tuples of vertices to the logic constructed above.

Definition 2.2.3. Given two (colored) graphs Γ_1 and Γ_2, and t-tuples $v_1 \in V(\Gamma_1)^t$ and $v_2 \in V(\Gamma_2)^t$ for some $t \leq k$, we say that (Γ_1, v_1) is equivalent to (Γ_2, v_2) with respect to $\mathcal{C}^k$, if and only if the following holds: for each $\mathcal{C}^k$-formula $\varphi = \varphi(x_1, \ldots, x_t)$ with at most t free variables, Γ_1 fulfills $\varphi((v_1)_1, \ldots, (v_1)_t)$, if and only if Γ_2 fulfills $\varphi((v_2)_1, \ldots, (v_2)_t)$. Here, $\varphi((v_1)_1, \ldots, (v_1)_t)$ denotes the logical expression obtained from φ by replacing each free variable x_i by $(v_1)_i$, so for a given instance of φ, the expression $\varphi((v_1)_1, \ldots, (v_1)_t)$ is either true or false.

2.2.3 The bijective pebble game

The concepts of stable WL-colorings and first order counting logic are tied together in [24] through the use of an Ehrenfeucht-Fraïssé-type pebble game. The version of the pebble game we use in this thesis, the bijective pebble game, originated in [61], and it is often used to show that graphs cannot be distinguished by k-WL.

The game is played on two given input graphs Γ_1, Γ_2 by two players called Duplicator and Spoiler. Initially $k+1$ pairs of pebbles, each pair uniquely colored, are placed next to the input graphs. Each round consists of the following steps:

1. Spoiler picks up a pebble pair (p_i, p'_i),

2. the winning condition is checked,

3. Duplicator chooses a bijection φ from $V(\Gamma_1)$ to $V(\Gamma_2)$,

4. Spoiler places pebble p_i on a vertex $v \in V(\Gamma_1)$ and places p'_i on $\varphi(v)$.

The winning condition is defined, so that Spoiler wins if and only if the graph induced by the vertices occupied by pebbles in $V(\Gamma_1)$ is not isomorphic to the graph induced by the vertices occupied by pebbles in $V(\Gamma_2)$ via a map that sends a pebble p_i to its corresponding pebble of the same color p'_i in the other graph. By default, Spoiler also wins (in round 0) if $|V(\Gamma_1)| \neq |V(\Gamma_2)|$.

A *configuration* of the game is a snapshot of the situation on the board at the start of a round. That is, a configuration describes the current pebble placement through an expression of the form $[(v_1^{(1)}, \dots, v_k^{(1)}), (v_1^{(2)}, \dots, v_k^{(2)})]$, where, for each i, we have that $v_i^{(1)}$ and $v_i^{(2)}$ are vertices of Γ_1 and Γ_2, respectively, indicating that the i-th pebble pair is placed on $(v_i^{(1)}, v_i^{(2)})$, or $v_i^{(1)} = v_i^{(2)} = \bot$, where $\bot$ is an extra symbol indicating that the i-th pebble pair is currently not placed on the board.

When using $k+1$ pebbles on two graphs, the game can be won by Spoiler exactly if k-WL distinguishes the graphs [61]. More formally, the following lemma ties together the different perspectives on stable WL-colorings.

Theorem 2.2.4 ([24, Theorem 5.2])**.** *Let Γ_1 and Γ_2 be colored graphs, and let $v_1 \in V(\Gamma_1)^k$ and $v_2 \in V(\Gamma_2)^k$ be k-tuples of vertices. Then the following are equivalent:*

1. $(\chi^k_{\text{graphs}}(\Gamma_1))(v_1) = (\chi^k_{\text{graphs}}(\Gamma_2))(v_2)$,
2. (Γ_1, v_1) *and* (Γ_1, v_2) *are equivalent with respect to the logic* $\mathcal{C}^{k+1}$,
3. *Spoiler has a winning strategy in the* $(k+1)$*-pebble game on* (Γ_1, Γ_2)*, starting from the configuration* $[(v_1, \bot), (v_2, \bot)]$.

2.2.4 The CFI-graphs

As mentioned previously, for each k there is a pair of non-isomorphic graphs not distinguished by k-WL, whose construction was first given by Cai, Fürer and Immerman in [24]. The CFI-graphs are among the most important examples of graphs with high WL-dimension, and they are linked to a multitude of hardness results in descriptive complexity theory and graph isomorphism testing (see for instance [5, 81]).

Theorem 2.2.5 (Cai, Fürer, Immerman [24])**.** *There is an infinite family of pairs of non-isomorphic 3-regular graphs on $\mathcal{O}(k)$ vertices not distinguished by the k-dimensional Weisfeiler-Leman algorithm.*

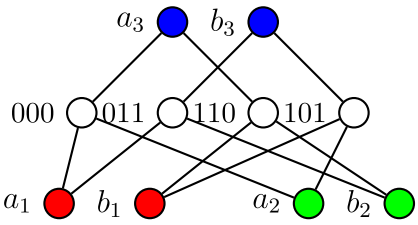


Figure 2.1: A depiction of the CFI-gadget F_3.

In the course of this thesis, we exploit the construction by embedding CFI-graphs into groups. To construct a pair of CFI-graphs, we start with a connected base graph Γ. In this graph every vertex is replaced by a particular gadget and the gadgets are interconnected according to the edges of Γ as follows. For a vertex v of degree d we use the gadget F_d, which is a graph whose vertex set consists of external vertices $O_d = \{a_1^v, b_1^v, a_2^v, b_2^v, \dots, a_d^v, b_d^v\}$ and internal vertices M_d. The internal vertices form a copy of the set of those 0-1-strings of length d that have an even number of entries equal to 1. For each i, each internal vertex m is adjacent to exactly one vertex of $\{a_i^v, b_i^v\}$, namely it is adjacent to a_i if the i-th bit of the string m is 0 and to b_i otherwise. An example of F_3 is depicted in Figure 2.1. We need to explain how the different gadgets are interconnected. For this, for a vertex $v \in \Gamma$ of degree d each edge is associated with one of the pairs a_i^v, b_i^v. For an edge $(u, v) \in E(\Gamma)$, assume u is associated with the pair (a_i^u, b_i^u) in the gadget corresponding to u, and that v is associated with the pair (a_j^v, b_j^v) in the gadget corresponding to v. Then we insert (parallel) edges $\{a_i^u, a_j^v\}$ and $\{b_i^u, b_j^v\}$. Adding such parallel edges for each edge of the base graph we obtain the graph $\mathrm{CFI}(\Gamma)$. The *twisted CFI-graph* $\widetilde{\mathrm{CFI}(\Gamma)}$ is obtained by replacing one pair of (parallel) edges $\{a_i^u, a_j^v\}$ and $\{b_i^u, b_j^v\}$ with the (twisted) edges $\{a_i^u, b_j^v\}$ and $\{b_i^u, a_j^v\}$. The untwisted and twisted versions of connecting two CFI-gadgets are visualized in Figure 2.2.

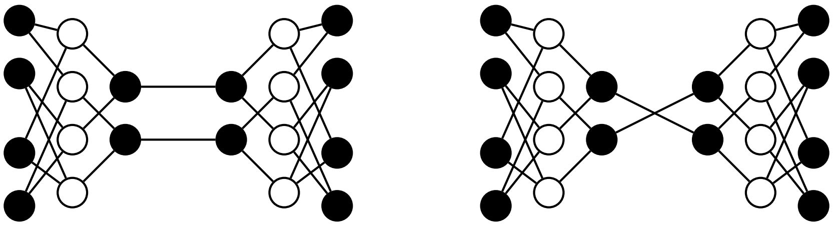


Figure 2.2: Untwisted and twisted connection of two CFI-gadgets.

It can be shown that for connected base graphs (up to isomorphism) it is irrelevant which edge is twisted [24]. For a subset of the edges of the base graph $E' \subseteq E(\Gamma)$, we can define the graph obtained by twisting exactly the edges in E'. The resulting graph is isomorphic to $\mathrm{CFI}(\Gamma)$ if $|E'|$ is even and isomorphic to $\widetilde{\mathrm{CFI}(\Gamma)}$ otherwise.

In many applications, the base graph is usually thought of as vertex colored with all vertices obtaining a different color. This makes all gadgets distinguishable. The colors can be removed by attaching gadgets retaining the property that the base graph is identified by 2-dimensional Weisfeiler-Leman. We want to record here the observation that it is possible to choose the base graph of WL-dimension 2 while maintaining the property that it is 3-regular.

Observation 2.2.6. *The 3-regular base graph Γ can be chosen to have Weisfeiler-Leman dimension at most 2.*

This can be seen in two ways, by adding gadgets on edges or by observing that random expanders, usually used in the construction, have this property.

2.2.5 Further results for WL on graphs

In the course of the thesis, we explicitly employ the following upper bound on the WL-dimension of trees.

Lemma 2.2.7 (see [66])**.** *Let Γ be a rooted tree, then* $1\text{-WL}_{\text{graphs}}$ *computes the orbit partition on Γ, and Γ is identified up to isomorphism.*

We also use the fact that the WL-algorithm identifies basic combinatorial properties, as specified in the next lemma.

Lemma 2.2.8 (see [40, Theorem 2])**.** *Let Γ_1 and Γ_2 be graphs and consider vertices $v_1 \in V(\Gamma_1)$ and $v_2 \in V(\Gamma_2)$. If v_1 is not distinguished from v_2 by 2-$\mathrm{WL}_{\mathrm{graphs}}$, then the number of cycles of length ℓ containing v_1 or v_2 is the same, where $3 \leq \ell \leq 6$.*

For the sake of exposition, we recall two of the strongest results on the distinguishing power of the WL-algorithm. Already the 1-dimensional WL-algorithm, sometimes also called color refinement, is powerful enough to identify almost all graphs in the following precise sense.

Theorem 2.2.9 (Babai-Erdős-Selkow [10])**.** *The 1-dimensional WL-algorithm for graphs identifies asymptotically almost all graphs, i.e., all but $o\left(2^{\binom{n}{2}}\right)$ of the $2^{\binom{n}{2}}$ graphs on n vertices for n sufficiently large.*

Moreover, there are deep connections between the WL-dimension and the structure of a graph. One of the most striking results in this direction is the fact that excluded minors impose very general bounds on the Weisfeiler-Leman dimension.

Theorem 2.2.10 (Grohe [54])**.** *Let $\mathcal{C}$ be a class of graphs that has excluded minors. Then the WL-dimension of $\mathcal{C}$ is a constant, depending on the set of excluded minors.*

Finally, we need to recall the concept of individualization. The idea is to artificially color a sequence of vertices with their own color (i.e., individualize them), with the interpretation that we only want to consider automorphisms that fix the vertices pointwise.

Definition 2.2.11. Let (Γ, γ) be a colored graph and consider a vertex $v \in V(\Gamma)$. The colored graph obtained by *individualizing* v is (Γ, γ_v), where for each $w \in V(\Gamma) \setminus \{v\}$, we have $\gamma_v(w) = \gamma(w)$, and $\gamma_v(v)$ is set to a new color not present in $\gamma(V(\Gamma))$. If multiple vertices $v_1, \ldots, v_m$ are subsequently individualized, we denote the resulting vertex coloring by $\gamma_{(v_1,\ldots,v_m)}$. If Γ is an uncolored graph, we also denote the resulting colored graph after individualizing $v_1, \ldots, v_m$ by $\Gamma_{(v_1,\ldots,v_m)}$.

In terms of the pebble game, individualization can be thought of as permanently placing pebbles on the individualized vertices and not moving them throughout the game. This immediately implies that the distinguishing power of k-WL with m individualizations is at most the distinguishing power of $(k + m)$-WL.

2.3 Finite groups

Throughout the thesis, we assume some familiarity with finite group theory and finite permutation groups. Given the longstanding history of these mathematical branches, it is infeasible to aim for a self-contained presentation. We do recall the most important definitions and results below. For proofs and further introductory material, we refer to [65, 59, 111].

2.3.1 Abstract group theory

We are interested in properties of groups that are invariant under the group's automorphisms.

Definition 2.3.1. Let G be a group and let $U \leq G$ be a subgroup. We say that U is *characteristic (in G)*, if every automorphism $\alpha \in \operatorname{Aut}(G)$ fixes U, i.e., for all $u \in U$ we have $u^\alpha \in U$. A group is called *characteristically simple*, if it does not contain proper, non-trivial characteristic subgroups.

Many well-known subgroup constructions yield characteristic subgroups, such as the center or the commutator subgroup of a group. The finite characteristically simple groups have an easy description.

Lemma 2.3.2 (Characteristically simple groups)**.** *If G is a finite, characteristically simple group, then G is isomorphic to a direct power of a fixed simple group S, i.e., $G \cong S^m$ for some $m \in \mathbb{N}$.*

Another example of a characteristic subgroup is the *socle* of a group, which is the subgroup generated by all minimal normal subgroups.

Lemma 2.3.3. *Let G be a finite group and let $N \trianglelefteq G$ be a minimal normal subgroup of G. Then N is characteristically simple. The socle* $\operatorname{Soc}(G)$ *of G is a direct product of finite simple groups.*

Moreover, we are interested in collections of subgroups, where the subgroups themselves are not necessarily characteristic, but the collection of subgroups is automorphism invariant as a whole. One example would be the collection of Sylow p-subgroups of a group, for a fixed prime p. The following definition captures this idea in a general context.

Definition 2.3.4. For a natural number k, the *k-profile* of a group is the collection (multiset) of isomorphism types of all possible k-generated subgroups.

An important class of groups is given by groups of prime power order. In a way, they control the structure of every finite group, for instance through the Sylow-Theorems. We repeatedly use the following fundamental observations on groups of prime power order.

Lemma 2.3.5 (Nilpotent groups)**.**

1. *Let G be a finite p-group, then for every normal subgroup N of G, it holds $Z(G) \cap N \neq \{1\}$. In particular, $Z(G) \neq 1$.*
2. *Let G be a finite p-group, then the Frattini-subgroup, i.e., the group of non-generators, is given by $\Phi(G) = G^pG'$. In particular, $G/\Phi(G)$ is elementary abelian.*
3. *The finite nilpotent groups are exactly the direct products of groups of prime power order. In other words, a finite nilpotent group is a direct product of its Sylow subgroups.*

Finally, we recall two fundamental results on group decompositions. The first is concerned with direct product decompositions.

Theorem 2.3.6 (Jordan-Hölder). *Let $G = G_1 \times \dots \times G_n = H_1 \times \dots \times H_m$ be two direct decompositions of G into directly indecomposable subgroups G_i and H_i, respectively. Then it holds $n = m$ and there exists a permutation $\pi \in S_n$ such that $G_i \cong H_{i^\pi}$ and $G_iZ(G) = H_{i^\pi}Z(G)$ hold.*

The second provides a general condition for the existence of semidirect complements of normal subgroups.

Theorem 2.3.7 (Schur-Zassenhaus). *Let G be a finite group with a nontrivial, proper normal subgroup $N \trianglelefteq G$, such that* $\gcd(|N|, |G/N|) = 1$ *holds. Then N has a complement $H \leq G$, i.e., it holds $H \cap N = \{1\}$ and G is a semidirect product $G = NH \cong N \rtimes H$. Furthermore, all complements for N in G are conjugate via elements of N.*

2.3.2 Permutation groups

For specific background information on permutation groups, we refer to the book by Dixon and Mortimer [32].

Given a permutation group $P \leq \operatorname{Sym}(\Omega)$ and a set of points $S := \{\omega_1, \dots, \omega_n\}$ with $\omega_i \in \Omega$, we denote its set-wise stabilizer in P by $P_S := \{\pi \in P \mid S^\pi = S\}$. We denote the point-wise stabilizer by $P_{(S)} := P_{\omega_1,\dots,\omega_n} := \{\pi \in P \mid \forall i\colon \omega_i^\pi = \omega_i\}$.

If π is a permutation on a finite domain Ω, then π has a decomposition into disjoint cycles, which is unique up to reordering. Consequently, we define the *cycle type* of π to be the multiset of cycle lengths appearing in a disjoint cycle decomposition. This is identical with the multiset of orbit sizes of $\langle \pi \rangle$ acting on Ω.

We collect basic properties of permutation actions in the following definition.

Definition 2.3.8. If G is a group with a group action $\alpha\colon G \to \operatorname{Sym}(\Omega)$, then α (or G acting on Ω) is called *faithful*, if $\ker(\alpha) = \{1\}$ holds. If this is the case, we usually identify G with $\alpha(G)$. A permutation group $P \leq \operatorname{Sym}(\Omega)$ is called *transitive*, if it leaves exactly one orbit on Ω. It is called *semi-regular*, if for each $\omega \in \Omega$, the point stabilizer P_ω is trivial. It is called *regular*, if it is both semi-regular and transitive. A *base* for $P \leq \operatorname{Sym}(\Omega)$ is a sequence of points $(\omega_1, \dots, \omega_n)$ with $\omega_i \in \Omega$, such that $P_{\omega_1,\dots,\omega_n} = \{1\}$ holds.

The following lemma recapitulates a well-known result on centralizers in the symmetric group, showing that transitive groups have very small centralizers.

Lemma 2.3.9. *Let $P \leq \operatorname{Sym}(\Omega)$ be transitive, then $C_{\operatorname{Sym}(\Omega)}(P)$ is semi-regular. In particular, we have $\left|C_{\operatorname{Sym}(\Omega)}(P)\right| \leq n$.*

In the case of permutation groups, there is a natural notion of isomorphism that takes the respective actions into account.

Definition 2.3.10. Two permutation groups $G \leq \operatorname{Sym}(\Omega)$ and $G^* \leq \operatorname{Sym}(\Omega^*)$ are *permutationally equivalent* or *permutationally isomorphic*, if there exists a group isomorphism $\varphi\colon G \to G^*$ and a bijection $b\colon \Omega \to \Omega^*$, fulfilling the property

$$\forall g \in G\colon\ \forall \omega \in \Omega\colon\ b(\omega^g) = b(\omega)^{\varphi(g)}.$$

In the language of permutational isomorphism, the permutational automorphisms of a given permutation group $G \leq \mathrm{Sym}(\Omega)$ are precisely given by the normalizing elements in the symmetric group, that is, the automorphism group of G as a permutation group can be identified with $N_{\mathrm{Sym}(\Omega)}(G) := \{\pi \in \mathrm{Sym}(\Omega) \mid G^\pi = G\}$, where $\pi \in N_{\mathrm{Sym}(\Omega)}(G)$ induces the automorphism $G \to G, x \mapsto \pi x \pi^{-1}$ and the bijection $\Omega \to \Omega, \omega \mapsto \omega^\pi$.

2.3.3 Representation theory of finite groups

In this section, we collect basics on representations of finite groups. In the course of this thesis we often encounter groups acting on subgroups via conjugation. In the case of groups acting on abelian groups, the actions are closely related to representations over finite fields of prime order. For a detailed treatment of representation theory, we refer to [70].

Definition 2.3.11. Let G be a group, F a field, and V a finite dimensional vector space over F. A *representation* of G over V is a homomorphism $\Delta\colon G \to \mathrm{GL}(V) \cong \mathrm{GL}_{\dim V}(F)$. Via Δ, we consider V as a G-module. A G-invariant subspace $W \leq V$ is *irreducible*, if it does not contain proper non-trivial G-invariant subspaces. We say that V (or Δ, respectively) is *completely reducible*, or *semisimple*, if V is a direct sum of irreducible G-invariant subspaces. The *character* associated to Δ is given by $\chi_\Delta\colon G \to F, g \mapsto \mathrm{trace}(\Delta(g))$, where we take the trace with respect to the linear map associated to the action of $\Delta(g)$ on V. A character is called *irreducible* if the associated representation is. An *irreducible constituent* of V is an irreducible G-submodule $W \leq V$ that admits a G-invariant complement W', i.e. we have a decomposition $V = W \oplus W'$ into G-invariant subspaces.

Linear representations come equipped with a natural equivalence relation.

Definition 2.3.12. For $i \in \{1, 2\}$, let $\Delta_i : G \to \mathrm{GL}(V)$ be a representation of G. Then Δ_1 and Δ_2 are *equivalent*, if they are conjugate homomorphisms, that is, there exists some $\alpha \in \mathrm{GL}(V)$ with $\forall g \in G\colon \Delta_2(g) = \alpha^{-1}\Delta_1(g)\alpha$. In this case we write $\Delta_2 = \Delta_1^\alpha$. They are called *twisted equivalent*, if there is exists an automorphism $\psi \in \mathrm{Aut}(G)$ such that $\Delta_1 \circ \psi$ and Δ_2 are equivalent.

A classical result from the representation theory of finite groups is that, up to equivalence, each group G has only finitely many irreducible representations over a fixed field F.

Lemma 2.3.13. *Let $\Delta\colon G \to \mathrm{GL}(V)$ be a representation of G over F. Assume that V is completely reducible, i.e., we have a decomposition $V = V_1 \oplus \cdots \oplus V_n$ into irreducible G-modules V_i. Then Δ is uniquely determined up to equivalence by the multisets of equivalence classes of $V_1, \ldots, V_n$.*

Character theory studies characters of linear representations with the aim of recovering as much of the representation's information as possible, just from the character. Characters are *class functions*, i.e., they are constant on conjugacy classes, and so we may identify a character of G over F with a vector over F, whose entries are indexed by conjugacy classes of G. Then characters of G over F can be added entry-wise and if Δ_i

is an F-representation of G over V_1 with character χ_i, then $\chi_1 + \chi_2$ is the character of $\Delta_1 \oplus \Delta_2 := G \to \mathrm{GL}(V_1 \oplus V_2), g \mapsto (\Delta_1(g), \Delta_2(g))$. The amount of information characters contain about their representations is quite surprising at first glance. A very thorough treatment of character theory can be found in [68], we just recall the most important aspects here.

Lemma 2.3.14. *Characters of distinct irreducible representations of G over F are linearly independent. In particular, if Δ is a completely reducible F-representation, then the character of Δ determines (modulo the characteristic of the field F) the number of occurrences of each irreducible F-representation of G as a constituent of Δ.*

So in characteristic 0, there is a one-to-one correspondence between characters and representations of a group, while in characteristic $p > 0$, the representations Δ and $\Delta^{p+1} := \Delta \oplus \cdots \oplus \Delta$ have the same character (but this is essentially the only source of ambiguity according to the previous lemma).

We recall two major classical milestones in the representation theory of finite groups. The first is a severe restriction on the structure of representations, whenever the characteristic does not divide the group order.

Theorem 2.3.15 (Maschke)**.** *Let Δ be a representation of G over F, such that the characteristic of F does not divide $|G|$. Then Δ is completely reducible.*

The second establishes a connection between the representations of a group and representations of its normal subgroups. In general this branch is known as "Clifford Theory".

Theorem 2.3.16 (Clifford)**.** *Let $\Delta\colon G \to \mathrm{GL}(V)$ be an irreducible representation and let $N \trianglelefteq G$ be a normal subgroup. Then the restriction $\Delta_{|N}$ is completely reducible and all irreducible constituents of $\Delta_{|N}$ are conjugate via G.*

Definition 2.3.17. Let $\Delta\colon G \to \mathrm{GL}(V)$ be a representation of G. Then V (or Δ, respectively) is called *homogeneous* (*twisted homogeneous*), if V is completely reducible and all irreducible constituents of V are equivalent (twisted equivalent) as G-modules.

In particular, Clifford's Theorem implies that restrictions of irreducible representations to normal subgroups are twisted homogeneous.

As a consequence of Maschke's Theorem, many basic principles carry over from the complex representation theory of finite groups to the coprime case in positive characteristic. Recall that irreducible complex representations of finite abelian groups are always one-dimensional. While this is not true anymore in positive characteristic, the following well-known generalization always holds in the coprime case.

Lemma 2.3.18 (see [103, Corollary 1.6(a)])**.** *Let $\Delta\colon A \to \mathrm{GL}_d(F)$ be an irreducible representation of a finite abelian group A, where the characteristic of F does not divide $|A|$. Then $\Delta(A)$ is cyclic.*

2.3.4 Word logic and group varieties

In the context of groups, a common definition of first order logic is given by so called *word logic*. It includes the logical standard operators $\neg$, $\vee$, $\wedge$, $\to$, $\exists$, and $\forall$, and additionally, all equations of the form $w(x_1, \dots, x_k) = 1$, where w is a word over the variables $x_1, \dots, x_k$ and their formal inverses $x_1^{-1}, \dots, x_k^{-1}$. For example, the first order sentence

$$\forall x\colon \forall y\colon xyx^{-1}y^{-1} = 1$$

holds in a group G if and only if G is abelian, and

$$\exists x\colon \neg(x = 1) \wedge \forall x\colon x \cdot x \cdot x = 1$$

expresses the fact that G is non-trivial of exponent 3. To increase readability, we would usually replace the expression $x \cdot x \cdot x$ by x^3 or replace the expression $xyx^{-1}y^{-1}$ by $[x, y]$, but we need to be careful about such compressions when defining the size of a logical formula.

This natural logic on groups is deeply connected to structural aspects of group theory, for instance through verbal subgroups and group varieties.

Definition 2.3.19. Let W be a set of finite words over variables $\{x_1, x_2, \dots\}$ and their formal inverses, and let G be a group. Let $W(G)$ denote the subgroup of G generated by the set $\{w(g_1, \dots, g_m) \mid w(x_1, \dots, x_m) \in W,\ g_1, \dots, g_m \in G\}$, and simply write $w(G)$ in the case $W = \{w\}$. Then $W(G)$ is called a *verbal* subgroup of G. Given a word $w := w(x_1, \dots, x_k)$ over k variables and their inverses, w is called a *k-group law*, if for all choices of $g_1, \dots, g_k \in G$ it holds that $w(g_1, \dots, g_k)$ is the trivial element in G. Let $\mathcal{L}$ denote the set of all group laws of G, then the *variety* of G, denoted by $\mathrm{Var}(G)$, is the class of all groups in which all laws of $\mathcal{L}$ hold.

We have the following characterization of isomorphisms relative to ordered generating sets.

Lemma 2.3.20. *Let G and H be finite groups with group elements $g_1, \dots, g_k \in G$ and $h_1, \dots, h_k \in H$. Then, there exists an isomorphism $\varphi\colon \langle g_1, \dots, g_k\rangle \to \langle h_1, \dots, h_k\rangle$ with $\varphi(g_i) = h_i$ for all i, if and only if for each word $w(x_1, \dots, x_k)$ over k variables it holds $w(g_1, \dots, g_k) = 1 \Leftrightarrow w(h_1, \dots, h_k) = 1$.*

Chapter 3

Weisfeiler-Leman algorithms on relational structures

This is the first chapter of the thesis that contains original results. In the following, we devise a general definition of the Weisfeiler-Leman algorithm on arbitrary relational structures. The important connections between WL-algorithms, bijective pebble games and first order counting logic that were observed in the case of graphs carry over to this general framework, the corresponding notions are developed in detail below. We always assume relational structures to be given *explicitly*, that is, each relation is given as a set of tuples over the ground set.

As with graphs, the stable colorings computed by the Weisfeiler-Leman algorithm of a fixed dimension serve as non-isomorphism tests and the running time to compute these colorings is polynomial in the size of the ground set, as long as the maximal arity of the given relations is fixed.

The algorithms presented here generalize our work in [17], where corresponding versions of the Weisfeiler-Leman algorithm are investigated only for finite groups. Versions I, II and III in [17] correspond to the *explicit*, *implicit* and *graph-encoded* WL-algorithm defined below, respectively. The results we present here are structured in a similar way as [17, Section 3], but we need to devise new technical definitions and arguments to allow for the treatment of (large classes of) relational structures. Lemma 3.4.5, Section 3.4.1, and Section 3.5 have not been published before.

In particular, the definition and construction of *set-extended structures* in Section 3.5 is a new concept, which enables us to investigate certain algorithmic reductions with respect to the WL-dimension in Chapter 6.

3.1 Colored relational structures

We begin with the central definition of a relational structure and recall concepts from the theory of the Weisfeiler-Leman algorithm in this general setting.

Definition 3.1.1. A *relational structure* is a tuple $\mathfrak{X} = (V, R_1, \dots, R_t)$ with a non-empty set V and a collection of relations $R_1, \dots, R_t$, where $R_i \subseteq V^{r_i}$ for some $r_i \geq 1$, the *arity* of R_i. We refer to V as $V(\mathfrak{X})$.

For our purposes, important examples of relational structures include graphs, semigroups, quasigroups, groups, and linear codes (regarded as elementary abelian groups with a distinguished basis). In the context of the Weisfeiler-Leman algorithm we also treat permutation groups as relational structures: Given $G \leq \mathrm{Sym}(\Omega)$, the ground set is $G \uplus \Omega$ and there are two relations $R_{\mathrm{mult}}(G) := \{(g,h,gh) \mid g,h \in G\}$ and $R_{\mathrm{act}}(G) := \{(g,\omega,\omega^g) \mid g \in G, \omega \in \Omega\}$, specifying the group and permutation structure of G.

Relational structures come equipped with a natural notion of isomorphism.

Definition 3.1.2. Let $\mathfrak{X} = (V, R_1, \dots, R_t)$ and $\mathfrak{X}^* = (V^*, R_1^*, \dots, R_t^*)$ be relational structures. An *isomorphism* between $\mathfrak{X}$ and $\mathfrak{X}^*$ is a bijection $\varphi : V \to V^*$, such that for each $i \in [t]$ we have that $R_i^\varphi := \{(v_1^\varphi, \dots, v_{r_i}^\varphi) \mid (v_1, \dots, v_{r_i}) \in R_i\} = R_i^*$ holds.

We denote the set of isomorphisms between $\mathfrak{X}$ and $\mathfrak{X}^*$ with $\mathrm{Iso}(\mathfrak{X}, \mathfrak{X}^*)$ and we set $\mathrm{Aut}(\mathfrak{X}) := \mathrm{Iso}(\mathfrak{X}, \mathfrak{X})$.

Colorings are used to restrict possible isomorphisms between relational structures.

Definition 3.1.3. Let $\mathfrak{X} = (V, R_1, \dots, R_t)$ be a relational structure. A *k-coloring* of $\mathfrak{X}$ is a coloring of k-tuples over the ground set, that is a map $\gamma : V^k \to \mathcal{C}$, where $\mathcal{C}$ is an arbitrary set of colors. We simply refer to 1-colorings as colorings. A *colored relational structure* is a relational structure $\mathfrak{X}$ together with a coloring $\gamma : V \to \mathcal{C}$, denoted as a pair $(\mathfrak{X}, \gamma)$. A subset $U \subseteq V(\mathfrak{X})$ is called *γ-induced* if U is a union of γ-color classes.

Given another colored relational structure $(\mathfrak{X}^*, \gamma^*)$, an isomorphism between the colored structures is an isomorphism $\varphi \in \mathrm{Iso}(\mathfrak{X}, \mathfrak{X}^*)$ that respects the colorings, that is for all $v \in V$ it holds $\gamma^*(v^\varphi) = \gamma(v)$. We write $\mathrm{Aut}(\mathfrak{X}, \gamma)$ to denote the set of color-respecting automorphisms of $\mathfrak{X}$. Conversely, given a subgroup $G \leq \mathrm{Aut}(\mathfrak{X})$, a coloring $\gamma : V^k :\to \mathcal{C}$ is *G-invariant* if for all $g \in G$ it holds that $\gamma(v_1^g, \dots, v_k^g) = \gamma(v_1, \dots, v_k)$.

To compare the expressiveness of different colorings it is often useful to convert between different arities. Consider a k-coloring $\gamma : V^k \to \mathcal{C}$ and natural numbers $k_- \leq k \leq k_+$. We define the induced colorings

$$\gamma^{(k_-)} : V^{k_-} \to \mathcal{C}, (v_1, \dots, v_{k_-}) \mapsto \gamma(v_1, \dots, v_{k_-}, v_1, \dots, v_1),$$
$$\gamma^{(k_+)} : V^{k_+} \to \mathcal{C}, (v_1, \dots, v_{k_+}) \mapsto \gamma(v_1, \dots, v_k).$$

In particular, any k-coloring $\gamma : V^k \to \mathcal{C}$ induces a coloring of the ground set $\gamma^{(1)} : V \to \mathcal{C}$ with respect to the same set of colors. Via these conversions, we usually just write γ for all induced colorings, omitting the exponent.

Graph encodings There is a folklore procedure that assigns a finite (colored) graph to each explicitly given finite (colored) relational structure, in a way that preserves isomorphism and non-isomorphism. Let $\mathfrak{X} = (V, R_1, \dots, R_t)$ be a relational structure. The idea is to encode each relation R_i in terms of specific graph gadget constructions on the vertex set V.

Definition 3.1.4. We start with the graph $(V, \emptyset)$ and successively add the following gadgets (see Figure 3.1): Let r_i denote the arity of R_i. For each $i \in [t]$ and each $\bar{v} = (v_1, \dots, v_{r_i}) \in V^{r_i}$, we add a gadget $M_i(\bar{v})$ that consists of new vertices $x_1, \dots, x_{r_i}$, the *gadget vertices*. The gadget vertices (for a fixed gadget) form a path from x_1 to x_{r_i}, and for each $j \in [r_i]$ we also connect x_j to v_j via an edge. We assign a new color to gadget vertices, distinguishing them from elements in V and we assign another special color to x_{r_i} to fix an ordering. We use distinct colors for distinct relations but the r_i-th gadget vertex of $M_i(\bar{v})$ will always obtain the same color for a fixed value of i, independent of $\bar{v}$. Moreover, the colors we pick for gadget vertices are picked consistently for relational structures of fixed arities $(r_1, \dots, r_t)$.

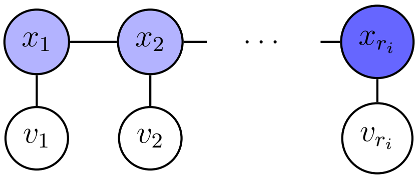


Figure 3.1: An instance of the multiplication gadget.

We thus obtain the graph $\Gamma_{\mathfrak{X}}$. If we additionally want to encode a coloring $\gamma : V \to \mathcal{C}$ we can just color the vertices in $\Gamma_{\mathfrak{X}}$ accordingly (without loss of generality, we may assume that these colors are always distinct from gadget colors).

To clarify the construction of $\Gamma_{\mathfrak{X}}$ we add to more examples. Assume x, y and z are distinct vertices in some relational structure $\mathfrak{X}$. If (x, y, z) and (y, x, z) both belong to the relation $\mathfrak{R}$ (for instance, if $\mathfrak{X}$ is a group in which $xy = yx = z$ holds), then this is expressed in the graph by two gadgets as follows:

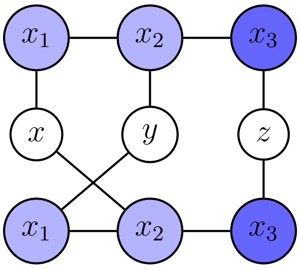


Figure 3.2: Gadgets expressing symmetry in a relation.

If (x, y, z) is contained in two distinct relations, say $\mathcal{R}$ and $\mathcal{R}'$, then this would be expressed though the use of distinct colors for the gadget vertices:

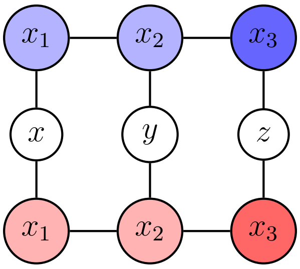


Figure 3.3: Tuple fulfilling distinct relations.

If necessary, the graph $\Gamma_{\mathfrak{X}}$ can also be converted into an uncolored graph via standard graph constructions, replacing colors with special color gadgets. We collect well-known facts about this encoding.

Lemma 3.1.5. *Let $\mathfrak{X} = (V, R_1, \ldots, R_t)$ and $\mathfrak{X}^* = (V^*, R_1^*, \ldots, R_s^*)$ be relational structures.*

1. *If the arity of R_i is r_i, then $\Gamma_{\mathfrak{X}}$ has $|V| + \sum_i r_i|R_i|$ vertices and $\sum_i (2r_i - 1)|R_i|$ edges. In particular, for fixed arities and fixed t, the size of $\Gamma_{\mathfrak{X}}$ is polynomial in $|V|$.*

2. *It holds $\mathfrak{X} \cong \mathfrak{X}^*$ if and only if $\Gamma_{\mathfrak{X}} \cong \Gamma_{\mathfrak{X}^*}$, where isomorphisms are always assumed to respect given colorings.*

Proof. 1. The first part is by construction. The given cardinalities are polynomially bounded in $|V|$ since it holds $|R_i| \leq |V|^{r_i}$.

2. If $(r_1, \ldots, r_t) \neq (r_1^*, \ldots, r_s^*)$ holds, neither the relational structures, nor the graphs are isomorphic. Thus, assume that we have $(r_1, \ldots, r_t) = (r_1^*, \ldots, r_s^*)$, so in particular, the gadget vertices encoding R_i and R_i^* have the same colors by construction. Furthermore, gadget vertices that correspond to fixed relations, R_i and R_i^* say, can be distinguished from all other vertices through their special coloring. In turn, the elements of V are distinguished from all gadget vertices. Thus, if $\varphi : \Gamma_{\mathfrak{X}} \cong \Gamma_{\mathfrak{X}^*}$ is an isomorphism of colored graphs, then the restriction $\varphi_{|V} : V \to V^*$ induces an isomorphism between the ground sets, where mapping gadgets to gadgets translates to mapping R_i to R_i^*. On the other hand, an isomorphism φ between the relational structures can be extended to a graph isomorphism by mapping the j-th gadget vertex in $M_i((v_1, \ldots, v_{r_i}))$ to the j-th gadget vertex in $M_i((\varphi(v_1), \ldots, \varphi(v_{r_i})))$ (this gadget exists since φ maps R_i to R_i^*).

□

3.2 Weisfeiler-Leman algorithms on colored relational structures

For each natural number $k \geq 2$, we devise a k-dimensional Weisfeiler-Leman algorithm, denoted by k-WL, that takes as input a finite colored relational structure $\mathfrak{X} = (V, R_1, \ldots, R_t)$ together with a coloring $\gamma : V \to \mathcal{C}$, and computes a k-coloring $\chi^k(\mathfrak{X}, \gamma)$ over $\mathfrak{X}$ which is $\mathrm{Aut}(\mathfrak{X}, \gamma)$-invariant. The algorithm computes an initial coloring from isomorphism invariant properties of k-tuples, and then iteratively refines color classes in a canonical way, until the process stabilizes. The *stable colorings* arising from k-WL provide (possibly incomplete) polynomial-time computable non-isomorphism tests.

The explicit Weisfeiler-Leman algorithm The *initial coloring*, which we denote by $\chi^{k,0}_{\text{explicit}}(\mathfrak{X}, \gamma)$ or simply $\chi^{k,0}_{\text{explicit}}$, compares k-tuples over $V(\mathfrak{X})$ with respect to the relations that define $\mathfrak{X}$, as well as the coloring γ. Let r_i denote the arity of R_i for all $i \in [t]$. Two k-tuples $\bar{v} = (v_1, \ldots, v_k)$ and $\bar{w} = (w_1, \ldots, w_k)$ over the ground set V obtain the same initial color, if and only if the following three conditions hold:

1. $\forall i \in [k] : (\gamma(v_i) = \gamma(w_i))$,

2. $\forall i, j \in [k] : (v_i = v_j \Leftrightarrow w_i = w_j)$,

3. $\forall s \in [t] : (\forall i_1, \ldots, i_{r_s} \in [k] : ((v_{i_1}, \ldots, v_{i_{r_s}}) \in R_i \Leftrightarrow (w_{i_1}, \ldots, w_{i_{r_s}}) \in R_i)$.

The coloring is then iteratively refined, by replacing single coordinates of a fixed tuple with elements from the ground set V in a structured way. The idea is to look at two k-tuples and to consider all their possible extensions by one additional element from the ground set: if the multisets of such extensions behave differently, then the k-tuples can be iteratively distinguished. More precisely, we define

$$\chi^{k,i}_{\text{explicit}}(\bar{v}) := \left(\chi^{k,i-1}_{\text{explicit}}(\bar{v}), \left\{\!\!\left\{ \left(\chi^{k,i-1}_{\text{explicit}}(\bar{v}_{1\leftarrow x}), \ldots, \chi^{k,i-1}_{\text{explicit}}(\bar{v}_{k\leftarrow x})\right) \mid x \in V \right\}\!\!\right\}\right),$$

where $\bar{v}_{i\leftarrow x}$ denotes the k-tuple obtained from replacing v_i in $\bar{v}$ with x. Encoding the old color of $\bar{v}$ into the iterated coloring ensures that this indeed defines a refinement.

Since V^k is finite, at some point the color classes induced on V^k by $\chi^{k,i}_{\text{explicit}}$ and $\chi^{k,i-1}_{\text{explicit}}$ agree for the first time (and then agree for all higher values of i), and we obtain the *stable coloring* computed by k-WL on $(\mathfrak{X}, \gamma)$. We denote it by $\chi^{k}_{\text{explicit}}(\mathfrak{X}, \gamma) := \chi^{k,i}_{\text{explicit}}$.

We formalize the algorithm in pseudo code below, see Algorithm 2.

Algorithm 2 Explicit WL-algorithm of dimension k (k-WL$_{\text{explicit}}$)

```
Input: a colored relational structure $(\mathfrak{X}, \gamma)$ with $\mathfrak{X} := (V, R_1, \ldots, R_t)$
Output: $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma)$          // $\text{Aut}(\mathfrak{X}, \gamma)$-invariant $k$-coloring on $\mathfrak{X}$
  for $\bar{v} := (v_1, \ldots, v_k) \in V^k$ do
    set $\chi^{k,0}_{\text{explicit}}(\bar{v}) := ($
                   $(\gamma(v_1), \ldots, \gamma(v_k))$,
                   $\{(i, j) \in [k]^{(2)} \mid v_i = v_j\}$,
                   $\{(i_1, \ldots, i_{r_1}) \in [k]^{(r_1)} \mid (v_{i_1}, \ldots, v_{i_{r_1}}) \in R_1\}$,
                   $\ldots$
                   $\{(i_1, \ldots, i_{r_t}) \in [k]^{(r_t)} \mid (v_{i_1}, \ldots, v_{i_{r_t}}) \in R_t\}$
                 $)$
  end for
  set $i := 0$
  repeat
    $i := i + 1$
    for $\bar{v} := (v_1, \ldots, v_k) \in V^{(k)}$ do
      $\chi^{k,i}_{\text{explicit}}(\bar{v}) := (\chi^{k,i-1}_{\text{explicit}}(\bar{v}), \{\{(\chi^{k,i-1}_{\text{explicit}}(\bar{v}_{1\leftarrow x}), \ldots, \chi^{k,i-1}_{\text{explicit}}(\bar{v}_{k\leftarrow x})) \mid x \in V\}\})$
    end for
  until the color class partitions induced on $V^k$ by $\chi^{k,i}_{\text{explicit}}$ and $\chi^{k,i-1}_{\text{explicit}}$ agree
  return $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma) := \chi^{k,i}_{\text{explicit}}$
```

We note that for $k \geq 2$, on the class of finite (colored) graphs, the two algorithms k-WL$_{\text{graphs}}$ and k-WL$_{\text{explicit}}$ coincide, but WL$_{\text{explicit}}$ can be applied to arbitrary relational structures.

We discuss the cost of computing the stable color classes induced by the output of Algorithm 2 in the following lemma. The arguments are essentially the same as for graphs instead of relational structures. In particular, we note that the refinement step is exactly identical to the refinement step for a graph with vertex set $|V|$ in the standard k-dimensional Weisfeiler-Leman algorithm for graphs, see Algorithm 1 for comparison.

Lemma 3.2.1. *Let $\chi^k_{\text{explicit}}(\mathfrak{X},\gamma)$ be the output of Algorithm 2 on a colored relational structure $(\mathfrak{X},\gamma)$ with $\mathfrak{X} := (V, R_1, \dots, R_t)$. Then, the color class partition of $\chi^k_{\text{explicit}}(\mathfrak{X},\gamma)$ induced on V^k can be computed in time*

$$\mathcal{O}\left(|V|^k k^{\sum_i r_i} + |V|^{k+1}\log|V|\right),$$

where r_i is the arity of R_i. In particular, for fixed arities and fixed values of t and k, the bound is polynomial with respect to $|V|$.

Proof. As the refinement step is identical to the refinement step of k-WL on graphs, it is sufficient to derive the given bound for the computation of the initial coloring. Given any k-coloring over V, computing the stable color classes (with respect to exhaustively applying the refinement step) can be done in time $\mathcal{O}(|V|^{k+1}\log|V|)$ by [66].

Now for each relation R_i, the set of indices $\{(i_1, \dots, i_{r_s}) \in [k]^{r_i} \mid (v_{i_1}, \dots, v_{i_{r_i}}) \in R_i\}$ can be computed by brute-force enumeration in time $\mathcal{O}(k^{r_i})$. Thus, the first for-loop of Algorithm 2 can be executed in time $\mathcal{O}(|V|^k k^{\sum_i r_i})$. □

We remark that, in Algorithm 2 as given above, the size of the color description grows exponentially. Thus, in practice, the iterated colors can not be stored as iterated multisets. Instead, the color descriptions have to be compressed, which can be efficiently done through a sort-and-relabel step after each iteration, for details see [67]). This is not a problem for canonicity, as long as one always compresses the same colors in the same way.

The implicit Weisfeiler-Leman algorithm For many classes of relational structures, substructures can be implicitly defined in terms of *generated substructures*. Our standard example for this is the class of groups, where subgroups can be represented in terms of generating sets. From a group theoretic perspective, it is most natural to investigate tuples of group elements through the subgroups they generate.

Definition 3.2.2. Given a relational structure $\mathfrak{X} = (V, R_1, \dots, R_m)$, an *induced substructure*, is a relational structure of the form $(S, R_1 \cap S^{r_1}, \dots, R_m \cap S^{r_m})$, where S is a subset of V and for each i, the arity of R_i is r_i. In particular, given two induced substructures $\mathfrak{X}_1$ and $\mathfrak{X}_2$ of $\mathfrak{X}$, we can define their intersection to be the unique induced substructure of $\mathfrak{X}$ with ground set $V(\mathfrak{X}_1) \cap V(\mathfrak{X}_2)$.

Now let $\mathcal{C}$ be a class of relational structures. We say that $\mathcal{C}$ is *admissible*, if for any two induced substructures $\mathfrak{X}_1$ and $\mathfrak{X}_2$ of a given relational structure, it holds that $\mathfrak{X}_1 \cap \mathfrak{X}_2$ belongs to $\mathcal{C}$, whenever $\mathfrak{X}_1$ and $\mathfrak{X}_2$ both belong to $\mathcal{C}$.

In other words, the admissible finite relational structures are those where we have a natural notion of generating sets and generated substructures.

Definition 3.2.3. Let $\mathcal{C}$ be an admissible class of finite relational structures. Assume that $\mathfrak{X} = (V, R_1, \dots, R_t)$ is a finite relational structure in $\mathcal{C}$, and denote the arity of R_i by r_i. Let $S \subseteq V$ be an arbitrary subset of elements. The *$\mathcal{C}$-structure generated by S* is the smallest induced substructure $\mathfrak{X}' = (V', (R_1)_{|V'^{(r_1)}}, \dots, (R_t)_{|V'^{(r_t)}}))$ such that $\mathfrak{X}'$ belongs to $\mathcal{C}$ and $S \subseteq V'$ holds (by smallest we mean smallest with respect to inclusion). We denote the $\mathcal{C}$-structure generated by S with $\langle S \rangle_{\mathcal{C}}$.

The substructure generated by S is indeed unique: Since $\mathcal{C}$ is closed under intersection, we can define $\langle S \rangle_{\mathcal{C}}$ as the intersection of all induced $\mathcal{C}$-substructures of $\mathfrak{X}$ that contain S.

If the class $\mathcal{C}$ is clear from the context, for example if we are working with groups, we may also just write $\langle S \rangle$ instead of $\langle S \rangle_{\mathcal{C}}$.

Example 3.2.4.

1. If $\mathcal{C}$ is the class of finite graphs, $\Gamma \in \mathcal{C}$ and $S \subseteq V(\Gamma)$, then $\langle S \rangle$ is just the subgraph induced on S, that is, $\langle S \rangle = \Gamma[S]$. In this case, there is no difference between implicit and explicit representation, the vertex set of $\Gamma[S]$ is exactly S itself.

2. If $\mathcal{C}$ is the class of finite groups, $G \in \mathcal{C}$ and $S \subseteq G$, then $\langle S \rangle$ is precisely the subgroup generated by S. In this case the order of the generated substructure can be exponential in $|S|$.

Through generated substructures we can pull back the notion of isomorphism from induced substructures to arbitrary tuples of elements over the ground set.

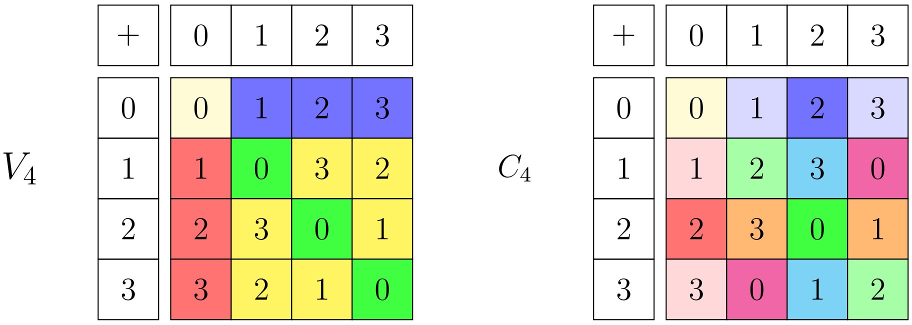
Definition 3.2.5. Let $\mathcal{C}$ be an admissible class of relational structures and let $\mathfrak{X} = (V, R_1, \dots, R_t)$ and $\mathfrak{X}^* = (V^*, R_1^*, \dots, R_t^*)$ be colored relational structures in $\mathcal{C}$. Let $x_1, \dots, x_k \in V$ and $x_1^*, \dots, x_k^* \in V^*$ be given. Then we say that $(x_1, \dots, x_k)$ and $(x_1^*, \dots, x_k^*)$ have the same *marked isomorphism type* (w.r.t. $\mathcal{C}$), if there is an isomorphism of colored relational structures $\varphi : \langle x_1, \dots, x_k \rangle_{\mathcal{C}} \to \langle x_1^*, \dots, x_k^* \rangle_{\mathcal{C}}$ with $\varphi(x_i) = x_i^*$ for all $i \in [k]$.

Marked isomorphism types provide an alternative, but equally natural definition of initial colors in the WL-algorithm, leading to what we call the *implicit* Weisfeiler-Leman algorithm or $k\text{-WL}^{\mathcal{C}}_{\text{implicit}}$ (again, if clear from the context we may omit $\mathcal{C}$ from the notation). The algorithm only differs from Algorithm 2 in terms of the initial coloring, assigning to each tuple $(x_1, \dots, x_k)$ its marked isomorphism type.

Algorithm 3 Implicit WL-algorithm of dimension k (k-$\mathrm{WL}^{\mathcal{C}}_{\mathrm{implicit}}$)

```
Input: a colored relational structure $(\mathfrak{X}, \gamma)$ in $\mathcal{C}$, with $\mathfrak{X} := (V, R_1, \dots, R_t)$
Output: $\chi^k_{\mathrm{implicit}}(\mathfrak{X}, \gamma)$          // $\mathrm{Aut}(\mathfrak{X}, \gamma)$-invariant $k$-coloring on $\mathfrak{X}$
  for $\bar{v} := (v_1, \dots, v_k) \in V^k$ do
    set $\chi^{k,0}_{\mathrm{implicit}}(\bar{v})$ to the marked isomorphism type of $\bar{v}$ w.r.t. $\mathcal{C}$
  end for
  set $i := 0$
  repeat
    $i := i + 1$
    for $\bar{v} := (v_1, \dots, v_k) \in V^k$ do
      $\chi^{k,i}_{\mathrm{implicit}}(\bar{v}) := (\chi^{k,i-1}_{\mathrm{implicit}}(\bar{v}), \{\{(\chi^{k,i-1}_{\mathrm{implicit}}(\bar{v}_{1\leftarrow x}), \dots, \chi^{k,i-1}_{\mathrm{implicit}}(\bar{v}_{k\leftarrow x})) \mid x \in V\}\})$
    end for
  until the color class partitions induced on $V^k$ by $\chi^{k,i}_{\mathrm{implicit}}$ and $\chi^{k,i-1}_{\mathrm{implicit}}$ agree
  return $\chi^k_{\mathrm{implicit}}(\mathfrak{X}, \gamma) := \chi^{k,i}_{\mathrm{implicit}}$
```

Let us consider another example, this time using the implicit WL-algorithm on the groups $C_4 \cong \mathbb{Z}/4\mathbb{Z}$ and $V_4 \cong (\mathbb{Z}/2\mathbb{Z})^2$, see Figure 3.4.



V_4

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

C_4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Figure 3.4: The initial color classes computed by 2-$\mathrm{WL}_{\mathrm{implicit}}$ on V_4 and C_4, respectively.

Example 3.2.6. For the 2-dimensional version of $\mathrm{WL}_{\mathrm{implicit}}$, we can use multiplication tables to visualize the color of pairs of group elements. In Figure 3.4, two pairs of group elements, say (g_1, g_2) and (h_1, h_2), obtain the same color, if and only if there exists an isomorphism $\varphi\colon \langle g_1, g_2\rangle \to \langle h_1, h_2\rangle$ with $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. The colors are chosen consistently for both groups, that is, the dark blue cell corresponding to the entry $(0, 2)$ in either of the multiplication tables expresses the fact that there is an isomorphism between the corresponding cyclic subgroups of order 2 in V_4 and C_4, respectively. The coloring also expresses that this subgroup is unique in the case of C_4, while we have a choice in V_4.

If we compare this with the definition of the initial coloring in $\mathrm{WL}_{\mathrm{implicit}}$, we see that the given colorings correspond exactly to the initial coloring of the algorithm. Already in the initial coloring, we can see that the groups are distinguished by 2-$\mathrm{WL}_{\mathrm{implicit}}$, as each group obtains at least one exclusive color. On the other hand, one can easily verify that the depicted color classes are already the orbits of the corresponding automorphism group acting on pairs of group elements. Hence, the color classes are also those of the stable coloring. In agreement with our conventions, the coloring induced by 2-WL$_{\text{implicit}}$ on the group elements (instead of pairs of group elements) can be interpreted as the colors on the (main) diagonals.

By treating $\mathcal{C}$ as a variable, we lose control over the complexity of computing the initial coloring: given two k-tuples over a relational structure, the complexity of deciding whether they are of the same marked isomorphism type may inherently depend on $\mathcal{C}$. In our main application, where $\mathcal{C}$ is the class of finite groups, we can easily derive a polynomial bound.

Lemma 3.2.7. *Let $f(n,k)$ denote the number of elementary operations that are necessary to compute the marked isomorphism type of a k-tuple over any relational structure of ground set size n in an admissible class $\mathcal{C}$. Consider a colored relational structure $(\mathfrak{X},\gamma)$ in $\mathcal{C}$ with $\mathfrak{X} := (V, R_1, \dots, R_t)$. Then the color class partition of $\chi^k_{\mathit{implicit}}(\mathfrak{X},\gamma)$ on V^k can be computed in time*

$$\mathcal{O}\left(f(|V|,k)|V|^k + |V|^{k+1}\log|V|\right),$$

where r_i is the arity of R_i. For $\mathcal{C}$ the class of finite groups, we have $f(n,k) \leq kn$.

Proof. Since Algorithm 3 only differs from Algorithm 2 in terms of the initial coloring, it is sufficient to prove the stated runtime bound for the initial coloring. The claim then follows from Lemma 3.2.1. By definition of f, we can compute the initial coloring for each k-tuple in time $\mathcal{O}(f(|V|,k)|V|^k)$.

If $\mathcal{C}$ is the class of finite groups, then the marked isomorphism type of $(g_1,\dots,g_k)$ can be uniquely described as follows. We start by listing all elements of $\langle g_1,\dots,g_k\rangle$ in lexicographical order with respect to their minimal representation as a word over $g_1,\dots,g_k$, where we fix an ordering $g_1 \leq g_2 \leq \dots \leq g_k$. Such a list, L say, can be computed by the orbit algorithm in time $k|\langle g_1,\dots,g_k\rangle| \leq kn$, where n is the order of the ambient group. Then, the marked isomorphism type is uniquely determined by the triples (i,m,n) such that $L[i]\cdot L[m] = L[n]$ holds, where $i \in [k]$ and $m \in [|L|]$. The number of such triples is bounded by kn. □

Since groups are generated by $\mathcal{O}(\log n)$ elements, when working with groups, we are mostly interested in the k-dimensional WL-algorithm for $k \leq \log n$. Under this assumption, the bound for $f(n,k)$ in the previous Lemma is no more than $n\log n$.

The graph-encoded Weisfeiler-Leman algorithm Instead of running the Weisfeiler-Leman algorithm on relational structures directly, one could also first convert the structure to a graph as described in Definition 3.1 and then run the standard Weisfeiler-Leman algorithm for graphs.

Algorithm 4 Graph-encoded WL-algorithm of dimension k (k-WL$_{\text{graph-encoded}}$)

```
Input: a colored relational structure $(\mathfrak{X},\gamma)$ with $\mathfrak{X} := (V, R_1, \dots, R_t)$
Output: $\chi^k_{\text{graph-encoded}}(\mathfrak{X},\gamma)$          // Aut$(\mathfrak{X},\gamma)$-invariant $k$-coloring on $\mathfrak{X}$
  compute $\Gamma_{\mathfrak{X}}$ (see Definition 3.1), color $V \subseteq V(\Gamma_{\mathfrak{X}})$ according to $\gamma$
  run $k$-WL$_{\text{graph}}$ on $\Gamma_{\mathfrak{X}}$, obtain $\chi^k_{\text{graph}}(\Gamma_{\mathfrak{X}},\gamma)$
  return $\chi^k_{\text{graph}}(\Gamma_{\mathfrak{X}},\gamma)$ restricted to $V^k$
```

Lemma 3.2.8. *Consider a colored relational structure* $(\mathfrak{X}, \gamma)$ *with* $\mathfrak{X} := (V, R_1, \dots, R_t)$ *and arities* r_i *of* R_i. *The color class partition of* $\chi^k_{\textit{graph-encoded}}(\mathfrak{X}, \gamma)$ *on* V^k *can be computed in time*

$$\mathcal{O}\left(\left(|V| + \sum_i r_i |V|^{r_i}\right)^{k+1} \log|V| \sum_i r_i\right).$$

In particular, it is polynomial in $|V|$ *for fixed values of* $r_1, \dots, r_t$, t *and* k.

Proof. This is just the bound for the WL-algorithm on graphs, parameterized by the size of the graph encoding, given in Lemma 3.1.5. □

In either case, the stable colorings computed by a version of the WL-algorithm as introduced above are invariant under color preserving automorphisms, which we discuss in the following lemma.

Lemma 3.2.9. *Consider two colored relational structures* $\mathfrak{X} = (V, R_1, \dots, R_t)$ *and* $\mathfrak{X}^* = (V^*, R_1^*, \dots, R_t^*)$ *with colorings* $\gamma : \mathfrak{X} \to \mathcal{C}$ *and* $\gamma^* : \mathfrak{X}^* \to \mathcal{C}$. *Let* χ *and* χ^* *denote the stable coloring computed by k-WL on* $(\mathfrak{X}, \gamma)$ *and* $(\mathfrak{X}^*, \gamma^*)$, *respectively, where the same version of k-WL (explicit, implicit, or graph-encoded) is used in both cases.*

If $\mathfrak{X}$ *and* $\mathfrak{X}^*$ *are isomorphic as colored relational structures, then there exists an isomorphism* $\varphi \in \operatorname{Iso}((\mathfrak{X}, \gamma), (\mathfrak{X}^*, \gamma^*))$ *such that* $\chi = \chi^* \circ \varphi$ *holds on* V^k. *In particular, the coloring* χ *and its induced color classes are invariant under* $\operatorname{Aut}(\mathfrak{X}, \gamma)$.

Proof. In the case of the graph-encoded WL-algorithm, the claim follows since the analogue claim holds for the usual WL-algorithm on graphs together with the isomorphism invariance of the graph encoding (cf. Lemma 3.1.5).

For the explicit or implicit version of k-WL, consider Algorithm 2 or Algorithm 3, respectively. In either case, the claim is true by definition of colored isomorphism for the initial colorings instead of the stable colorings. Assume that the iterated colorings $\chi^{k,i}(\mathfrak{X}, \gamma)$ and $\chi^{k,i-1}(\mathfrak{X}^*, \gamma^*) \circ \varphi$ in the respective version of k-WL are equal on V^k. Then, for each j and each $x \in V$ we have that

$$\left(\chi^{k,i-1}(\mathfrak{X}, \gamma)\right)(\bar{v}_{j \leftarrow x}) = \left(\chi^{k,i-1}(\mathfrak{X}^*, \gamma^*)\right)(\varphi(\bar{v}_{j \leftarrow x})) = \left(\chi^{k,i-1}(\mathfrak{X}^*, \gamma^*)\right)(\varphi(\bar{v})_{j \leftarrow \varphi(x)})$$

which by definition of the iteration step implies $\chi^{k,i}(\mathfrak{X}, \gamma) = \chi^{k,i}(\mathfrak{X}^*, \gamma^*) \circ \varphi$. The claim follows by induction on i. □

We compare the three different interpretations of the WL-algorithm in the following subsections. First, we need to recall central concepts from the theory of Weisfeiler-Leman algorithms.

Definition 3.2.10. Let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures over the ground sets V and V^*. Fix one version of the Weisfeiler-Leman algorithm discussed above (explicit, implicit, graph-encoded) and call it k-WL. We say $\mathfrak{X}$ is *distinguished* from $\mathfrak{X}^*$ by k-WL, if the multisets of stable colors computed by k-WL on k-tuples over $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$, respectively, are not equal. We say k-WL *identifies* $(\mathfrak{X}, \gamma)$ if it distinguishes $(\mathfrak{X}, \gamma)$ from all other (non-isomorphic) colored relational structures. We write $(\mathfrak{X}, \gamma) \equiv^k_{\text{explicit}} (\mathfrak{X}, \gamma)$ to indicate that $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ are not distinguished by k-WL$_{\text{explicit}}$ (similarly define $\equiv^k_{\text{implicit}}$ and $\equiv^k_{\text{graph-encoded}}$). Furthermore, for $m \leq k$, tuples

$\bar{v} \in V^m$ and $\bar{h} \in (V^*)^m$ are *distinguished* by k-WL if they obtain different colors in the respective m-colorings induced by the stable colorings computed by k-WL on $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$. We extend the symbols $\equiv^k_{\text{explicit}}$, $\equiv^k_{\text{implicit}}$ and $\equiv^k_{\text{graph-encoded}}$ to k-tuples of elements over the respective ground sets in the obvious way.

By the definition of colorings computed by (a version of) the WL-algorithm, eventually each color occurring in the WL-algorithm encodes the complete color distribution. We formalize this in the following observation.

Observation 3.2.11. *If $(\mathfrak{X}, \gamma)$ is distinguished from $(\mathfrak{X}^*, \gamma^*)$ by a version of k-WL, then each stable color occurring in $\mathfrak{X}$ is distinct from each stable color occurring in $\mathfrak{X}^*$.*

3.2.1 Bijective k-pebble games

The distinguishing power of Weisfeiler-Leman algorithms on general relational structures can be characterized via bijective pebble games. This game-theoretic perspective provides a main tool in the context of the present thesis. The characterization closely follows the theory of WL-algorithms on graphs, specifically [24], and the reader familiar with these concepts might want to skip this subsection.

Pebble games for different version of WL: We devise a version of the bijective k-pebble game for each of the versions of k-WL we introduced in the previous subsection.

The k-pebble game is played on a pair of (colored) relational structures $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$, where $\mathfrak{X} = (V, R_1, \dots, R_t)$ and $\mathfrak{X}^* = (V^*, R^*_1, \dots, R^*_t)$ with $|V| = |V^*|$. There are two players, called *Spoiler* and *Duplicator*, and k pairs of pebbles $(p_1, p'_1), \dots, (p_k, p'_k)$ such that pebbles from different pairs can be distinguished. A state of the game is called a *configuration*, denoted by $[(v_1, \dots, v_k), (v^*_1, \dots, v^*_k)]$ with $v_i \in V \uplus \{\bot\}$ and $v^*_i \in V^* \uplus \{\bot\}$. The interpretation is that either $v_i \in V$ and $v^*_i \in V^*$ which means that the pebble p_i is placed on v_i while p'_i is placed on v^*_i, or $v_i = v^*_i =\bot$ and then the i-th pebble pair is currently not on the board. If we do not specify an initial configuration the game starts on the *trivial configuration* $[(\bot, \dots, \bot), (\bot, \dots, \bot)]$. One round of the game consists of the following steps:

1. Spoiler picks up a pebble pair (p_i, p'_i),
2. the winning condition is checked (see below),
3. Duplicator chooses a bijection $f : V \to V^*$,
4. Spoiler places p_i on some $v \in V$ and p'_i on $f(v) \in V^*$.

The winning condition is based on the initial coloring and this is the only difference between the *explicit k-pebble game* and the *implicit k-pebble game*: the pebble pairs apart from (p_i, p'_i) define $(k-1)$-tuples $\widehat{v}$ and $\widehat{v^*}$ over $V \uplus \{\bot\}$ and $V^* \uplus \{\bot\}$, respectively.

Then the winning condition precisely states that Spoiler wins if $\widehat{v}$ and $\widehat{v^*}$ obtain different colors in the initial coloring of $(k-1)$-WL, where the explicit (implicit) version of $(k-1)$-WL corresponds to the explicit (implicit) k-pebble game.

In particular, for Spoiler to win we additionally require that there are no occurrences of $\bot$ in $\widehat{v}$ or $\widehat{v^*}$. If Spoiler does not win, the game continues. We say that Duplicator wins the game if Duplicator has a strategy to keep the game going ad infinitum.

Example 3.2.12. Consider the implicit 3-pebble game on two groups (G, H) with equal orders. We assume that G is non-abelian and H is abelian, and we describe a winning strategy for Spoiler to win the game. The corresponding situations on the board are visualized in Figure 3.5.

1. Spoiler picks up the first pebble pair (blue), and Duplicator chooses a bijection $f\colon G \to H$. By assumption, there is some $g \in G$ that is not contained in $Z(G)$. Spoiler places the pebble pair on $(g, f(g))$.

2. Spoiler picks up the second pebble pair (green), and Duplicator chooses a new bijection $f'\colon G \to H$. If $f'(g) \neq f(g)$ holds, then Spoiler can win immediately, so Duplicator chooses f' with $f'(g) = f(g)$. By assumption, there is some $h \in G$ such that g and h do not commute. Spoiler places the pebble pair on $(h, f'(h))$.

3. Spoiler picks up the third pebble pair (red). Now the winning condition is fulfilled for Spoiler: By choice of g and h, the subgroup $\langle g, h\rangle$ is non-abelian, while $\langle f(g), f'(h)\rangle$ is abelian. The tuples induced by the current pebble pairs on the board thus have different marked isomorphism types. Spoiler wins the game (the winning condition might have been fulfilled earlier, depending on f and f', but it is definitely fulfilled at this point).

Since all Duplicator moves in this run of the game are arbitrary bijections without any restrictions, the steps above describe a winning strategy for Spoiler.

As with graphs, the distinguishing power of k-WL on relational structures can be precisely characterized in terms of winning strategies in the corresponding k-pebble game. In particular, the previous example shows that 2-WL$_{\text{implicit}}$ distinguishes abelian from non-abelian groups.

Lemma 3.2.13. *Let k be at least 2. Consider colored relational structures $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ over ground sets V and V^*, respectively, and fix k-tuples $\bar{v} \in V^k$ and $\bar{v}^* \in (V^*)^k$. Then we have that $\left(\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma)\right)(\bar{v}) = \left(\chi^k_{\text{explicit}}(\mathfrak{X}^*, \gamma^*)\right)(\bar{v}^*)$ if and only if Spoiler has a winning strategy in the configuration $[(v_1, \ldots, v_k, \bot), (v_1^*, \ldots, v_k^*, \bot)]$ in the explicit $(k+1)$-pebble game. In particular, it holds $(\mathfrak{X}, \gamma) \equiv^k_{\text{explicit}} (\mathfrak{X}^*, \gamma^*)$ if and only if Spoiler has a winning strategy in the trivial configuration of the explicit $(k+1)$-pebble game on $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$. The lemma also holds if we replace* explicit *with* implicit *everywhere.*

To present the proof of the previous lemma, which goes back to Cai, Fürer and Immerman (see [24]) in the case of graphs, we first need to introduce another perspective on the Weisfeiler-Leman algorithm.

3.2.2 First order counting logic

In this subsection, we recall the well-known connections between WL-algorithms and descriptive complexity theory. In particular, we provide the logics to capture the explicit and the implicit version of k-WL we introduced above.

Let us briefly recall the central aspects of first order logic. There is a countable set of variables $\{x_1, x_2, \ldots\}$. Formulas are inductively defined so that $x_i = x_j$ is a formula for

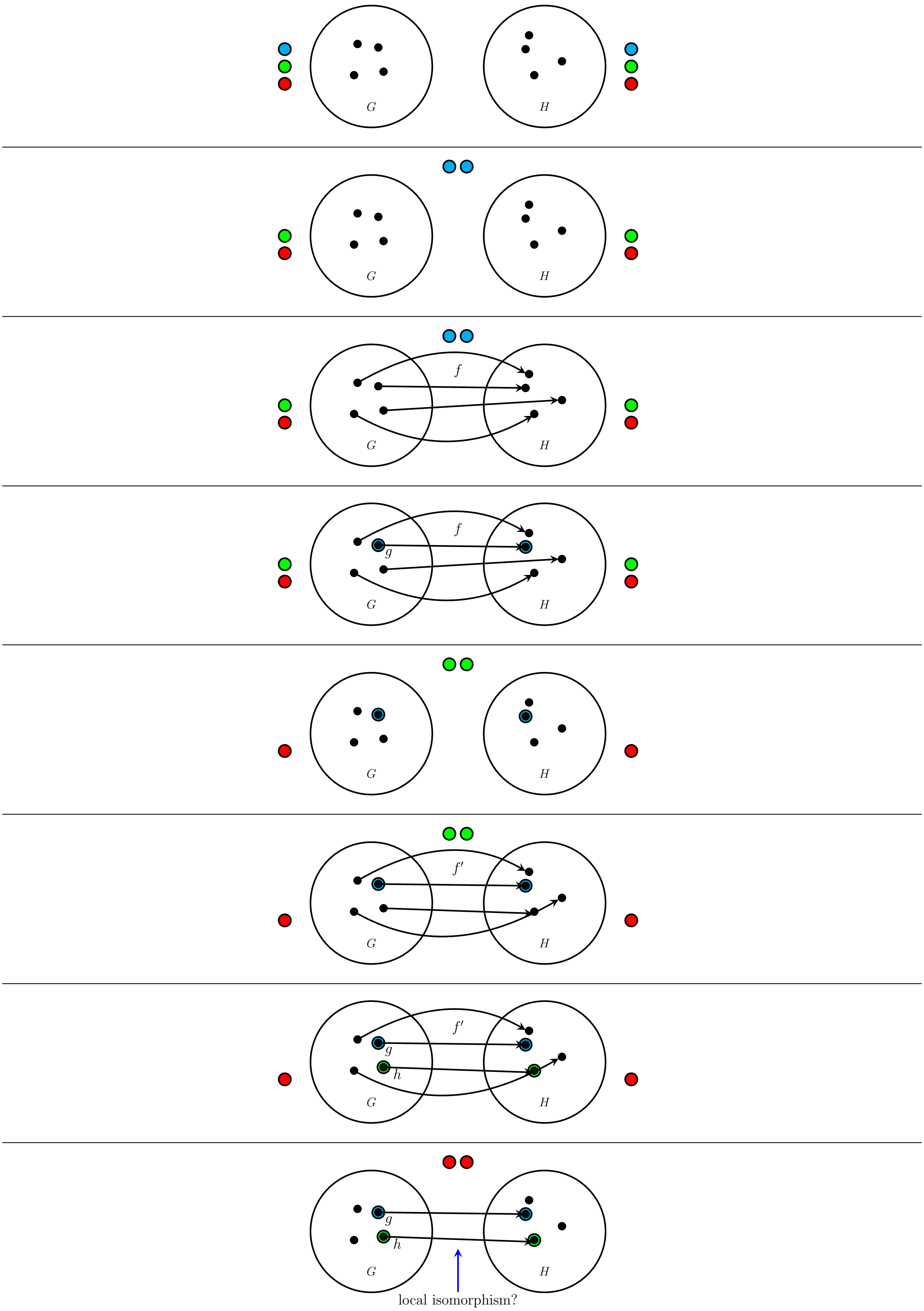


Figure 3.5: A few rounds of the 3-pebble game, see Example 3.2.12.

all pairs of variables and if φ and ψ are formulas then $\varphi \wedge \psi$, $\varphi \vee \psi$,$\neg\varphi$, $\exists x_i\varphi$ and $\forall x_i\varphi$ are formulas. The semantics are defined in the obvious way, so from left to right the symbols are read as *and*, *or*, *not*, *it exists*, and *for all.* First order logic with counting allows additionally formulas of the form $\exists^{\geq t} x_i\varphi(x_i)$ with the semantic meaning that there are at least t distinct elements that satisfy φ. Finally, a sentence in a logic is a formula without quantifiers.

To define logics on relational structures we need to additionally incorporate the given relations and moreover, we need to somehow capture generation of substructures by generating sets.

Explicit: To define a logic on relational structures $\mathfrak{X} = (V, R_1, \ldots, R_t)$ with arities $r_1, \ldots, r_t$, we add the relations R_i for $i \in [t]$ to the logic, with which we can create terms of the form $R_i(x_{j_1}, \ldots, x_{j_{r_i}})$. The semantic interpretation is that $R(x_{j_1}, \ldots, x_{j_{r_i}})$ holds, if and only if $(x_{j_1}, \ldots, x_{j_{r_i}}) \in R_i$ holds. We call $\mathcal{L}_{\text{explicit}}$ the first order logic with counting arising this way and we denote by $\mathcal{L}^k_{\text{explicit}}$ the fragment of $\mathcal{L}_{\text{explicit}}$ which uses at most k variables and relations R_i of maximal arity $k-1$.

Implicit: Let $\mathcal{C}$ be a class of admissible relational structures (so $\mathcal{C}$ is closed under taking intersections of induced substructures). For the logic $\mathcal{L}^{\mathcal{C}}_{\text{implicit}}$ we extend first order counting logic with an additional relation to access substructures via generating sets. First we need to fix a natural number k and an enumeration of marked isomorphism types of k-tuples (with respect to $\mathcal{C}$) over relational structures with arities $r_1, \ldots, r_t$. Denote the enumeration by $(\mathfrak{m}_1, \mathfrak{m}_2, \ldots)$. We introduce relations $R_{\mathfrak{m}_i}(x_1, \ldots, x_k)$ that hold for $x_1, \ldots, x_k \in V(\mathfrak{X})$, if and only if the marked isomorphism type of $(x_1, \ldots, x_k)$ is $\mathfrak{m}_i$. We denote by $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$ the fragment of the logic that uses at most k variables and relations $R_{\mathfrak{m}_i}$ of maximal arity $k-1$.

As such, the logic $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$ is defined by infinitely many relations since there are potentially infinitely many isomorphism types of k-generated $\mathcal{C}$-structures for fixed k. However, we only ever compare the expressiveness of $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$ on $\mathcal{C}$-structures of a fixed size, and then it is sufficient to consider finitely many isomorphism types.

Groups: In the specific case of groups, the well-known word logic provides a more natural choice of logic to capture the implicit Weisfeiler-Leman algorithm. We define $\mathcal{L}_{\text{groups}}$ as the extension of first order logic with counting by relations of the form $R_w(x_1, \ldots, x_t)$, where w is a word over the variables $x_1, \ldots, x_t$ and their formal inverses. The interpretation is that $R_w(x_1, \ldots, x_t)$ is fulfilled by a t-tuple $(g_1, \ldots, g_t)$ of group elements, if and only if $w(g_1, \ldots, g_t) = 1$ holds in G. We let $\mathcal{L}^k_{\text{groups}}$ be the fragment of the logic that uses at most k variables and relations R_w, where w ranges through $k-1$ variable words defined over these k variables and their inverses (we note that the corresponding definition in [17] contains a typo, as it allows for the use of words over k variables, instead of $k-1$).

This logic is equivalent to $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$ for $\mathcal{C}$ the class of groups, as shown in the following lemma. Consequently, we do not distinguish between these logics for groups.

Lemma 3.2.14. *Let $\mathcal{C}$ be the class of groups, let G and G^* be a groups, and let $\bar{g} \in G^k$ and $\bar{g}^* \in G^*$ be fixed k-tuples. Then $\bar{g}$ and $\bar{g}^*$ fulfill the same $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$-sentences, if and only if $\bar{g}$ and $\bar{g}^*$ fulfill the same $\mathcal{L}^k_{\text{groups}}$-sentences.*

Proof. The marked isomorphism type of any tuple of group elements, say $(h_1, \dots, h_{k-1})$ where $h_1, \dots, h_{k-1}$ are chosen from the same parent group, is the isomorphism type of the subgroup generated by $h_1, \dots, h_{k-1}$, relative to this fixed, ordered generating set. In particular, the marked isomorphism type is precisely characterized by the collection of all words w in $k-1$ variables that fulfill $w(h_1, \dots, h_{k-1}) = 1$. Hence, the claim follows by induction over the structure of first order logic. □

The perspective of first order logic provides a bridge between WL-algorithms and bijective pebble games. In the case of the WL-algorithm on graphs, this result is due to Cai, Fürer and Immerman [24]. Their proof easily generalizes to the present setting, we include it for the sake of exposition.

Lemma 3.2.15. *Let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures. Consider k-tuples $\bar{x} := (x_1, \dots, x_k)$ over $V(\mathfrak{X})$ and $\bar{x}^* := (x_1^*, \dots, x_k^*)$ over $V(\mathfrak{X}^*)$. The following are equivalent:*

1. $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma)(\bar{x}) \neq \chi^k_{\text{explicit}}(\mathfrak{X}^*, \gamma^*)(\bar{x}^*)$,
2. $(\mathfrak{X}, x)$ *and* $(\mathfrak{X}^*, x^*)$ *are not equivalent with respect to the logic* $\mathcal{L}^{k+1}_{\text{explicit}}$,
3. *Spoiler has a winning strategy in the explicit* $(k+1)$*-pebble game on* $(\mathfrak{X}, \gamma)$ *and* $(\mathfrak{X}^*, \gamma^*)$*, starting from the configuration* $[(\bar{x}, \perp), (\bar{x}^*, \perp)]$.

If $\mathcal{C}$ is an admissible class of relational structures, then the lemma also holds if we replace every occurrence of explicit *with* implicit *(with respect to $\mathcal{C}$).*

Proof. It suffices to show that the initial coloring of the algorithm, the winning condition of the corresponding game, and the sentences of the corresponding logic all have the same distinguishing power. Since the refinement step of all versions of k-WL defined in this chapter is identical to the refinement step of $\text{WL}_{\text{graphs}}$ (see Algorithm 1), the claim then follows inductively, using the exact same arguments that are used in the proof of [24, Theorem 5.2].

By definition, for two k tuples of vertices, say $v := (v_1, \dots, v_k)$ and $v' := (v_1', \dots, v_k')$ over relational structures $\mathfrak{X}$ and $\mathfrak{X}'$, the configuration $[(v_1, \dots, v_k, \perp), (v_1', \dots, v_k', \perp)]$ fulfills the winning condition for Spoiler in the explicit (implicit) k-pebble game, if and only if v and v' obtain distinct colors in the initial coloring of $\text{WL}_{\text{explicit}}$ ($\text{WL}_{\text{implicit}}$, respectively).

For the implicit version, the latter is equivalent to v and v' having distinct marked isomorphism types, which is in turn equivalent to v and v' fulfilling distinct sentences of the form $R_{\mathfrak{m}_1}(x_1, \dots, x_k)$ from the logic $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$, where $\mathfrak{m}_1$ denotes the isomorphism type of the $\mathcal{C}$-structure generated by v. Due to Lemma 3.2.14, it does not matter here if we use the logic $\mathcal{L}^{\mathcal{C},k}_{\text{implicit}}$ or $\mathcal{L}^k_{\text{groups}}$ when dealing with the class of groups. On the other hand, if there is any relation of the form $R_{\mathfrak{m}'}$ with arity at most k such that v and v' are distinguished by $R_{\mathfrak{m}'}$, then $R_{\mathfrak{m}_1}$ also distinguishes v and v'.

For the explicit version, it is equivalent to the existence of an index set $\{i_1, \dots, i_t\}$, such that $(v_{i_1}, \dots, v_{i_t})$ fulfills the i-th relation of $\mathfrak{X}$, but $(v_{i_1}', \dots, v_{i_t}')$ does not fulfill the i-th relation of $\mathfrak{X}'$ (or $t = 2$ and they differ with respect to the equation $x_{i_1} = x_{i_2}$), which is the case if and only if there is a $\mathcal{L}^k_{\text{explicit}}$-sentence distinguishing v from v', since the sentences of this logic are precisely formed from atoms that check if these relations are fulfilled. □

In particular, the previous lemma proves Lemma 3.2.13 via Observation 3.2.11.

3.2.3 A hierarchy of versions of the Weisfeiler-Leman algorithm

At this point we want to mention a certain dichotomy in the way we approach different versions of the WL-algorithm. On the one hand, we claim, in a sense that will be made precise below, that the details do not really matter. Different versions agree in terms of their distinguishing power, at least up to a constant factor. Thus, in the big picture, we are free to work with the version that is best suited to a specific context or easiest to analyze. On the other hand, each version of the WL-algorithm is natural under a certain point of view. In fact, it is open on which structures different versions have the exact same distinguishing power. Working with several distinct versions enables us to establish new connections between algorithmic problems, ultimately enhancing our understanding of the concept of isomorphism.

We investigate the relation between the explicit, implicit and graph-encoded Weisfeiler-Leman algorithm of varying dimensions. Since the graph encoding of a relational structure is just a straightforward realization of the defining relations in terms of graph gadgets, intuitively the WL-dimension should not increase when going from structures to graphs. We formalize this in the following lemma.

Lemma 3.2.16. *Let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures. Consider m-tuples $\bar{x} = (x_1, \dots, x_m)$ over $\mathfrak{X}$, and $\bar{x}^* = (x_1^*, \dots, x_m^*)$ over $\mathfrak{X}^*$ and let k be a natural number with $k \geq m$. If $\bar{x}$ is distinguished from $\bar{x}^*$ by k-$\mathrm{WL}_{\mathrm{explicit}}$ then $\bar{x}$ is distinguished from $\bar{x}^*$ by $(k+1)$-$\mathrm{WL}_{\mathrm{graph-encoded}}$. In particular, it holds*

$$(\mathfrak{X}, \gamma) \equiv^{k+1}_{\mathrm{graph-encoded}} (\mathfrak{X}^*, \gamma^*) \Longrightarrow (\mathfrak{X}, \gamma) \equiv^{k}_{\mathrm{explicit}} (\mathfrak{X}^*, \gamma^*).$$

Proof. Consider the $(k+1)$-pebble games on $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ that correspond to $\mathrm{WL}_{\mathrm{explicit}}$ and $\mathrm{WL}_{\mathrm{graph-encoded}}$, respectively (so the latter is just the standard k-pebble game on the graphs $\Gamma_{\mathfrak{X}}$ and $\Gamma_{\mathfrak{X}^*}$). In each case, the starting configurations are given by placing pebble pairs on $(x_1, x_1^*), \dots, (x_m, x_m^*)$ and, using Lemma 3.2.13, we assume that Spoiler has a winning strategy in the explicit game. The idea is that Spoiler simulates a winning strategy from the explicit pebble game in the graph-encoded game.

By definition of the graph encoding, gadget-vertices are distinctly colored compared to vertices belonging to $V(\mathfrak{X})$ and $V(\mathfrak{X}^*)$. Thus, if $f : \Gamma_{\mathfrak{X}} \to \Gamma_{\mathfrak{X}^*}$ is a bijection chosen by Duplicator in the game on graphs, then $f(V(\mathfrak{X})) = V(\mathfrak{X}^*)$ holds or otherwise Spoiler can win immediately by definition of the winning condition. So we might assume that f restricts to a bijection $\bar{f} : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$. Then, by assumption, Spoiler has a move in the explicit game that is part of a winning strategy as an answer to $\bar{f}$. In this way Spoiler can copy the winning strategy from the explicit game and use it in the game on graphs while never placing pebbles on gadget vertices. Eventually, a configuration $[(y_1, \dots, y_k), (y_1^*, \dots, y_k^*)]$ with $y_i \in V(\mathfrak{X})$ and $y_i^* \in V(\mathfrak{X}^*)$ is reached that is winning for Spoiler in the explicit game. By definition this means that there is some relation R_i of $\mathfrak{X}$ and the corresponding relation R_i^* of $\mathfrak{X}^*$ such that exactly one of $(y_1, \dots, y_k) \in R_i$ and $(y_1^*, \dots, y_k^*) \in R_i^*$ holds. Without loss of generality, assume that $(y_1^*, \dots, y_k^*) \notin R_i^*$ holds. Then, by definition of the graph encoding, there is a gadget $M_{\mathfrak{X}}$ that is exactly joined with $(y_1, \dots, y_k)$ in $\Gamma_{\mathfrak{X}}$, while no gadget of the same color is exactly joined with

$(y_1^*, \ldots, y_k^*)$ in $\Gamma^*_{\mathfrak{X}}$. Using one additional pebble pair on the gadget $M_{\mathfrak{X}}$, Spoiler can exploit this to win on the graphs as well. □

Spoiler strategies could additionally use gadget vertices to fix several element-vertices (those that are directly attached) at the cost of only one pebble-pair, placed on the corresponding gadget. This compression effect is the key observation to tighten the connections between explicit and graph-encoded WL.

Definition 3.2.17. Let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures. Let $c := [(y_1, \ldots, y_t), (y_1^*, \ldots, y_t^*)]$ be a configuration in the explicit pebble game on $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ and fix a natural number r. A configuration $c' = [(v_1, \ldots, v_m), (v_1^*, \ldots, v_m^*)]$ in the graph-encoded pebble-game is called an *r-compressed version* of c, if the following conditions hold:

1. for each $i \in [m]$, we have that v_i is a gadget-vertex of some gadget M_i in $\Gamma_{\mathfrak{X}}$ and v_i^* is a gadget-vertex of some gadget M_i^* in $\Gamma_{\mathfrak{X}^*}$,
2. for each $j \in [t]$ with $y_j \neq \perp$, we have that there is some $i \in [m]$ and $n \in [r_i]$, such that y_j is connected to the n-th gadget vertex of M_i in $\Gamma_{\mathfrak{X}}$ and y_j^* is connected to the n-th gadget vertex of M_i^* in $\Gamma_{\mathfrak{X}^*}$,
3. it holds $m \leq t/r + 1$.

We say that $\mathfrak{X}$ is *r-compressible*, if for each tuple $(x_1, \ldots, x_r)$ over $V(\mathfrak{X})$, there is some $x_{r+1} \in V(\mathfrak{X})$ and a relation R_i of $\mathfrak{X}$, such that $(x_1, \ldots, x_{r+1}) \in R_i$ holds.

For example, the multiplication relation of a group is 2-compressible, as each pair of group elements, say g and h, define a (unique) third group element x with $x = gh$.

Intuitively, the idea is that each pebble pair in c' covers r distinct pebble pairs in c, through placing pebbles on gadget vertices in an appropriate way. We visualize this for our example above in Figure 3.6.

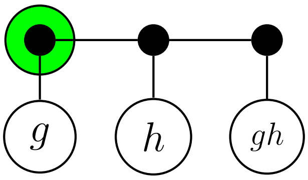


Figure 3.6: A pebble (green) on a gadget vertex (black) implicitly fixes the vertices that are contained in or directly attached to the gadget. In particular, both g and h are fixed simultaneously.

When transferring a winning strategy for Spoiler from the explicit pebble game to the graph-encoded pebble game, we show in the following lemmas that Spoiler can use compressed configurations to reduce the total pebble count.

Lemma 3.2.18. *Let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures. Assume that c is a configuration of the graph-encoded k-pebble game ($k > 2$) on $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$, such that a pebble-pair is placed on (v, v^*) for gadget-vertices v and v^*, belonging to gadgets M and M^*. Let $(x_1, \ldots, x_d)$ and $(x_1^*, \ldots, x_{d^*}^*)$ be the ordered lists of element-vertices* *connected to M and M^*, respectively. If Duplicator chooses a bijection $f : \Gamma_{\mathfrak{X}} \to \Gamma_{\mathfrak{X}^*}$ with $f(x_i) \neq x_i^*$ for some i, then Spoiler can win. In particular this is the case if $d \neq d^*$.*

Proof. We assume that Spoiler has a pebble pair in their hands and without loss of generality, Duplicator chooses a bijection f with $f(x_1) \neq x_1^*$. Then Spoiler places the pebble pair in their hands on $(x_1, f(x_1))$. Since we assume $k > 2$, Spoiler can pick up another pebble pair next, leaving the pebble pairs on $(x_1, f(x_1))$ and (v, v^*), and Duplicator chooses a new bijection f'. By assumption, x_1 is connected to v via a path of gadget vertices that belong to M, spanning from the first gadget vertex to v, while $f(x_1)$ is not connected to v^* by any path that is contained in a single gadget. If f' does not map the first gadget-vertex of M, m_1 say, to the first gadget vertex of M^*, then Spoiler places the pebble pair in their hands on $(m_1, f'(m_1))$ and picks the pebble pair on (v, v^*), resulting in a configuration that fulfills the winning condition (x_1 is connected to m_1 but $f(x_1)$ is not connected to $f'(m_1)$ by assumption). Otherwise, Spoiler places the pebble pair on $(m_1, f'(m_1))$ and picks up the pebble pair on $(x_1, f(x_1))$. The claim follows inductively since the distance between m_1 and v is shorter than the distance between x_1 and v. □

Next, we show that compressed versions of winning configurations provide a winning strategy for Spoiler in the graph-encoded pebble game.

Lemma 3.2.19. *Let $c := [(y_1, \dots, y_t), (y_1^*, \dots, y_t^*)]$ be a configuration in the explicit k-pebble game ($k > t$) on $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$. Let $c' = [(v_1, \dots, v_m), (v_1^*, \dots, v_m^*)]$ be an r-compressed version of c in the graph-encoded k'-pebble game. If c fulfills the winning condition for Spoiler in the explicit k-pebble game, then Spoiler has a winning strategy in the graph-encoded k'-pebble game starting on c', provided that $k' > m + 1$ holds.*

Proof. By Lemma 3.2.18 and the definition of compressed configurations, we may always assume that Duplicator's bijections map y_i to y_i^* for all $i \in [t]$, provided that $k' > m + 1$ holds. But then, in terms of winning strategies, we might as well assume that the pairs (y_i, y_i^*) are actually pebbled in the graph-encoded game. Then Spoiler has a winning strategy according to Lemma 3.2.16, provided that there is one additional pebble pair available in the game, which is guaranteed by assuming $k' > m + 1$. □

We now show how to extend the previous result from configurations in which Spoiler has won to configurations in which Spoiler has a winning strategy. The only restriction is that we need to ensure that compression of configurations is always possible, which is a non-trivial property of the given relational structures.

Lemma 3.2.20. *Let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures. Assume that $\mathfrak{X}$ is r-compressible for a fixed $r \in \mathbb{N}$, that is, for each r-tuple $x = (x_1, \dots, x_r)$ over $\mathfrak{X}$ there is some $x_{r+1} \in V(\mathfrak{X})$ and some relation R_i of $\mathfrak{X}$, such that $(x_1, \dots, x_r, x_{r+1}) \in R_i$ holds. Then we have*

$$(\mathfrak{X}, \gamma) \equiv^{k/r+2}_{\text{graph-encoded}} (\mathfrak{X}^*, \gamma^*) \Longrightarrow (\mathfrak{X}, \gamma) \equiv^{k}_{\text{explicit}} (\mathfrak{X}^*, \gamma^*).$$

Proof. The idea is that the condition on $\mathfrak{X}$ ensures that r-compressions exist for each possible configuration. As before, Spoiler transfers a winning strategy from the explicit pebble game to the graph-encoded pebble game. Let c be a configuration in the explicit

$(k+1)$-pebble game and assume that Spoiler has a winning strategy starting on c by picking up the i-th pebble pair. For each possible Duplicator bijection $f : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$, denote by $S(c, f)$ a new configuration that is reached after Spoiler places the pebble pair in their hands according to a winning strategy. We show the claim $\circledast$: if c' is an r-compressed version of c, then Spoiler can use one additional pebble pair to reach a configuration $S(c, f)'$ that is an r-compressed version of $S(c, f)$. Once we have established $\circledast$, the claim of the lemma follows inductively, where we use Lemma 3.2.19 once c fulfills the winning condition for Spoiler. To prove $\circledast$, assume that Spoiler picks up an additional pebble pair (one that is currently not on the board) in the configuration c' and asks Duplicator for a bijection $f : \Gamma_{\mathfrak{X}} \to \Gamma_{\mathfrak{X}^*}$. Recall that, by definition of the graph encodings, Spoiler can certainly win with one additional pebble-pair if f does not restrict to a bijection $\bar{f} : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$. If it does restrict, there is a configuration $S(c, \bar{f})$ in the explicit pebble game, in which Spoiler has a winning strategy and which differs from c by moving the i-th pebble pair to $(x, \bar{f}(x)) = (x, f(x))$ for an appropriate $x \in V(\mathfrak{X})$. In the graph-encoded game, Spoiler places the pebble pair in their hands on $(x, f(x))$. If the i-th pebble pair was previously not on the board in the explicit pebble game, then, by assumption, Spoiler can pick up another pebble pair in the graph-encoded game that is currently not on the board and place it on a pair of gadgets (m, m^*) such that m is connected to x and m^* is connected to $f(x)$ (such gadgets exists by our assumptions on $\mathfrak{X}$ and Duplicator has to map these gadgets accordingly or otherwise Spoiler can win immediately.) Then Spoiler removes the pebble pair on $(x, f(x))$, reaching a configuration c''.

Now either c'' is an r-compressed version of $S(c, \bar{f})$ or otherwise, the total number of pebbles on the board in c'' is exactly one too high. But then there must be some gadget m_0 of $\Gamma_{\mathfrak{X}}$ and some index j, such that the j-th pebble pair of c'' is placed on (m_0, m_0^*) and m_0 is connected to less than r vertices that are pebbled in c. Let us say the pebbled vertices in configuration c covered by m_0 are $x_1, \ldots, x_d$ with $d < r$, and the corresponding pebbles are placed on $x_1^*, \ldots, x_d^*$. By assumption, there is another pebble pair in the graph-encoded game that is currently not on the board, and Spoiler picks up this pebble pair next. Duplicator provides a new bijection f''. By Lemma 3.2.18, we can assume that $f''(x_i) = x_i^*$ holds for all $i \in [m]$. Similarly, we can assume that $f''(x) = f(x)$ holds, due to the pebble pair on (m, m^*). By our assumptions on $\mathfrak{X}$, there exists some gadget that is connected to $(x_1, \ldots, x_d, x)$ (in this order) in $\Gamma_{\mathfrak{X}}$, say m_1. Spoiler places the pebble pair in their hands on m_1. Now either $f''(m_1)$ is connected to $(x_1^*, \ldots, x_d^*, f(x))$ (in this order), in which case Spoiler successively removes both pebble pairs on (m_0, m_0^*) and $(x, f(x))$, reaching a configuration $S(c, \bar{f})'$ that is an r-compressed version of $S(c, \bar{f})$. Or otherwise, Spoiler can exploit the fact that $f''(m_1)$ is not connected to $(x_1^*, \ldots, x_d^*, f(x))$, to win the game (again, this follows from Lemma 3.2.18). Note that in the latter case, all pebbles that are not placed on m, x or m_0 can be re-used.

Finally, in the case where the i-th pebble pair was previously on the board in configuration c of the explicit game, Spoiler can use an analogous strategy. Note that the i-th pebble pair in c is covered by some gadget in c' and then Spoiler can replace the corresponding gadget because the i-th pebble pair does not need to be covered anymore by any gadget in $S(c, \bar{f})'$. □

We point out that groups are always 2-compressible, where for each $g_1, g_2 \in G$ we have a (unique) product $g_1 g_2 \in G$.

In the other direction it is also possible to capture the graph-encoded game in terms of the explicit game. We also have to account for possible compression here.

Lemma 3.2.21. *Let $(\mathfrak{X},\gamma)$ and $(\mathfrak{X}^*,\gamma^*)$ be colored relational structures. Let r be the maximal arity of $\mathfrak{X}$. Then we have*

$$(\mathfrak{X},\gamma) \equiv^k_{\text{explicit}} (\mathfrak{X}^*,\gamma^*) \Longrightarrow (\mathfrak{X},\gamma) \equiv^{(k-1)/r}_{\text{graph-encoded}} (\mathfrak{X}^*,\gamma^*).$$

Proof. We basically invert the strategy from the previous proof: Spoiler simulates a winning strategy from the graph-encoded k-pebble game in the $(rk+1)$-pebble game on $(\mathfrak{X},\gamma)$ and $(\mathfrak{X}^*,\gamma^*)$.

Assume there is a configuration c in the k-pebble game on $\Gamma_{\mathfrak{X}}$ and $\Gamma^*_{\mathfrak{X}}$ in which Spoiler has a winning strategy. A configuration c' in the explicit $(rk+1)$-pebble game is a *decompressed version* of c if the following holds: For each pebble pair that is placed on element-vertices (v,v^*) in c, there is a pebble pair on (v,v^*) in c' and for each pebble pair that is placed on gadget-vertices (M,M^*) in c, assume that there are pebble pairs on $(x_1,x_1^*),\dots,(x_t,x_t^*)$, where M is exactly connected with $(x_1,\dots,x_t)$ (in this order) and M^* is exactly connected with $(x_1^*,\dots,x_t^*)$ (in this order). In the following we write $M = M(x_1,\dots,x_t)$ to express the relation between the gadget M and the ground set vertices it connects to.

By our assumption on the maximal arity of $\mathfrak{X}$, we have that $t \le r$ holds, so if the number of pebble pairs involved in c is T, then c' can be specified with at most rT pebble pairs.

We now simulate r rounds of the explicit pebble-game, without actually changing the configuration. We think of Duplicator's strategy as being pre-computable by Spoiler due to the deterministic nature of the game. If c' is a decompressed version of c, assume Spoiler picks up an additional pebble pair in the explicit pebble game that is not used in configuration c'. Duplicator chooses a new bijection $f_{i_1} : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$. for each $x \in V(\mathfrak{X})$, there is a follow-up move by Duplicator, after Spoiler places the pebble pair in their hands on $(x, f_{i_1}(x))$ and picks up the i_2-th pebble pair next. Call the corresponding follow-up move by Duplicator $f_{i_2}^{(x)}$. We iterate the argument for another $r-1$ rounds and thus we obtain a bijection $F^{(s)}$ for each $1 \le s \le r$ as follows:

$$F^{(s)} : V(\mathfrak{X})^s \to V(\mathfrak{X}^*)^s, (x_1,\dots,x_s) \mapsto (f_{i_1}(x_1), f_{i_2}^{(x_1)}(x_2),\dots, f_{i_s}^{(x_1,\dots,x_{s-1})}(x_s)).$$

We can patch these bijections together to obtain a bijection $F : \Gamma_{\mathfrak{X}} \to \Gamma_{\mathfrak{X}^*}$, by mapping each gadget $M(x_1,\dots,x_s)$ to $M(F(x_1,\dots,x_s))$ and mapping element-vertices according to f_{i_1}. Starting from configuration c, Spoiler has a winning strategy in the graph-encoded pebble game, by picking up the i-th pebble pair from $(M(y_1,\dots,y_\ell), M(y_1^*,\dots,y_\ell^*))$ say. According to this winning strategy, Spoiler would answers the Duplicator move F by placing the pebble pair in their hands on $(M(x_1,\dots,x_s), M(F(x_1,\dots,x_s)))$ say, reaching a new configuration c_1 (if Spoiler chooses to place the pebble pair on element-vertices, Spoiler can directly copy this move in the explicit game and reach a decompressed version of c_1 immediately). In the explicit game, Spoiler places the pebble pair on $(x_1, f_{i_1}(x_1))$ and asks Duplicator for a new bijection. Since all the bijections $f_{i_j}^{(x_1,\dots,x_j)}$ where chosen according to a strategy Duplicator would be willing to play in the explicit pebble game, we can assume without loss of generality that Duplicator actually picks these bijections, provided Spoiler places the subsequent pebble pairs on $x_1, x_2, \ldots, x_s$ (from a game theory perspective, by definition this does not change the fact that Duplicator has or does not have a winning strategy in the subsequent configuration). But then Spoiler eventually reaches a configuration c_1' with additional pebble pairs on $(x_s, f_{i_j}^{(x_1,\ldots,x_{j-1})}(x_j)$ for all $j \in [s]$. We note that the pebble pairs that where used in c' to cover the i-th pebble pair on $(M(y_1, \ldots, y_\ell), M(y_1^*, \ldots, y_\ell^*))$ in configuration c can be re-used if they do not appear in other pebbled gadgets in the configuration c. Thus, the total amount of pebbles necessary to carry out the strategy is still bounded by $rk + 1$ and c_1' is a decompressed version of c_1. By definition of the graph encoding, if c_1 fulfills the winning condition of the graph-encoded game then c_1' fulfills the winning condition of the explicit game. Thus, the claim follows by induction. □

In the next step, we compare the explicit version of WL to the implicit version.

Lemma 3.2.22. *Let $\mathcal{C}$ be an admissible class of relational structures and let $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ be colored relational structures in $\mathcal{C}$. Consider k-tuples $\bar{x} := (x_1, \ldots, x_k)$ over $V(\mathfrak{X})$ and $\bar{x}^* := (x_1^*, \ldots, x_k^*)$ over $V(\mathfrak{X}^*)$.*

1. *If $\left(\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma)\right)(\bar{x}) \neq \left(\chi^k_{\text{explicit}}(\mathfrak{X}^*, \gamma^*)\right)(\bar{x}^*)$ holds, then we also have*

$$\left(\chi^{\mathcal{C},k}_{\text{implicit}}(\mathfrak{X}, \gamma)\right)(\bar{x}) \neq \left(\chi^{\mathcal{C},k}_{\text{implicit}}(\mathfrak{X}^*, \gamma^*)\right)(\bar{x}^*).$$

2. *Assume that there exists a constant $d = d(\mathcal{C})$, such that $(k + d)$-WL$_{\text{explicit}}$ distinguishes any two k-tuples of distinct marked isomorphism types (with respect to $\mathcal{C}$). If $\left(\chi^{\mathcal{C},k}_{\text{implicit}}(\mathfrak{X}, \gamma)\right)(\bar{x}) \neq \left(\chi^{\mathcal{C},k}_{\text{implicit}}(\mathfrak{X}^*, \gamma^*)\right)(\bar{x}^*)$ holds, then we also have $\left(\chi^{k+d}_{\text{explicit}}(\mathfrak{X}, \gamma)\right)(\bar{x}) \neq \left(\chi^{k+d}_{\text{explicit}}(\mathfrak{X}^*, \gamma^*)\right)(\bar{x}^*)$.*

Proof. We use the correspondence between pebble games and the WL-algorithm from Lemma 3.2.13. Regarding both claims of the present lemma, the idea is that Spoiler can copy a winning strategy of the explicit $(k+1)$-pebble game (implicit $(k+1)$-pebble game) game and use it in the implicit $(k+1)$-pebble game (explicit $(k+d+1)$-pebble game). We have to argue that, given a configuration that fulfills the winning condition for Spoiler in the original game, Spoiler has a winning strategy in the other game, starting from this configuration.

1. By the definition of marked isomorphism types, every winning configuration for Spoiler in the explicit $(k + 1)$-pebble game is also a winning configuration in the implicit $(k + 1)$-pebble game.

2. If a configuration c fulfills the winning condition for Spoiler in the implicit $(k + 1)$-pebble game, then the k-tuples corresponding to c have different marked isomorphism types. So by assumption, they are distinguishable by $(k + d)$-WL$_{\text{explicit}}$ and using Lemma 3.2.13 once more, we see that Spoiler has a winning strategy in the explicit $(k + d + 1)$-pebble game, starting from configuration c. □

In particular, for groups we can take $d = 1$ as shown in the next lemma.

Lemma 3.2.23. *Consider the k-pebble game on a pair of groups (G, H), where we assume $k \geq 4$ for the* explicit *version and $k \geq 3$ for the* implicit *version. Assume pebble pairs are placed on $(g_1, h_1), \dots, (g_n, h_n)$ where $g_i \in G$, $h_i \in H$ and $0 \leq n \leq k-2$. If Duplicator chooses a bijection $f : G \to H$ such that*

$$f(w(g_1, \dots, g_n)) \neq w(h_1, \dots, h_n)$$

holds for some word w (allowing inverses), then Spoiler has a winning strategy. (In the case $n = 0$ we still require $f(1) = 1$).

Proof. By definition of the pebble game, Duplicator chooses the bijection f in Step 2 of the current round and Spoiler previously picked up a pebble pair in Step 1. Set $w_G := w(g_1, \dots, g_n)$ and $w_H := w(h_1, \dots, h_n)$. In the implicit k-pebble game, Spoiler wins immediately by placing the pebble pair in their hands on $(w_G, f(w_G))$ and then picking up any pebble pair that is currently not on the board (such a pebble pair exists since $n \leq k-2$). Then the respective pebbled tuples in G and H have different marked isomorphism types by assumption. So let us consider the explicit k-pebble game.

If $n = 0$, then $w_G = w_H = 1$ and we have $f(w_G) \neq w_H = 1$ by assumption, so Spoiler wins by pebbling $(w_G, f(w_G))$ and then picking up any other pebble pair. Since $f(w_G)^2 \neq f(w_G)$ but $w_H^2 = w_H$ hold, the resulting configuration is winning for Spoiler.

If $n > 0$, Spoiler places the pebble pair in their hands on $(w_G, f(w_G))$ and picks up a pebble pair that is currently not on the board. Duplicator then chooses a new bijection $f_1 : G \to H$, and without loss of generality, we may assume that f_1 maps pebbled group elements according to the pebbles on the board (otherwise we arrive in the $n = 0$ case again). Now either there is some word $w'(x_1, \dots, x_n)$ with $|w'| < |w|$ and $f_1(w'(g_1, \dots, g_n)) \neq w'(h_1, \dots, h_n)$ or otherwise we can write $w_G = w'(g_1, \dots, g_n)g_i$ for some i, such that $|w'| = |w_G| - 1$ and $f(w'(g_1, \dots, g_n)) = w'(h_1, \dots, h_n)$. In the first case, Spoiler places the pebble pair in their hands on $(w'(g_1, \dots, g_n), f_1(w'(g_1, \dots, g_n)))$ and picks up the pebble pair on $(w_G, f(w_G))$. In this case we iterate the argument. In the second case, since $k \geq 4$, up to permuting pebble pairs, Spoiler can reach the configuration

$$[(g_i, w'(g_1, \dots, g_n), w_G, \perp, \dots, \perp), (h_i, w'(h_1, \dots, h_n), f(w_G), \perp, \dots, \perp)]$$

which fulfills the winning condition by construction of w'. Since the first case can only occur finitely many times, the Lemma follows. □

Corollary 3.2.24. *Let $\mathcal{C}$ be the class of finite groups. Then $(k+1)$-WL$_{\text{explicit}}$ distinguishes any two k-tuples (defined over any pair of groups) of distinct marked isomorphism types.*

In conclusion, we have proved the following theorem, constructing a hierarchy of versions of the Weisfeiler-Leman algorithm. If $\mathcal{A}$ and $\mathcal{B}$ denote specific versions and dimensions of the WL-algorithm, let us use the notation $\mathcal{A} \preceq \mathcal{B}$ to express that the distinguishing power of $\mathcal{A}$ is less than or equal to that of $\mathcal{B}$.

Theorem 3.2.25. *The following relations hold between different versions of k-WL:*

1. *Let $\mathcal{C}$ be an admissible class of relational structures, and assume that there exists a constant $d = d(\mathcal{C})$, such that $(k+d)$-WL$_{\text{explicit}}$ distinguishes any two k-tuples of distinct marked isomorphism types (with respect to $\mathcal{C}$). Then it holds*

$$k\text{-WL}_{\text{explicit}} \preceq k\text{-WL}^{\mathcal{C}}_{\text{implicit}} \preceq (k+d)\text{-WL}_{\text{explicit}}.$$

2. *Let $\mathcal{C}$ be a class of relational structures that is r-compressible for some $r \in \mathbb{N}$. Then, over the class $\mathcal{C}$, it holds*

$$k\text{-WL}_{\text{explicit}} \preceq (k/r+2)\text{-WL}_{\text{graph}-\text{encoded}} \preceq (k+2r+1)\text{-WL}_{\text{explicit}}.$$

3. *Over the class of finite groups it holds*

$$k\text{-WL}_{\text{explicit}} \preceq k\text{-WL}_{\text{implicit}} \preceq (k/2+2)\text{-WL}_{\text{graph}-\text{encoded}} \preceq (k+5)\text{-WL}_{\text{explicit}}.$$

Moreover, the constant d from Part 1) is at most 1 *for groups.*

3.2.4 Induced colorings & refinements

We collect some basic observations on induced colorings. The first lemma is well-known in the setting of graphs (or more generally for cellular algebras, see [37, Theorem 6.1]).

Lemma 3.2.26. *Let χ^k denote the stable coloring of a version of k-WL, either* explicit *or* implicit*. Consider colored relational structures $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ with $v_i \in V(\mathfrak{X})$ and $v_i^* \in V(\mathfrak{X}^*)$ for $i \in [k]$. Assume that k is at least* 2 *and let $\pi \in S_k$. It holds that*

1. $\chi^k(\mathfrak{X}, \gamma)(v_1 \dots, v_k) = \chi^k(\mathfrak{X}^*, \gamma^*)(v_1^*, \dots, v_k^*) \iff$
   $\chi^k(\mathfrak{X}, \gamma)(v_{\pi(1)} \dots, v_{\pi(k)}) = \chi^k(\mathfrak{X}^*, \gamma^*)(v_{\pi(1)}^*, \dots, v_{\pi(k)}^*)$,
2. $\forall i \in [k] : \big(\chi^k(\mathfrak{X}, \gamma)(v_1 \dots, v_k) = \chi^k(\mathfrak{X}^*, \gamma^*)(v_1^*, \dots, v_k^*) \implies$
   $\chi^k(\mathfrak{X}, \gamma)(v_i) = \chi^k(\mathfrak{X}^*, \gamma^*)(v_i^*)\big)$.

Proof. Regarding Part 1), by definition the color classes induced by the respective initial coloring, and then inductively each refined coloring, are invariant under permuting entries.

Regarding Part 2), if Spoiler has a winning strategy in the corresponding pebble game, starting with a pebble pair on (v_i, v_i^*), then Spoiler has a winning strategy in every configuration that includes a pebble pair on (v_i, v_i^*). The claim follows from Lemma 3.2.13. □

Lemma 3.2.27. *Let χ^k denote the stable coloring of the* explicit *or* implicit *version of k-WL. Consider colored relational structures $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$ with $x \in V(\mathfrak{X})$ and $x^* \in V(\mathfrak{X}^*)$. Assume that there is some k-tuple $t \in V(\mathfrak{X})^k$ with i-th entry $t_i = x$, such that for each $t^* \in V(\mathfrak{X}^*)^k$ with $t_i^* = x^*$ it holds that $\chi^k(\mathfrak{X}, \gamma)(t) \neq \chi^k(\mathfrak{X}^*, \gamma^*)(t^*)$. Then it follows $\chi^k(x) \neq \chi^k(x^*)$.*

Proof. We argue via Lemma 3.2.13, i.e., we show that Spoiler has a winning strategy in the corresponding $(k+1)$-pebble game where the initial configuration is given by $[(x, \perp, \dots, \perp), (x^*, \perp, \dots, \perp)]$. First, Spoiler picks up the i-th pebble pair. Duplicator's bijection has to map x to x^* due to the initial configuration or otherwise Spoiler wins immediately. Spoiler places the i-th pebble pair on (x, x^*). Independent of Duplicators next moves, Spoiler can subsequently pebble the entries of t resulting in a configuration $[(t, \perp), (t', \perp)]$ for some tuple $t' \in H^k$ with $t'_i = x^*$. For any such t', the resulting configuration is winning for Spoiler by assumption. □

Definition 3.2.28. Given a relational structure $\mathfrak{X}$, a coloring $\gamma_2 : V(\mathfrak{X})^k \to \mathcal{C}_2$ *refines* a coloring $\gamma_1 : V(\mathfrak{X})^k \to \mathcal{C}_1$, denoted $\gamma_2 \leq \gamma_1$, if each γ_1-color class in $V(\mathfrak{X})^k$ is a union of γ_2-color classes.

Lemma 3.2.29. *Let γ_1 and γ_2 be element colorings on a relational structure $\mathfrak{X}$ such that*

$$\left(\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1)\right) \leq \gamma_2 \leq \gamma_1$$

holds. Then $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1)$ and $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_2)$ induce the same color classes on $V(\mathfrak{X})^k$.

Proof. Fix k-tuples $\bar{g}, \bar{h} \in V(\mathfrak{X})^k$. Since $\gamma_2 \leq \gamma_1$ holds, we also have $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_2) \leq \chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1)$. Assume the initial coloring fulfills $\chi^{k,0}_{\text{explicit}}(\mathfrak{X}, \gamma_2)(\bar{g}) \neq \chi^{k,0}_{\text{explicit}}(\mathfrak{X}, \gamma_2)(\bar{h})$, then $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1)(\bar{g}) \neq \chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1)(\bar{h})$ by Lemma 3.2.26 together with the assumption $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1) \leq \gamma_2$. So for some i we have $\chi^{k,i}_{\text{explicit}}(\mathfrak{X}, \gamma_1) \leq \chi^{k,0}_{\text{explicit}}(\mathfrak{X}, \gamma_2)$ and therefore we obtain $\chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_1) \leq \chi^k_{\text{explicit}}(\mathfrak{X}, \gamma_2)$. □

Intuitively, the previous lemma says that a coloring which is coarser than the stable WL-coloring can never lead to a finer stable WL-coloring if used as an additional input to WL. Or in other words, in terms of the distinguishing power, we may as well assume that all the information computed by the WL-algorithm is already given in advance, as a coloring of the input structure. We use this interpretation of the previous lemma to simplify several proofs below.

3.3 Subset selectors

We introduce the notion of *subset selectors* to formally compare substructures in distinct relational structures in terms of the colors they obtain during the Weisfeiler-Leman algorithm.

Ultimately, we want to define what it means for some subset of an input structure to be *detectable* by the WL-algorithm. The first property we need is that detectable subsets are unions of stable color classes. The elements of a stable color class are not distinguished among each other, but the fact that they form a color class means that the WL-algorithm structurally distinguishes them from all other elements. Our definition of detectability is slightly more restrictive. We additionally ensure that the structural reasons that distinguish a set of elements into color classes are consistent over all possible input structures, in the following precise sense.

Definition 3.3.1. A *subset selector $\mathcal{S}$* associates with each colored relational structure $(\mathfrak{X}, \gamma)$ a subset $\mathcal{S}(\mathfrak{X}, \gamma) \subseteq V(\mathfrak{X})$. A subset selector $\mathcal{S}$ is called k-WL$_{\text{explicit}}$-*detectable* (or k-WL$_{\text{implicit}}$-*detectable*, respectively), if

$$\chi^k(\mathfrak{X}, \gamma)(\mathcal{S}(\mathfrak{X}, \gamma)) \cap \chi^k(\mathfrak{X}^*, \gamma^*)(V(\mathfrak{X}^*) \setminus \mathcal{S}(\mathfrak{X}^*, \gamma^*)) = \emptyset$$

holds for all pairs of colored relational structures $(\mathfrak{X}, \gamma)$ and $(\mathfrak{X}^*, \gamma^*)$, where χ^k denotes the stable coloring of the respective version of k-WL. To simplify notation, in the following we simply say that $\mathcal{S}(\mathfrak{X}, \gamma)$ is WL-detectable instead of saying that $(\mathfrak{X}, \gamma) \mapsto \mathcal{S}(\mathfrak{X}, \gamma)$ is.

We can naturally consider subset selectors over subclasses of relational structures, for example the class of finite groups, by associating the empty set to each relational structure that is not a group. Then, examples of 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable subset selectors include the association of every group with its center or the subset selector associating with each group the subset of elements of order 2 (we formally prove this later).

We should remark that in our sense, being *detectable* means that the subset of interest is a union of stable color classes of the respective Weisfeiler-Leman algorithm, but we make no statement on how to algorithmically determine which color classes form the set. It might a priori not be clear that the subset is even computable.

The following lemma follows immediately from the definition of a subset selector.

Lemma 3.3.2. *If $\mathcal{S}$ is a k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable subset selector, then, for each colored relational structure $(\mathfrak{X}, \gamma)$, we have that $\mathcal{S}(\mathfrak{X}, \gamma)$ is a union of $\chi^k_{\mathrm{explicit}}(\mathfrak{X}, \gamma)$-color classes, and hence $\mathrm{Aut}_\gamma(\mathfrak{X})$-invariant. If $\mathcal{S}$ and $\mathcal{T}$ are k-WL_{explicit}-detectable, so are their union and intersection in $V(\mathfrak{X})$, as well as $V(\mathfrak{X}) \setminus \mathcal{S}(\mathfrak{X}, \gamma)$. All statements remain true after replacing* explicit *with* implicit *everywhere.*

3.4 Restricting strategies in the bijective pebble game

We point out certain general situations, in which detectable substructures can be used to restrict strategies in the k-pebble game.

In the first instance, we show that Spoiler can "trade off" one pebble pair to enforce that Duplicator's bijections are simultaneously compatible with detectable substructures.

Definition 3.4.1. Let M be a set and $\mathcal{P}$ a partition of M. Let $\sim_{\mathcal{P}}$ denote the equivalence relation on M corresponding to $\mathcal{P}$. We call $\mathcal{P}$ an *equipartition*, if there is a constant m such each partition class of $\mathcal{P}$ on M is of cardinality m. Given a sequence $\mathcal{P}_1, \dots, \mathcal{P}_n$ of partitions of M, we call it a *nested sequence of partitions* if for all $i \in [n-1]$ it holds that each partition class of $\mathcal{P}_i$ is partitioned by partition classes of $\mathcal{P}_{i+1}$.

Example 3.4.2. To provide some context for the previous definition, consider a finite group G and a subgroup $U \leq G$. Then the coset space G/U of cosets of U in G forms an equipartition of G. If $U_1 \leq \cdots \leq U_n$ is a sequence of subgroups of G, then the sequence of coset spaces $G/U_1, \dots, G/U_n$ forms a nested sequence of equipartitions of G.

Similarly to subset selectors, we can also define *partition selectors*, that associate a partition of the ground set to any (colored) relational structure. Consequently, we say that a partition selector $\mathcal{P}$ is *k-WL-detectable* (for a fixed of version of k-WL as introduced above), if k-WL distinguishes pairs of elements that are equivalent with respect to $\sim_{\mathcal{P}}$ from pairs of non-equivalent elements.

We introduce a combinatorial tool that is attributed to van der Waerden, Sperner and König in [90] (see [90], Theorem 6.2 and below).

Lemma 3.4.3. *Let $f : A \to B$ be a bijection of finite sets and let $P := \{A_1, \dots, A_t\}$ and $Q := \{B_1, \dots, B_t\}$ be equipartitions of A and B, i.e., $m := |A_i| = |B_j|$ for all i, j. Then there exist m full systems of representatives $R_1, \dots, R_m$ of A modulo P such that $A = \biguplus_{i=1}^m R_i$ and for all i, $f(R_i)$ is a system of representatives modulo Q. In particular, for each i, $f|_{R_i}$ induces a bijection $P \to Q$.*

Proof. The claim follows by interpreting f as a bipartite graph on $(A \cup B)$ with edges given by all pairs $(a, f(a))$ and repeatedly applying Hall's matching theorem. □

Lemma 3.4.4. *Fix a version of the WL algorithm and the corresponding bijective pebble game (*explicit *or* implicit*), as well as an integer $k \geq 3$. Consider relational structures $\mathfrak{X}$ and $\mathfrak{X}^*$ with $\mathfrak{X} \equiv^k \mathfrak{X}^*$, so Duplicator has a winning strategy in the $(k+1)$-pebble game. Assume that $(\mathcal{P}_i)_{i\in[s]}$ and $(\mathcal{P}_i^*)_{i\in[s]}$ are sequences of nested, k-WL-detectable equipartitions of $V(\mathfrak{X})$ and $V(\mathfrak{X}^*)$, respectively, such that the stable colors of $\sim_{\mathcal{P}_i}$-equivalent pairs in $\mathfrak{X}$ correspond to stable colors of $\sim_{\mathcal{P}_i^*}$-equivalent pairs in $\mathfrak{X}^*$. Then Duplicator has a winning strategy in the k-pebble game on $(\mathfrak{X}, \mathfrak{X}^*)$, such that each bijection $f : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$ chosen by Duplicator's strategy fulfills the following condition:*

$$\circledast \ \forall x, y \in V(\mathfrak{X}) \ \forall i : x \sim_{\mathcal{P}_i} y \Leftrightarrow f(x) \sim_{\mathcal{P}_i^*} f(y).$$

In other words, for each i, f maps partition classes of $\mathcal{P}_i$ to partition classes of $\mathcal{P}_i^*$.

Proof. Consider a configuration $c := [(x_1, \dots, x_k), (x_1^*, \dots, x_k^*)]$ in the k-pebble game and assume that Duplicator has a winning strategy in this configuration, even in the $(k+1)$-pebble game.

Claim 1: For all $1 \leq j \leq k$ there is a bijection $F^{(j)} : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$ with the following properties:

1. after Spoiler picks up the j-th pebble pair in configuration c, Duplicator can play $F^{(j)}$ as a winning move in the $(k+1)$-pebble game.
2. $\forall i \in [s] : F^{(j)}(\mathcal{P}_i) = \mathcal{P}_i^*$.

We show Claim 1 by induction on s. The case $s = 1$ follows in analogy to the induction step. Thus assume that, after Spoiler picks up the j-th pebble pair, Duplicator has a winning move $f : G \to H$ in the $(k+1)$-pebble game such that for some fixed i_0 it holds that

$$\forall i \leq i_0 : f(\mathcal{P}_i) = \mathcal{P}_i^*.$$

We construct a new bijection $F : G \to H$ that satisfies the desired properties from Claim 1 for all $i \leq i_0 + 1$. By Lemma 3.4.3, there is a system of representatives R of the partition classes of $\mathcal{P}_{i_0+1}$, such that $f(R)$ is a set of representatives of the partition classes of $\mathcal{P}_{i_0+1}^*$. For $x \in V(\mathfrak{X})$, let $r_x \in R$ denote the representative of x. In the $(k+1)$-pebble game, Spoiler could place the j-th pebble pair on $(r_x, f(r_x))$ and then pick up the $(k+1)$-th pebble pair. In this case, since f is a winning move for Duplicator, there exists a subsequent winning move $f_x : V(\mathfrak{X}) \to V(\mathfrak{X}^*)$ for Duplicator. We set $F(x) := f_x(x)$. By construction, f_x only depends on the fixed representative r_x, so $f_x = f_{r_x}$ holds for all $x \in V(\mathfrak{X})$.

Intuitively, Spoiler hypothetically marks the partition class of x in $\mathcal{P}_{i_0+1}$ with an extra pebble pair and then f_x demonstrates how this coset should be mapped as a whole. The proof will now show that piecing together the different maps for all the choices of x gives a global bijection F with the desired properties. We denote the partition class of x in $\mathcal{P}_i$ with $\mathcal{P}_i(x)$.

F **is bijective:** Since the partition class of x is k-WL-detectable as long as a pebble is placed on x, and since for all choices of x, the bijection f_x is a winning move for Duplicator, it holds that $f_x(\mathcal{P}_i(x)) = \mathcal{P}^*_i(f_x(x))$ for all $i \in [s]$. In particular, for all $x \in V(\mathfrak{X})$ it holds that $f_{r_x}(\mathcal{P}_{i_0+1}(r_x)) = \mathcal{P}^*_{i_0+1}(f_{r_x}(r_x)) = \mathcal{P}^*_{i_0+1}(f(r_x))$. By construction of F, for all $x \in V(\mathfrak{X})$ it holds that $F(\mathcal{P}_{i_0+1}(x)) = f_{r_x}(\mathcal{P}_{i_0+1}(r_x))$. Using the definition of R, we note that $r_x \neq r_y$ implies $\mathcal{P}^*_{i_0+1}(f(r_x)) \cap \mathcal{P}^*_{i_0+1}(f(r_y)) = \emptyset$. Altogether this implies

$$F(V(\mathfrak{X})) = \bigcup_{x\in V(\mathfrak{X})} F(\mathcal{P}_{i_0+1}(x)) = \bigcup_{x\in V(\mathfrak{X})} f_{r_x}(\mathcal{P}_{i_0+1}(r_x)) = \bigcup_{x\in V(\mathfrak{X})} \mathcal{P}^*_{i_0+1}(f(r_x)) = V(\mathfrak{X}^*),$$

hence F is surjective and then also bijective.

F **respects cosets:** Using the same arguments as in the bijectivity proof, together with the assertion $\forall i \leq i_0 : f(\mathcal{P}_i) = \mathcal{P}^*_i$ from the induction hypothesis, we obtain

$$F(\mathcal{P}_i(x)) = \bigcup_{y\in\mathcal{P}_i(x)} \mathcal{P}^*_{i_0+1}(f(r_y)) = \mathcal{P}^*_i(F(x))$$

for all $x \in G$ and for all $i \leq i_0 + 1$.

F **is a winning move for Duplicator:** Consider configurations of the form

$$[(x_1, \dots, x_{j-1}, x, x_{j+1}, \dots, x_k), (x^*_1, \dots, x^*_{j-1}, F(x), x^*_{j+1}, \dots, x^*_k))]$$

with $x \in V(\mathfrak{X})$. By construction, $F(x) = f_x(x)$ where f_x is a winning move for Duplicator (even with $(k + 1)$ pebble pairs) from which the configuration above is reachable for Spoiler. Thus, in all configurations reachable from c via F, Duplicator has a winning strategy. This proves Claim 1. ◀

By Lemma 3.2.13, Duplicator has a winning strategy in the k-pebble game on the empty configuration and by Claim 1, Duplicator can always choose bijections according to condition ⊛. □

In the second instance, our technique is specific to structures that admit a well-defined multiplication of some kind. In the context of this thesis, we formulate this just for groups.

Consider the pebble game on a group G with a detectable normal subgroup $N \trianglelefteq G$. When analyzing the pebble game on G, it is desirable to treat G as an extension of G/N by N. However, the fact that Duplicator's bijections do not have to preserve cosets modulo N, makes it difficult to formally relate the extension structure of G to strategies in the pebble game. In the following lemma, we show that we can partially circumvent this, by doubling the total number of pebble pairs. In fact, this type of trade-off (number of pebbles vs. possible strategies in the pebble game) is very general and works with arbitrary subgroups instead of detectable normal subgroups.

Lemma 3.4.5. *Let G and H be finite groups of the same order. We choose arbitrary subgroups $U \leq G$ and $V \leq H$ with $|U| = |V|$, together with arbitrary coset representatives $g_1, \dots, g_m$ and $h_1, \dots, h_m$, representing all cosets of U in G and V in H, respectively. If Spoiler wins the explicit (implicit) k-pebble game on (G, H), then Spoiler wins the* restricted explicit (implicit) $(2k + \mathcal{O}(1))$-pebble game on (G, H), *in which Duplicator always maps U to V and $\{g_1, \dots, g_m\}$ to $\{h_1, \dots, h_m\}$ but Spoiler only ever places pebbles on $U \cup \{g_1, \dots, g_m\}$.*

Proof. In a given configuration with Duplicator move f, Spoiler can ask Duplicator for new bijections f_i, assuming that Spoiler places the current pebble on $(g_i, f(g_i))$. As before, we use the deterministic nature of the pebble game to argue that Spoiler can, in this sense, pre-compute Duplicator's strategy. This defines an injective map $(g_i, u) \mapsto (f(g_i), f_i(u))$ with $u \in U$. We obtain a bijection $F : G \to H$ with $F(r_i u) := f(r_i)f_i(u)$, using the fact that Duplicator maps U to V and respects the given sets of representatives to make sure that it is indeed a bijection. By assumption, Spoiler has a winning strategy, say by placing a pebble on $r_i u$, in the standard pebble-game. In the restricted pebble game, Spoiler can place two pebbles on r_i and u, where we may assume that Duplicator sticks to the map f_i chosen earlier. But f_i was freely chosen via Duplicator's strategy, justifying our assumption that Duplicator indeed chooses f_i. □

3.4.1 Individualization

We review the concept of individualization in the context of the versions of the WL-algorithm defined above.

Definition 3.4.6. Let $(\mathfrak{X}, \gamma)$ be a colored relational structure. *Individualization* of an element $v \in V(\mathfrak{X})$ describes the process of assigning a new coloring γ_v to $\mathfrak{X}$, such that v ends up in a color class of cardinality 1. More formally, for each $x \in V(\mathfrak{X}) \setminus \{v\}$, we have $\gamma_v(x) = \gamma(x)$ and $\gamma_v(v)$ is set to some new color which is not present in the original coloring γ. Instead of $(\mathfrak{X}, \gamma_v)$ we also write $\mathfrak{X}_{(v)}$ (in particular, we do so if the original coloring only defined one single color class or in the case that $\mathfrak{X}$ is just an uncolored structure). Consequently, we denote the structure we obtain by subsequently individualizing $v_1, \ldots, v_r \in V(\mathfrak{X})$ by $\mathfrak{X}_{(v_1,\ldots,v_r)}$.

The following well-known connection between individualizations and the Weisfeiler-Leman dimension is an important tool in the theory of isomorphism testing.

Lemma 3.4.7. *Let $\mathfrak{X}$ be a (colored) relational structure. If the Weisfeiler-Leman dimension of $\mathfrak{X}$ with r individualizations is bounded by k (for some choice of individualizations), then the Weisfeiler-Leman dimension of $\mathfrak{X}$ is bounded by $k + r$, where we use the same version of the Weisfeiler-Leman algorithm in both cases.*

Specifically for the class of finite groups, we devise the following lemma that shows how products of group elements can be used in some instances to implicitly fix the group elements over which the products are taken.

Lemma 3.4.8. *Let (G, γ) be a finite colored group. Assume that there is a subgroup $U \leq G$ which admits a direct product decomposition*

$$U = U_1 \times \cdots \times U_t,$$

where each U_i is a union of γ-color classes. For each i, let u_i be an element of U_i and define $u := u_1 \cdots u_t$. Then the coloring computed by 3-WL$_{\text{implicit}}$ *on (G, γ_u) places each u_i in a color class of size* 1.

Proof. By assumption, $U_0 := U_2 \times \cdots \times U_t$ is again a union of γ-color classes, so, by induction, it suffices to show the claim for $t = 2$. Since U_1 and U_2 are disjoint and each is a union of γ-color classes, we have that u_1 is the unique element of G such that $\gamma(u_1)$ is contained in $\gamma(U_1)$ and simultaneously $\gamma(u_1^{-1}u) = \gamma(u_2)$ is contained in $\gamma(U_2)$. Hence, the color that 3-WL$_{\text{implicit}}$ assigns to the triple (u_1^{-1}, u, u_2) uniquely identifies u_1 (see Lemma 3.2.26). The analogous statement holds for u_2. □

3.5 Set-extended structures

When working with groups and related objects, in the present thesis we often encounter situations where we reason about the information encoded in products of group elements. We capture an important instance of this phenomenon through the introduction of set-extended structures.

Definition 3.5.1. Let $\mathfrak{X}$ be a relational structure over the ground set V. The *set-extended structure* derived from $\mathfrak{X}$, denoted by $\mathfrak{X}_{\text{set-extended}}$, is the relational structure with ground set $\text{Pow}(V)$, and the following relations:

1. for each relation R of $\mathfrak{X}$, of arity r say, we have a relation $R_{\text{set-extended}}$ of $\mathfrak{X}_{\text{set-extended}}$ that is derived from R by identifying each element of V with its corresponding singleton set. So it holds
$$(v_1, \dots, v_r) \in R \Leftrightarrow (\{v_1\}, \dots, \{v_r\}) \in R_{\text{set-extended}},$$
2. there is a relation R_{set} that captures the subset structure as follows: R_{set} contains exactly those tuples $(M, \{v_i\})$, such that M is a subset of V that contains v_i.

We call the vertices M with $|M| > 1$ *set-vertices.*

So intuitively, when going from $\mathfrak{X}$ to $\mathfrak{X}_{\text{set-extended}}$, we add new vertices that point to all possible subsets of $V(\mathfrak{X})$.

The benefit of working with set-extended structures is that individualizing a set vertex M lets the WL-algorithm distinguish M from $V(\mathfrak{X}) \setminus M$. We can exploit this observation to discretize a number of elements from the original ground set that is exponential in the number of individualizations, as described in the following lemma. This is the main motivation for us to introduce set-extended structures, as it captures an important property of products in groups, as will be made precise later on.

Lemma 3.5.2. *Consider a relational structure $\mathfrak{X}$ together with the set-extended version $\mathfrak{X}_{\text{set-extended}}$. If $v_1, \dots, v_t$ is any sequence of elements in $V(\mathfrak{X})$, then there exist $\ell := \lceil \log t \rceil$ set-vertices $M_1, \dots, M_\ell \in V(\mathfrak{X}_{\text{set-extended}})$, such that* 2-WL$_{\text{implicit}}$ *applied to $(\mathfrak{X}_{\text{set-extended}})_{(M_1,\dots,M_\ell)}$ computes a coloring in which each of $v_1, \dots, v_t$ is individualized. In other words, any sequence of t individualizations in $\mathfrak{X}$ can be realized by* $\log t$ *individualizations in the set-extended structure. Moreover, the same statement holds for each substructure $\mathfrak{X}'$ of $\mathfrak{X}_{\text{set-extended}}$ that contains at least those set-vertices which define the subsets of $\{v_1, \dots, v_t\}$.*

Proof. Let M_1 denote the set-vertex that is exactly connected with the first half of $v_1, \dots, v_t$, let M_2 denote the set-vertex that is exactly connected with the first and third quarter of $v_1, \ldots, v_t$, and so on. This classical combinatorial construction defines a sequence of ℓ subsets of $\{v_1, \ldots, v_t\}$, such that each v_i has a unique relationship to the sequence of subsets, i.e., if c_i denotes the vector in $\mathbb{F}_2^\ell$ where the j-th component is equal to 1 if and only if v_i is contained in the set defined by M_j, then the vectors $c_1, \ldots, c_\ell$ are pairwise distinct. Thus, through individualizing $M_1, \ldots, M_\ell$, that is, fixing an ordering of the sets defined by $M_1, \ldots, M_\ell$, implicitly an ordering of $v_1, \ldots, v_t$ is fixed, which is detectable by 2-$\mathrm{WL}_{\mathrm{implicit}}$, since for any given M_j, the vertices connected to M_j are 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable. To prove the final claim of the lemma, we note that all set pebbles used in this proof belong to elements in the power set of $\{v_1, \ldots, v_t\}$. □

More generally, we can use similar arguments to show that k pebble pairs in the bijective pebble game on $\mathfrak{X}$ can be captured by $\mathcal{O}(\log k)$ pebble pairs in the bijective pebble game on $\mathfrak{X}_{\mathrm{set-extended}}$.

Lemma 3.5.3. *If $\mathcal{C}$ is a class of relational structures of* $\mathrm{WL}_{\mathrm{explicit}}$*-dimension d, then the class of set-extended structures over $\mathcal{C}$ has* $\mathrm{WL}_{\mathrm{explicit}}$*-dimension at most $\mathcal{O}(\log d)$.*

Proof. We can interpret Lemma 3.5.2 as follows: given a configuration c of k pebble pairs in the bijective pebble game on two relational structures, say $\mathfrak{X}$ and $\mathfrak{X}^*$, there is a corresponding configuration $c_{\mathrm{set-extended}}$ in the pebble game on $\mathfrak{X}_{\mathrm{set-extended}}$ and $\mathfrak{X}^*_{\mathrm{set-extended}}$, which uses $\mathcal{O}(\log k)$ pebble pairs and which captures c. Here, capturing c means that for each pebble pair in c, say on (x, x^*), if Duplicator does not map x to x^* in the configuration $c_{\mathrm{set-extended}}$, then Spoiler can win the game on the set-extended structures. Moreover, whenever a pebble pair in $c_{\mathrm{set-extended}}$ is placed on set-vertices, say M and M^*, then the configuration c contains pairs $(m_1, m_1^*), \ldots, (m_t, m_t^*)$ with $M = \{m_1, \ldots, m_t\}$ and $M^* = \{m_1*, \ldots, m_t^*\}$. We note that we refer to the same version of the game (explicit or implicit) in each case.

Now consider a pair of configurations c and $c_{\mathrm{set-extended}}$ as above and assume that Spoiler has a winning strategy in the configuration c. By the definition of set-extended structures, set-vertices differ from ground set vertices through the relation $\mathcal{R}_{\mathrm{set}}$, which can be easily exploited by Spoiler. In particular, winning moves for Duplicator have to preserve ground set vertices of the original structures. If Duplicator choose the bijection f in the configuration $c_{\mathrm{set-extended}}$, then Spoiler uses the induced bijection between the ground set vertices of the original structures, say f_{ground}, to obtain a winning move in the configuration c as a response to f_{ground}. Such a winning move for Spoiler exists by assumption, and it consists of placing the pebble pair in Spoilers hands on a pair of ground set vertices, say (x, x^*) and lifting afterwards lifting a pebble pair, say from (y, y^*), ultimately reaching a new configuration c'.

In the configuration $c_{\mathrm{set-extended}}$, Spoiler also places the pebble pair in their hands on (x, x^*) and picks up an additional pebble pair that is currently not on the board. The goal now is to reach a configuration that captures c' by using $\mathcal{O}(1)$ additional pebble pairs. To this end, Spoiler has to move every pebble pair on set-vertices, say M and M^*, such that M contains x and M^* contains x^*, to set vertices $(M \cup \{x\}) \setminus \{y\}$ and $(M^* \cup \{x^*\}) \setminus \{y^*\}$. Through the pebble pairs on (x, x^*) and (M, M^*), this can be easisly achieved using two additional pebble pairs, by replacing the pebble pair on (M, M^*) with one on $(M \cup \{x\}) \setminus \{y\}$ and $(M^* \cup \{x^*\}) \setminus \{y^*\}$. Since $c_{\mathrm{set-extended}}$ captures c in the above sense, if Duplicator does not map $(M \cup \{x\}) \setminus \{y\}$ to $(M^* \cup \{x^*\}) \setminus \{y^*\}$, then Spoiler can win immediately. □

Even for graphs it is currently unclear if set-extension improves the WL-dimension beyond the observations above. It is currently not even clear if the WL-dimension of set-extended graphs is unbounded.

Corollary 3.5.4. *For any graph* Γ *it hols*

$$\dim_{\mathrm{WL}_{\mathrm{graphs}}}(\Gamma_{\mathrm{set-extended}}) \leq \log(\dim_{\mathrm{WL}}^{\mathrm{graphs}}(\Gamma)) + \mathcal{O}(1).$$

We point out that it is currently an open problem to determine the WL-dimension of set-extended graphs, in particular, it could be bounded.

Chapter 4

The structure of finite groups through the lens of WL-refinement

From now on we focus our attention on finite groups. In the following chapter we provide a compendium of structural properties and group theoretic constructions that are detectable through, and can be exploited by, the Weisfeiler-Leman algorithm. This includes numerous major building blocks of group theory, and we provide a comprehensive framework to extend this catalog or adapt it to more specific situations. One of the main results we present here is that groups not distinguished by a constant dimensional WL-algorithm share the same multiset of composition factors (Theorem 4.2.34).

A part of these results is covered in a publication by the author together with Pascal Schweitzer [18]. The presentation here is more general in some aspects and it treats a larger variety of group theoretic concepts than [18], including, for instance, verbal subgroups, groups of prime power order, and group actions. Compared to [18], additionally some bounds on the WL-dimension have been improved, for example, we proof here that 2-$\mathrm{WL}_{\mathrm{implicit}}$ already detects p-radicals, as well as the Fitting subgroup, where the previous bound was 3.

The framework's flexibility is subsequently show-cased, first in the discussion of the Weisfeiler-Leman dimension of direct products of groups at the end of this chapter, and then in the later chapters of the thesis, where we derive bounds on the Weisfeiler-Leman dimension of important group classes.

4.1 Group theoretic closures & quotient groups

We consider the question, what basic group theoretic information is encoded in the stable color classes computed by the Weisfeiler-Leman algorithm. For instance, we investigate if subgroups generated by color classes are themselves unions of color classes. We take a fairly general approach here, working with arbitrary expressions in the first order word logic over groups. This later allows us to cover many well-known group theoretic constructions in a unified manner.

Definition 4.1.1. A *group expression* $\mathcal{E} := (\mathcal{S}_1, \dots, \mathcal{S}_t; \mathcal{R})$ of length t is a sequence of subset selectors $\mathcal{S}_i$ together with a set $\mathcal{R}$ of words $w(x_1, \dots, x_t)$ over t variables $x_1, \dots, x_t$, allowing inverses. Let (G, γ) be a colored group, then a t-tuple $(g_1, \dots, g_t) \in G^t$ is a *solution* to $\mathcal{E}$, if for each i it holds that $g_i \in \mathcal{S}_i(G,\gamma)$ and additionally, for each $w \in \mathcal{R}$ we have $w(g_1,\dots,g_t) = 1$. Let $Sol_{\mathcal{E}}(G,\gamma) \subseteq G^t$ denote the set of all solutions to $\mathcal{E}$ over the colored group (G,γ).

Group expressions are closely related to the concept of group laws (words w with $Sol_{(G,\dots,G,\{w\})} = G$) and verbal subgroups (subgroups generated by images of word maps evaluated over G). We study these connections in greater detail at the end of this section. In the case of group expressions, the presence of subset selectors allows one to restrict the domain of each variable independently. In the following lemma, we show that certain subgroups derived from a group expression inherit the property of being WL-detectable from the defining subset selectors.

Lemma 4.1.2. *Consider a group expression $\mathcal{E} := (\mathcal{S}_1,\dots,\mathcal{S}_t;\mathcal{R})$. Let $k \geq \max\{t,2\}$ and assume that each $\mathcal{S}_i$ is k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

1. *Let (G,γ_G) and (H,γ_H) be colored groups. Then all t-tuples in $Sol_{\mathcal{E}}(G,\gamma_G)$ can be distinguished from all t-tuples in $H^t \setminus Sol_{\mathcal{E}}(H,\gamma_H)$ via k-$\mathrm{WL}_{\mathrm{implicit}}$.*

2. *For an integer $j \in [t]$ and a colored group (G,γ), set $\mathcal{S} := Sol_{\mathcal{E}}(G,\gamma)$ and define*

$$Sol_j^{\exists}(G,\gamma) := \{x \in G \mid \exists (x_1,\dots,x_t) \in \mathcal{S} : x_j = x\}$$
$$Sol_j^{\forall}(G,\gamma) := \{x \in G \mid (\forall x_i \in \mathcal{S}_i(G,\gamma))_{i\in[t]} : (x_1,\dots,x_{j-1},x,x_{j+1},\dots,x_t) \in \mathcal{S}\}.$$

   Then $Sol_j^{\exists}$ and $Sol_j^{\forall}$ are k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable subset selectors for all j.

The same holds if we replace implicit *with* explicit *everywhere (including the assumptions), provided $k > \max\{t,2\}$.*

Proof. 1. Let $\bar{g} = (g_1,\dots,g_t) \in Sol_{\mathcal{E}}(G,\gamma_G)$ and $\bar{h} = (h_1,\dots,h_t) \in H^t \setminus Sol_{\mathcal{E}}(H,\gamma_H)$. First consider the case that there is some word $w \in \mathcal{R}$ such that $w(\bar{h}) \neq 1$. Then there is no isomorphism between $\langle g_1,\dots,g_t\rangle$ and $\langle h_1,\dots,h_t\rangle$ that maps g_i to h_i for all i. Thus, by definition, the k-tuples $(g_1,\dots,g_t,1,\dots,1)$ and $(h_1,\dots,h_t,1,\dots,1)$ obtain different initial colors in k-$\mathrm{WL}_{\mathrm{implicit}}$. In the other case, since $\bar{h} \notin Sol_{\mathcal{E}}(H,\gamma_H)$, there must be some index j such that $h_j \notin \mathcal{S}_j(H,\gamma_H)$. By assumption $\mathcal{S}_j$ is detectable by k-$\mathrm{WL}_{\mathrm{implicit}}$ and $g_j \in \mathcal{S}_j(G,\gamma_G)$, so by definition $(\chi^k_{\mathrm{implicit}}(G,\gamma_G)(g_j)) \neq (\chi^k_{\mathrm{implicit}}(H,\gamma_H))(h_j)$. In particular, $\bar{g}$ and $\bar{h}$ can be distinguished by k-$\mathrm{WL}_{\mathrm{implicit}}$ via Lemma 3.2.26.

   The proof for k-$\mathrm{WL}_{\mathrm{explicit}}$ is almost identical. Note that for the explicit version, we assume that $k \geq t+1$ holds. Then, in the first case where the tuples fulfill different relations we use Lemma 3.2.23 to obtain the result for k-$\mathrm{WL}_{\mathrm{explicit}}$. Note that the Lemma requires $k \geq 4$ in the explicit k-pebble game, which corresponds to $k \geq 3$ in $\mathrm{WL}_{\mathrm{explicit}}$ through Lemma 3.2.13. The second case can be treated identically for both versions.

2. Using Part 1, if we consider $g \in Sol_j^{\exists}(G,\gamma_G)$ and $h \in H \setminus Sol_j^{\exists}(H,\gamma_H)$ we are exactly in the situation of Lemma 3.2.27 and so g and h can be distinguished via k-$\mathrm{WL}_{\mathrm{implicit}}$, i.e., $Sol_j^{\exists}$ is detectable. The same argument works for $g \in Sol_j^{\forall}(G,\gamma_G)$ and $h \in H \setminus Sol_j^{\forall}(H,\gamma_H)$. The latter condition is equivalent to the existence of $h_i \in \mathcal{S}_i(H,\gamma_H)$ such that $(h_1,\dots,h_{j-1},h,h_{j+1},\dots,h_t) \notin Sol_{\mathcal{E}}(H,\gamma_H)$, so in this situation we use Lemma 3.2.27 for $H^t \setminus Sol_{\mathcal{E}}(H,\gamma_H)$. □

We apply the previous lemma to common group theoretic closure operations, such as generated subgroups or conjugacy classes.

Lemma 4.1.3. *Consider k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable subset selectors $\mathcal{S}$ and $\mathcal{T}$ for $k \geq 2$. Then the following subset selectors are again k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable:*

1. *e-th powers over $\mathcal{S}$ for each $e \in \mathbb{Z}$, that is, the subset selector associating the set $\{s^e \mid s \in \mathcal{S}(G,\gamma)\}$ to (G,γ),*

2. *$C_{\mathcal{S}}(\mathcal{T})$, where $C_{\mathcal{S}}(\mathcal{T})(G,\gamma) := \{s \in \mathcal{S}(G,\gamma) \mid [s, \mathcal{T}(G,\gamma)] = \{1\}\}$.*

Provided k is at least 3, k-$\mathrm{WL}_{\mathrm{implicit}}$ further detects the following subset selectors:

3. *$\{s_1 \dots s_e \mid s_i \in \mathcal{S}(G,\gamma)\}$ for each $e \in \mathbb{N}$, in particular also $\langle \mathcal{S}(G,\gamma)\rangle$,*

4. *$\{s^t := tst^{-1} \mid s \in \mathcal{S}(G,\gamma), t \in \mathcal{T}(G,\gamma)\}$, in particular also $\langle \mathcal{S}(G,\gamma)^G\rangle$,*

5. *$\mathcal{N}_{\mathcal{S}}(\mathcal{T})$, where $\mathcal{N}_{\mathcal{S}}(\mathcal{T})(G,\gamma) := \{s \in \mathcal{S}(G,\gamma) \mid \mathcal{T}(G,\gamma)^s = \mathcal{T}(G,\gamma)\}$,*

6. *$[\mathcal{S},\mathcal{T}]$, where $[\mathcal{S},\mathcal{T}](G) := \langle [s,t] \mid s \in \mathcal{S}(G,\gamma),\ t \in \mathcal{T}(G,\gamma)\rangle$.*

All statements remain true if we replace the implicit *version by the* explicit *version everywhere (including the assumptions), provided $k > 2$ in Parts 1) and 2) and $k > 3$ in Parts 3)–6).*

Proof. We make repeated use of Lemma 4.1.2 here. Given a group expression $\mathcal{E} := (\mathcal{S}_1, \dots, \mathcal{S}_t; \mathcal{R})$, define $Sol_j^{\exists}$ and $Sol_j^{\forall}$ $(j = 1, \dots, t)$ as in Lemma 4.1.2.

1. Set $\mathcal{E} = (\mathcal{S}, Id; \{x_1^e x_2^{-1}\})$. Then $\{s^e \mid s \in \mathcal{S}(G,\gamma)\} = Sol_2^{\exists}(G,\gamma)$.

2. Set $\mathcal{E} = (\mathcal{S}, \mathcal{T}; \{[x_1, x_2]\})$. Then $\mathcal{S}(G,\gamma) \cap C_G(\mathcal{T}(G,\gamma)) = Sol_1^{\forall}(G,\gamma)$.

3. We argue by induction over e. Let us write $\mathcal{S}^{[e]}(G,\gamma) := \{g_1 \dots g_e \mid g_i \in \mathcal{S}(G,\gamma)\}$. Assume that $\mathcal{S}^{[e]}$ can be detected for $k \geq 3$ and consider $\mathcal{E} = (\mathcal{S}^{[e]}, \mathcal{S}, Id; \{x_1 x_2 x_3^{-1}\})$. Then $Sol_3^{\exists}$ is exactly $\mathcal{S}^{[e+1]}$ and since $\mathcal{S}$ and $\mathcal{S}^{[e]}$ are both detectable, so is $\mathcal{S}^{[e+1]}$. In particular, $\langle \mathcal{S}(G,\gamma)\rangle = \bigcup_e \mathcal{S}^{[e]}(G,\gamma)$ is detectable by k-$\mathrm{WL}_{\mathrm{implicit}}$ as a union of detectable subset selectors.

4. Set $\mathcal{E} = (\mathcal{S}, \mathcal{T}, Id; \{x_2^{-1} x_1 x_2 x_3^{-1}\})$. The $\mathcal{S}(G,\gamma)$-conjugates of elements in $\mathcal{T}(G,\gamma)$ are precisely $Sol_3^{\exists}$. Together with Part 3, this shows that the normal closure of $\mathcal{T}$ is detectable by k-$\mathrm{WL}_{\mathrm{implicit}}$ for $k \geq 3$.

5. Set $\mathcal{E} = (\mathcal{T}, \mathcal{S}, G \backslash \mathcal{T}; \{x_2^{-1} x_1 x_2 x_3^{-1}\})$. If $\mathcal{T}$ is detectable then so is $G \backslash \mathcal{T}(G,\gamma)$, which implies that $G \setminus Sol_2^{\exists}(G,\gamma)$ is detectable. Finally note that elements of $\mathcal{S}(G,\gamma)$ do not normalize $\mathcal{T}(G,\gamma)$ if and only if they belong to $Sol_2^{\exists}(G,\gamma)$.

6. Set $\mathcal{E} = (\mathcal{T}, \mathcal{S}, Id; \{[x_1, x_2] x_3^{-1}\})$. Then $Sol_3^{\exists}$ is the set of all $\mathcal{T}(G,\gamma)$-$\mathcal{S}(G,\gamma)$-commutators and using Part 3, we obtain detectability of the group they generate, namely $[\mathcal{T}, \mathcal{S}]$.

The analogue statements for k-$\mathrm{WL}_{\mathrm{explicit}}$ follow from Lemma 4.1.2 in the same way, provided $k > t$ in each case. □

We highlight two direct implications of the previous lemma.

Corollary 4.1.4. *If $k \geq 3$, then k-$\mathrm{WL}_{\mathrm{implicit}}$ distinguishes elements with respect to the coloring that $(k-1)$-$\mathrm{WL}_{\mathrm{implicit}}$ assigns to their normal closures. More precisely, consider $x \in (G, \gamma_G)$ and $y \in (H, \gamma_H)$. If $\left(\chi^k_{\mathrm{implicit}}(G, \gamma_G)\right)(x) = \left(\chi^k_{\mathrm{implicit}}(H, \gamma_H)\right)(y)$ holds, then*

$$\left(\langle x^G \rangle, \gamma_G|_{\langle x^G \rangle}\right) \equiv^{k-1}_{\mathrm{implicit}} \left(\langle y^H \rangle, \gamma_H|_{\langle y^H \rangle}\right).$$

The same holds for the explicit *version with $k \geq 4$.*

Proof. Via Lemma 3.2.13, we need to show that Spoiler has a winning strategy in the implicit $(k+1)$-pebble game starting with pebble pairs on (x, y). The claim follows from Lemma 4.1.3, where Spoiler strategies can re-use the pebble pair on (x, y), to ensure that Duplicator has to map the nomral closure of x to the normal closure of y (or loses right away). As long as Duplicator maps the normal closures accordingly, Spoiler can freely use the remaining k pebble pairs on the normal closures, and then the claim follows from Lemma 3.2.13. □

Similarly, k-WL distinguishes the normal $(k-1)$-generated subgroups from non-normal subgroups.

Corollary 4.1.5. *Let $k \geq 3$ and consider group elements $x_i \in (G, \gamma_G)$ and $y_i \in (H, \gamma_H)$ for $i \in [k-1]$. If $\left(\chi^k_{\mathrm{implicit}}(G, \gamma_G)\right)(x_1, \ldots, x_{k-1}) = \left(\chi^k_{\mathrm{implicit}}(H, \gamma_H)\right)(y_1, \ldots, y_{k-1})$ then $\langle x_1, \ldots, x_{k-1} \rangle$ is normal in G if and only if $\langle y_1, \ldots, y_{k-1} \rangle$ is normal in H.*

Proof. Via Lemma 3.2.13, we need to show that Spoiler has a winning strategy in the implicit $(k+1)$-pebble game starting with pebble pairs on (x_i, y_i) for all $i \in [k-1]$. Since k is at least 3, Duplicator has to map conjugates of x_i to conjugates of y_i for all i. Otherwise, Spoiler can reach a configuration with pebble pairs on (x_i, y_i) and (x_i^g, y), such that no $h \in H$ fulfills $y = y_i^h$, and Spoiler can clearly win from there. Now assume without loss of generality that x_1^g is not contained in $\langle x_1, \ldots, x_{k-1} \rangle$, while $\langle y_1, \ldots, y_{k-1} \rangle$ is normal in H. Then Duplicator has to map x_1^g to y_1^h for some $h \in H$, by what we just argued, and Spoiler can reach a configuration with pebble pairs on (x_1^g, y_1^h) and (x_i, y_i) for all i. By choice of g, the marked isomorphism types of $(x_1^g, x_1, \ldots, x_{k_1})$ and $(y_1^h, y_1, \ldots, y_{k_1})$ are distinct, so Spoiler wins. □

In the following example we employ the previous lemma to identify groups as direct products of detectable subgroups via the Weisfeiler-Leman algorithm.

Example 4.1.6. Suppose G and H are finite groups with $G \equiv^3_{\mathrm{implicit}} H$, and further assume that G has a direct decomposition $G = G_1 \times G_2$ with $\chi^3_{\mathrm{implicit}}(G)$-induced subgroups $G_i \leq G$. We can use the colors of elements in G_i to define a subset selector

$$K \mapsto K_i := \left\{x \in K \mid \left(\chi^3_{\mathrm{implicit}}(K)\right)(x) \in \left(\chi^3_{\mathrm{implicit}}(G)\right)(G_i)\right\},$$

which is 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable by definition. Since we assume that $G \equiv^3_{\mathrm{implicit}} H$ holds, it must hold that $H_i \leq H$ is indistinguishable from G_i via 3-$\mathrm{WL}_{\mathrm{implicit}}$. By the previous lemma, 3-$\mathrm{WL}_{\mathrm{implicit}}$ detects $[G_1, G_2]$ and $G_1 \cap G_2$, which are both trivial in this case, as well as $\langle G_1, G_2 \rangle$, which is equal to G. By the definition of detectability, the same conditions must apply for H_1 and H_2, thus $H = H_1 \times H_2$ with $H_i \equiv^3_{\mathrm{implicit}} G_i$.

The same inductively applies to an arbitrary number of detectable direct factors.

Corollary 4.1.7. *Assume $k \geq 3$ for the k-$\mathrm{WL}_{\mathrm{implicit}}$ version, or $k \geq 4$ for the k-$\mathrm{WL}_{\mathrm{explicit}}$. Consider a group G with direct product decomposition $G = G_1 \times \cdots \times G_t$ and assume that each G_i is k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable ($k$-$\mathrm{WL}_{\mathrm{explicit}}$-detectable). Then, if H is another group that is not distinguished from G by k-$\mathrm{WL}_{\mathrm{implicit}}$ (k-$\mathrm{WL}_{\mathrm{explicit}}$), we have a decomposition of H as $H = H_1 \times \cdots \times H_t$ with $H_i \equiv^k_{\mathrm{implicit}} G_i$ ($H_i \equiv^k_{\mathrm{explicit}} G_i$, respectively) for all $i \in [t]$.*

In Section 4.3 we discuss the (much harder) case of arbitrary direct decompositions, without the assumption that each direct factor is detectable as a subgroup.

Up until this point we considered concrete substructures inside of groups. For the remainder of this section we prove that the Weisfeiler-Leman algorithm also exploits properties of quotients over detectable subgroups, resulting in rich interplay between group theory and the Weisfeiler-Leman algorithm.

Recall Lemma 3.4.3, of which the main consequence is that any bijection $f : G \to H$ between two groups with normal subgroups $N_G \trianglelefteq G$ and $N_H \trianglelefteq H$ of the same order *automatically* induces (possibly multiple distinct) bijections $f : G/N_G \to H/N_H$. This allows us to form a connection between the bijective pebble game played on pairs of groups, and played on pairs of suitable quotients of these groups, respectively. This is the main idea behind the following lemma.

Definition 4.1.8. Given a coloring $\gamma : G \to \mathcal{C}$ and a normal subgroup $N \trianglelefteq G$ define the induced *quotient coloring* $\overline{\gamma}$ on G/N via $\overline{\gamma}(gN) := \{\{\gamma(gn) \mid n \in N\}\}$.

Lemma 4.1.9. *Let $k \geq 4$ and consider colored groups (G, γ_G) and (H, γ_H). Assume that there are normal subgroups $N_G \trianglelefteq G$ and $N_H \trianglelefteq H$ which are induced by γ_G and γ_H, respectively, such that $\gamma_G(N_G) = \gamma_H(N_H)$ holds. Then*

$$\left(\chi^k_{\mathrm{explicit}}(G/N_G, \overline{\gamma_G})\right)(g_1N_G, \ldots, g_kN_G) \neq \left(\chi^k_{\mathrm{explicit}}(H/N_H, \overline{\gamma_H})\right)(h_1N_H, \ldots, h_kN_H) \Longrightarrow$$
$$\left(\chi^k_{\mathrm{explicit}}(G, \gamma_G)\right)(g_1, \ldots, g_k) \neq \left(\chi^k_{\mathrm{explicit}}(H, \gamma_H)\right)(h_1, \ldots, h_k)$$

for all choices of $g_i \in G$ and $h_i \in H$.

Proof. Using Lemma 3.2.13, we argue via the corresponding $(k+1)$-pebble games. The idea is to lift a winning strategy for Spoiler from the game on $(G/N_G, H/N_H)$ to (G, H), where initial configurations are given by $[(g_1N_G, \ldots, g_kN_G, \perp), (h_1N_H, \ldots, h_kN_H, \perp)]$ and $[(g_1, \ldots, g_k, \perp), (h_1, \ldots, h_k, \perp)]$, respectively.

If $|N_G| \neq |N_H|$, Duplicator can not even win on (G, H) from the empty configuration, since by assumption N_G and N_H are induced by γ_G and γ_H, respectively, and obtain the same colors. Hence, the cardinality of some color class differs for a fixed color in the image of γ_G and γ_H, and Duplicator has to respect these color classes to be able to win. We may therefore assume that $|N_G| = |N_H|$.

By assumption, Spoiler has a winning strategy on the quotients by picking up the i-th pebble pair, say. Spoiler picks up the i-th pebble pair in the game on (G, H) as well. Consider a subsequent Duplicator move $f : G \to H$. By Lemma 3.4.3, there are representatives modulo N_G, $r^G_1, \ldots, r^G_t$ say, that are mapped to a full set of representatives for H/N_H, $r^H_i := f(r^G_i)$ say. The representatives define a bijection $\bar{f} : G/N_G \to H/N_H, r^G_iN_G \mapsto r^H_iN_H$. If $\bar{f}$ is used as a Duplicator move in the game on $(G/N_G, H/N_H)$, then Spoiler has a corresponding winning strategy by placing the i-th pebble pair on $(r_j^G N_G, r_j^H N_H)$, say. In the game on (G, H), Spoiler places the i-th pebble pair on (r_j^G, r_j^H). The new configurations reached in the two games we consider relate to each other in the same way the initial configurations do: If the m-th pebble pair on (G, H) is placed on (g, h) then the m-th pebble pair on $(G/N_G, H/N_H)$ is placed on (gN_G, hN_H). Spoiler can iteratively employ this strategy until eventually a configuration $[(g'_1, \dots, g'_{k+1}), (h'_1, \dots h'_{k+1})]$ is reached such that the corresponding configuration on the quotients is winning for Spoiler. Then we are in one of three cases: Either $\bar{\gamma_G}(g'_i N_G) \neq \bar{\gamma_H}(h'_i N_H)$ for some i, or there exist i, j with $g'_i = g'_j$ modulo N_G and $h'_i \neq h'_j$ modulo N_H, or there exist i, j, m with $g'_i g'_j = g'_m$ modulo N_G and $h'_i h'_j \neq h'_m$ modulo N_H (the last two cases could occur with G and H interchanged but this would not affect the proof).

In the first case, for each bijection $f' : g'_i N_G \to h'_i N_H$ there is some $n \in N_G$ with $\gamma_G(g'_i n) \neq \gamma_H(f'(g'_i n))$. Thus, if Duplicator maps $g'_i N_G$ to $h'_i N_H$ Spoiler can win in one move by exploiting the mismatched colors. Otherwise Duplicator maps some $g \in g'_i N_G$ to $h \in H \setminus h'_i N_H$ and Spoiler can put a pebble pair (p_j, p'_j) on (g, h) for some $j \neq i$. Then $g'_i g^{-1} \in N_G$ and $h'_i h^{-1} \notin N_H$. Since $k \geq 4$, Spoiler can use additional pebbles to successively fix g^{-1} and $g'_i g^{-1}$. Then $g'_i g^{-1}$ must be mapped to $h'_i h^{-1}$ (or otherwise Duplicator can not respect the multiplication relation on the current pebbles) and then $\gamma_G(g'_i g^{-1}) \neq \gamma_H(h'_i h^{-1})$.

In the second case $g'_i {g'_j}^{-1} \in N_G$ and $h'_i {h'_j}^{-1} \notin N_H$ and we end up in the same situation we just discussed.

In the third case $g'_i g'_j {g'_m}^{-1} \in N_G$ but $h'_i h'_j {h'_m}^{-1} \notin N_H$. Spoiler can first put a fourth pebble pair on $(g'_i g'_j, h'_i h'_j)$ (as above, if Duplicator does not map $g'_i g'_j$ to $h'_i h'_j$, Spoiler can win immediately) and then we end up in the situation we encountered at the end of the first case again. □

We collect the previous results in our first main theorem which states that, for any pair of indistinguishable groups $G \equiv^k_{\text{explicit}} H$, establishes a correspondence between detectable substructures of G and detectable substructures of H, that preserves the stable colors computed by k-WL$_{\text{explicit}}$.

Theorem 4.1.10. *Let k be at least 4.*

1. *Consider subset selectors N, U and U/N such that for all (G, γ) it holds that $N(G, \gamma) \trianglelefteq G$, $N(G, \gamma) \leq U(G, \gamma)$ and $U/N(G/N(G), \bar{\gamma}) = U(G)/N(G)$. If N and U/N are k-WL$_{\text{explicit}}$-detectable then so is U.*

2. *Consider colored groups $(G, \gamma_G) \equiv^k_{\text{explicit}} (H, \gamma_H)$. Let $\Psi : G \to H$ be a bijection with $\chi^k_{\text{explicit}}(G, \gamma_G) \circ \Psi = \chi^k_{\text{explicit}}(H, \gamma_H)$. Then $M \subseteq G$ is $\chi^k_{\text{explicit}}(G, \gamma_G)$-induced if and only if $\Psi(M) \subseteq H$ is $\chi^k_{\text{explicit}}(H, \gamma_H)$-induced. In this case it holds that*

   $$\Psi(\langle M \rangle) = \langle \Psi(M) \rangle.$$

   In particular, if M is a subgroup then so is $\Psi(M)$ and it holds

   $$(M, \gamma_G|_M) \equiv^k_{\text{explicit}} (\Psi(M), \gamma_H|_{\Psi(M)}).$$

   Additionally, M is normal if and only if $\Psi(M)$ is and then it also holds that

   $$(G/M, \overline{\gamma_G}) \equiv^k_{\text{explicit}} (H/\Psi(M), \overline{\gamma_H}).$$

Proof. 1. Since $\chi^k_{\text{explicit}}(G, \gamma_G)$ is a refinement of γ, the detectability of U/N implies that, with the quotient coloring induced on $G/N(G)$ by $\chi^k_{\text{explicit}}(G, \gamma_G)$, k-$\text{WL}_{\text{explicit}}$ distinguishes elements $uN(G)$ with $u \in U$ from elements $xN(G)$ with $x \in G \setminus U$. Since N is also k-$\text{WL}_{\text{explicit}}$-detectable, we are in the situation of Lemma 4.1.9 with both groups equal to $(G, \chi^k_{\text{explicit}}(G, \gamma))$ which implies

$$\left(\chi^k_{\text{explicit}}(G, \chi^k_{\text{explicit}}(G, \gamma))\right)(u) \neq \left(\chi^k_{\text{explicit}}(G, \chi^k_{\text{explicit}}(G, \gamma))\right)(x)$$

for all $u \in U$ and $x \in G \setminus U$. Via Lemma 3.2.29, this implies

$$\left(\chi^k_{\text{explicit}}(G, \gamma)\right)(u) \neq \left(\chi^k_{\text{explicit}}(G, \gamma)\right)(x)$$

for all $u \in U$ and $x \in G \setminus U$, so U is detectable by k-$\text{WL}_{\text{explicit}}$.

2. By definition, Ψ maps k-$\text{WL}_{\text{explicit}}$-color classes in G to k-$\text{WL}_{\text{explicit}}$-color classes in H. Given a $\chi^k_{\text{explicit}}(G, \gamma_G)$-induced subset $M \subseteq G$, define a subset selector $\mathcal{S}_M$ by associating with a colored group K the preimage of $\left(\chi^k_{\text{explicit}}(G, \gamma_G)\right)(M)$ in K. By definition, $\mathcal{S}_M$ is k-$\text{WL}_{\text{explicit}}$-detectable and $\Psi(M) = \mathcal{S}_M(H, \gamma_H)$. Thus, by Lemma 4.1.3, the groups generated by M and $\Psi(M)$ are k-$\text{WL}_{\text{explicit}}$-detectable and since $(G, \gamma_G) \equiv^k_{\text{explicit}} (H, \gamma_H)$ holds, $\langle M \rangle$ and $\langle \Psi(M) \rangle$ must also be indistinguishable via k-$\text{WL}_{\text{explicit}}$, i.e., $\Psi(\langle M \rangle) = \langle \Psi(M) \rangle$. Furthermore, in the pebble game on (G, H) Spoiler could restrict their moves to $(\langle M \rangle, \langle \Psi(M) \rangle)$, hence $(\langle M \rangle, \gamma_G|_{\langle M \rangle}) \equiv^k_{\text{explicit}} (\langle \Psi(M) \rangle, \gamma_H|_{\langle \Psi(M) \rangle})$. Analogous arguments work for normal closures instead of generated subgroups. In particular, M is a normal subgroup of G if and only if $\Psi(M)$ is a normal subgroup of H. For the last claim that $(G/M, \bar{\gamma_G}|_M) \equiv^k_{\text{explicit}} (H/\Psi(M), \bar{\gamma_H}|_{\Psi(M)})$, note that otherwise all elements of $(G/M, \bar{\gamma_G}|_M)$ would be distinguishable from all elements of $(H/\Psi(M), \bar{\gamma_H}|_{\Psi(M)})$ via k-$\text{WL}_{\text{explicit}}$ and then, by Lemma 4.1.9, (G, γ_G) and (H, γ_H) would be distinguishable as well, contradicting the assumptions. □

Observation 4.1.11. *For uncolored groups G and H, the k-WL-induced subgroups, that is, the subgroups that are union of stable color classes, are always characteristic subgroups. For such groups, the previous theorem states a correspondence $C_G \equiv^k_{\text{explicit}} C_H$ between k-WL-induced characteristic subgroups in G and H, respectively, together with a correspondence $G/C_G \equiv^k_{\text{explicit}} H/C_H$ of their respective quotients.*

4.2 Aspects of finite group theory in terms of stable Weisfeiler-Leman-colorings

We revisit fundamental aspects of finite group theory and investigate their relationship with stable Weisfeiler-Leman colorings. On the one hand, this enhances our understanding of the Weisfeiler-Leman algorithm and provides a foundation for the analysis of WL-colorings on specific groups. On the other hand, this advances the descriptive complexity theory of finite groups, where the Weisfeiler-Leman dimension serves as a novel measure of complexity.

Our starting point is 2-$\text{WL}_{\text{explicit}}$, as it is the weakest algorithm in the sequence of WL-algorithms we defined above. In fact, we can still precisely describe what the stable colorings look like on an arbitrary group. We introduce further notational conventions.

Definition 4.2.1. Given a prime p, a group G and a group element $g \in G$, let $\nu_p(g)$ denote the largest $i \in \mathbb{N}_0$, such that p^i divides the order of g. Moreover, we use $o'_p(g)$ to denote the order of $g^{p^{\nu_p(g)}}$.

It turns out that the characterization of 2-WL$_{\text{explicit}}$-color classes is simpler than the characterization of 2-WL$_{\text{graphs}}$-color classes, since intuitively, 2-WL$_{\text{explicit}}$ does not consider the whole multiplication relation of a group, but only the less expressive collapsed relation $\{(g, g^2) \mid g \in G\}$. So we can run the algorithm on a very structured digraph, where arcs are given by squares in the group, instead of the given input group itself.

Definition 4.2.2. Let G be a finite group and let $g \in G$. The 2-*tree* assigned to g, denoted by $T_2(g)$, is the rooted tree with root $g^{\nu_2(g)}$, such that the children of each node n are its proper square roots in G, that is, elements x with $x^2 = n$ and $|n| < |x|$.

Lemma 4.2.3. *Let G be a finite group and let χ denote the stable coloring computed on G by* 2-WL$_{\text{explicit}}$.

1. *Let g_1, g_2, h_1, h_2 be elements of G. If $\chi(g_1, g_2) = \chi(h_1, h_2)$ holds, then, for all $m \in \mathbb{N}$, we have*
$$g_i^{2m} = g_j \Leftrightarrow h_i^{2m} = h_j,$$
where $\{i, j\} = \{1, 2\}$.

2. *Let $g, h \in G$. We have $\chi(g) = \chi(h)$ if and only if the following conditions hold:*

   (a) $o'_2(g)$ and $o'_2(h)$ divide $2^j - 1$ for the same minimal value of $j \in \mathbb{N}$,

   (b) There is an isomorphism $\varphi\colon T_2(g) \to T_2(h)$ of rooted trees with $\varphi(g) = h$.

   In particular, $\chi(g) = \chi(h)$ implies $\nu_2(g) = \nu_2(h)$.

Proof. 1. We show the claim by induction over the iteration number of 2-WL$_{\text{explicit}}$. By definition, the initial coloring distinguishes pairs of group elements with respect to the relation $x_i^2 = x_j$, where $\{i, j\} = \{1, 2\}$. Assume inductively that in the current iteration of 2-WL$_{\text{explicit}}$, we have that pairs are distinguished with respect to the relation $x_i^{2m-1} = x_j$. Then pairs (g_1, g_2) with $g_1^{2m} = g_2$ are uniquely determined by the existence of an $x \in G$ with $g_1^{2m-1} = x$ and $x^2 = g_2$. By definition, the existence or non-existence of such an element x is encoded in the next iterated coloring.

2. By definition of 2-WL$_{\text{explicit}}$, we can replace the input group G by a directed graph on G with arc set $\{(g, g^2) \mid g \in G\}$.

   We describe the connected components of this graph: The component of $1 \in G$ is the unique 2-tree with root 1 and apart from 1, it contains exactly the elements whose orders are powers of 2. We note that the identity is identified by 2-WL$_{\text{explicit}}$, as $(1, 1)$ is the unique pair (g_1, g_2) with $g_1^2 = g_1 = g_2$. So we may assume that 1 obtains a special color.

   Any other component is built from a directed cycle of even length, consisting of the set $\{x^{2^j} \mid j \in \mathbb{N}\}$ for some $x \in G$ of odd order, and each vertex of this cycle additionally has its 2-tree attached to it (if the order of x is odd, then, by definition, x is the root of $T_2(x)$). Since the order of x is odd, $T_2(x)$ and $T_2(x^{2^j})$ are isomorphic as rooted trees for each $j \in \mathbb{N}$. Moreover, the length of the directed cycle induced on $\{x^{2^j} \mid j \in \mathbb{N}\}$ is entirely determined by the minimal $j \in \mathbb{N}$ such that $|x|$ divides $2^j - 1$, which is encoded in the stable 2-WL$_{\text{explicit}}$ coloring by Part 1).

With this description of connected components, the orbit of $g \in G$ under the automorphism group of this digraph is uniquely determined by its orbit in $T_2(g)$ and the isomorphism type of $T_2(g)$ (this information is equivalent to Condition *b*)) and the length of the even cycle they are connected to (in case that the order of g is not a power of 2) via a path of outgoing arcs (this information is equivalent to Condition *a*)).

Now 2-WL$_{\text{explicit}}$ (applied to graphs) computes the orbit partition of each rooted tree (see Lemma 2.2.7), so it also computes the orbit partition on G, regarded as a digraph, by our description of the connected components. The claim follows, since the Weisfeiler-Leman algorithm, by automorphism invariance, can never distinguish elements from the same orbit. □

Recall that, in contrast to the explicit version, k-WL$_{\text{implicit}}$ encodes isomorphism types of k-generated subgroups in the initial coloring, giving us the following lemma.

Lemma 4.2.4. *For $k \geq 2$, k-WL$_{\text{implicit}}$ identifies all finite k-generated groups. If two groups G and H are not distinguished by k-WL$_{\text{implicit}}$, then they have the same k-*profiles*, that is, the same multiset of isomorphism types of k-generated subgroups.*

Lemma 4.2.5. *Let G be a finite group and let x and y be elements of G. Assume that $\left(\chi^2_{\text{implicit}}(G)\right)(x) = \left(\chi^2_{\text{implicit}}(G)\right)(y)$ holds. Then*

1. *$|x| = |y|$,*

2. *for all $e \in \mathbb{N}$, x is an e-th power in G if and only if y is,*

3. *for all $e \in \mathbb{N}$, x and y have the same number of e-th roots in G.*

Proof. The order of x and y is implicitly encoded in the marked isomorphism type, i.e., the initial coloring, of $(x, 1)$ and $(y, 1)$. The second and third claim follow from the fact that, iteratively, 2-WL$_{\text{implicit}}$ counts the number of pairs of the form (r, r^e) with $r^e = x$. □

In particular, we can apply the previous lemma to groups that are indistinguishable via the Weisfeiler-Leman algorithm.

Corollary 4.2.6. *If two groups G and H are not distinguished by 2-WL$_{\text{implicit}}$, then we have $\{\{|x| \mid x \in G\}\} = \{\{|x| \mid x \in H\}\}$ and $\frac{1}{|G|}\sum_{x\in G}|x| = \frac{1}{|H|}\sum_{x\in H}|x|$.*

By the classification of abelian groups, finite abelian groups are uniquely determined up to isomorphism by their multisets of element orders. Using the observation that 2-WL$_{\text{implicit}}$ distinguishes elements with respect to the orders of their centralizers (see Lemma 4.1.3), we can now state this well-known result in terms of the Weisfeiler-Leman algorithm.

Corollary 4.2.7. *Each finite abelian group is identified by 2-WL$_{\text{implicit}}$.*

4.2.1 Derived subgroups, central series & conjugacy classes

We now consider various fundamental notions from the theory of finite groups related to commutation. A detailed treatment can be found in [59], for example.

Lemma 4.2.8. *Consider finite groups G, G_1 and G_2.*

1. *If $G_1 \equiv^2_{\text{implicit}} G_2$ holds, then there exists a bijection $f\colon G_1 \to G_2$, such that for all $g \in G_1$ we have $|C_{G_1}(g)| = |C_{G_2}(f(g))|$.*

2. *The center $Z(G)$ is 2-$\mathrm{WL}_{\text{implicit}}$-detectable.*

Proof. For each $g \in G$, we observe that 2-$\mathrm{WL}_{\text{implicit}}$ iteratively counts the number of pairs (g, g') with $g' \in G$ such that $\langle g, g' \rangle$ is abelian, which readily implies both claims. □

Every $g \in G$ induces an *inner* automorphism $\kappa_g \in \mathrm{Aut}(G)$ of G via $\kappa_g(h) := ghg^{-1}$. Recall the definition of the *inner automorphism group* $\mathrm{Inn}(G) = \{\kappa_g \mid g \in G\}$, which is isomorphic to $G/Z(G)$ through the homomorphism $G \mapsto \mathrm{Aut}(G), g \mapsto \kappa_g$. Through the previous result and Theorem 4.1.10, we observe restrictions on the inner automorphism groups of WL-indistinguishable groups.

Corollary 4.2.9. *For any $k \geq 4$ it holds $G \equiv^k_{\text{explicit}} H \Rightarrow \mathrm{Inn}(G) \equiv^k_{\text{explicit}} \mathrm{Inn}(H)$.*

Moreover, through the identity $|x^G| \cdot |C_G(x)| = |G|$, the element-wise correspondence of centralizer orders implies a correspondence of conjugacy class sizes.

Corollary 4.2.10. *If two groups G and H are not distinguished by 2-$\mathrm{WL}_{\text{implicit}}$, then there is a bijection $f\colon G \to H$, such that for all $x \in G$ we have $|x^G| = |f(x)^H|$, and hence G and H have the same number of conjugacy classes (of each fixed length $\ell \in \mathbb{N}$).*

When discussing group theoretic closure operators (Lemma 4.1.3), we saw that commutators defined with entries in detectable subsets are again detectable. We apply this to the group regarded as a detectable subset itself.

Corollary 4.2.11. *For $k \geq 3$, $G' := [G, G]$ is 3-$\mathrm{WL}_{\text{implicit}}$-detectable.*

Let us point out that $k \geq 3$ is a necessary requirement in the previous corollary, as computations on SmallGroup(128,171) and SmallGroup(128,1122) from the Small Groups Library in GAP [43] show. These groups are not distinguished by 2-$\mathrm{WL}_{\text{implicit}}$, despite the fact that they can be distinguished by the logical expression $\forall x\colon x^2 \in G'$. Hence, the derived subgroup is *not* 2-$\mathrm{WL}_{\text{implicit}}$-detectable.

Set $G_{(0)} := G$ and for all $i > 0$ let $G_{(i)} := \big(G_{(i-1)}\big)'$. This defines a chain of characteristic subgroups $G = G_{(0)} \geq G_{(1)} \geq \cdots \geq G_{(t)} = G_{(t+1)}$ for some $t \geq 0$ (we assume G to be finite), the *derived series* of G. Furthermore, let $G_{(\infty)} := G_{(t)}$ denote the stable term of the derived series.

Lemma 4.2.12. *Let G and H be groups with $G \equiv^k_{\text{explicit}} H$. If $k \geq 4$, then $G/G_{(\infty)}$ and $H/H_{(\infty)}$ have step-wise isomorphic derived series, that is, it holds $G_{(i)}/G_{(i+1)} \cong H_{(i)}/H_{(i+1)}$ for all i. Additionally, for all i we have $G_{(i)} \equiv^k_{\text{explicit}} H_{(i)}$.*

Proof. We show the following: If G and H are not distinguished then $G/G' \cong H/H'$ and G' is not distinguished from H'. Then the claim follows by induction. By the previous corollary, the derived subgroup is detectable by k-$\mathrm{WL}_{\mathrm{explicit}}$ for $k \geq 4$. Theorem 4.1.10 together with $G \equiv^k_{\mathrm{explicit}} H$ implies $G' \equiv^k_{\mathrm{explicit}} H'$, as well as $G/G' \equiv^k_{\mathrm{explicit}} H/H'$. The latter is actually equivalent to $G/G' \cong H/H'$ by Corollary 4.2.7, since G/G' and H/H' are abelian. □

Recall that a group G is solvable, if and only if $G_{(\infty)}$ is the trivial group.

Corollary 4.2.13. *For $k \geq 4$, k-$\mathrm{WL}_{\mathrm{explicit}}$ distinguishes solvable from non-solvable groups.*

Similar arguments can be used to cover the lower and upper central series. Set $Z_0 := G$ and $Z_{i+1} := [Z_i, G]$ for $i \geq 0$. Then $Z_i' \leq [Z_i, G] = Z_{i+1}$ and thus Z_i/Z_{i+1} is again abelian. Define Z_∞ as the stable term of this series, the *lower central series* of G. Then G is nilpotent if and only if $Z_\infty = \{1\}$ holds, and in this case the nilpotency class of G is the minimal c with $Z_\infty(G) = Z_c(G)$.

Lemma 4.2.14. *Let G and H be groups with $G \equiv^k_{\mathrm{explicit}} H$. If $k \geq 4$, then we have $Z_i(G)/Z_{i+1}(G) \cong Z_i(H)/Z_{i+1}(H)$ for all i. Additionally, for all i we have $Z_i(G) \equiv^k_{\mathrm{explicit}} Z_i(H)$ and $G/Z_i(G) \equiv^k_{\mathrm{explicit}} H/Z_i(H)$. In particular, G and H have the same nilpotency class (including the possibility that both G and H are not nilpotent).*

We omit the proof since it is analogous to the proof for the derived series. The *upper central series* is defined implicitly via $Z^0 := \{1\}$, $Z^1 := Z(G)$ and $Z^{i+1}/Z^i := Z(G/Z^i)$.

Lemma 4.2.15. *Let G and H be groups with $G \equiv^k_{\mathrm{explicit}} H$. If $k \geq 4$, then we have $Z^{i+1}(G)/Z^i(G) \cong Z^{i+1}(H)/Z^i(H)$ for all i. Additionally, for all i we have $Z^i(G) \equiv^k_{\mathrm{explicit}} Z^i(H)$ and $G/Z^i(G) \equiv^k_{\mathrm{explicit}} H/Z^i(H)$.*

Proof. By definition, $x \in G$ is in $Z^{i+1}(G)$ if and only if for all $y \in G$ it holds $[x, y] \in Z^i(G)$. If $Z^i(G)$ is k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable with $k \geq 4$, then $Z^{i+1}(G)$ is detectable as well. To see this, consider the group expression $(G, G, G \setminus Z^i(G); \mathcal{R} := \{[x_1, x_2] = x_3\})$. Then $Z^{i+1}(G)$ is the complement of $T_1^\exists$ in G, where $T_1^\exists$ is defined as in Lemma 4.1.2, and in particular this set is k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable. So the first claim of the lemma follows by induction. Furthermore, the indistinguishability of G and H now inductively implies $Z^i(G) \equiv^k_{\mathrm{explicit}} Z^i(H)$ for all i. Theorem 4.1.10 gives us $Z^{i+1}(G)/Z^i(G) \equiv^k_{\mathrm{explicit}} Z^{i+1}(H)/Z^i(H)$ for all i, which can be replaced by isomorphism since these quotients are abelian by definition. □

4.2.2 Groups of prime power order

In this subsection, p always denotes a prime. The structure of finite p-groups is largely controlled by their power-structure and the behavior of commutators. For a detailed account of the theory of p-groups, see [65].

Much of the behavior of commutators is encoded in the lower and upper central series, and we already proved that these are 4-$\mathrm{WL}_{\mathrm{explicit}}$-detectable. Similarly, concerning the power-structure of a p-group, one frequently encounters the omega series and the agemo series.

Lemma 4.2.16. *Let G be a finite p-group. For $i \in \mathbb{N}$, the i-th omega subgroup of G is*

$$\Omega_i(G) = \langle \{x \in G \mid |x| \leq p^i\} \rangle,$$

the i-th agemo subgroup of G is

$$\mho_i(G) = \langle \{x^{p^i} \in G \mid x \in G\} \rangle.$$

For each i, we have that $\Omega_i(G)$ and $\mho_i(G)$ are 3-WL_{implicit}-detectable.

Proof. The detectability follows from the detectability of elements of a fixed order and detectability of p^i-th powers (Lemma 4.2.5), together with Lemma 4.1.3 to obtain detectability of the generated subgroups. □

Corollary 4.2.17. *Let G be a finite p-group. Then the Frattini subgroup $\Phi(G)$ is* 3-WL$_{\text{implicit}}$*-detectable. If H is not distinguished from G by* 4-WL$_{\text{explicit}}$*, then H is also a p-group with $G/\Phi(G) \cong H/\Phi(H)$. In particular, G and H have the same minimal number of generators.*

Proof. Since G is a finite p-group, we have $\Phi(G) = \Omega_1(G)G'$. The detectability claim follows from Lemmas 4.1.3 and 4.2.16. The claim about isomorphism of quotients follows from Theorem 4.1.10, together with the fact that the given quotients are abelian. Finally, the minimal number of generators of a p-group is the dimension of the elementary abelian group $G/\Phi(G)$ regarded as an $\mathbb{F}_p$-vector space. □

Definition 4.2.18. A p-group G is called *regular*, if for any $a, b \in G$, there exists an element c in the derived subgroup of $\langle a, b\rangle$, such that $(ab)^p = a^p b^p c^p$ holds. A p-group G is called *powerful*, if $G' \leq \Omega_1(G)$ holds, in the case that p is odd, or if $G' \leq \Omega_2(G)$ holds, otherwise.

P. Hall pioneered the investigation of regularity properties of abelian p-groups in the broader context of arbitrary p-groups, leading to the definition of a regular p-group. For a regular p-group G, it holds that $\Omega_i(G)$ is just the set of elements of order at most p^i.

For instance, a p-group is regular if its nilpotency class is less than p. All groups of exponent p are regular, see [65]. An important characterization is given by the fact that a p-group is regular, if and only if every 2-generated subgroup is regular [65]. This implies the following corollary in the context of Weisfeiler-Leman.

Corollary 4.2.19. *Regular p-groups are distinguished from non-regular p-groups and powerful p-groups are distinguished from non-powerful p-groups by* 3-WL$_{\text{implicit}}$.

4.2.3 Radicals

Let $\mathcal{F}$ be a class of finite groups that is closed under isomorphism and normal products (that is, whenever two normal subgroups of a group, say N_1 and N_2 are in $\mathcal{F}$, then so is $\langle N_1 N_2\rangle$). Furthermore, let G be an arbitrary finite group. Then the *$\mathcal{F}$-radical $\mathcal{O}_{\mathcal{F}}(G)$* of G is defined as the subgroup generated by normal subgroups of G belonging to $\mathcal{F}$, and by definition of $\mathcal{F}$, this is the largest normal $\mathcal{F}$-subgroup in G. We consider the following explicit standard examples:

1. the π-radical $\mathcal{O}_\pi(G)$, where π is a collection of primes and $\mathcal{F}$ is the class of π-groups (groups whose order is divisible by primes in π only),
2. the nilpotent radical, also known as the *Fitting subgroup*, denoted $\mathrm{Fit}(G)$, where where $\mathcal{F}$ is the class of nilpotent groups,
3. the solvable radical $\mathcal{R}(G)$, where $\mathcal{F}$ is the class of solvable groups,
4. moreover, we consider the largest abelian normal subgroup $\mathcal{A}(G)$, assuming that it exists (here, the product of abelian subgroups is not necessarily abelian).

We work in the general setting first and later come back to the examples from above. The following lemma is well-known in the theory of radical subgroups.

Lemma 4.2.20. *Assume $\mathcal{F}$ is closed under taking normal subgroups. Then $\mathcal{O}_\mathcal{F}(G)$ is the set of all elements whose normal closure belongs to $\mathcal{F}$.*

Proof. By definition $\mathcal{O}_\mathcal{F}(G)$ is the unique largest normal $\mathcal{F}$-subgroup in G. Thus, if $x \in \mathcal{O}_\mathcal{F}(G)$ then the normal closure of x is a normal subgroup contained in the radical and hence belongs to $\mathcal{F}$ since $\mathcal{F}$ is assumed to be closed under normal subgroups. On the other hand it is always the case that elements with normal closure in $\mathcal{F}$ contribute to $\mathcal{O}_\mathcal{F}(G)$, since this is the unique largest normal $\mathcal{F}$-subgroup in G. □

Lemma 4.2.21. *Let $k \geq 3$. If $\mathcal{F}$ is closed under taking normal subgroups and $(k-1)$-$\mathrm{WL}_{\mathrm{implicit}}$ distinguishes $\mathcal{F}$-groups from all other groups, then k-$\mathrm{WL}_{\mathrm{implicit}}$ detects $\mathcal{O}_\mathcal{F}(G)$ in G.*

Proof. In Corollary 4.1.4 we proved that k-$\mathrm{WL}_{\mathrm{implicit}}$ can distinguish elements based on $(k-1)$-dimensional properties of their normal closures. Then by the assumptions above and the previous lemma, k-$\mathrm{WL}_{\mathrm{implicit}}$ detects the set of group elements whose normal closure belongs to $\mathcal{F}$, which is precisely the radical in this case. □

Also note that in all examples we consider above, $\mathcal{F}$ is indeed closed under normal subgroups.

In the previous section we showed that 2-$\mathrm{WL}_{\mathrm{implicit}}$ identifies all abelian groups and distinguishes π-groups from other groups for fixed π.

Corollary 4.2.22. *The π-radical $\mathcal{O}_\pi(G)$ is 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable, where π is an arbitrary collection of primes. If G has a unique maximal abelian normal subgroup $\mathcal{A}(G)$, then it is also 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

Proof. The claim for $\mathcal{O}_\pi(G)$ is a direct consequence of Lemma 4.2.21. If we consider groups with unique maximal abelian normal subgroups, then the class of abelian subgroups fulfills all our assumptions on $\mathcal{F}$. So the same detectability claim holds. □

Regarding the Fitting subgroup, recall that finite nilpotent groups are direct products of p-groups (see e.g. [111]) and thus the nilpotent radical of a finite group, i.e., $\mathrm{Fit}(G)$, is the largest normal subgroup that is a direct product of p-groups. By definition this means

$$\mathrm{Fit}(G) = \bigtimes_{p \mid |G|} \mathcal{O}_p(G).$$

The detectability of the Fitting subgroup therefore follows from the discussion of π-radicals for $\pi := \{p\}$ and Corollary 4.1.7.

However, in the specific case of p-radicals for a prime p, we can improve the bound through the following characterization.

Lemma 4.2.23. *Let G be a finite group and let $x \in G$ be a p-element. Then x lies in $\mathcal{O}_p(G)$, if and only if $\langle x, x^g \rangle$ is a p-group for every $g \in G$. In particular, the p-radical $\mathcal{O}_p(G)$ for each prime p, and hence the Fitting subgroup $\mathrm{Fit}(G)$, is 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

Proof. The characterization of elements in the p-radical is taken from [46].

We have to proof the detectability claim. Let G^* be another group and let $x^* \in G^*$ be a p-element. If x is not distinguished from x^* by 2-$\mathrm{WL}_{\mathrm{implicit}}$, then there is a bijection $f\colon G \to G^*$ such that the map $x \mapsto x^*$, $g \mapsto f(g)$ extends to an isomorphism between $\langle x, g \rangle$ and $\langle x^*, f(g) \rangle$ for every $g \in G$. Thus, for every $g \in G$, we have that $\langle x, x^g \rangle$ is a p-group if and only if $\langle x^*, (x^*)^{f(g)} \rangle$ is a p-group. It follows that $x \in \mathcal{O}_p(G)$ holds if and only if $x^* \in \mathcal{O}_p(G^*)$ holds. □

In terms of the Fitting subgroup, we thus reach the following bound.

Corollary 4.2.24. *The Fitting subgroup $\mathrm{Fit}(G)$ is 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

There is another well-known characterization of the π-radical as the intersection of all maximal π-subgroups of G. More generally, the Weisfeiler-Leman algorithm is capable of exploiting arbitrary intersections of maximal π-subgroups.

Lemma 4.2.25. *Let π be a set of primes and consider two π-elements $g \in G$ and $h \in H$. Let $S_g \leq G$ and $S_h \leq H$ be the intersections of all maximal π-subgroups of G and H, containing g and h, respectively. If $\left(\chi^k_{\mathrm{implicit}}(G)\right)(g) = \left(\chi^k_{\mathrm{implicit}}(H)\right)(h)$ then we have $S_g \equiv^{k-1}_{\mathrm{implicit}} S_h$.*

Proof. Let Π_K be the set of maximal π-subgroups of K for $K \in \{G, H\}$. For π-elements $g \in G$ consider $M_g := \{x \in G \mid \langle x, g \rangle \text{ is a } \pi\text{-group}\}$ and similarly define M_h for $h \in H$. Then for all π-elements $x \in G$ it holds that $M_x = \bigcup_{P \in \Pi_G, x \in P} P$ and $S_x = \{g \in G \mid M_x \subseteq M_g\}$ and the same holds for π-elements in H. If x is not distinguished from y by k-$\mathrm{WL}_{\mathrm{implicit}}$, then by Lemma 3.2.13, Duplicator has a winning strategy in the implicit $(k+1)$-pebble game on (G, H) starting in the configuration $[(x, \perp^k), (y, \perp^k)]$. As long as the pair (x, y) is pebbled, Duplicator has to map M_x to M_y, or otherwise Spoiler can immediately reach a configuration where a π-element is matched with a non-π-element in a fixed pebble pair and win. But then the same holds for S_x and S_y by the way we characterized these sets above. Since Spoiler can leave the first pebble pair on (x, y) and still use the remaining k pebble pairs freely, the claim follows. □

Lastly, the solvable radical can be handled using the detectability of the derived series we proved earlier in this section (see Corollary 4.2.13). We can slightly improve the bound on the WL-dimension by using the following "Thompson-like" characterization of the solvable radical.

Theorem 4.2.26 ([57], Theorem 1.1)**.** *Let G be a finite group and $\mathcal{R}(G)$ the solvable radical of G. An element $g \in G$ belongs to $\mathcal{R}(G)$ if and only if for every $h \in G$ the subgroup $\langle g, h \rangle$ is solvable.*

Corollary 4.2.27. *The solvable radical $\mathcal{R}(G)$ is* 2-WL$_{\text{implicit}}$*-detectable.*

Proof. By Theorem 4.2.26, membership to $R(G)$ can be decided in terms of isomorphism types of subgroups generated by pairs (x, y) for fixed $x \in G$. □

4.2.4 Simple groups, simple quotients & composition factors

Recall that a group is called *almost simple* if its socle is a non-abelian simple group. As a consequence of the classification of finite simple groups, finite simple and almost simple groups can be generated with 2 and 3 elements, respectively (see [107], for instance). The following is a direct consequence of Lemma 4.2.4.

Lemma 4.2.28. *Each finite simple group is identified by* 2-WL$_{\text{implicit}}$. *Each finite almost simple group is identified by* 3-WL$_{\text{implicit}}$.

In the case of simple groups, there is an even stronger result, stating that simple groups are uniquely identified among all groups up to isomorphism by their order and the orders of their elements [106].

Next, we take a closer look at direct products of simple groups. For these groups, the lattice of normal subgroups has a particularly simple structure.

Lemma 4.2.29. *Let G be a group admitting a direct decomposition $G = G_1 \times \cdots \times G_k \times A$, where for all i, G_i is non-abelian simple and A is abelian. Let $S \trianglelefteq G$ be non-abelian simple, then*

$$S = \{1\} \times \cdots \times \{1\} \times G_i \times \{1\} \times \cdots \times \{1\}$$

for some $i \in [k]$.

Proof. Otherwise [32, Theorem 4.3A] would imply $S \leq C_G(G_1 \times \cdots \times G_k \times \{1\}) = Z(G)$ which contradicts the fact that S is non-abelian. □

Let us recall that a group is called *characteristically simple* if it does not contain any proper, non-trivial characteristic subgroups. Finite characteristically simple groups are precisely the finite direct products of isomorphic simple groups (see for instance [111]).

Lemma 4.2.30. *Every finite characteristically simple group is identified by* 3-WL$_{\text{implicit}}$.

Proof. Let G and H be finite groups such that G is characteristically simple and indistinguishable from H by 3-WL$_{\text{implicit}}$. By assumption we have $G \cong T^m$ for a simple group T. If T is abelian then so is G and we already discussed the abelian case. Thus assume that T is non-abelian. Since simple groups are 2-generated, Lemma 4.1.5 shows that 3-WL$_{\text{implicit}}$ detects the set M_G of all pairs $(g_1, g_2) \in G^2$ that generate a normal subgroup isomorphic to T. Set $E_G := \{g \in G \mid \exists x \in G : (g, x) \in M_G\}$. By Lemma 4.2.29, the normal subgroups of G isomorphic to T are exactly the m different copies of T defining G, so $|E_G| = m|\{t \in T \mid \exists x \in T : \langle t, x\rangle = T\}|$. Since we assume $G \equiv^3_{\text{implicit}} H$, the corresponding sets $E_H \subseteq H$ and $M_H \subseteq H^2$, which are defined in the same way as E_G and M_G, must be indistinguishable from E_G and M_G via 3-WL$_{\text{implicit}}$. Thus, H contains at least m different normal subgroups isomorphic to T. Due to simplicity of T they must intersect trivially and centralize each other (given distinct normal subgroups $T_1, T_2 \cong T$, $T_1 \cap T_2$ is normal in T_i and thus $[T_1, T_2] \leq T_1 \cap T_2 = \{1\}$) and considering $|H| = |G| = |T|^m$ we obtain $H \cong T^m$. □

Lemma 4.2.31. *For $k \geq 3$, k-$\mathrm{WL}_{\mathrm{implicit}}$ identifies finite direct products of finite simple groups. More precisely, consider $T_1^{m_1} \times \cdots \times T_r^{m_r}$ with pairwise non-isomorphic simple groups $T_1, \ldots, T_r$. Then, for all $i \in \mathbb{N}$, it holds that $\{1\} \times \cdots \times \{1\} \times T_i^{m_i} \times \{1\} \times \cdots \times \{1\}$ is 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

Proof. As in the previous proof, 3-$\mathrm{WL}_{\mathrm{implicit}}$ can distinguish pairs that generate a normal subgroup isomorphic to some fixed non-abelian simple group from other pairs. Together with Lemma 4.2.29, this implies that direct factors of the form $\{1\} \times \cdots \times \{1\} \times T_i^{m_i} \times \{1\} \times \cdots \times \{1\}$ for non-abelian simple T_i are detected in G by 3-$\mathrm{WL}_{\mathrm{implicit}}$. In the case that T_i is abelian, we note that $T_i \cong C_{p_i}$ for some prime p_i and then $\{1\} \times \cdots \times \{1\} \times T_i^{m_i} \times \{1\} \times \cdots \times \{1\}$ coincides with the 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable set of central p_i-elements in G.

In conclusion, G is identified by 3-$\mathrm{WL}_{\mathrm{implicit}}$ as a direct product of detectable subgroups (see Corollary 4.1.7), all of which are characteristically simple, and hence themselves identified by 3-$\mathrm{WL}_{\mathrm{implicit}}$ due the Lemma 4.2.30. □

From our discussion of derived series above, we can deduce that 4-$\mathrm{WL}_{\mathrm{implicit}}$ distinguishes solvable groups with respect to composition factors and their respective multiplicities. We show that this is true for non-solvable groups as well.

Recall that the *socle* $\mathrm{Soc}(G)$ of a group G is the subgroup generated by all minimal normal subgroups of G. In case that G is finite, the socle is a direct product of minimal normal subgroups, and minimal normal subgroups are characteristically simple. So for a finite group G, we can decompose its socle as

$$\mathrm{Soc}(G) = N_1 \times \cdots \times N_t,$$

where each N_i is a minimal normal subgroup of G, it holds that $N_i \cong S_i^{m_i}$ is a direct power of some simple group S_i, and we may assume that the simple groups are pairwise non-isomorphic [32, Section 4.3].

Lemma 4.2.32. *Let G be a finite group and write $\mathrm{Soc}(G) = N_1 \times \cdots \times N_t$ as above. Then for all i, 4-$\mathrm{WL}_{\mathrm{implicit}}$ detects N_i in G. In particular, the socle $\mathrm{Soc}(G)$ is 4-$\mathrm{WL}_{\mathrm{implicit}}$ detectable.*

Proof. We first show that 4-$\mathrm{WL}_{\mathrm{implicit}}$ detects the set of elements $x \in G$ whose normal closures are minimal normal subgroups of G. Assume x has a normal closure N_x that is minimal normal in G and suppose $y \in G$ has non-minimal normal closure N_y. By Corollary 4.1.4, if x is not distinguished from y then $N_x \equiv^3_{\mathrm{implicit}} N_y$. But by minimality of N_x, for each $x' \in N_x$ it holds $\langle x'^G \rangle = N_x$ while there is some $y' \in N_y$ with $\langle y'^G \rangle \lneq N_y$. So by Corollary 4.1.4 y' is distinguished from each $x' \in N_x$ by 3-$\mathrm{WL}_{\mathrm{implicit}}$. Thus, 4-$\mathrm{WL}_{\mathrm{implicit}}$ identifies elements whose normal closures are minimal normal subgroups and together they generate $\mathrm{Soc}(G)$, so the latter is also 4-$\mathrm{WL}_{\mathrm{implicit}}$ according to Lemma 4.1.3.

The claim then follows from Lemma 4.2.31 together with the fact that $\mathrm{Soc}(G)$ is a direct product of simple groups. □

By repeatedly taking the socle and dividing it out we can define a series of subgroups $\mathrm{Soc}_1(G) \leq \mathrm{Soc}_2(G) \leq \cdots \leq \mathrm{Soc}_t(G) = G$ such that for all i it holds $\mathrm{Soc}_{i+1}(G)/\mathrm{Soc}_i(G) = \mathrm{Soc}(G/\mathrm{Soc}_i(G))$. We refer to this as the *socle series*, and we note that, inductively, the quotient groups $\mathrm{Soc}_{i+1}(G)/\mathrm{Soc}_i(G)$ are direct products of simple groups.

Lemma 4.2.33. *Consider a finite group G and finite simple groups $T_1, \dots, T_m$. Let $N_{T_1,\dots,T_m}$ denote the (unique) normal subgroup of G that is minimal with respect to the following property: the quotient is isomorphic to a direct product of simple groups, such that each simple factor is in $\{T_1, \dots, T_m\}$. Then $N_{T_1,\dots,T_m}$ is 5-$\mathrm{WL}_{\mathrm{explicit}}$-detectable.*

Proof. Let $\mathrm{Soc}_{-1}(G)$ be the last term of the socle series of G that is not equal to G. Then $G/\mathrm{Soc}_{-1}(G)$ is a direct product of simple groups by definition of the socle series. Now $N_{T_1,\dots,T_m}$ is precisely the subgroup $N \trianglelefteq G$ such that $\mathrm{Soc}_{-1}(G) \leq N$ and $N/\mathrm{Soc}_{-1}(G)$ contains each simple factor of $G/\mathrm{Soc}_{-1}(G)$ that is not contained in $\{T_1, \dots, T_m\}$. We have that $N/\mathrm{Soc}_{-1}(G)$ is 4-$\mathrm{WL}_{\mathrm{implicit}}$-detectable by Lemma 4.2.31 and then $N = N_{T_1,\dots,T_m}$ is 5-$\mathrm{WL}_{\mathrm{explicit}}$-detectable by Lemma 4.2.32 and Theorem 4.1.10. □

The findings of this subsection are condensed into the following theorem. It establishes a correspondence between the composition factors of pairs of groups that are indistinguishable via the Weisfeiler-Leman algorithm.

Theorem 4.2.34. *Let $k \geq 5$ and let G and H be two groups that are indistinguishable via 5-$\mathrm{WL}_{\mathrm{explicit}}$. Then G and H have the same composition factors (with multiplicities).*

Proof. By Lemma 4.2.32, the socle is 5-$\mathrm{WL}_{\mathrm{explicit}}$-detectable. By Theorem 4.1.10 we obtain $\mathrm{Soc}(G) \equiv^k_{\mathrm{explicit}} \mathrm{Soc}(H)$ as well as $G/\mathrm{Soc}(G) \equiv^k_{\mathrm{explicit}} H/\mathrm{Soc}(H)$. Then first $\mathrm{Soc}(G)$ and $\mathrm{Soc}(H)$ have the same composition factors (with multiplicities) by Lemma 4.2.31, and inductively the same holds for $G/\mathrm{Soc}(G)$ and $H/\mathrm{Soc}(H)$. We note that in the base case, it holds $G = \mathrm{Soc}(G)$ and $H = \mathrm{Soc}(H)$, so in this case we are done. Now by normality of $\mathrm{Soc}(G)$, the composition factors of G are precisely the composition factors of $\mathrm{Soc}(G)$ together with the composition factors of $G/\mathrm{Soc}(G)$ (in each case considered with multiplicities) and the same holds for H, so the claim follows inductively. □

4.2.5 Verbal subgroups

In this subsection, we return to the consideration of word logic on finite groups. More concretely, we investigate the relationship between stable Weisfeiler-Leman colorings, verbal subgroups and group laws.

As a consequence of Lemma 4.1.2, we obtain the following statement on group laws and verbal subgroups.

Lemma 4.2.35.

1. *Let W be a set of words over variables $\{x_1, \dots, x_{k-1}\}$ and their inverses and let G be a finite group. Then $W(G)$ is k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

2. *If G and H are finite groups indistinguishable by k-$\mathrm{WL}_{\mathrm{implicit}}$, then they obey the same t-group laws for each $t \leq k$.*

Proof.

1. For each word w over $k-1$ variables, the marked isomorphism type of $(x_1, \dots, x_k)$ encodes if x_k is of the form $w(x_1, \dots, x_{k-1})$ or not. Hence, the claim follows from Lemma 4.1.2.

2. Given natural numbers $t' < t$, we can always interpret a t'-group law as a t-group law, so it is sufficient to prove the claim for $t = k$. Thus, let w be k-group law for G and assume that w is not a group law for H. By definition, there exist $h_1, \dots, h_k \in$

H such that $w(h_1, \ldots, h_k) \neq 1$ holds in H, while $w(g_1, \ldots, g_k) = 1$ is always fulfilled for $g_1, \ldots, g_k \in G$. Hence Spoiler has a winning strategy in the implicit $k+1$-pebble game by successively placing pebble pairs on $(h_1, g_1), \ldots, (h_k, g_k)$, where $g_1, \ldots, g_k$ can be arbitrarily chosen by Duplicator's moves: the resulting configuration fulfills the winning condition for Spoiler by definition. This contradicts the assumption that G and H are indistinguishable. □

Recall that a 1-fold commutator is just a regular commutator and an $(n+m)$-fold commutator is any expression of the form $[x, y]$ or $[y, x]$, where y is an n-fold commutator and x is an m-fold commutator. Verbal subgroups of nilpotent groups are particularly restricted through the fact that c-fold commutators vanish, where c is the nilpotency class.

Lemma 4.2.36. *Let G be a finite nilpotent group of nilpotency class c. Then it holds that* $\max\{c, 3\}$-$\mathrm{WL}_{\mathrm{implicit}}$ *detects every verbal subgroup of G.*

Proof. Let W be a set of words over variables $\{x_1, x_1^{-1}, x_2, x_2^{-2}, \ldots, \}$. Since $W(G)$ is generated by $\bigcup_{w \in W} w(G)$, in view of Lemma 4.1.3, it is sufficient to show the claim for $|W| = 1$. So assume $W = \{w\}$ for a single word $w = w(x_1, \ldots, x_n)$, and we need to argue that $w(G)$ is c-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.

Since G is nilpotent of class c, we have that c-fold commutators vanish in G. Thus, by reordering subwords in w and collecting commutators on the right hand side, we may assume without loss of generality that w is of the form $\prod_{I \subseteq [n]} w_I$, where w_I is a product of $(|I|-1)$-fold commutators over the variables x_i with $i \in I$ (or a power of x_i, respectively, in the case $I = \{i\}$) and such that w_I appears before w_J, whenever $|I| < |J|$ holds. In particular, it holds $w_I(g_1, \ldots, g_{|I|}) = 1$ in G, whenever one of the g_i is the identity of G. Let us call this latter assertion Property ⊛.

Set $W' := \{w_I \mid I \subseteq [n]\}$. By definition we have $w(G) \leq W'(G)$. We now show by induction on $|I|$ that $w_I(G) \leq w(G)$ holds for each $I \subseteq [n]$. If $I = \{x_j\}$ for some $j \in [n]$, then, by Property ⊛, we have $w(1, \ldots, 1, x_j, 1, \ldots, 1) = w_I(x_j) = x_j^d$ for some integer d, and hence, $w_I(G) \leq w(G)$ holds.

Now let I be an arbitrary subset of $[n]$. Denote by $w(I)$ the word obtained from w by setting $x_j = 1$ for each $j \notin I$, so in particular we have $(w(I))(G) \leq w(G)$. By Property ⊛, we have a factorization $w(I) = w_{I_1} \cdots w_{I_m}$, where each I_j is a subset of I and the cardinality of these subsets is non-decreasing from left to right. We note that then $I_m = I$ holds and that each I_j with $j \neq m$ is a strict subset of I. By the induction hypothesis, for each $j < m$, we have $w_{I_j}(G) \leq w(G)$. Thus, for each sequence of group elements $\bar{g} = (g_1, \ldots, g_{|I|})$, it follows that

$$w_I(\bar{g}) = (w_{I_1}(\bar{g}))^{-1} \cdots \left(w_{I_{m-1}}(\bar{g})\right)^{-1} (w(I))(\bar{g}) \in w(G),$$

where we use the notation $w_{I_j}(\bar{g})$ for the word obtained by substituting x_k in w_{I_j} with g_k, if $k \in I_j$, and ignoring the other inputs. Since this holds for any sequence of $|I|$ group elements, we have $w_I(G) \leq w(G)$.

In conclusion, we have $w(G) = W'(G)$. Since, by assumption, all c-fold commutators vanish in G, we may now assume that W' only contains words w_I with $|I| < c$. Hence, each word $w' \in W'$ is a word in at most $c-1$ variables, so c-$\mathrm{WL}_{\mathrm{implicit}}$ detects each $w'(G)$ and thus also $W'(G) = w(G)$. □

For broader classes of groups, verbal subgroups can be approached through an equivalence relation on minimal normal subgroups, that is called similarity in [76].

Definition 4.2.37. Let G and H be groups and let $N \trianglelefteq G$ and $M \trianglelefteq H$ be minimal normal subgroups. Then N is *similar* to M if there exist isomorphisms $\varphi\colon N \to M$ and $\psi\colon G/C_G(N) \to H/C_H(M)$ such that

$$\forall g \in G, \forall x \in N\colon \left(x^{gC_G(N)}\right)^{\varphi} = (x^{\varphi})^{\psi(gC_G(N))},$$

so via φ and ψ, the conjugation action of G on N is permutationally isomorphic to the conjugation action of H on M.

The following result relates similarity of minimal normal subgroups to the structure of minimal verbal subgroups.

Lemma 4.2.38 (see [76])**.** *Let V be a minimal verbal subgroup of a finite group G. Then V is a direct product of similar minimal normal subgroups of G. In particular, V is characteristically simple.*

To investigate similarity of non-abelian minimal normal subgroups, we need to introduce additional group theoretic concepts.

Definition 4.2.39. A group is called *monolithic* if it has a unique minimal normal subgroup (which is then called the *monolith* of G), or in other words, if its socle is a minimal normal subgroup. A group is called *semisimple*, if it does not contain abelian normal subgroups, and *anabelian* if it does not admit any abelian composition factors.

Lemma 4.2.40. *Let G be anabelian and let V_1 and V_2 be verbal subgroups of G. Then $V_1 \cap V_2$ is again verbal in G.*

Proof. Since G is anabelian, every normal subgroup of G is perfect. Furthermore, $[V_1, V_2]$ is always verbal by definition. Now we have

$$V_1 \cap V_2 = [V_1 \cap V_2, V_1 \cap V_2] \leq [V_1, V_2] \leq V_1 \cap V_2,$$

so $V_1 \cap V_2 = [V_1, V_2]$ is verbal. □

Isomorphism of semisimple groups reduces to compatibility of the induced actions on the socle, in the following sense.

Lemma 4.2.41 ([9])**.** *Let G and H be semisimple groups. Then $G \cong H$ holds, if and only if there are isomorphisms $\varphi\colon \operatorname{Soc}(G) \to \operatorname{Soc}(H)$ and $\psi\colon G/\operatorname{Soc}(G) \to H/\operatorname{Soc}(H)$ such that the conjugation action of G on $\operatorname{Soc}(G)$ is permutationally isomorphic to the conjugation action of H on $\operatorname{Soc}(H)$ via φ and ψ.*

In particular, we can understand the similarity relation on non-abelian minimal normal subgroups in terms of isomorphism types of semisimple groups.

Lemma 4.2.42. *Let G and H be finite groups. If N is a non-abelian minimal normal subgroup of G, then $G/C_G(N)$ is monolithic with socle N. In particular, $G/C_G(N)$ is semisimple, and for any non-abelian minimal normal subgroup M in H, we find that N is similar to M, if and only if $G/C_G(N) \cong H/C_H(M)$ holds.*

Proof. Since N is non-abelian and G acts transitively on the simple factors of N, we have that $NC_G(N)/C_G(N)$ is a minimal normal subgroup of $G/C_G(N)$. Let $x \in G \setminus C_G(N)$. Then there is some $n \in N$ with $1 \neq nxn^{-1}x^{-1} \in N \cap \langle x^G \rangle$. In particular, $N \leq \langle x^G \rangle$, so $NC_G(N)/C_G(N)$ is contained in every normal subgroup of $G/C_G(N)$. Hence, G is monolithic with socle N. Then the claim about similarity of minimal normal subgroups follows from the definition of similarity and Lemma 4.2.41. □

We can use the previous lemma to derive a complete description of minimal verbal subgroups of anabelian groups.

Lemma 4.2.43. *Let G be a finite anabelian group and write* $\mathrm{Soc}(G) = M_1 \times \cdots \times M_t$*, such that two minimal normal subgroups of G are similar, if and only if they are contained in the same M_i (so each M_i is a product over a similarity class of minimal normal subgroups). Then then the minimal verbal subgroups of G are exactly $M_1, \ldots, M_t$.*

Proof. Let N be a minimal normal subgroup of G. Since G is anabelian, $G/C_G(N)$ is monolithic with monolith $NC_G(N)/C_G(N)$ and then we obtain that $NC_G(N)/C_G(N)$ is verbal in $G/C_G(N)$. Then, by definition, there is some verbal subgroup of G containing N. By [76, Lemma 2.2 and Lemma 2.3], the minimal verbal subgroup of G containing N is a direct product over minimal normal subgroups of G, each of which is similar to N. Hence, for each $i \in [t]$, there exists a non-trivial subgroup $V_i \leq M_i$ that is verbal in G.

Now let $V = W(G)$ be minimal verbal in G, where W is some set of group theoretic words, and let $N \leq V$ be a minimal normal subgroup of G. If $W(G/C_G(N)) = NC_G(N)/C_G(N)$, then the same holds for each minimal normal subgroup N^* that is similar to N (i.e., $W(G/C_G(N^*)) = N^*C_G(N^*)/C_G(N^*)$), since Lemma 4.2.42 provides isomorphisms between $G/C_G(N)$ and $G/C_G(N^*)$. But $W(G/C_G(N^*)) = N^*C_G(N^*)/C_G(N^*)$ implies $N^* \leq W(G)$. Hence, if $W(G)$ is minimal verbal with respect to containing N, then $W(G) = M_i$, where M_i is generated by the similarity class of N. □

We now complement our result on detectability of verbal subgroups in nilpotent groups, that is, groups without non-abelian composition factors, by investigating verbal subgroups in anabelian groups, that is, groups without abelian composition factors.

Lemma 4.2.44. *Let D denote the* $\mathrm{WL}_{\mathrm{explicit}}$*-dimension of the class of anabelian, monolithic groups (so by definition of* $\mathrm{WL}_{\mathrm{explicit}}$*, we have $D \geq 2$). If G is a finite anabelian group, then* $(D+2)$-$\mathrm{WL}_{\mathrm{explicit}}$ *detects every verbal subgroup of G.*

Proof. By Lemma 4.2.43, the minimal verbal subgroups of G are generated by similarity classes of minimal normal subgroups. By Lemma 4.2.42 and the choice of D, we note that $(D+1)$-$\mathrm{WL}_{\mathrm{implicit}}$ distinguishes minimal normal subgroups up to similarity (see Corollary 4.1.4). Hence, the minimal verbal subgroups of G are $(D+2)$-$\mathrm{WL}_{\mathrm{explicit}}$-detectable. Inductively, every verbal subgroup V is $(D+2)$-$\mathrm{WL}_{\mathrm{explicit}}$-detectable in G/V_0, where V_0 is a minimal verbal subgroup of G that is contained in V. By Theorem 4.1.10, the claim follows. □

In view of the previous lemma, we remark that we later bound the WL-dimension of arbitrary semisimple groups by $\log \log n$, where n is the group order.

4.2.6 Group actions

In this subsection we additionally consider the Weisfeiler-Leman algorithm on permutation groups, regarded as relational structures. In terms of the bijective pebble game this means that the board consists of the permutation groups together with their domains, and Spoiler can place pebbles either on group elements or on domain elements. If we consider a sequence of permutations $\sigma_1, \dots, \sigma_n \in \mathrm{Sym}(\Omega)$ and a sequence of domain elements $\omega_1, \dots, \omega_m \in \Omega$, we simply define the permutation group generated by $\sigma_1, \dots, \sigma_n, \omega_1, \dots, \omega_m$ to be $\langle \sigma_1, \dots, \sigma_n \rangle$ acting on Ω (so formally, the given domain elements are just ignored). This ensures that we do not lose track of the ambient domain and more importantly, the resulting groups still act faithfully on Ω, whereas this does not need to be the case for the orbits containing $\omega_1, \dots, \omega_m$, for instance. We note that the domain elements *do* make a difference in the definition of marked isomorphism types though, that is, $(\sigma_1, \dots, \sigma_n, \omega_1, \dots, \omega_m)$ and $(\sigma_1^*, \dots, \sigma_n^*, \omega_1^*, \dots, \omega_m^*)$ obtain the same marked isomorphism type, if and only if there is a permutational isomorphism between $\langle \sigma_1, \dots, \sigma_n \rangle$ and $\langle \sigma_1^*, \dots, \sigma_n^* \rangle$ that maps σ_i to σ_i^* and ω_j to ω_j^*, for all i and j (in particular, the number of domain and group elements is an invariant of the marked isomorphism type).

A specific application we have in mind is the situation where a group G acts on a WL-detectable subgroup by conjugation.

Definition 4.2.45. The *orbit type* of a group G acting on a set Ω is the multiset of the sizes of G-orbits on Ω.

We first consider basic information about orbit partitions.

Lemma 4.2.46. *Let $Q \leq \mathrm{Sym}(\Omega)$ and $Q^* \leq \mathrm{Sym}(\Omega^*)$ be permutation groups on finite domains Ω and Ω^*.*

1. *Let $\sigma \in Q$ and $\sigma^* \in Q^*$. Assume that $3\text{-WL}_{\text{implicit}}$ applied to (Q, Ω) and (Q^*, Ω^*) does not distinguish σ from σ^*. Then σ and σ^* have the same cycle type.*

2. *If (Q, Ω) is not distinguished from (Q^*, Ω^*) by $3\text{-WL}_{\text{implicit}}$, then Q and Q^* have the same orbit type.*

Proof. 1. The length of the cycle of σ that contains some fixed $\omega \in \Omega$ is encoded in the number of tuples of the form $(\sigma, \omega, \omega')$ with $\omega' \in \Omega$ and $\omega^{\sigma^i} = \omega'$ for some i. So the cycle type of σ is encoded in the stable coloring of the pairs (σ, ω) with $\omega \in \Omega$.

2. The length of the orbit of a point $\omega \in \Omega$ is encoded in the number of pairs (ω, ω') with $\omega' \in \Omega$, such that some $x \in Q$ exists with $\omega^x = \omega'$. By definition, $3\text{-WL}_{\text{implicit}}$ counts the number of such pairs, so the stable color for each $(\omega, 1, 1)$ ultimately encodes the orbit size of w^Q. □

Recall that winning Duplicator moves, restricted to subgroups whose generating sets are currently pebbled, have to coincide with the isomorphism induced by the pebble pairs (we proved this for groups in Lemma 3.2.23). We obtain an analogous statement for permutation groups, the proof is essentially identical.

Lemma 4.2.47. *Consider the implicit k-pebble-game on permutation groups (Q, Q^*) acting on finite sets Ω and Ω^*, respectively. Assume there are currently t pebble pairs on the board, placed on $(g_1, g_1^*), \dots, (g_t, g_t^*) \in Q \times Q^*$ for $t < k-2$, and assume that there is another pebble pair on $(\omega, \omega^*) \in \Omega \times \Omega^*$. Then Duplicator's bijections must restrict to*

1. *the unique ordered isomorphism defined through $g_i \mapsto g_i^*$ on the subgroup $\langle g_1, \dots, g_t \rangle$,*
2. *the unique bijection extending the map $g_i \mapsto g_i^*$, $\omega \mapsto \omega^*$ to a permutational isomorphism, restricted to $\langle g_1, \dots, g_t \rangle$ and the orbit of ω under this group,*

or otherwise Spoiler can win (in particular, these maps have to exist for Duplicator to be able to win).

Corollary 4.2.48. *Given a permutation group (Q, Ω) and $m \in \mathbb{N}$, let $o_m(Q, \Omega)$ denote minimal number of orbits of any m-generated subgroup of Q. It holds*

$$\dim_{\mathrm{WL}_{\mathrm{implicit}}}(Q, \Omega) \leq \min_m (m + o_m(Q, \Omega)) + \mathcal{O}(1).$$

As with groups, various aspects of permutation group theory can be phrased in the framework of the Weisfeiler-Leman algorithm. To cover one important example, we discuss primitivity in more detail.

Definition 4.2.49. Let $Q \leq \mathrm{Sym}(\Omega)$ be a permutation group acting on a finite set Ω and let A be an orbit of Q in the induced action on Ω^2. The *orbital graph* associated with A is the digraph Orb_A with vertex set Ω and arc set A. We say that A, and hence Orb_A, is *diagonal*, if A is a subset of $\{(\omega, \omega) \mid \omega \in \Omega\}$.

A classical result in the area of permutation groups relates components of orbital graphs to block systems of the action.

Lemma 4.2.50 (see [62]). *Let $Q \leq \mathrm{Sym}(\Omega)$ be a permutation group acting on a finite set Ω and let α and β be distinct points in Ω. Then the smallest block of imprimitivity that contains both α and β is precisely the (undirected) connected component of α in the orbital graph Orb_A, where $A := (\alpha, \beta)^Q$.*

In particular, all non-diagonal orbital graphs of a permutation group are connected if and only if the group acts primitively.

We now show that the Weisfeiler-Leman algorithm can *define* the orbital graph of $(\alpha, \beta)^Q$ for any fixed pair (α, β). Denote the smallest block of imprimitivity containing both α and β by $B(\alpha, \beta)$.

Lemma 4.2.51. *Let $Q \leq \mathrm{Sym}(\Omega)$ be a permutation group acting on a finite set Ω and let α and β be points in Ω. Assume that Q is colored with exactly three color classes $\{\alpha\}$, $\{\beta\}$ and $Q \setminus \{\alpha, \beta\}$. Then $B(\alpha, \beta)$ is 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.*

Proof. For all $\omega, \omega' \in \Omega$ and for all $\sigma \in Q$, the marked isomorphism type of $(\omega, \omega', \sigma)$ encodes the colors of ω^σ and $(\omega')^\sigma$. Hence, by definition of the refinement step, pairs (ω, ω') that form arcs in $\mathrm{Orb}_{B(\alpha,\beta)}$ are distinguished from pairs that correspond to non-edges. Consequently (see Lemma 3.2.27), 3-$\mathrm{WL}_{\mathrm{implicit}}$ correctly identifies for each $\omega \in \Omega$, if ω is covered by some arc, that is, if ω belongs to $B(\alpha, \beta)$. □

In terms of the bijective pebble game, the pre-coloring in the previous lemma can be replaced by two pebble pairs that Spoiler leaves fixed throughout the game. This gives the following corollary via Lemma 3.2.13.

Corollary 4.2.52. *Primitive permutation groups are distinguished from imprimitive permutation groups by* 5-$\mathrm{WL}_{\mathrm{implicit}}$.

Finally, we take a look at linear actions on vector spaces, that is, representations of finite groups. We later use the following results to investigate semidirect products where the normal subgroup is abelian. Similar to permutation groups, we consider a pair consisting of a vector space V and a subgroup $G \leq \mathrm{GL}(V)$ as a relational structure (G, V) over the ground set $G \uplus V$, with relations $R_{\mathrm{mult}} := \{(g, h, gh) \mid g, h \in G\}$, $R_{\mathrm{act}} := \{(g, v, gv) \mid g \in G, v \in V\}$ and an additional relation $R_{\mathrm{add}} := \{(v, w, v + w) \mid v, w \in V\}$ to capture the vector space structure.

We recall the Smith normal form and how it can be used to classify endomorphisms of vector spaces.

Lemma 4.2.53 (see [91, Chapters 5 & 6])**.** *Let F be a field, V a finite dimensional F-vector space, of dimension d, and let $E \in F^{d\times d}$. We denote the polynomial ring over F by $F[x]$. Then there exist matrices L and R in $(F[x])^{d\times d}$, such that $L(E - xI_d)R$ is a diagonal matrix with diagonal entries $(e_1(x), \dots, e_r(x))$, where each $e_i(x)$ divides $e_{i+1}(x)$ in $F[x]$. The matrix $L(E - xI_d)R$ is called the* Smith normal form *of $(E - xI_d)$ and the diagonal entries are called the* elementary divisors*. Moreover, the following properties hold:*

1. *the minimal polynomial of E acting on V is $e_r(x)$,*
2. *the characteristic polynomial of E acting on V is $\prod_i e_i(x)$,*
3. *E is uniquely defined up to conjugation by the multiset of elementary divisors,*
4. *V is an $F[x]$-module via letting $f(x) \in F[x]$ act as $f(E)$. With this module structure, V is isomorphic to*

$$F[x]/(e_1F[x]) \oplus \cdots \oplus F[x]/(e_rF[x]).$$

In particular, V is a direct sum of cyclic modules with respect to the action of E.

We first need a general result on cyclic modules over principal ideal domains.

Lemma 4.2.54. *Let R be a principal ideal domain and let M a finite module over R. Then M is uniquely determined up to isomorphism by the multiset of isomorphism types of its cyclic submodules.*

Proof. By the classification of finitely generated modules over principal ideal domains, we can write

$$M = R/(a_1R) \oplus R/(a_2R) \oplus \cdots \oplus R/(a_mR)$$

for appropriate non-zero $a_1, \dots, a_m \in R$ such that a_i divides a_{i+1} for all i. We first note that the multiset of cyclic submodules of M determines a_m (up to multiplication with units in R).

We then observe that all a_i are equal and prime, if and only if each non-trivial, cyclic submodule of M is isomorphic to $R/(a_1R)$ with a_1 prime, and then the number of such modules uniquely determines m. So assume that some a_i is not prime.

We consider the unique submodule of M that is isomorphic to $(R/(a_1R))^m$, say M_0. It is the union over all cyclic submodules of M, that are isomorphic to a submodule of $R/(a_1R)$. If some a_i is not prime, then M_0 and M/M_0 are non-trivial and strictly smaller than M. Hence, the number of cyclic submodules of M that are isomorphic to a submodule of $R/(a_1R)$ uniquely determines M_0 up to isomorphism by induction. Via the epimorphism $M \to M/M_0$, every cyclic submodule of M/M_0 corresponds to a fixed number of cyclic submodules of M that are not contained in M_0. The distribution of isomorphism types of such submodules of M, together with the isomorphism type of M_0, inductively determines M/M_0 up to isomorphism.

By the classification of finitely generated modules over principal ideal domains, M is uniquely determined up to isomorphism by the isomorphism types of M_0 and M/M_0. □

We now use this to prove a general criterion for conjugacy of matrices and then derive an analogue of Lemma 4.2.46 for linear actions.

Lemma 4.2.55. *Let F be a finite field, set $V := F^d$ and let $A, B \in F^{d\times d}$ be two matrices. For $v \in V$, denote the matrix induced by A acting on $\langle v, Av, A^2v, \dots\rangle$ with respect to the basis $(v, Av, \dots)$ by A_v. If there exists a bijection $f : V \to V$ with $A_v = B_{f(v)}$ for all $v \in V$, then A and B are conjugate in* $\mathrm{GL}(V)$.

Proof. Via Lemma 4.2.53, the existence of f implies that V contains the same cyclic submodules (up to isomorphism), when regarded as an $F[X]$ module with respect to the action of A or B, respectively. Then the claim follows from Lemma 4.2.54. □

Lemma 4.2.56. *Let V and V^* be finite vector spaces and assume that $\varphi : V \to V^*$ is a linear isomorphism. Consider groups $G \leq \mathrm{GL}(V)$ and $G^* \leq \mathrm{GL}(V^*)$ and their corresponding relational structures (G, V) and (G^*, V^*), where we encode both the permutation group structure and the vector space structure. If* 4-$\mathrm{WL}_{\mathrm{implicit}}$ *applied to (G, V) and (G^*, V^*) does not distinguish $g \in G$ from $g^* \in G^*$, then g and $\varphi^{-1} \circ g^* \circ \varphi$ are conjugate in* $\mathrm{GL}(V)$.

Proof. Assume that there is be a bijection $f : V \to V^*$ such that the action of g on the $\langle g\rangle$-module generated by v is permutationally equivalent to the action of g^* on the $\langle g^*\rangle$-module generated by $f(v)$, via an isomorphism induced by $g \mapsto g^*$ and $v \mapsto f(v)$. Then $\varphi \circ f$ fulfills the assumptions of Lemma 4.2.55, and we are done.

If such a bijection does not exist, consider the implicit 5-pebble game on (G, V) and (G^*, V^*), starting with a pebble pair on (g, g^*). Since a bijection as above does not exist, independent of Duplicator's choices, Spoiler can place an additional pebble pair on a pair of vectors, say (v, v^*), such that mapping $g \mapsto g^*$ and $v \mapsto f(v)$ does not induce a permutational isomorphism between $\langle v\rangle$ regarded as a $\langle g\rangle$-module and $\langle v^*\rangle$ regarded as a $\langle g^*\rangle$-module. With pebble pairs on (g, g^*) and (v, v^*), Duplicator has to map the vectors $(v, gv, g^2v, \dots)$ to $(v^*, g^*v^*, (g^*)^2v^*, \dots)$ in this order, or otherwise Spoiler can win from the given configuration. By assumption, these tuples fulfill distinct linear relations, which can be exploited by Spoiler to win, using the three additional pebble pairs (this is essentially the same argument that we used to prove Lemma 3.2.23). □

4.3 The Weisfeiler-Leman dimension of direct products of groups

As a first application of our catalog of WL-detectable substructures in finite groups, we now analyze the Weisfeiler-Leman algorithm on direct products of finite groups. The section is organized similar to [73], in the sense that we first consider direct products where one factor is an abelian group (the *semiabelian* case) and reduce to these the general case later on. There is also a similarity in the way the direct factors are computed modulo central elements. However, a crucial difference between our setting and the one in [73] is that in the latter computations can be executed as long as they are efficient, where in our case, we are analyzing a fixed algorithm that cannot make non-canonical choices.

Definition 4.3.1. Given groups G_1 and G_2, central subgroups $Z_1 \leq Z(G_1)$, $Z_2 \leq Z(G_2)$ and an isomorphism $\varphi : Z_1 \to Z_2$, we can form the *central product* of G_1 and G_2 with respect to φ via

$$G_1 \times_\varphi G_2 := G_1 \times G_2/\{(g, \varphi(g^{-1})) \mid g \in Z_1\}.$$

A group G is the *(internal) central product* of subgroups $G_1, G_2 \leq G$, if it holds that $G = \langle G_1, G_2 \rangle$ and $[G_1, G_2] = \{1\}$.

Our main difficulty is that a group can admit several inherently different central decompositions. In contrast to that recall that indecomposable *direct* decompositions are unique in the following sense.

Lemma 4.3.2. *Let $G = G_1 \times \cdots \times G_m = H_1 \times \cdots \times H_n$ be two decompositions of G into directly indecomposable factors. Then $n = m$ and there is a permutation $\sigma \in S_m$ such that for all i we have $G_i \cong H_{\sigma(i)}$ and $G_i Z(G) = H_{\sigma(i)} Z(G)$.*

Proof. The first part is the well-known Krull-Remak-Schmidt Theorem and the addition that $G_i Z(G) = H_{\sigma(i)} Z(G)$ can be easily derived (see for example [73, Corollary 6]) □

In particular, the collection of subgroups $\{G_i Z(G)\}_{1 \leq i \leq m}$ is invariant under automorphisms. Later we show that the union of these subgroups, i.e., $\bigcup_{i=1}^m G_i Z(G)$, is 5-WL$_{\text{explicit}}$-detectable.

Definition 4.3.3. We say a central decomposition $G = H_1 H_2$ is *directly induced* if there are subgroups $K_i \leq H_i$ such that $G = K_1 \times K_2$ and $H_i = K_i Z(G)$.

Whenever there is a pairing between the indecomposable direct factors of two groups, such that each pair is indistinguishable via WL-refinement, then the groups themselves are indistinguishable as well. This is a simple observation in terms of pebble games (given in the next lemma). The other direction, namely that indistinguishable groups always admit such a pairing of indecomposable direct factors, is investigated in the remainder of this section and turns out to be highly non-trivial.

Lemma 4.3.4. *For $k \geq 3$, if we have $G_1 \equiv^k H_1$ and $G_2 \equiv^k H_2$, then $G_1 \times G_2 \equiv^k H_1 \times H_2$, where $\equiv^k$ denotes indistinguishability under a fixed version (*explicit *or* implicit*) of k-*WL.

Proof. Consider the $(k+1)$-pebble game that corresponds to the fixed version of k-WL, played on $(G_1 \times G_2, H_1 \times H_2)$. Assume Duplicator always chooses bijections component-wise, $f_1 : G_1 \to H_1$ and $f_2 : G_2 \to H_2$ say, and combines them to a move $f : (g,h) \mapsto (f_1(g_1), f_2(g_2))$. Given k-tuples $((g_{1,1}, g_{2,1}), \dots, (g_{1,k}, g_{2,k})) \in (G_1 \times G_2)^k$ and $((h_{1,1}, h_{2,1}), \dots, (h_{1,k}, h_{2,k})) \in (H_1 \times H_2)^k$, there is an isomorphism mapping $(g_{1,i}, g_{2,i})$ to $(h_{1,i}, h_{2,i})$ for all i if and only if there is a component-wise isomorphism $G_1 \to H_1$ mapping $g_{1,i}$ to $h_{1,i}$ and a component-wise isomorphism $G_2 \to H_2$ mapping $g_{2,i}$ to $h_{2,i}$, for all $i \in [k]$. In particular, Duplicator can choose f_1 and f_2 according to winning strategies in the $(k+1)$-pebble games on (G_1, H_1) and (G_2, H_2), such strategies exist due to Lemma 3.2.13, and obtain a winning strategy on the direct products. □

4.3.1 Abelian and semi-abelian case

Direct products with abelian groups are easier to handle than the general case and serve as a basis for reduction later on.

Definition 4.3.5. An element $1 \neq x \in G$ *splits* from the group G if there is a *complement* $H \leq G$ of $\langle x \rangle$ in G, that is, $G = \langle x \rangle \times H$.

Lemma 4.3.6. *Let A be a finite, abelian p-group and consider an arbitrary cyclic decomposition $A = A_1 \times \cdots \times A_m$. Then $a = (a_1, \dots, a_m) \in A$ splits from A if and only if there is some i with $|a| = |a_i|$ and $a_i \in A_i \setminus (A_i)^p$.*

Proof. First assume that $|a| = |a_i|$ and $a_i \in A_i \setminus (A_i)^p$ for some i. Then $A_i = \langle a_i \rangle$ and $A = \langle a \rangle \times \langle \{e_j : j \in [m] \setminus \{i\}\} \rangle$, where e_j is a generator of $\{1\} \times \cdots \times \{1\} \times A_j \times \{1\} \times \cdots \times \{1\}$. For the other direction, assume that $A = \langle a \rangle \times B$ holds for some subgroup $B \leq A$. Then it also holds that $A = \langle a' \rangle \times B$ for every element $a' = ax$ with $|x| < |a|$. So we may assume for all i that either $|a_i| = |a|$ or $a_i = 1$ holds. If $e_i^{\frac{|e_i|}{p}} \in B$ holds for all i with $|a_i| = |a|$, then $a^{\frac{|a|}{p}} \in B$ which is a contradiction to $\langle a \rangle \cap B = \{1\}$. So there is some i with $|a_i| = |a|$ and $e_i^{\frac{|e_i|}{p}} \notin B$. Hence, $\langle e_i \rangle \cap B = \{1\}$ and then $A = \langle e_i \rangle \times B$ since $|e_i| \geq |a|$. This finally implies $|a_i| = |a| = |e_i|$ and so $a_i \in A_i \setminus (A_i)^p$. □

Corollary 4.3.7. *Let A be a finite, abelian p-group and $x \in A$. Then $1 \neq x$ splits from A if and only if there is no $y \in A$ such that $|xy^p| < |x|$. Moreover,* 2-WL$_{\text{implicit}}$ *detects the set of all elements that split from A.*

Proof. The first part is a restatement of the previous lemma. Regarding the 2-WL$_{\text{implicit}}$-detectability, recall that, by Lemma 4.1.3, the subgroup $\{a^p \mid a \in A\} \leq A$ is detectable and x does not split from A if and only if for all $a \in A$ and it holds $(xa^p)^{|x|/p} \neq 1$. Thus, the claim follows from Lemma 4.1.2. □

Lemma 4.3.8. *Let A be a finite abelian group and $A = P_1 \times \cdots \times P_m$ the decomposition of A into Sylow subgroups. Then $1 \neq x = (x_1, \dots, x_m)$ splits from A if and only if each x_i is either trivial or splits from P_i. In particular,* 2-WL$_{\text{implicit}}$ *detects the set of elements that split from an abelian group.*

Proof. By the Chinese Remainder Theorem we have $\langle x \rangle \cong \langle x_1 \rangle \times \cdots \times \langle x_m \rangle$. Regarding the detectability note that x_i splits from P_i if and only if $x^{|A|/|P_i|}$ splits from A, so the claim follows from the previous lemma and Lemma 4.1.3. □

Lemma 4.3.9. *Let G be a finite group and $z \in Z(G)$. Then z splits from G if and only if zG' splits from G/G' and $\langle z \rangle \cap G' = \{1\}$.*

Proof. Assume that $G/G' = \langle zG' \rangle \times K$. For a generating set $(k_1G', \dots, k_mG')$ of K, let $\hat{K} := \langle k_1, \dots, k_m \rangle G' \leq G$. Then $G = \hat{K}\langle z \rangle$, and $\langle zG' \rangle \cap K = \{1\}$ together with $\langle z \rangle \cap G' = \{1\}$ implies $\langle z \rangle \cap \hat{K} = \{1\}$. Thus z splits with complement $\hat{K}$. On the other hand, if $G = \langle z \rangle \times H$ then $G' = H'$, so $G/G' = \langle zH' \rangle \times H/H'$ follows. □

Corollary 4.3.10. *The set of elements that split from G is 4-WL$_{\text{explicit}}$-detectable.*

Proof. First note that 3-WL$_{\text{implicit}}$ detects both G' and $Z(G)$ (Corollary 4.2.11 and Lemma 4.2.8) and thus also the set of central elements z with $\langle z \rangle \cap G' = \{1\}$. Furthermore, G/G' is abelian and elements splitting from G/G' are detectable by 2-WL$_{\text{implicit}}$. By Lemma 4.1.10 a), this information can be lifted to G by k-WL$_{\text{explicit}}$ for $k \geq 4$, that is, 4-WL$_{\text{implicit}}$ detects the set of elements $z \in G$ such that zG' splits from G' as well as central elements $z \in G$ with $\langle z \rangle \cap G' = \{1\}$. □

We analyze the splitting of elements in two special instances.

Lemma 4.3.11. *Consider groups U and G with $U \leq G$, and let $x \in Z(G) \cap U$. If x splits from G then x splits from U.*

Proof. If x splits from G, we can write $G = \langle x \rangle \times K$ for a suitable complement $K \leq G$ of x in G. Then $U := \langle x^{m_1}k_1, \dots, x^{m_t}k_t \rangle$ where $k_1, \dots, k_t \in K$ and $m_1, \dots, m_t$ are suitable natural numbers, and since $x \in U$ we obtain $U = \langle x, k_1, \dots, k_t \rangle = \langle x \rangle \times \langle k_1, \dots, k_t \rangle$. □

Lemma 4.3.12. *Consider a direct product $G = G_1 \times G_2$ and a prime p, as well as a p-element $z := (z_1, z_2) \in Z(G)$. Then z splits from G if and only if z_i splits from G_i for some $i \in \{1, 2\}$ which fulfills $|z_i| = |z|$.*

Proof. Since z is a p-element, so is $z_1 \in G_1$ and $z_2 \in G_2$. First assume that $G = \langle z \rangle \times B$ for some suitable $B \leq G$. Without loss of generality assume that $|z_1| = |z|$. If $(z_1, 1) \cap B = \{1\}$ then $G = \langle (z_1, 1) \rangle \times B$, so z_1 splits from G_1 by the previous lemma. Otherwise $(z_1^m, 1) \in B$ for some m such that $z_1^m \neq 1$. By assumption it holds that $z^m \notin B$, thus it must be the case that $|z_2| = |z|$ and $\langle (1, z_2) \rangle \cap B = \{1\}$, so z_2 splits from G_2.

For the other direction, if G_i admits a decomposition $G_i = \langle z_i \rangle \times B_i$ for some $i \in \{1, 2\}$ with $|z_i| = |z|$, then it holds $G = \langle (z_1, z_2) \rangle \times (B_i \times G_j)$ for $\{i, j\} = \{1, 2\}$. □

Let us move on to the semi-abelian case, by which we mean groups of the form $H \times A$ where A is abelian and H does not have abelian direct factors.

Lemma 4.3.13. *Let $G = H \times A$ with A a maximal abelian direct factor. Then the isomorphism type of A is identified by 4-WL$_{\text{explicit}}$, that is, whenever $G^* \equiv^4_{\text{explicit}} G$ holds, then G^* has a maximal abelian direct factor isomorphic to A.*

Proof. Consider a prime p that divides $|G|$. If G^* is another group with $G^* \equiv^4_{\text{explicit}} G$, then $|G| = |G^*|$ and by Lemma 4.2.8 we have $Z(G^*) \cong Z(G)$. Since abelian groups are direct products of their Sylow subgroups, there must be an isomorphism between the respective Sylow p-subgroups of the centers $Z := Z(G)$ and $Z^* := Z(G^*)$. Write $G^* = H^* \times A^*$, where A^* denotes a maximal abelian direct factor of G^*. We can decompose

Z as $Z = Z_1 \times \cdots \times Z_m$ with $Z_i \cong C_{p^i}^{e_i}$, $e_i \geq 0$, and for each i there are subgroups $H_i \leq Z(H)$ and $A_i \leq A$ such that $Z_i = H_i \times A_i$. Analogously define Z_i^*, H_i^* and A_i^*. Since $Z \cong Z^*$ holds, it also holds that $Z_i \cong Z_i^*$ for all i. Therefore it is enough to show that $|A_i| = |A_i^*|$ holds for all i. Since H does not admit abelian direct factors, Lemma 4.3.12 implies that central elements of order p^i split from G if and only if $|A_i(x)| = p^i$, where $A_i(x)$ is the projection of x onto the component A_i in the decomposition of Z from above. The same then holds for G^* and A_i^*. By Lemma 4.3.10, 4-WL$_{\text{explicit}}$ detects the set of central elements of order p^i that split from a group. In particular, if $G^* \equiv_{\text{explicit}}^4 G$ holds, then $|\{x \in Z \mid |x| = p^i = |A_i(x)|\}| = |\{x \in Z^* \mid |x| = p^i = |A_i^*(x)|\}|$ which in turn shows $|A_i| = |A_i^*|$, since both of these groups are some direct power of C_{p^i} by definition. □

Controlling the non-abelian part is more complicated. We first introduce a new technical framework.

Definition 4.3.14. Let $G = L \times R$. A *component-wise filtration* of $U \leq G$ w.r.t. L and R is a chain of subgroups $\{1\} = U_0 \leq \cdots \leq U_r = U$ such that for all $1 \leq i < r$, we have $U_{i+1} \leq U_i(L \times \{1\})$ or $U_{i+1} \leq U_i(\{1\} \times R)$. The filtration is called k-WL$_{\text{explicit}}$-*detectable* if all subgroups in the chain are k-WL$_{\text{explicit}}$-detectable.

Lemma 4.3.15. *Let $G = H \times A$ with maximal abelian direct factor A. There exists a component-wise filtration of $Z(G)$ with respect to H and A, say $\{1\} = U_0 \leq \cdots \leq U_r = Z(G)$, that is* 4-WL$_{\text{explicit}}$*-detectable.*

Proof. First let $p_1 < \cdots < p_n$ denote the primes dividing $|G|$ and write Z_{p_i} for the Sylow p_i-subgroup of $Z(G) = Z(H) \times A$. Assume we already have a component-wise filtration of

$$U = Z_{p_1} \times \cdots \times Z_{p_{i-1}} \times \{z \in Z_{p_i} \mid |z| < p_i^m\}$$

with respect to H and A which is furthermore 4-WL$_{\text{I}}$-detectable. We will argue how to extend it to $U\{z \in Z_{p_i} \mid |z| \leq p_i^m\}$ and then the claim follows by induction. To simplify our notation let $p := p_i$ and let N be maximal such that p^N divides $|Z(G)|$.

Set $V_0 := \{z \in Z_p \mid |z| < p^m\}$ and for $j \geq 1$ define

$$V_j := \langle \{z^{p^{N-j}} \mid z \in Z_p, |z^{p^{N-j}}| \leq p^m\}\rangle V_{j-1},$$

so we aim to extend the filtration such that elements with roots of higher order are added in earlier steps. Further define

$$W_j := \langle \{z^{p^{N-j}} \mid z \in Z_p, |z| \leq p^{N-j+m} \text{ and } z \text{ does not split from } G\}\rangle V_{j-1}.$$

By construction, we have

$$U = UV_0 \leq UW_1 \leq UV_1 \leq \cdots \leq UW_N \leq UV_N = U\{z \in Z_{p_i} \mid |z| \leq p_i^m\}.$$

It remains to show that all W_j and V_j are detectable in G and that the sub-chain $V_{j-1} \leq W_j \leq V_j$ ascends component-wise for all $j \geq 1$.

To show that W_j and V_j are detectable, recall that the set of elements that split from G is 4-WL$_{\text{explicit}}$-detectable according to Corollary 4.3.10 and central e-th powers are 4-WL$_{\text{explicit}}$-detectable for all $e \in \mathbb{Z}$ according to Lemma 4.1.3, thus V_j and W_j are detectable for all j.

To show component-wise ascension, note that if $A = \langle a \rangle \times K_a$ then for all $h \in Z(H)$ with $|h| \leq |a|$ it holds $G = (H \times K_a) \times \langle (h, a) \rangle$. So if $(h, a) \in Z(H) \times A$ does not split from G then either $|h| > |a|$ or a does not split from A and then there is some $b \in A$ with $|ab^p| < |a|$ according to Corollary 4.3.7. Consider $x := (h, a)^{p^{N-j}} \in W_j$ where $|(h, a)| = p^{N-j+m}$ and (h, a) does not split from G. If $|h| > |a|$ then $x \in (h^{p^{N-j}}, 1)V_{j-1}$ since V_{j-1} contains all p-elements of order smaller than p^m. Otherwise $|a| = p^{N-j+m}$ and there is some $b \in A$ with $|ab^{-p}| < |a|$. First, this implies $x \in (h, b^p)^{p^{N-j}} V_{j-1}$, again using the fact that V_{j-1} contains V_0. Now by definition $(1, b^{p^{N-j+1}}) \in V_{j-1}$ and thus $x \in (h^{p^{N-j}}, 1)V_{j-1}$. In conclusion, $V_{j-1} \leq W_j$ is a component-wise extension. The same holds for $W_j \leq V_j$, since H has no abelian direct factors and so if $(h, a) \in V_j$ splits from G then also $(1, a)$ splits from G (this follows from Lemma 4.3.12) and so it holds that $V_j \leq (\{1\} \times A)W_j$. □

Lemma 4.3.16. *Consider groups $G = H \times A$ and $\hat{G} = \hat{H} \times \hat{A}$ where $A \leq G$ and $\hat{A} \leq \hat{G}$ are each a maximal abelian direct factor of their respective parent group. Then, for each $k \geq 5$, we have that $G \equiv^k_{\text{explicit}} \hat{G}$ implies $H \equiv^{k-1}_{\text{explicit}} \hat{H}$.*

Proof. Assume that $G \equiv^k_{\text{explicit}} \hat{G}$ holds. By Lemma 4.3.13 we obtain $A \cong \hat{A}$. Consider the component-wise filtrations from the proof of the previous lemma, $1 = U_0 \leq \cdots \leq U_r = Z(G)$ and $1 = \hat{U}_0 \leq \cdots \leq \hat{U}_r = Z(\hat{G})$, with respect to the decompositions $G := H \times A$ and $\hat{G} = \hat{H} \times \hat{A}$. Then U_i and $\hat{U}_i$ are 4-WL$_{\text{explicit}}$-detectable. Since we assume G and $\hat{G}$ to be indistinguishable via k-WL$_{\text{explicit}}$, we can also assume that U_i and $\hat{U}_i$ obtain the same stable colors for all i. Furthermore, $G \equiv^k_{\text{explicit}} \hat{G}$ implies $U_i \lneq (\{1\} \times A)U_{i+1}$ if and only if $\hat{U}_i \lneq (\{1\} \times \hat{A})\hat{U}_{i+1}$ for all i, as well as $U_i \lneq (H \times \{1\})U_{i+1}$ if and only if $\hat{U}_i \lneq (\hat{H} \times \{1\})\hat{U}_{i+1}$ for all i.

We first show the following claim ⊛: For all $1 \neq x \in Z(H) \times \{1\}$ and $1 \neq y \in \{1\} \times A$ we have $\min\{i \mid x \in U_i\} \neq \min\{i \mid y \in U_i\}$. To see this, let i be minimal with $x \in U_i$. By definition of component-wise filtrations and minimality of i, there are $h_i \in Z(H)$ with $U_i = \langle U_{i-1}, h_1, \ldots, h_t \rangle$. In particular, if $y \in U_i$ then $y \in U_{i-1}$ which shows the claim. In the same way elements of $Z(H) \times \{1\}$ can be distinguished from those in $\{1\} \times \hat{A}$, since we assume $G \equiv^k_{\text{explicit}} \hat{G}$.

We make use of Lemma 3.4.4 regarding the subgroup chains that are defined by the chosen filtrations. Since $G \equiv^k_{\text{explicit}} \hat{G}$ holds, Duplicator has a winning strategy in the explicit $(k+1)$-pebble game on $(G, \hat{G})$ (Lemma 3.2.13) and then, via Lemma 3.4.4, Duplicator has a winning strategy in the k-pebble game where all bijections $f : G \to \hat{G}$ Duplicator chooses respect the subgroup chains and their respective cosets, i.e. $f(gU_i) = f(g)\hat{U}_i$ for all i. Then ⊛ implies that whenever $g_1 g_2^{-1} \in Z(H) \times \{1\}$ we have $f(g_1)f(g_2)^{-1} \notin \{1\} \times \hat{A}$.

Next, we show that Duplicator must map $H \times \{1\}$ to a system of representatives modulo $\{1\} \times \hat{A}$ in each move. Otherwise there would be $(h_1, 1), (h_2, 1) \in G = H \times A$ and $(h, a_1), (h, a_2) \in \hat{G} = \hat{H} \times \hat{A}$ with $f(h_i, 1) = (h, a_i)$. Then $(h, a_1)(h, a_2)^{-1}$ is central so the same must hold for $(h_1 h_2^{-1}, 1)$ (since f must in particular fulfill $fg(Z(G)) = f(g)Z(G)$ for all $g \in G$) but then the latter is contained in $Z(H) \times \{1\}$ while $(h, a_1)(h, a_2)^{-1} \in \{1\} \times \hat{A}$, a contradiction.

In particular, this means that Spoiler can restrict the game to $H \times \{1\}$ and if it is the case that $H \not\equiv^{k-1}_{\text{explicit}} \hat{H}$, then Spoiler can ultimately reach a configuration

$[((h_1,1),\dots,(h_{k-1},1),\perp),((x_1,a_1),\dots,(x_{k-1},a_{k-1}),\perp)]$ such that the induced configuration over $(G/(1\times A),\hat{G}/(1\times\hat{A}))$ fulfills the winning condition for Spoiler. The only possibility for the original configuration not to fulfill the winning condition for Spoiler is that there exist i,j,m and either $h_i\neq h_j$, $x_i=x_j$ and $a_i\neq a_j$, but then $(h_ih_j^{-1},1)$ is distinguished from $(x_i,a_i)(x_j,a_j)^{-1}=(1,a_ia_j^{-1})$ via $\circledast$, or $h_ih_j\neq h_m$, $x_ix_j=x_m$ and $a_ia_j\neq a_m$ in which case $(h_ih_jh_k^{-1},1)$ is distinguished from $(x_i,a_i)(x_j,a_j)(x_m,a_m)^{-1}=(1,a_ia_ja_m^{-1})$ via $\circledast$. Since $k\geq 5$ holds, both cases can be exploited by Spoiler to win the explicit k-pebble game on $(G,\hat{G})$ by Lemma 3.2.23, which is a contradiction. □

4.3.2 General case

Building on the previous subsection, we reduce the general case to the semi-abelian case. Consider an indecomposable direct decomposition $G=G_1\times\cdots\times G_d$, then we know that the collection of subgroups $\{G_iZ(G)\mid 1\leq i\leq d\}$ is independent of the chosen decomposition. We first show that $\bigcup_i G_iZ(G)$ is WL-detectable and then we exploit the fact that the non-commuting graph of G induces components on $\bigcup_i G_iZ(G)$ which correspond to the groups $G_iZ(G)$ (see also Figure 4.3.2).

Definition 4.3.17. Given a group G, we define the *non-commuting graph* Γ_G with vertex set G, in which two elements $g,h\in G$ are joined by an edge if and only if $[g,h]\neq 1$.

Lemma 4.3.18 ([1], Prop. 2.1)**.** *If G is non-abelian then $\Gamma_G[G\setminus Z(G)]$ is connected.*

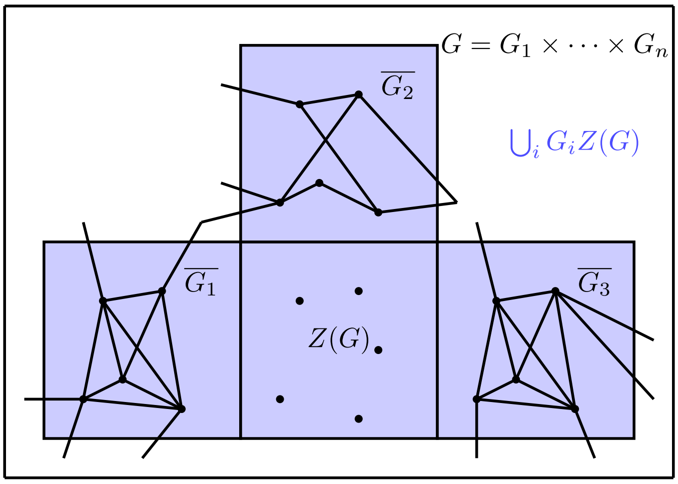


Figure 4.1: The non-commuting graph of $G_1\times\cdots\times G_n$ induces connected components on the canonical subset $\bigcup_i G_iZ(G)$.

We now approximate $\bigcup_i G_iZ(G)$ from below by constructing a canonical central decomposition of G which is WL-detectable.

Definition 4.3.19. Consider a finite, non-abelian group G. Define $M_1 \subseteq G$ to be the set of non-central elements g whose centralizers $C_G(g)$ have maximal order among all non-central elements. Iteratively define M_{i+1} by adding those elements g to M_i that have maximal centralizer order $|C_G(g)|$ among the remaining elements $G \setminus \langle M_i \rangle$. Set $M := M_\infty$ to be the stable set resulting from this process. Consider the subgraph of Γ_G induced on M and let $K_1 \dots, K_m$ be its connected components. Set $N_i := \langle K_i \rangle$. We call $N_1, \dots, N_m$ the *non-abelian components* of G.

Lemma 4.3.20. *In the notation of the previous definition, the following hold:*

1. *M is* 3-WL$_{\text{implicit}}$*-detectable.*

2. *$G = N_1 \cdots N_m$ is a central decomposition of G. For all i, $Z(G) \leq N_i$ and N_i is non-abelian. In particular M generates G.*

3. *If $G = G_1 \times \cdots \times G_d$ is an arbitrary direct decomposition, then for each $1 \leq i \leq m$ there is exactly one $1 \leq j \leq d$ with $N_i \subseteq G_j Z(G)$. Collect all such i for one fixed j in an index set I_j. Then the product over all N_i for $i \in I_j$ is equal to $G_j Z(G)$.*

Proof. 1. M_1 is 2-WL$_{\text{implicit}}$-detectable, since group elements are generally distinguishable by the orders of their centralizers (Lemma 4.1.3). Assume that M_i is 3-WL$_{\text{implicit}}$-detectable. Then $\langle M_i \rangle$ is again 3-WL$_{\text{implicit}}$-detectable by Lemma 4.1.3 and so is $G \setminus \langle M_i \rangle$. Thus, elements of $G \setminus \langle M_i \rangle$ are distinguishable from all other elements and can then be further distinguished by the orders of their centralizers. So M_{i+1} is 3-WL$_{\text{implicit}}$-detectable and the claim follows inductively.

2. By definition, the construction of M does not terminate until M_i contains a generating set of G, so $G = \langle M \rangle$. For $g \in G$ and $z \in Z(G)$ it holds that $C_G(gz) = C_G(g)$, thus $M_1 Z(G) = M_1$ and then $M_i Z(G) = M_i$ via induction.

   We claim that the connected components of Γ_G induced on M all contain more than one element. Otherwise say $K_i = \{x\}$ and so $[x, M] = \{1\}$. Since $\langle M \rangle = G$, it follows that x must be central. But by construction we never add central elements to M. In conclusion, $\Gamma_G[M]$ is a disjoint union of non-trivial components. So if $x \in K_i$, there is some $y \in K_i$ with $xy \neq yx$ and hence, N_i is non-abelian for all i. For all $z \in Z(G)$ we also have $(xz)y \neq y(xz)$ and conclude that $xz \in K_i$. Overall we obtain $K_i Z(G) = K_i$, implying that $Z(G) \leq N_i$. Finally we note that by definition of Γ_G, N_i and N_j centralize each other for $i \neq j$.

3. We first argue that all elements in M belong to some $G_j Z(G)$. Assume otherwise that $x = (x_1, \dots, x_d) \in M$ with $x_i \in G_i$ and more than one x_i is non-central. Then $x = (x_1, 1 \dots, 1) \cdot (1, x_2, 1, \dots, 1) \dots (1, \dots, 1, x_d)$ is a product of elements, each with a strictly bigger centralizer than x, and so x would have never been selected to be added to M. Thus, each element of M belongs to exactly one $G_j Z(G)$ and if two elements from M do not commute they must belong to the same $G_j Z(G)$. Finally assume that $\prod_{I_j} N_i = H_j \lneq G_j Z(G)$. Since all N_i contain $Z(G)$, there must be some non-central element x in $G_j Z(G) \setminus H_j$. But then x is also not contained in $H_j \times (\times_{i \neq j} G_i) Z(G)$ contradicting the fact that $G = N_1 \dots N_m$. □

Definition 4.3.21. Let $G = N_1 \cdots N_m$ be the decomposition into non-abelian components and let $G = G_1 \times \cdots \times G_d$ be an arbitrary direct decomposition. We say $x \in G$ is *full for* $(G_{j_1}, \ldots, G_{j_r})$, if $\{1 \leq i \leq m \mid [x, N_i] \neq 1\} = I_{j_1} \cup \cdots \cup I_{j_r}$. For all $x \in G$ define $C_x := \Pi_{[x,N_i]=\{1\}} N_i$ and $N_x := \Pi_{[x,N_i]\neq\{1\}} N_i$.

Observation 4.3.22. *Given an arbitrary collection of indices $J \subsetneq [m]$, the group elements $x \in G$ for which $C_x = \Pi_{i \in J} N_i$ holds are exactly those elements of the form $x = z\Pi_{i\in J} n_i$ with $z \in Z(G)$ and $n_i \in N_i \setminus Z(G)$. In particular, full elements exist for every collection of non-abelian direct factors and any direct decomposition. They are exactly given by products over non-central elements from the corresponding non-abelian components.*

Lemma 4.3.23. *Let G be non-abelian and let $G = G_1 \times \cdots \times G_d$ be an indecomposable direct decomposition. For all $x \in G$ we have a central decomposition $G = C_x N_x$ with $Z(G) \leq C_x$ and $Z(G) \leq N_x$. The decomposition is directly induced if and only if x is full for a collection of direct factors of G.*

Proof. If x is full for $(G_{j_1}, \ldots, G_{j_r})$ then by Lemma 4.3.20, we have $N_x = (G_{j_1} \times \cdots \times G_{j_r})Z(G)$ and $C_x = (\prod_{i \notin \{j_1,\ldots,j_r\}} G_i)Z(G)$, so the central decomposition $G = C_x N_x$ is directly induced.

For the other direction assume the decomposition $G = C_x N_x$ is directly induced and consider subgroups $\tilde{C}_x \leq C_x$, $\tilde{N}_x \leq N_x$ with $G = \tilde{C}_x \times \tilde{N}_x$, $C_x = \tilde{C}_x Z(G)$ and $N_x = \tilde{N}_x Z(G)$. Consider indecomposable direct decompositions $\tilde{C}_x = \times_{t \in I_C} \tilde{C}_t$ and $\tilde{N}_x = \times_{t \in I_N} \tilde{N}_t$, where I_C and I_N are suitable index sets. Then, for all $t \in I_C$, the group $\tilde{C}_t$ is an indecomposable direct factor of G, so $\tilde{C}_t Z(G) = G_{j_t} Z(G)$ for some j_t by Lemma 4.3.2. In particular, $[x, N_i] = 1$ for all $i \in I_{j_t}$. Similarly, for $\tilde{N}_t$ and $t \in I_N$, $[x, N_i] \neq 1$ for all $i \in I_{j_t}$. Since each $G_j Z(G)$ is either contained in C_x or N_x, the claim follows. □

Lemma 4.3.24. *Suppose $G = G_1 \times G_2$. For $k \geq 4$ assume that $G_1 Z(G)$ and $G_2 Z(G)$ are k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable and that k-$\mathrm{WL}_{\mathrm{implicit}}$ does not distinguish G from some other group H. Then for $i \in \{1, 2\}$ there are subgroups $H_i \leq H$ with $\left(\chi^k_{\mathrm{implicit}}(G)\right)(G_i Z(G)) = \left(\chi^k_{\mathrm{implicit}}(H)\right)(H_i Z(H))$ and $H_i Z(H) \equiv^k_{\mathrm{implicit}} G_i Z(G)$ such that H has a direct decomposition $H = H_1 \times H_2$.*

Proof. Set $\tilde{G}_i := G_i Z(G)$. As a consequence of Lemma 4.1.3, there exist subgroups of H, $\tilde{H}_i$ say, that correspond to $\tilde{G}_i$ with respect to stable color classes of k-$\mathrm{WL}_{\mathrm{implicit}}$. It is also implied that $Z(H) \leq \tilde{H}_i$ holds. Consider the decompositions $Z(G) = Z(G_1) \times Z(G_2)$ and $\tilde{G}_i = G_i \times Z(G_{i+1 \bmod 2})$ and observe the following: If x splits from $Z(G)$ then, using Lemma 4.3.12, we see that x also splits from $\tilde{G}_1$ or $\tilde{G}_2$. The observation is used to prove Claim 1 below. Write $\tilde{H}_i := R_i \times B_i$ where B_i is a maximal abelian direct factor of $\tilde{H}_i$.

Claim 1: For all possible choices of R_i and B_i it holds that $R_1 \cap R_2 = \{1\}$.

By assumption, $\tilde{H}_1 \cap \tilde{H}_2 = Z(H)$ so $R_1 \cap R_2 \leq Z(H)$. For the sake of contradiction assume that there exists $z \in R_1 \cap R_2$ such that $|z| = p$ for some prime p. Then there also exists a central p-element w that splits form $Z(H)$ such that $z \in \langle w \rangle$ (this is always true for central elements of prime order, as we can take w to be a root of z of highest p-power order in the abelian group $Z(H)$). Write $w = (r_i, b_i)$ with respect to the chosen decompositions of $\tilde{H}_i$. For some $m \in \mathbb{N}$ we have that $w^m = z \in R_1 \cap R_2$, so $1 \neq w^m =$

$(r_1^m, 1) = (r_2^m, 1)$, in particular $|b_i| < |r_i|$ for $i = 1, 2$, since w has p-power order. Then w does not split from $\tilde{H}_i$ or otherwise, by Lemma 4.3.12, r_i would split from R_i but R_1 and R_2 do not admit abelian direct factors.

Hence, w splits from $Z(H)$ but not from $\tilde{H}_1$ or $\tilde{H}_2$ and such elements do not exist with respect to G, $\tilde{G}_1$ and $\tilde{G}_2$ as pointed out above. Claim 1 follows, since k-WL$_{\text{implicit}}$ detects the set of elements splitting from $Z(H)$, $\tilde{H}_1$ or $\tilde{H}_2$, respectively. ■

Next we consider maximal abelian direct factors A and B of G and H, respectively. Write $H := R \times B$. By Lemma 4.3.13, we have $A \cong B$.

Claim 2: R_1 and R_2 can be chosen such that $R_1R_2 \cap B = \{1\}$.

Let $\tilde{H}_1 = \langle (r_1, b_1), \dots, (r_t, b_t)\rangle \leq R \times B$ then, since $B \leq \tilde{H}_1$,

$$\tilde{H}_1 = \langle (r_1, 1)(1, b_1), \dots, (r_t, 1), (1, b_t)\rangle = \langle (r_1, 1) \dots (r_t, 1)\rangle \times B.$$

An analogous statement holds for $\tilde{H}_2$, so R_1R_2 can be chosen as a subgroup of R. ■

To finally prove the Lemma, let R_1 and R_2 be as in Claim 2. By Claim 1, $R_1 \cap R_2 = \{1\}$, so $R_1R_2B = R_1 \times R_2 \times B \leq H$. By Lemma 4.3.13, $G \equiv^k_{\text{implicit}} H$ implies that $|R_1||R_2||B| = |H|$ holds, so $H = R_1 \times R_2 \times B$ and this can be written as $(R_1 \times B_1) \times (R_2 \times B_2)$, where $B_i \leq H_i$ are chosen such that $B_1 \times B_2 = B$ and B_i is isomorphic to a maximal abelian direct factor of G_i. Furthermore, we have $R_iZ(H) = \tilde{H}_i$ by construction. □

Lemma 4.3.25. *Let $G = N_1 \cdots N_m$ be the decomposition into non-abelian components and $G = G_1 \times \cdots \times G_d$ a decomposition into indecomposable direct factors. For $k \geq 5$, the set of elements that are full for only one G_i as well as the pairs of elements that are full for the same collection of direct factors are k-WL$_{\text{implicit}}$-detectable.*

Proof. Let $x, y \in G$ and assume x is full for $G_{j_1}, \dots, G_{j_r}$. Using Lemma 3.2.13, we consider the $(k+1)$-pebble game with initial configuration $[(x, \perp^k), (y, \perp^k)]$. As long as there is a pebble pair on (x, y), by Lemma 4.3.20, Duplicator has to map C_x to C_y and N_x to N_y. If x is not distinguished from y then by Lemma 4.3.24, the central decomposition $G = C_yN_y$ has to be directly induced, since the same holds for $G = C_xN_x$ and $k \geq 5$. By Lemma 4.3.23 the element y is full as well.

So let $F \subseteq G$ be the set of elements that are full for some collection of direct factors. We just showed that F is 5-WL$_{\text{implicit}}$-detectable. Note that for $x, y \in F$ it is easily checked by the WL-algorithm if x and y are full for the same collection of direct factors since this is equivalent to $C_x = C_y$. It remains to show that elements that are full for only one direct factor can be distinguished from the rest of F. This follows from the fact that $x \in F$ is full for a single direct factor if and only if C_x is minimal with respect to inclusion among C_f, $f \in F$ and this can be exploitet by Spoiler, given that $k \geq 3$. □

Corollary 4.3.26. *If $G = G_1 \times \cdots \times G_d$ is a decomposition into indecomposable direct factors then $\bigcup_i G_iZ(G)$ is 5-WL$_{\text{implicit}}$-detectable.*

Proof. For $k \geq 5$, by the previous result k-WL$_{\text{implicit}}$ distinguishes elements that are full for one fixed direct factor from other elements. Call the set of full elements $\mathcal{F}$. Then for each $g \in \mathcal{F}$ it holds that N_g is of the form $G_iZ(G)$ for some i and by Observation 4.3.22 each i occurs through some full element of G. Thus, via Lemma 4.1.3, the union $\bigcup_{g \in \mathcal{F}} N_g = \bigcup_i G_iZ(G)$ is 5-WL$_{\text{implicit}}$-detectable. □

Theorem 4.3.27. *Let $G = G_1 \times \cdots \times G_d$ be a decomposition into indecomposable direct factors and $k \geq 5$. If $G \equiv^k_{\text{implicit}} H$ then there are indecomposable direct factors $H_i \leq H$ such that $H = H_1 \times \cdots \times H_d$ and $G_i \equiv^{k-1}_{\text{implicit}} H_i$ for all $i \in [d]$. Moreover G and H have isomorphic maximal abelian direct factors and $G_iZ(G) \equiv^k_{\text{implicit}} H_iZ(H)$ for all $i \in [d]$.*

Proof. Since $\mathcal{F}_G := \bigcup_i G_iZ(G)$ is 5-$\mathrm{WL}_{\text{implicit}}$-detectable, the group H must be decomposable into indecomposable direct factors $H = \times_j H_j$ such that $\mathcal{F}_H = \bigcup_j H_jZ(H) \subseteq H$ is indistinguishable from $\mathcal{F}_G$. Consider the non-commuting graphs of G and H induced on these sets and recall that non-commuting graphs of non-abelian groups are connected (Lemma 4.3.18). Since different direct factors in a fixed decomposition centralize each other, we obtain that for each non-singleton connected component K of $\Gamma_G[\mathcal{F}_G]$ there exists a unique indecomposable direct factor G_i such that $K = G_iZ(G) \setminus Z(G)$ and thus $\langle K \rangle = G_iZ(G)$. Again by Lemma 4.3.18, all non-abelian direct factors appear in this way.

The same holds for H and so if G is not distinguishable from H, there must be a bijection between the components of $\Gamma_G[\mathcal{F}_G]$ and $\Gamma_H[\mathcal{F}_H]$, such that the subgroups generated by corresponding components are indistinguishable via 5-$\mathrm{WL}_{\text{implicit}}$. This defines a correspondence $G_iZ(G) \equiv^k_{\text{implicit}} H_iZ(H)$ after reordering the factors of H in an appropriate way. From Lemma 4.3.16 it follows that $G_i \equiv^{k-1}_{\text{implicit}} H_i$ holds. By Lemma 4.3.15, G and H must have isomorphic maximal abelian direct factors, so for abelian factors we even have $G_i \cong H_i$. □

Chapter 5

Upper Bounds on the Weisfeiler-Leman dimension for various group classes

In this chapter, we present bounds on the Weisfeiler-Leman dimension of various classes of finite groups. Here, we are first concerned with upper bounds, where we investigate specific classes of groups, analyze their structure and show how the Weisfeiler-Leman algorithm can exploit these structural aspects to identify groups up to isomorphism. In the following Chapter we go on to investigate lower bounds.

The results of Chapter 5 have not been published before, with the exception of the construction of groups from CFI-graphs in Section 5.3, which is identical to [17, Sections 4–6].

5.1 Small groups

We present some computational results on stable Weisfeiler-Leman colorings of finite groups. A cooresponding GAP-implementation of 2-$\mathrm{WL}_{\mathrm{implicit}}$ can be found in Appendix A. For simplicity, we only reference concrete groups in terms of their identifier in the Small Groups Library in GAP [43]. To ensure that the results presented here remain correct and comprehensible, independent of the Small Groups Library, we list presentations for all groups we explicitly reference in Appendix B.

We find that groups of order up to 243 are always identified by 3-$\mathrm{WL}_{\mathrm{implicit}}$. Indeed, as far as we were able to run computations, there are no known exceptions, even for higher orders. In particular, we currently do not have examples of groups of WL-dimension four or higher.

Lemma 5.1.1. *Each group of order at most* $127 = 2^7 - 1$ *is identified up to isomorphism by* 2-$\mathrm{WL}_{\mathrm{implicit}}$. *The groups* $\mathrm{SmallGroup}(2^7, i)$ *and* $\mathrm{SmallGroup}(2^7, j)$ *are not distinguished by* 2-$\mathrm{WL}_{\mathrm{implicit}}$ *if and only if* (i, j) *is one of* $(164, 999)$, $(165, 1011)$, $(166, 1014)$, $(167, 1013)$, $(171, 1122)$, $(173, 1126)$, $(174, 177)$, $(555, 556)$, $(807, 808)$, *or* $(831, 832)$. *Presentations for these groups can be found in the appendix. Each group of order at most* $243 = 3^5$ *is identified up to isomorphism by* 3-$\mathrm{WL}_{\mathrm{implicit}}$.

In particular, we see from the indistinguishability of $G :=$ SmallGroup$(2^7, 173)$ and $H :=$ SmallGroup$(2^7, 1126)$, that 2-WL$_{\text{implicit}}$ does not detect the derived subgroup: G/G' has exponent 4, while H/H' has exponent 2. If the derived subgroup was 2-WL$_{\text{implicit}}$-detectable, then G and H would be distinguished since the square of any element of H lies in H', while the same does not hold in G. Similarly, we can derive from the indistinguishability of $G :=$ SmallGroup$(2^7, 164)$ and $H :=$ SmallGroup$(2^7, 999)$, that 2-WL$_{\text{implicit}}$ does not necessarily detect subgroups generated by detectable subsets: the 8 squares in H form a subgroup while the 8 squares in G generate a subgroup of order 16. By our investigations in Chapter 3, such examples are not possible for k-WL$_{\text{implicit}}$ with $k \geq 3$. In this sense, 2-WL$_{\text{implicit}}$ is severely limited by not being able to access triplets and hence not being able to access the full multiplication relation.

We consider another interpretation of groups having “small” order, namely groups whose order is a prime power with small exponent, but arbitrary prime base. There are ongoing lines of research with the aim of enumerating classes of p-groups, for example the enumeration of p-groups by coclass, or the enumeration of groups of order p^n for increasing values of n. Currently the maximal value of n for which a complete enumeration, independent of p, has been given is $n = 7$, see [93]. For small values of p, higher exponents have been completed, for instance in the case of groups of order 2^9 [14].

Lemma 5.1.2. *Let p be a prime and let P be a p-group with $|P| \leq p^5$. Then P is identified up to isomorphism by* 3-WL$_{\text{implicit}}$. *Furthermore,* 3-WL$_{\text{implicit}}$ *identifies the groups of order* 2^8 *and order* 3^6 *up to isomorphism.*

Proof. For $p = 2$ and for groups of order 3^6, we checked the claim explicitly in GAP [43]. Consider the groups of order p^5 with an odd prime p. For abelian P, we know that 2-WL$_{\text{implicit}}$ is sufficient due to Corollary 4.2.7. For $p > 2$, up to isomorphism, there are five distinct groups of order p^5 that are not 3-generated and not abelian. Among these, each group is uniquely identified by the isomorphism type of $Z(P)$ together with $\exp(P)$ (see [13]), and these quantities are identified by 3-WL$_{\text{implicit}}$. □

In the case of groups of order 3^6, it already appears difficult to find a collection of group theoretic properties which distinguishes these groups up to isomorphism. However, all such groups are uniquely identified by the initial coloring of 3-WL$_{\text{implicit}}$.

Let us finally mention the case of SmallGroup$(3^7, 8106)$ and SmallGroup$(3^7, 8108)$. These groups define the same multisets of isomorphism types of subgroups (normal subgroups, quotient groups, respectively) and can not be distinguished through the initial coloring of 3-WL$_{\text{implicit}}$. They are distinguished by the first refined coloring, according to how elements of order 3 distribute among the 2-generated subgroups.

5.2 Groups with stable initial WL-colorings

Next, we consider groups where the WL-algorithm terminates after the initial coloring. Such groups have the property that any two k-tuples of the same marked isomorphism type are not distinguished by k-WL$_{\text{implicit}}$. For graphs, this property is known as *tuple-regularity* (see for instance, see [27]).

Lemma 5.2.1. *Assume that the initial coloring of* k-WL$_{\text{implicit}}$ *on G is stable. Then the following property holds: for any two k-tuples $\bar{g}$ and $\bar{h}$ over G, if these are of the same* *marked isomorphism type, then there exists a bijection $f\colon G \to G$, such that $\bar{g}_{i\leftarrow x}$ is of the same marked isomorphism type as $\bar{h}_{i\leftarrow f(x)}$, for all $i \in [k]$ and all $x \in G$.*

In contrast to the situation for graphs, in the previous lemma it is not necessarily implied that the marked isomorphism types of $(g_1, \ldots, g_k, x)$ and $(h_1, \ldots, h_k, f(x))$ agree, as the k-dimensional WL-algorithm only ever explicitly considers k-generated subgroups.

Definition 5.2.2. A group G is called *homogeneous*, if for each pair of isomorphic subgroups of G, say U and V, any isomorphism $\varphi : U \to V$ is induced by an automorphism $\phi \in \mathrm{Aut}(G)$, that is, $\phi_{|U} = \varphi$.

Regularity in groups is more restricted compared to regularity in graphs, as 2-tuple-regular groups are always homogeneous, while the class of k-tuple-regular graphs is strictly increasing until $k = 5$ (from $k = 5$ onward, k-tuple-regular graphs are also homogeneous [25]).

Lemma 5.2.3 ([19])**.** *Every 2-tuple regular finite group is homogeneous.*

In particular, for $k \geq 3$, the initial coloring of k-$\mathrm{WL}_{\mathrm{implicit}}$ is stable on a group G, if and only if G is homogeneous, as stability of the k-$\mathrm{WL}_{\mathrm{implicit}}$-initial coloring implies $(k-1)$-tuple regularity. The finite homogeneous groups are classified in [80].

We still have to consider the case of 2-$\mathrm{WL}_{\mathrm{implicit}}$, as, in contrast to graphs, stability of the initial coloring only implies 1-tuple-regularity and not necessarily 2-tuple-regularity. Again, this comes down to the fact that the marked isomorphism type of a triple of group elements is not determined by the marked isomorphism type of the pairs of group elements in the triple: consider (g_1, g_2, g_3) where for each $i \neq j$, we have $\langle g_i, g_j \rangle \cong C_p^2$. Then it may or may not be the case that $\langle g_1, g_2, g_3 \rangle$ is isomorphic to C_p^2.

By a result of Guralnick and Kantor [58], finite simple groups have a property known as $\frac{3}{2}$*-generation*, which means that every non-identity element of a finite simple group is contained in some generating pair.

The following definition is taken from [71].

Definition 5.2.4. A group G is called an *AT-group*, if any two elements of the same order are in the same orbit under the action of $\mathrm{Aut}(G)$.

We first use $\frac{3}{2}$-generation to characterize simple groups with stable initial colorings.

Lemma 5.2.5. *If the initial coloring of* 2-$\mathrm{WL}_{\mathrm{implicit}}$ *on a finite simple group G is stable, then G is an AT-group. More precisely, G is one of* $\mathrm{PSL}_2(5)$, $\mathrm{PSL}_2(7)$, $\mathrm{PSL}_2(8)$, $\mathrm{PSL}_2(9)$, *or* $\mathrm{PSL}_3(4)$.

Proof. Since G is $\frac{3}{2}$-generated, the orbits of elements of G under $\mathrm{Aut}(G)$ are completely determined by the orbits of generating pairs and by definition, the initial coloring of 2-$\mathrm{WL}_{\mathrm{implicit}}$ is already as fine as the orbit partition of generating pairs under $\mathrm{Aut}(G)$. On the other hand, the initial coloring of $(g, 1)$ only encodes the order of g and contains no other information. Hence, if the initial coloring on G is already stable, then the orbit partition on G is the partition into elements of equal orders. The finite simple AT-groups are classified in [71] and agree with the list given above. □

Lemma 5.2.6. *Let G be a finite group and assume that the initial coloring of* 2-WL$_{\text{implicit}}$ *on G is stable. Then* $\mathrm{Soc}(G)$ *admits a decomposition* $\mathrm{Soc}(G) = A \times T$*, where A is abelian (possibly trivial), T is either trivial, or non-abelian simple and it holds* $\gcd(|A|, |T|) = 1$.

Proof. Otherwise, the socle contains a normal subgroup of the form $T \times C_p$, with T non-abelian simple and $|T|$ divisible by p, or a subgroup of the form $T \times S$ with T and S non-abelian simple.

In the former case, consider elements $t \in T$ and $x \in G$, such that t has order p and the normal closure of x is a minimal normal subgroup isomorphic to $C_p^{m'}$ for some m'. Then, for each $g \in G$, we have that $[x^g, x] = 1$, while there is some $g \in G$ such that $[t^g, t] \neq 1$ (this follows from the fact that the conjugacy class of t in T has to generate the simple group T), and then the marked isomorphism type of (g, t) is distinct from the marked isomorphism type of (g', x) for each $g' \in G$. This means that the first iterated coloring distinguishes $(x, 1)$ from $(t, 1)$, but $(x, 1)$ and $(t, 1)$ obtain the same initial color since $|x| = |t|$.

In the latter case, let $t \in T$ and $s \in S$ be involutions. Since finite simple groups are $\frac{3}{2}$-generated, there exists a $g \in G$ of odd order, such that $\langle st, g\rangle \cong T \times C_2$. We claim that no odd order element $g \in G$ fulfills $\langle t, g\rangle \cong T \times C_2$. To prove the claim, we first note that the derived subgroup of $T \times C_2$ is isomorphic to T.

Since t is contained in a normal subgroup of $\mathrm{Soc}(G)$, there is some normal subgroup of G, say N, with $t \in N$ and $N \cong T^m$ for an appropriate $m \geq 1$. In particular, g normalizes N, and since the automorphisms of T^m permute the minimal normal subgroups of T^m, that is, the normal copies of T in T^m, we have that either g normalizes T in G, or otherwise t^g is contained in a minimal normal subgroup of N which intersects T trivially, so $[t^g, t] = 1$.

In the former case, $\langle T, g\rangle$ does not contain a subgroup of the form $T \times C_2$, since we assume that g has odd order, and so $\langle t, g\rangle$ cannot be isomorphic to $T \times C_2$.

In the latter case, the derived subgroup of $\langle t, g\rangle$ is generated by conjugates of $[t, g]$, that is, by involutions none of which is contained in a minimal normal subgroup of N. Now, if the derived subgroup of $\langle t, g\rangle$ is not isomorphic to T, then $\langle t, g\rangle$ cannot be isomorphic to $T \times C_2$. But if the derived subgroup of $\langle t, g\rangle$ is isomorphic to T, then it must be a non-normal copy of T in N that projects onto the minimal normal subgroup generated by t. In this case, $\langle t, (\langle t, g\rangle)'\rangle$ contains a subgroup isomorphic to $T \times T$, and again, $\langle t, g\rangle$ cannot be isomorphic to $T \times C_2$.

In conclusion, t is distinguishable from ts by 2-WL$_{\text{implicit}}$, despite t and ts both having order 2. This contradicts the assumption that the initial coloring is stable. □

We can use the ideas of the previous proof in a more general setting and show that groups with stable 2-WL$_{\text{implicit}}$-initial coloring are close to being solvable, in the following sense.

Lemma 5.2.7. *Let G be a finite group and assume that the initial coloring of* 2-WL$_{\text{implicit}}$ *on G is stable. Let $R := R(G)$ denote the solvable radical of G. Then the initial coloring of* 2-WL$_{\text{implicit}}$ *on R is stable and G/R is almost simple. Furthermore, if G/R is simple, then G/R is an AT-group.*

Proof. The initial coloring of 2-WL$_{\text{implicit}}$ on R is stable, since the solvable radical is 2-WL$_{\text{implicit}}$-detectable (see Corollary 4.2.27), and hence the color classes computed by

2-$\mathrm{WL}_{\mathrm{implicit}}$ on R as a subgroup in G are at least as fine as the color classes computed on R as an input group.

Now, for the sake of contradiction, assume that $\mathrm{Soc}(G/R)$ contains a subgroup isomorphic to $T \times S$ for non-abelian simple groups S and T (potentially isomorphic), and choose two elements $t, s \in G$, such that they map onto involutions $tR \in T$ and $sR \in S$ in the epimorphism $G \to G/R$. Via the same argument we used in the previous proof, there exists some odd order element $g \in G$, such that $\langle ts, g\rangle$ is isomorphic to $T \times C_2$ extended by a (potentially trivial) solvable group, while the groups $\langle t, g\rangle$ with odd order $g \in G$ are never of this form.

Hence, the marked isomorphism type of (t, g) is distinct from the marked isomorphism type of (ts, g') for each $g' \in G$ and iteratively, t is distinguished from xs by 2-$\mathrm{WL}_{\mathrm{implicit}}$.

Since the initial coloring is stable on G, it must be the case that distinguishable elements have different orders in G. By choice of s and t, we note that tR and sR have order 2 in G/R, so we may replace s and t with arbitrary odd powers in the argument above. In particular, we may assume without loss of generality that the orders of s, t and x are powers of 2. Assume then, also without loss of generality, that we have $|s| > |t|$. Then $|x^{2^j}| = |t|$ for some $j \geq 1$ and x^{2^j} is contained in R (by choice of s and t). But if the initial coloring on G is stable, then, by detectability of the radical, no two elements $r \in R$ and $g \in G \setminus R$ can share the same order, a contradiction. The same argument applies to x in place of s.

In conclusion, $\mathrm{Soc}(G/R)$ is simple, that is, G/R is almost simple. Now if G/R is simple, we can exploit $\frac{3}{2}$-generation again to show that there are elements x and y in G/R, of the same order, such that no pair (x, g) generating G modulo R can be mapped to a pair (y, g') generating G modulo R. □

We finally note that there indeed exist groups whose initial 2-$\mathrm{WL}_{\mathrm{implicit}}$-coloring is stable, but which are not 2-tuple regular. Examples are given by SmallGroup(36,3), of the form $V_4 \rtimes C_9$ for a non-trivial action of C_9, and SmallGroup(72,3), of the form $Q_8 \rtimes C_9$ for a non-tricial action of C_9, in the Small Groups Library of GAP [43].

5.3 Groups presented over finite graphs

Next, we describe a construction of finite groups from graphs such that structural properties of the resulting groups are primarily determined by the graphs. We will make this statement more precise in the following. From now on fix an odd prime p.

Definition 5.3.1. For each natural number $n > 1$ there is a relatively free group of exponent $p \neq 2$ and (nilpotency) class 2 generated by n elements. It admits a finite presentation

$$F_{n,p} = \langle x_1, \dots, x_n \mid R(p, n)\rangle$$

where $R(p, n)$ consists of the following relations:

1. For all $1 \leq i \leq n$ there is a relation $x_i^p = 1$, and

2. for all $1 \leq i, j, k \leq n$ there is a relation $[[x_i,x_j],x_k] = 1$.

Thus, the group is generated by $x_1, \ldots, x_n$, each of these generators is an element of order p, and the commutator of two generators commutes with every generator and thus every element of the group. It follows from these properties that elements of $F_{n,p}$ can be uniquely written as

$$x_1^{d_1} \cdot \ldots \cdot x_n^{d_n} [x_1, x_2]^{d_{1,2}} [x_1, x_3]^{d_{1,3}} \cdot \ldots \cdot [x_{n-1}, x_n]^{d_{n-1,n}}$$

where exponents are defined modulo p. In particular, $|F_{n,p}| = p^{n+n(n-1)/2}$.

The main goal is to construct quotients of $F_{n,p}$ using graphs on the vertex set $[n]$ as templates, in a way that translates combinatorial similarity of the graphs (with respect to Weisfeiler-Leman-refinement) to similar subgroup profiles. We will see that this affects other isomorphism invariants as well.

Definition 5.3.2. To each (simple, undirected) graph $\Gamma = (\{v_1, \ldots, v_n\}, E)$ and odd prime number p we assign a finite exponent p group of nilpotency class (at most) 2 via

$$G_\Gamma := \langle x_1, \ldots, x_n \mid R(p,n), [x_i, x_j] = 1 : \{v_i, v_j\} \in E \rangle .$$

Thus, in G_Γ two generators x_i, x_j commute, if the corresponding vertices form an edge in Γ. We usually identify x_i with v_i and use the latter to refer to the vertex as well as the respective element of G_Γ. We fix an order on generators $v_1, \ldots, v_n$ and call these the *standard generators* for G_Γ. The specific presentation above is called the *presentation of G_Γ on* Γ.

This construction has also been used in other contexts. It is sometimes called *Mekler's construction* in the literature (see [88] for Mekler's original work) and has been primarily investigated for infinite graphs with respect to model theoretic properties. We first collect some possibly well known combinatorial and group theoretic properties.

Lemma 5.3.3. *We have $\Phi(G_\Gamma) = G_\Gamma'$ and the vertices of Γ form a generating set of G_Γ of minimal cardinality.*

Proof. By construction G_Γ has exponent p and thus $\Phi(G_\Gamma) = G_\Gamma'$ (since for p-groups the Frattini-subgroup is the minimal subgroup with elementary abelian quotient). The cardinality of a minimal generating set of G_Γ is the dimension of the $\mathbb{F}_p$-space $G_\Gamma/\Phi(G_\Gamma)$ which is now equal to G_Γ/G_Γ'. We have

$$G_\Gamma/G_\Gamma' \cong \langle V(\Gamma) \mid \text{exponent } p, \text{ abelian} \rangle \cong \mathbb{F}_p^{|V(\Gamma)|}$$

showing the claim. □

Lemma 5.3.4. *Denote by m the number of non-edges in Γ. Then $G_\Gamma' \cong \mathbb{F}_p^m$, i.e., the set of non-edges of Γ forms a basis in G_Γ', regarded as a vector space over $\mathbb{F}_p$.*

Proof. We have $G_\Gamma' = (F_{n,p}/N)'$ for some normal subgroup $N \leq F_{n,p}'$ with $|N| = p^{|E(\Gamma)|}$, and since commutators are central in $F_{n,p}$, it holds that $(F_{n,p}/N)' = F_{n,p}'/N$, where $|F_{n,p}'|/|N| = p^{\binom{n}{2} - |E(\Gamma)|} = p^m$. □

The previous lemma gives rise to normal forms for elements of G_Γ.

Corollary 5.3.5. *Let Γ be a (simple) graph. Then we have $|G_\Gamma| = p^{|V(\Gamma)|+\left|\binom{V}{2}\right) - E(\Gamma)|}$. In particular, every element of G_Γ can be written in the form*

$$v_1^{d_1} \dots v_n^{d_n} c_1^{d_{n+1}} \dots c_k^{d_{n+k}}$$

where $\{c_1, \dots, c_k\}$ is the set of non-trivial commutators between generators (i.e., the non-edges of the graph Γ) and each d_i is uniquely determined modulo p.

In what follows, we conclude that a lot of information on commutation and centralizers can be deduced from Γ directly. We first need to recall some well known properties of commutators in (nilpotent) groups (see [65] for instance).

Lemma 5.3.6 (Commutator relations)**.** *Let G be a group of nilpotency class 2. Then for all $a, b, c \in G$ we have*

1. *$[a, b] = [b, a^{-1}]$, and*

2. *$[a, bc] = [a, b][a, c]$.*

In particular for all $n, m \in \mathbb{N}$ we have $[a^m, b^n] = [a, b]^{mn}$.

Proof. Recall that nilpotency class 2 means that all commutators are central in G. We thus have $[a, b] = aba^{-1}b^{-1} = aba^{-1}b^{-1}aa^{-1} = a[b, a^{-1}]a^{-1} = [b, a^{-1}]$ and we have that $[a, bc] = abca^{-1}c^{-1}b^{-1} = abca^{-1}c^{-1}aa^{-1}b^{-1} = ab[c, a^{-1}]a^{-1}b^{-1} = [a, b][c, a^{-1}] = [a, b][a, c]$. By induction $[a, b^n] = [a, b]^n$. Finally, $[a^m, b^n] = [a^m, b]^n = [b, a^{-m}]^n = [b, a]^{-mn} = [a, b]^{mn}$. □

Given a graph vertex v, we denote the closed neighborhood of v by $N[v] := N(v) \cup \{v\}$.

Lemma 5.3.7. *It holds $Z(G_\Gamma) = G'_\Gamma \times \langle v : N[v] = V(\Gamma)\rangle$. In particular, if no vertex of Γ is adjacent to all other vertices, then we have $Z(G_\Gamma) = G'_\Gamma$.*

Proof. We can assume that no vertex in Γ is adjacent to all other vertices. Now take an arbitrary element $x := v_1^{d_1} \dots v_n^{d_n} c_1^{d_{n+1}} \dots c_k^{d_{n+k}}$ like above. If d_i is non-trivial modulo p for some $i \leq n$ then by assumption we find some vertex v_j such that $[v_i, v_j]$ is non-trivial. By the counting argument above, commutators of different pairs of generators are linearly independent and using commutator relations we see that thus $[x, v_j]$ is non-trivial as well. So either d_i is 0 modulo p for all $i \leq n$ and then x is a product of commutators, or x is not central. □

From now on let us fix a graph Γ on the vertex set $\{v_1, \dots, v_n\}$ and let $G := G_\Gamma$. We set $m := |\Phi(G)| = |G'|$. Then m is the number of non-edges in Γ and $|G| = p^{m+n}$. Furthermore, fix an ordering of non-trivial commutators $c_1, \dots, c_m$ of pairs of standard generators $[v_i, v_j] \neq 1$ with $i < j$.

Definition 5.3.8. Let $x \in G_\Gamma$ be an element with normal form

$$x := v_1^{d_1} \dots v_n^{d_n} c_1^{e_1} \dots c_m^{e_m}$$

The *support* of x is $\{v_i \mid d_i \not\equiv_p 0\}$. For a subset of vertices $S \subseteq V(\Gamma)$ let x_S be the subword $v_{i_1}^{d_{i_1}} \dots v_{i_s}^{d_{i_s}}$ where $S = \{v_{i_1}, \dots, v_{i_s}\}$ with $i_1 < \dots < i_s$.

Towards analyzing commutation in G_Γ we consider an example.

Example 5.3.9. Note that for two connected components C_1, C_2 of the complement graph $\mathrm{co}(\Gamma)$ and every group element $x \in G$ we always have $x_{C_1}x_{C_2} = x_{C_2}x_{C_1}$. Consider the complete bipartite graph Γ on parts $\{v_1, v_2\}$ and $\{v_3, v_4\}$ and its complement $\mathrm{co}(\Gamma)$, see Figure 5.1:

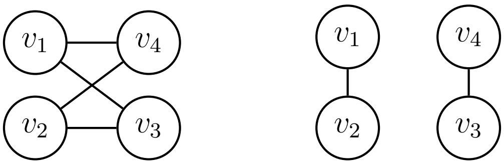


Figure 5.1: A complete bipartite graph on 4 vertices (left) and its complement (right).

Then it holds

$$C_{G_\Gamma}(v_1v_2v_3v_4) = \langle v_1v_2\rangle\langle v_3v_4\rangle Z(G_\Gamma).$$

The following lemma states that the example essentially captures how commutation works in general.

Lemma 5.3.10. *For $x \in G_\Gamma$ let $C_1, \dots, C_s$ be the connected components of the complement graph $\mathrm{co}(\Gamma[\mathrm{supp}(x)])$. Then we have $x = x_{C_1} \cdots x_{C_s}c$ for some $c \in G'_\Gamma \leq Z(G_\Gamma)$ and $y \in G_\Gamma$ commutes with x if and only if*

$$y \in \langle x_{C_1}\rangle \cdots \langle x_{C_s}\rangle \cdot \langle w : [v, w] = 1 \text{ for all } v \in \mathrm{supp}(x)\rangle \cdot G'_\Gamma.$$

Proof. By definition of G_Γ for $i \neq j$ all elements belonging to C_i commute with all elements from C_j, giving rise to a decomposition of x into parts belonging to components of $\mathrm{co}(\Gamma)$. Furthermore, it shows that commutation of group elements x and y is the same as simultaneous commutation with all of the respective parts. Consider now the case $x = x_{C_i}$ for some i. If $v \in \mathrm{supp}(x) \setminus \mathrm{supp}(y)$ then, due to commutators being independent, $[x, y] = 1$ if and only if v commutes with every element from $\mathrm{supp}(y)$ and the same holds after interchanging roles of x and y. Thus, we can reduce to the case that $\mathrm{supp}(x) = \mathrm{supp}(y)$ and we will argue that x and y are powers of each other or trivial. For ease of notation assume that $x = v_1^{d_1} \dots v_r^{d_r}$ and $y = v_1^{f_1} \dots v_r^{f_r}$ where d_i and f_i are non-zero modulo p. Using commutator relations we obtain

$$[x, y] = [v_1, v_2]^{d_2f_1 - d_1f_2} \dots [v_{r-1}, v_r]^{d_rf_{r-1} - d_{r-1}f_3}$$

and for $[x, y]$ to vanish, all of these exponents have to be divisible by p. That is, modulo p, f_2 is uniquely determined by d_1, d_2 and f_1 or $[v_1, v_2]$ is trivial. Since all v_i lie in one connected component of $\mathrm{co}(\Gamma[\mathrm{supp}(x)])$, there is a sequence of non-edges from v_1 to every v_i within the component and it follows in an inductive fashion that the values of $d_1, \dots, d_r$ together with a choice of f_1 uniquely determine all other values of the f_i (modulo p). Now clearly one admissible system of exponents is given by choosing y as a power of x and due to uniqueness these are the only possible configurations. □

Corollary 5.3.11. *Let $x = v_{i_1}^{d_1} \dots v_{i_r}^{d_r} c$ with $i_1 < i_2 < \dots < i_r$, c central in G_Γ and $d_i \not\equiv_p 0$ for all i. Then*

$$C_{G_\Gamma}(x) = \langle x_{C_1} \rangle \cdots \langle x_{C_s} \rangle \cdot \big\langle \{ v_m \mid [v_m, v_{i_j}] = 1 \textit{ for all } j \} \big\rangle \cdot G'_\Gamma.$$

Where, $C_1, \dots, C_s$ are the connected components of the complement graph $\mathrm{co}(\Gamma[\mathrm{supp}(x)])$.

This (almost) distinguishes single support vertices.

Lemma 5.3.12. *For $x \in G_\Gamma$ and $v \in \mathrm{supp}(x)$ we have that $|C_{G_\Gamma}(x)| \leq |C_{G_\Gamma}(v)|$. Set $M(x) := \{ w \in V(\Gamma) \mid [w, y] = 1 \textit{ for all } y \in \mathrm{supp}(x) \}$. Then if $|C_{G_\Gamma}(x)| = |C_{G_\Gamma}(v)|$ either $M(x) = M(v)$ in which case $\Gamma[\mathrm{supp}(x)]$ is a complete graph, or $M(x) = M(v) \setminus \{v\}$ and in both cases all components of $\mathrm{co}(\Gamma[\mathrm{supp}(x)])$ not containing v are singletons.*

Proof. Write $x = v_{i_1}^{d_1} \dots v_{i_r}^{d_r} c$ and

$$C_{G_\Gamma}(x) = \langle x_{C_1} \rangle \cdots \langle x_{C_s} \rangle \cdot \big\langle \{ v_m \mid [v_m, v_{i_j}] = 1 \text{ for all } j \} \big\rangle \cdot G'_\Gamma$$

as above. Assume, w.l.o.g., that v is contained in the component C_1 of $\mathrm{co}(\Gamma[\mathrm{supp}(x)])$. Then clearly $x_{C_2}, \dots, x_{C_s} \in C_{G_\Gamma}(v)$ and whenever $[v_m, v_{i_j}] = 1$ for all j then $[v_m, v] = 1$ in particular. Both $C_{G_\Gamma}(x)$ and $C_{G_\Gamma}(v)$ contain $G'_\Gamma \leq Z(G_\Gamma)$ and form $\mathbb{F}_p$-spaces modulo G'_Γ. Thus $|C_{G_\Gamma}(x)| \leq |C_{G_\Gamma}(v)|$ is equivalent to $\dim_{\mathbb{F}_p}(C_{G_\Gamma}(x)/G'_\Gamma) \leq \dim_{\mathbb{F}_p}(C_{G_\Gamma}(v)/G'_\Gamma)$.

Now $C_1, \dots, C_s$ partition $\mathrm{supp}(x) \subseteq V(\Gamma)$ and $V(\Gamma)$ is linearly independent modulo G'_Γ by definition of G_Γ. Assume $w \in M(x) \cap C_i$ for some i then w commutes with all vertices from $\mathrm{supp}(x)$ and this is equivalent to $C_i = \{w\}$. So $C_{G_\Gamma}(x)/G'_\Gamma$ has a basis of the form $\{ x_{C_i} G'_\Gamma \mid |C_i| > 1 \} \cup \{ w G'_\Gamma \mid w \in M(x) \}$ and these sets are disjoint. Now we always have $M(x) \subseteq M(v)$ and for $i > 1$ it holds $C_i \subseteq M(v)$ (so in particular $x_{C_i} \in M(v)$ as well). If $|C_1| = 1$ (so $C_1 = \{v\}$) then $\{ x_{C_i} G'_\Gamma \mid |C_i| > 1 \} \cup \{ w G'_\Gamma \mid w \in M(x) \}$ is completely contained in $C_{G_\Gamma}(v)$. If $|C_1| > 1$ then $v \notin M(x)$ and by the argument above $\{ x_{C_i} G'_\Gamma \mid i > 1, |C_i| > 1 \} \cup \{ w G'_\Gamma \mid w \in M(x) \} \cup \{ v G'_\Gamma \}$ is a union of disjoint sets which is linearly independent modulo G'_Γ. In both cases $|C_{G_\Gamma}(x)| \leq |C_{G_\Gamma}(v)|$ and if $|C_i| > 1$ for some $i > 1$ then actually we get a proper inequality (all elements from C_i contribute to $\dim_{\mathbb{F}_p}(C_{G_\Gamma}(v)/G'_\Gamma)$ separately). So if equality holds then $\dim_{\mathbb{F}_p}(C_{G_\Gamma}(x)/G'_\Gamma) \leq M(x) + 1$ (since all C_i apart from maybe C_1 are covered by $M(x)$) and assuming $M(x) \neq M(v)$ we additionally must have $|M(v)| = |M(x)| + 1$ showing that in this case $|C_1| > 1$ and $v \notin M(x)$. □

This means that elements of the form vz with $v \in V(\Gamma)$ and $z \in G'_\Gamma$ are almost canonical in G_Γ in the following sense: Define a set $\mathcal{C}$ as the union of all minimal generating sets $\{g_1, \dots, g_n\}$ of G_Γ (so $n = |V(\Gamma)|$) for which the value of $\sum_i |C_{G_\Gamma}(g_i)|$ is maximal among minimal generating sets of G_Γ. Then $\mathcal{C}$ contains $V(\Gamma)$ since $V(\Gamma)$ is such a generating set itself. Furthermore $\mathcal{C}$ is canonical in G_Γ (invariant under all automorphisms) and we can use it to analyze possible automorphisms.

In the following part we want to compare different groups presented on graphs. Let us fix graphs Γ_1 and Γ_2 on the vertex set $\{v_1, \dots, v_n\}$ with edges given by E_1 and E_2 and corresponding groups $G_i := G_{\Gamma_i}$. The standard generators on which the G_i are presented will again be called $(v_j)_{1 \leq j \leq n}$.

Theorem 5.3.13. *It holds that $\Gamma_1 \cong \Gamma_2$, if and only if $G_1 \cong G_2$.*

Proof. Let $\varphi\colon \Gamma_1 \to \Gamma_2$ be a graph isomorphism. Then φ induces an automorphism of $F_{n,p}$ by permuting generators and we have $G_{\Gamma_i} = F_{n,p}/N_i$ where N_i is the central subgroup generated by edges of Γ_i. Thus, as a group automorphism, φ maps N_1 to N_2 giving an isomorphism of the corresponding quotients.

For the other direction consider a group isomorphism $\varphi : G_1 \to G_2$. From Lemma 5.3.12 we see that for $x \in G_i$ and $v \in \operatorname{supp}(x)$ we have

$$\circledast : \ |C_{G_i}(x)| \leq |C_{G_i}(v)|.$$

As in the last lemma let $M(x) := \{v \in V(\Gamma_i) \mid [v, w] = 1 \text{ for all } w \in \operatorname{supp}(x)\}$ for $x \in G$ be the set of standard generators commuting with the entire support of x. In fact $M(x) = \bigcap_{w \in \operatorname{supp}(x)} N[w]$.

Our strategy is now to alter the group isomorphism $\varphi : G_1 \to G_2$ until we can extract sufficiently much information on the graphs. We do so by redefining the images $y_i = \varphi(v_i)$ and double checking that the new map is still a homomorphism onto a generating set and thus an isomorphism.

Consider the case that $y := y_j$ is supported in G_2 by more than one vertex for some index $j \leq n$. There must be some vertex $v \in \operatorname{supp}(y)$ such that replacing y with v still leaves us with a generating set for G_2. Indeed, this is true in the elementary abelian group $G_2/(G_2)'$ and commutators are non-generators in G_2. Furthermore, from $\circledast$ it follows that $(v_1, \dots, v_n)$ is a generating set of G_1 which maximizes the sum of centralizer orders $\sum_i |C_{G_1}(v_i)|$ among minimal generating sets and since φ is an isomorphism, the same must be true for $(y_1, \dots, y_n)$ in G_2. For $i > 1$, consider y_i such that $[y, y_i] = 1$. From Corollary 5.3.11 we see that (up to multiplication with commutators which can be ignored) $y_i = y_{C_1}^{t_1} \dots y_{C_s}^{t_s} v_{i_1}^{e_1} \dots v_{i_k}^{e_k}$ for some vertices $v_{i_j} \in M(y)$ and where $C_1, \dots C_s$ are the components of $\operatorname{co}(\Gamma[\operatorname{supp}(y)])$ and we also get that $[y_i, v] = [y_{C_1}^{t_1}, v]$ where we, w.l.o.g., assume that $v \in C_1$. The last Corollary furthermore shows that $|C_i| = 1$ for $i > 1$, so actually we can write $y_i = y_{C_1}^{t_1} v_{i_1}^{e_1} \dots v_{i_{k'}}^{e_k}$ for $v_{i_j} \in M(y)$. Using the same argument as for y and v there is some $w \in \operatorname{supp}(y_i)$ such that y_i can be replaced with w while still keeping a generating set and for this w we again have $|C_{G_2}(y_i)| = |C_{G_2}(w)|$. Also note that if $|C_1| = 1$ then $[v, y_i] = 1$ which is what we want to show. Similarly we are done if $t_1 \equiv_p 0$, so assume otherwise. If $|C_1| > 1$ there is some $v' \in C_1$ such that $[v, v'] \neq 1$ and in particular $v, v' \notin M(y_i)$ implying that $v, v' \in \operatorname{supp}(y_i)$ from the expression for y_i above. Now w can be chosen such that $w \notin C_1$ (since the exponents of y and y_i over elements of C_i agree this follows from rank considerations and the fact that $(y_1 G_2', \dots, y_n G_2')$ forms a basis of G_2/G_2'). Thus $M(y_i) \subseteq M(w) \setminus \{v, v'\}$ contradicting the previous Corollary.

In conclusion, $[y, y_i] = 1$ implies $[v, y_i] = 1$ (And we even see that this only happens if $\operatorname{supp}(y)$ induces a complete graph or if $\operatorname{supp}(y_i) \cap C_1 = \emptyset$). Hence exchanging y for v gives us a generating set which is still a valid image of $(v_1, \dots, v_n)$. We can iterate this process to obtain an isomorphism mapping vertices to elements supported by single vertices as well which gives rise to a bijection between vertices. The fact that the isomorphism respects commutators then translates to respecting edges of the graphs and we conclude that $\Gamma_1 \cong \Gamma_2$. □

It is not always the case that the original vertices $V(\Gamma)$ of the graph form a canonical subset of G_Γ, even when taken modulo commutators. However, we can precisely describe the conditions under which they do (In a previous version of the paper we neglected the inclusion of commutators in the canonical set. We thank Ilia Ponomarenko for pointing this out to us).

Lemma 5.3.14. *Assume $\Gamma_1 \cong \Gamma_2$. Then $\Gamma_i G_i'$ is canonical in G_i, if and only if in Γ_1 (and thus Γ_2) there is no pair of distinct vertices v, w with $N(v) \subseteq N[w]$.*

In this case, each element of $\mathrm{Iso}(G_1, G_2)$ *uniquely determines an element of* $\mathrm{Iso}(\Gamma_1, \Gamma_2)$ *by restriction to $\{vG_1' \mid v \in \Gamma_1\}$.*

Proof. Following the last proof we see that elements with single-vertex support are canonical in G_1 and G_2 under the condition above. Assume the condition does not hold in Γ_1 and for distinct vertices $v \neq w$ we have $N(v) \subseteq N[w]$. Then mapping v to vw and fixing other generators extends to an automorphism of G_1 via the given presentation of G_1 from Γ_1. □

5.3.1 Constructing groups with equal k-profiles

In this section, we want to apply the construction from the previous section to specific graphs. The idea is to start with a family of 3-regular base graphs such that the CFI-construction gives us two non-isomorphic graphs Γ_1 and Γ_2 for each of the base graphs, which can be distinguished by k-WL only for k scaling linearly with the size of the CFI-graphs (recall Theorem 2.2.5). We show below that the resulting groups $G_i := G_{\Gamma_i}$ have equal $\Theta(k)$-profiles.

Definition 5.3.15. For a group G, a tuple $(g_1, \dots, g_k) \in G^k$ is *minimal* if $\langle g_1, \dots, g_k \rangle$ is not generated by $k-1$ elements.

When working with $F := F_{n,p}$ we will fix a standard basis for $Z(F) = \Phi(F) \cong \mathbb{F}_p^{\binom{n}{2}}$. If F is presented on generators $v_1, \dots, v_n$ we choose

$$([v_1, v_2], [v_1, v_3], \dots, [v_1, v_n], [v_2, v_3], \dots, [v_{n-1}, v_n])$$

as our fixed basis for the center of F. We call these commutators the *standard commutators.*

Definition 5.3.16. Let $\bar{g} := (g_1, \dots, g_k) \in F_{n,p}^k$. We define two matrices over $\mathbb{F}_p$. In the $(k \times n)$-matrix $B_1(\bar{g})$, the i-th row corresponds to (the exponents of) g_i expressed in the normal form with respect to the standard generators. In the $\left(\binom{k}{2} \times \binom{n}{2}\right)$-matrix $B_2(\bar{g})$, the rows correspond to $[g_1, g_2], [g_1, g_3], \dots, [g_{k-1}, g_k]$ expressed in terms of the standard commutators, in this order. We sometimes index the columns by these labels, i.e., the column belonging to $[v_i, v_j]$ will be referenced as $B_2(\bar{g})([v_i, v_j])$.

Example 5.3.17. Assume $n = 3$ and $k = 2$ and assume $\bar{g} := (g_1, g_2)$ with $g_1 = v_1 v_2^5 v_3$ and $g_2 = v_1^2 v_2 [v_1, v_2]$. Then $[g_1, g_2] =$

$$[v_3, v_1^2][v_2^5, v_1^2][v_3, v_2][v_1, v_2] = [v_1, v_2]^{-9}[v_1, v_3]^{-2}[v_2, v_3]^{-1}.$$

In this case $B_1(\bar{g}) = \begin{pmatrix} 1 & 5 & 1 \\ 2 & 1 & 0 \end{pmatrix}$ and $B_2(\bar{g}) = (-9, -2, -1)$

where entries are to be read modulo p.

Lemma 5.3.18. *Let $\bar{g} := (g_1, \dots, g_t) \in (F_{n,p})^t$. Then we have $B_2(\bar{g}) = B_1(\bar{g}) \wedge B_1(\bar{g})$, where $\wedge$ denotes the exterior product of matrices with respect to our chosen ordering for the standard bases.*

Proof. Express the commutator $c_{i,j} := [g_i, g_j]$ in terms of the standard commutators. Then $c_{i,j} = \left([v_k, v_\ell]^{m(k,\ell)}\right)_{k<\ell}$ where $m(k,\ell) = (B_1(\bar{g}))_{i,k}(B_1(\bar{g}))_{j,\ell} - (B_1(\bar{g}))_{i,\ell}(B_1(\bar{g}))_{j,k} =$

$$\det \begin{pmatrix} (B_1(\bar{g}))_{i,k} & (B_1(\bar{g}))_{i,\ell} \\ (B_1(\bar{g}))_{j,k} & (B_1(\bar{g}))_{j,\ell} \end{pmatrix}.$$

Thus, the row of $B_2(\bar{g})$ belonging to $c_{i,j}$ corresponds to the row of $B_1(\bar{g}) \wedge B_1(\bar{g})$ belonging to rows $B_1(\bar{g})_{i,-}$ and $B_1(\bar{g})_{j,-}$ □

In particular, this shows that subgroups of $F_{n,p}$ are direct products of relatively free groups and central groups. In the following we will use the fact that for $M \in \mathbb{F}_p^{k \times n}$ we have $\operatorname{rank}(M \wedge M) = \binom{\operatorname{rank}(M)}{2}$, see for example [26, Section 10.1].

Lemma 5.3.19. *Let $G \leq F_{n,p}$ be generated by $\bar{g} := (g_1, \dots, g_t)$ and set $r := \operatorname{rank}(B_1(\bar{g}))$. Then there are r elements g_{i_j} among $\{g_1, \dots, g_t\}$ and central elements $c_1, \dots, c_k \in Z(F_{n,p})$ for some $0 \leq k \leq (n-r)$ such that $G = \langle g_{i_1}, \dots, g_{i_r} \rangle \times \langle c_1, \dots, c_k \rangle$. Furthermore, G' has $\mathbb{F}_p$-dimension $\binom{r}{2}$.*

Proof. If $B_1(\bar{g})$ has rank r, we can choose r linearly independent rows corresponding to certain generators g_{i_j}. Other rows can then be expressed via these chosen rows which by definition of $B_1(\bar{g})$ means that all other generators can be replaced by central elements $c_1, \dots, c_{n-r}$ without changing G. Set $G_r := \langle g_{i_1}, \dots, g_{i_r} \rangle$. The corresponding rows in $B_1(\bar{g})$ are now independent meaning that no set of cardinality less than r can generate G_r. Since all other generators are now central we have $[G, G] = [G_r, G_r]$ and the latter is of dimension $\operatorname{rank}(B_2(\bar{g})) = \binom{r}{2}$. Choose a subset of c_i's that is maximal with respect to the property $G_r \cap \langle c_{i_1}, \dots, c_{i_k} \rangle = \emptyset$. Then $G = \langle G_r, c_{i_1}, \dots, c_{i_k} \rangle$ as desired. □

The following observation is elementary but will help us compare subgroups of G_Γ for different values of Γ.

Lemma 5.3.20. *Let $H := \langle g_1, \dots, g_t, z_1, \dots, z_r \rangle \leq G_\Gamma$ and $R := \dim(\Phi(H))$. Assume that all z_i are central in G_Γ, that $\langle g_1, \dots, g_t \rangle / Z(G_\Gamma) \cong \mathbb{F}_p^t$ holds. Furthermore assume that H is not generated by less than $t + r$ elements. Let $c_1, \dots, c_R$ be generators of $\Phi(H)$ of the form $c_i = [g_{i_1}, g_{i_2}]$ and express all other commutators $c_{R+1}, \dots, c_{\binom{t}{2}}$ between the g_i as words $w_{R+1}, \dots, w_{\binom{t}{2}}$ in the c_i. Then*

$$H \cong \langle g_1, \dots, g_t \mid \text{exponent } p, \text{ class } 2\ , w_{R+1}, \dots, w_{\binom{t}{2}} \rangle \times C_p^r.$$

Proof. By assumption $|\langle g_1, \dots, g_t \rangle| = p^{t+R}$. Clearly the presentation above defines a group admitting an epimorphism onto $\langle g_1, \dots, g_t \rangle$. Due to the given relations its order is at most p^{t+R}. Since $(g_1, \dots, g_t, z_1, \dots, z_r)$ is assumed to be minimal, the central group $\langle z_1, \dots, z_r \rangle \cong C_p^r$ splits from H. □

Let $\Gamma_0 = (\{V_1, \ldots, V_t\}, E)$ be a 3-regular graph with $N := |E|$ edges and such that $\Gamma_1 := \mathrm{CFI}(\Gamma_0)$ and $\Gamma_2 := \widetilde{\mathrm{CFI}(\Gamma_0)}$ are not isomorphic (cf. Theorem 2.2.5). Let $n := 10t$ be the number of vertices of Γ_1 and Γ_2.

To improve readability, we use capital letters for the vertices of the base graph in the following.

We assume Γ_0 and $\mathrm{co}(\Gamma_0)$ to be connected and then the same holds for the corresponding CFI-graphs. Recall that the CFI-graphs are again 3-regular. In the following we call a pair of edges between two CFI-gadgets together with their adjacent vertices a *link* and *twisting* is understood as replacing the edges in a link with their twisted version. Note that two gadgets or two links are always disjoint or equal and that links correspond bijectively to edges in the base graph Γ_0. We call vertices of links external (w.r.t. their gadget) and other vertices internal. We fix $F := F(n, p)$, the relatively free group on vertices of the CFI-graphs above. We also fix normal subgroups $N_1, N_2 \leq F$ corresponding to edges of Γ_1 and Γ_2, respectively. Thus $G_i := G_{\Gamma_i} = F/N_i$. Finally, let e be any edge in the base graph and let ${}^{(e)}\colon F \to F$ be the following map: Say $e = (V, W) \in E(\Gamma_0)$ (so we actually chose an orientation). Then twisting along e can be seen as swapping in all normal forms the standard commutators $[a_i^V, a_j^W]$ and $[a_i^V, b_j^W]$ and also swapping all occurrences of $[b_i^V, b_j^W]$ and $[b_i^V, a_j^W]$. This is of course not a group isomorphism but it induces an automorphism $\varphi\colon Z(F) \to Z(F)$. If $x \in F$ has a normal form that factors as vc where v is the part of x in standard generators and c is the product of standard commutators then $x^{(e)} := v\varphi(c)$ and this defines a bijection of F into itself.

Definition 5.3.21. A group $H \leq F$ is called *essentially k-generated* if

1. $F' = Z(F) \leq H$ and
2. $\dim_{\mathbb{F}_p}(H/F') = k$.

Intuitively this means that the group is k generated modulo the center. Define $\mathcal{H}_k \subseteq \mathrm{Sub}(F)$ to be the set of all essentially k-generated subgroups of F.

Lemma 5.3.22. *For every subgroup $S \leq G_i = F/N_i$ for which $\dim_{\mathbb{F}_p}(S/G_i') = k$ there is a unique essentially k-generated subgroup $H \leq F$ such that $S \leq H/N_i$.*

Proof. Let $\nu : F \to F/N_i$ be the natural epimorphism then H can be uniquely defined as $\nu^{-1}(S)F'$. □

Set $\mathcal{H}_k^{N_i} := \{H/N_i \mid H \in \mathcal{H}_k\}$. Our goal is for various k to construct a bijection

$$\mathcal{H}_k^{N_1} \to \mathcal{H}_k^{N_2}$$

that preserves isomorphism-types of groups. Since all k-generated subgroups have the property that $\dim_{\mathbb{F}_p}(S/G_i') = k$, the lemma above then gives an isomorphism-type preserving bijection between k-generated subgroups of G_1 and G_2. Note that $\mathcal{H}_k^{N_i} = \{S \leq G_i \mid \dim_{\mathbb{F}_p}(S/G_i') = k \text{ and } G_i' = Z(G_i) \leq S\}$.

Lemma 5.3.23. *Let $1 \leq k < N/10$ where N is the number of edges in Γ_0. For $H \in \mathcal{H}_k$ there is some edge e in the base graph such that $H/N_1 \cong H/N_1^{(e)}$.*

Proof. Let $H := \langle f_1, \dots, f_\ell \rangle$ and for each i set $g_i := f_i N_1 \in G_1$. We want to investigate the group $(H/N_1)' = H'/N_1$. Since it is generated by commutators between the g_i its structure is mostly described by $B_2(\bar{f}) = B_1(\bar{f})^{\wedge 2}$ after replacing columns indexed by elements of N_1 with zero-columns. Call this new matrix $B_2(\bar{g})$.

Twisting along edge $e = (V, W) \leq E(\Gamma_0)$ results in mapping $([a_i^V, a_j^W], [b_i^V, b_j^W])$ to $([a_i^V, b_j^W], [b_i^V, a_j^W])$ (and vice versa, see Section 2.2.4). This can also be interpreted in terms of the matrices from above as replacing the two zero-columns $B_2(\bar{g})([a_i^V, a_j^W])$ and $B_2(\bar{g})([b_i^V, b_j^W])$ by the original columns in $B_2(\bar{f})$ and replacing the columns corresponding to $[a_i^V, b_j^W]$ and $[b_i^V, a_j^W]$ with zero-columns instead. This defines a matrix $B_2(\bar{g}^{(e)})$ that describes linear dependencies between commutators among the $(f_1^{(e)} \dots, f_k^{(e)})$ modulo $N_1^{(e)}$.

We will now argue that e can be chosen in such a way that $B_2(\bar{g})$ and $B_2(\bar{g}^{(e)})$ have the same column spaces. For this, we argue that we can fix a system of columns of rank r in $B_2(\bar{g})$ that does not contain the columns affected by twisting along e, then for e as above these columns also form a system of maximal rank in $B_2(\bar{g}^{(e)})$ and thus linear dependency relations for rows of the two matrices are exactly the same. Using Lemma 5.3.20 we see that $H/N_1 \cong H/N_1^{(e)}$ for this choice of e.

By assumption the rank of $B_1(\bar{f})$ is k and $k < N$. We assume w.l.o.g. that the first k columns of $B_1(\bar{f})$ are linearly independent. Then the same holds for the first $\binom{k}{2}$ columns in $B_2(\bar{f}) = B_1(\bar{f}) \wedge B_1(\bar{f})$. Now these columns may not contain a system of full rank anymore in $B_2(\bar{g})$ but they belong to commutators of the form $[i, j]$ for $1 \leq i < j \leq k$. Since Γ_i is 3-regular, for a fixed i at most three of these commutators are contained in N_1. Thus the rank of the first $\binom{k}{2}$ columns in $B_2(\bar{g})$ is at least $\binom{k}{2} - 3k$ and we may choose $r' \leq 3k$ additional columns such that they contain a system of full rank together with the first $\binom{k}{2}$ columns. Now every such column belongs to a pair of vertices and the number of relevant vertices for the full rank system in total is smaller than $2r' + k \leq 7k < N$ and thus there are still links in Γ_1 that are not adjacent to any of these vertices. Let us say these links correspond at least to edges $e_1, \dots, e_{N-7k}$. For each of these links there are two zero-columns in $B_2(\bar{g})$ and two columns agreeing with $B_2(\bar{f})$ corresponding to the twisted/non-twisted version of this link. Due to the choice of the edges we can now replace all four of these columns by zero-columns without reducing the rank of the resulting matrix. We will argue that among the edges $e_1, \dots, e_{N-7k}$ there are some edges where twisting also does not change the rank.

For this, note that for vertices v, w, column $(B_2(\bar{f}))([v, w])$ is a linear combination of columns $(B_2(\bar{f}))([v, y])$ and also a linear combination of columns $(B_2(\bar{f}))([y, w])$ where y runs through the first k columns of $B_1(\bar{f})$ since we assumed the first k columns of $B_1(\bar{f})$ to be linearly independent and since the entries of $B_2(\bar{f})$ are sub-determinants of $B_1(\bar{f})$. Say the first k columns of $B_1(\bar{f})$ correspond to vertices $v_1, \dots, v_k$ in the CFI-graphs. We say that $1 \leq i \leq k$ is *bad* for some link if v_i is adjacent to this link. Since each index is bad for at most three links and $3k < N - 7k$, there exist links over the edges $e_1, \dots, e_{N-7k}$ for which no index is bad. For such a link, belonging to edge e say, all columns in the linear combination described above are still present in $B_2(\bar{g})$ and thus the rank of this matrix is the same as for $B_2(\bar{g}^{(e)})$. □

Definition 5.3.24. Set $\mathcal{V} := V(\Gamma_1)$ and identify $\mathrm{Sym}(\mathcal{V})$ as a subgroup of $\mathrm{Aut}(F)$ in the natural way. We set A to be the group of permutations of $\mathrm{Sym}(\mathcal{V})$ that map each gadget to itself with an automorphism. (I.e., A consists of the graph automorphisms after link edges have been removed.)

Note that the group A is abelian. It is generated by the permutations of $\mathcal{V}$ twisting two incident links in Γ_1 while permuting the inner vertices of their common gadget accordingly to a graph automorphism of the gadget. In particular, A stabilizes all links and gadgets setwise.

If $H \in \mathcal{H}_k$ then for any edge e of Γ_0 we have $H^{(e)} = H$ (even if ${}^{(e)}$ is not a group isomorphism). Lemma 5.3.23 shows that for $H/N_1 \leq G_1$ there is some edge e of Γ_0 such that $H/N_1 \cong H/N_1^{(e)}$ and by the properties of the CFI-construction the twist ${}^{(e)}$ can be altered to become the original twist via suitable elements from A. More precisely, in the situation above there is some $\sigma_e \in A$ (only depending on e) such that $H/N_1^{(e)} \cong \sigma_e(H_1)/N_2$. This defines an isomorphism-type preserving map

$$\Phi : \mathcal{H}_k^{N_1} \to \mathcal{H}_k^{N_2},\ H/N_1 \mapsto \sigma_e(H_1)/N_2,$$

where e depends on H and we will show that the edges can be chosen in a way that makes Φ bijective.

Definition 5.3.25. Let $i \in \{1, 2\}$. We say that subgroups $H_1/N_i, H_2/N_i \in \mathcal{H}_k^{N_i}$ are of the same *type* if there is some $\sigma \in A$ such that $H_1 = \sigma(H_2)$.

An inspection of Lemma 5.3.23's proof shows the choice of edge e only depends on the type of the subgroups involved.

Lemma 5.3.26. *If $k < N/10$, the edge e in Lemma 5.3.23 can be chosen to be the same for all subgroups of a fixed type.*

Proof. Since A fixes links setwise, positions where twisting preserves the isomorphism type are the same for groups that get mapped to each other via elements from A. □

Lemma 5.3.27. *For each edge e compatible with Lemma 5.3.23, Φ maps subgroups of different types to subgroups of different types.*

Proof. Assume that 5.3.23 gives edges e_1 and e_2 for groups $S, \tilde{S} \leq G_1$. Write $S = H/N_1$, $\tilde{S} = \tilde{H}/N_1$ and assume that $\sigma_{e_1}(H)/N_2$ and $\sigma_{e_2}(\tilde{H})/N_2$ have the same type. Then there is some $\sigma \in A$ with $(\sigma_{e_2}^{-1}\sigma\sigma_{e_1})(H) = \tilde{H}$ and thus S and $\tilde{S}$ have the same type. □

Lemma 5.3.28. *For a fixed type and a fixed edge e (as in Lemma 5.3.23), Φ is isomorphism-type preserving and injective.*

Proof. Keep the notation from the last lemma but assume $S_1 \neq S_2$ are of the same type. Then $H_1 \neq H_2$. Thus $\sigma_e(H_1) \neq \sigma_e(H_2)$ which is equivalent to $\sigma_e(H_1)/N_2 \neq \sigma_e(H_2)/N_2$ due to $\sigma_e(H_i)$ containing $Z(F)$ and in particular N_2. □

All arguments also work for interchanged roles of G_1 and G_2. In particular this shows that $|\mathcal{H}_k^{N_1}| = |\mathcal{H}_k^{N_2}|$ for each k.

Corollary 5.3.29. *G_1, G_2 have equal k-profiles for $k < N/10$.*

Proof. Since bijection Φ is isomorphism-type preserving, the collection of subgroups in $\mathcal{H}_k^{N_1}$ is mapped bijectively to $\mathcal{H}_k^{N_2}$, such that isomorphism types are respected. Every k-generated subgroup is contained in a unique factor of an essentially k-generated subgroup (Lemma 5.3.22) so this induces a bijection from k-generated subgroups to k-generated subgroups. □

Finally, by the CFI-construction and by 3-regularity of the base graph, N is linear in $n = |V(\Gamma_i)|$, thus $n \in \Theta(\sqrt{\log|G_i|})$.

Corollary 5.3.30. *G_1 and G_2 have equal $\Theta(\sqrt{\log(n)})$-profiles.*

After the constructions given in [44] and [110], the results of the present section provide a third construction of infinitely many pairs of groups, whose subgroup profiles, in an asymptotic sense, are highly similar. All three constructions that are currently known work in the class of p-groups, whereas the question is still open for non-nilpotent groups.

For the commuting graphs of G_1 and G_2, note that non-central elements in G_1 that are not powers of one another cannot commute if one of the elements has a support of 4 or larger. Whether the Weisfeiler-Leman algorithm of a particular dimension distinguishes the graphs therefore does not change when restricting the commuting graphs to group elements with support size at most 3. In particular, the commuting graphs cannot be distinguished by the $\mathcal{O}(\sqrt{\log(n)})$-dimensional Weisfeiler-Leman algorithm.

5.3.2 The Weisfeiler-Leman Dimension of groups constructed from CFI-graphs is 3

In the previous section we constructed groups $G_i := G_{\Gamma_i}$ based on two CFI-graphs Γ_1 and Γ_2. The groups agree in terms of traditional group theoretical invariants (such as exponent, nilpotency class, and the combinatorics of their conjugacy classes) and also with respect to their k generated subgroups for large k. On first sight this might indicate that these groups should be hard to distinguish by combinatorial means but as we will see in this section their $\mathrm{WL}_{\mathrm{implicit}}$-dimension is only 3. The main theorem of this section is the following.

Theorem 5.3.31. *Let Γ_0 be a 3-regular connected graph and let $\Gamma_1 := \mathrm{CFI}(\Gamma_0)$ and $\Gamma_2 := \widetilde{\mathrm{CFI}(\Gamma_0)}$ be the corresponding CFI-graphs. Then 3-$\mathrm{WL}_{\mathrm{implicit}}$ distinguishes G_1 from G_2. If additionally Γ_0 has (graph) WL-dimension at most 3 then 3-$\mathrm{WL}_{\mathrm{implicit}}$ identifies G_1 as well as G_2 up to isomorphism.*

Requiring that Γ_0 has WL-dimension at most 3 is not a severe restriction (Observation 2.2.6). Towards proving the theorem we collect several observations on the pebble game that are particular to the groups arising from CFI-graphs.

Lemma 5.3.32. *For each $k \geq 3$, throughout the implicit k-pebble game on G_1 and G_2, Duplicator has to choose bijections that respect the set of elements with single-vertex support $\{x \mid |\mathrm{supp}(x)| = 1\}$. Moreover $\mathrm{supp}(x) = \mathrm{supp}(y)$ and $|\mathrm{supp}(x)| = |\mathrm{supp}(y)| = 1$ must imply $\mathrm{supp}(f(x)) = \mathrm{supp}(f(y))$.*

Proof. To see this, it suffices to realize that centralizers of elements with single-vertex support have a different cardinality than other elements. Indeed, since the graphs Γ_1 and Γ_2 are 3-regular, by Corollary 5.3.11 each single support vertex has a centralizer of cardinality $p^4|Z(G_i)|$. However, since $\mathrm{co}(\Gamma)$ is connected, has no triangles and no cycles of length 4, other elements have a centralizer of cardinality at most $p^3|Z(G_i)|$.

To see the second part of the theorem, note the following: for two elements x, y with $|\operatorname{supp}(x)| = |\operatorname{supp}(y)| = 1$ we have $\operatorname{supp}(x) = \operatorname{supp}(y)$ exactly if $C(x) = C(y)$. Since commutation and support sizes must be respected this shows the lemma. □

Lemma 5.3.33. *Consider the implicit k-pebble game with $k \geq 4$. If Duplicator does not respect support sizes at some point then Spoiler has a winning strategy.*

Proof. Assume Duplicator chooses a bijection $f \colon G_1 \to G_2$ during the implicit k-pebble game with $k \geq 4$ such that $|\operatorname{supp}(x)| \neq |\operatorname{supp}(f(x))|$ for some $x \in G_1$. We already discussed that Spoiler has a winning strategy in this situation in the case that one of the supports has cardinality at most 1. Since the distribution of support sizes in G_1 and G_2 is the same there is some $x \in G_1$ with $|\operatorname{supp}(f(x))| > |\operatorname{supp}(x)| > 1$. We can choose some $v_i \in V(\Gamma_1)$ and a natural number m such that $x' := xv_i^m$ has strictly smaller support than x. Now $f(v_i^m)$ must also be supported by exactly one element, or otherwise Duplicator loses anyway. Using 4 pebbles, Spoiler can force Duplicator to map x' to $f(x)f(v_i^m)$. Thus, after three additional rounds, the support of $f(x')$ is still strictly bigger than $\operatorname{supp}(x')$ and the result follows by induction. □

Lemma 5.3.34. *For each $k \geq 4$, throughout the implicit k-pebble game on G_1 and G_2, Duplicator has to choose bijections respecting internal vertices and gadgets of the underlying CFI-graphs. Here, elements corresponding to a gadget vertex v are all elements of $vZ(G_i)$. Moreover pairs of vertices lying in a common gadget have to be mapped to pairs in a common gadget.*

Proof. By Lemma 5.3.32 the bijection chosen by Duplicator induces a permutation of the vertices $V(\Gamma_1)$. By Construction, the CFI-graphs Γ_i have the property that every 6-cycle and every 8-cycle runs entirely within one gadget. Moreover every pair of vertices lying in a common gadget lies on a common 6-cycle or on a common 8-cycle. This implies that Duplicator has to map vertices v, w in a common gadget to vertices in a common gadget (and vice versa). Indeed, otherwise Spoiler can show that v and w are contained in a small cycle but $f(v)$ and $f(w)$ are not (and vice versa). This in turn implies that Duplicator has to map internal vertices to internal vertices, because internal vertices are not adjacent to vertices in another gadget, but external vertices are. □

Using these observation we can finally prove the theorem.

Proof of Theorem 5.3.31. We first define a set $\mathcal{V}$ of special vertices in Γ_1: For each gadget put exactly one internal vertex in $\mathcal{V}$ and add all adjacent external vertices. Let $v \in G_1$ denote the ordered product of all vertices in $\mathcal{V}$. By Lemma 5.3.33, in the implicit 4-pebble game, Duplicator must choose a bijection for which $f(v)$ has the same support size as v. Spoiler puts a pebble on v. The Lemma furthermore shows that all future bijections have to map $\operatorname{supp}(v)$ to $\operatorname{supp}(f(v))$ or otherwise Spoiler can pebble some $v_i \in \operatorname{supp}(v)$ with $f(v_i) \notin \operatorname{supp}(f(v))$ and Duplicator will not be able to respect support sizes from here on. Using Lemma 5.3.34 we see that $\operatorname{supp}(f(v)) =: \mathcal{V}'$ has to be composed exactly as $\operatorname{supp}(v) = \mathcal{V}$, that is, $\mathcal{V}'$ can also be constructed by choosing sets of internal vertices, one per gadget, and adding all their adjacent external vertices. The set $\mathcal{V}$ induces a subgraph of Γ_1 and similarly $\mathcal{V}'$ induces a subgraph of Γ_2. We argue these subgraphs have a different number of edges modulo 2. For this observe the following: if we alter $\mathcal{V}$ by replacing one internal vertex with another one in the same gadget, this changes exactly two neighbors among the external vertices. The new induced subgraph differs then in exactly two locations of two different links. Thus the number of edges in the induced subgraph remains the same modulo 2. By induction this is true for all possible choices of $\mathcal{V}$. We can thus assume that $\mathcal{V} = \mathcal{V}'$. However, this implies that $\Gamma_1[\mathcal{V}]$ and $\Gamma_2[\mathcal{V}']$ disagree in exactly one edge, namely at the twisted link. This shows the graphs have a different number of edges modulo 2.

However, we already argued that Duplicator has to map $\mathcal{V}$ to $\mathcal{V}'$. Since the number of edges of $\Gamma_1[\mathcal{V}]$ and $\Gamma_2[\mathcal{V}']$ disagree, for any suitable bijection some vertex is mapped to a vertex of incorrect degree, which can be exploited by Spoiler. This shows G_1 can be distinguished from G_2.

Assume now that additionally the base graph Γ_0 has Weisfeiler-Leman dimension at most 3. Suppose that G is any group with $|G| = |G_1|$ that is indistinguishable from G_1. The vertices of Γ_1 form a canonical copy of Γ_1 inside of G_1 (up to central elements), so there must be a corresponding set in G as well. If the induced commutation graph Γ on this set is distinguishable from Γ_1 then G_1 is distinguishable from G. From the commutation graph, we can reconstruct a corresponding base graph Γ. Which must be indistinguishable by 3-$\mathrm{WL}_{\mathrm{implicit}}$ from Γ_0. This means it is isomorphic to Γ_0 since its (graph) Weisfeiler-Leman dimension is at most 3 by assumption. Thus, Γ is isomorphic to Γ_1 or Γ_2. This gives a presentation of G isomorphic to a presentation of G_1 or G_2. □

5.4 Groups with small solvable radical

The study of the solvable radical in relation to the isomorphism problem of finite groups was initiated by Babai et al., based on the Babai-Beals filtration of groups (see [7]). The crucial observation is that any group can be interpreted as a group extension of a group without normal abelian subgroups, that is a *semisimple* group, by a solvable group. The latter is precisely the solvable radical of the original group, and by [9], the automorphisms of $G/R(G)$ can be listed in time $|G|^{\mathcal{O}(\log\log|G|)}$. More generally, [9] showed that isomorphism of semisimple groups is solvable in the same runtime bound. In a subsequent paper [9], Babai et al. obtain the stronger result that isomorphism of semisimple groups can be solved in polynomial time.

We give a new proof of the $n^{\log\log n}$ bound (for both isomorphism of semisimple groups of order n, as well as enumeration of their automorphisms) by proving a $\mathcal{O}(\log\log n)$-bound for the WL-dimension of semisimple groups. For the next lemma, we recall Lemma 3.5.2, and we rephrase it for the specific situation of semisimple groups.

Lemma 5.4.1 (Logarithmic ordering scheme for semisimple groups). *Let G be a finite group and let $k \geq 5$ be an integer. Assume that G contains a center-less subgroup $U \leq G$ with a direct product decomposition $U = U_1 \times \cdots \times U_t$ for $t \in \mathbb{N}$. Let γ be a coloring of the elements of G, such that U is a union of γ-color classes. Then there are $\ell := \lceil \log t \rceil$*

elements $x_1, \dots, x_\ell \in U$, such that k-$\mathrm{WL}_{\mathrm{implicit}}$ applied to $(G, \gamma_{(x_1,\dots,x_\ell)})$ distinguishes the elements of U_i from the elements of U_j for all $i \neq j$. Here, $\gamma_{(x_1,\dots,x_\ell)}$ denotes the coloring obtained after individualizing $x_1, \dots, x_\ell$ in (G, γ). In other words, after $\log t$ individualizations, the stable k-$\mathrm{WL}_{\mathrm{implicit}}$-color classes induce an ordering of the direct factors of U.

Proof. By Corollary 4.3.26, the set $\bigcup_i U_i Z(U)$ is 5-$\mathrm{WL}_{\mathrm{explicit}}$-detectable and by the assumption that U is centerless, we have $\bigcup_i U_i Z(U) = \bigcup_i U_i$. Moreover, 5-$\mathrm{WL}_{\mathrm{explicit}}$ can distinguish pairs (u, u') of elements from the same subgroup U_i from pairs with $u \in U_i$ and $u' \in U_j$ for $i \neq j$, since the first case is distinguished from the second through the existence of some $u'' \in \bigcup_i U_i$ such that u and u'' do not commute and u' and u'' do not commute.

Through Lemma 4.1.3, for each subset $I \subseteq [t]$, it follows that 5-$\mathrm{WL}_{\mathrm{explicit}}$ inductively detects the set of $u \in U$ such that the non-identity components of $u = (u_1, \dots, u_t)$ with respect to the decomposition $U = U_1 \times \dots \times U_t$ are exactly given by u_i with $i \in I$. If u is individualized, then the elements u_i^{-1} with $i \in I$ are the unique elements in $\bigcup_i U_i$, such that, after multiplying with u, the resulting element has strictly less non-identity components than u. Hence, after individualizing u, we obtain that k-$\mathrm{WL}_{\mathrm{implicit}}$ detects the set $\{u_i \mid i \in I\}$. Therfore, we can use u exactly in the same way as a set-vertex in a set-extended structure, and by choosing u accordingly, we can define every set of the form $\{u_i \mid i \in I\}$ with $I \subseteq [t]$ and $u_i \in U_i$. In this sense, the assumptions of Lemma 3.5.2 are fulfilled by the set-up of the present lemma. □

We can use the idea of the previous proof, namely that products of group elements can be used as set-pebbles in certain contexts, to derive the following relationship between the WL-dimension of semisimple groups and the WL-dimension of permutation groups.

Definition 5.4.2. Let (Q, Ω) be a permutation group, regarded as a relational structure, so Q is a subgroup of $\mathrm{Sym}(\Omega)$. Then we define the *domain-extended* version of (Q, Ω), denoted by $(Q, \Omega)_{\text{domain-extended}}$ as the induced substructure of $(Q, \Omega)_{\mathrm{set-extended}}$, where we only include set pebbles for subsets of domain elements.

Lemma 5.4.3. *The $\mathrm{WL}_{\mathrm{explicit}}$-dimension of semisimple groups is bounded, up to some additive constant, by the $\mathrm{WL}_{\mathrm{explicit}}$-dimension of domain-extended permutation groups.*

Proof. Let G and H be semisimple groups. If their socles are not isomorphic, then by Lemma 4.2.32 and Lemma 4.2.30, G and H are distinguished by a constant dimensional WL-algorithm. Assume that $\mathrm{Soc}(G)$ and $\mathrm{Soc}(H)$ are isomorphic to

$$S_1 \times \dots \times S_t,$$

with non-abelian simple groups S_i.

Via Lemma 4.1.9 and Corollary 4.3.26, in the explicit pebble game, Spoiler can choose to interpret the pebble game on a pair of semisimple groups, say G and H, as the pebble game on $G/\mathrm{Soc}(G) \cup \{S_1, \dots, S_t\}$ and $H/\mathrm{Soc}(H) \cup \{S_1, \dots, S_t\}$, with $G/\mathrm{Soc}(G)$ and $H/\mathrm{Soc}(H)$ acting on $\{S_1, \dots, S_t\}$ as permutation groups through the resepctive conjugation action on the socles. By Lemma 4.2.41, to distinguish G and H, it is sufficient to distinguish these induced permutation groups up to permutational isomorphism, so the $\mathrm{WL}_{\mathrm{explicit}}$-dimension of semisimple groups is bounded, up to some additive constant, by the $\mathrm{WL}_{\mathrm{explicit}}$-dimension of permutation groups. To see that we can even reduce to the case of domain-extended permutation groups, we note that, as in the proof of the previous Lemma, Spoiler can use pebbles on products of vertices to implicitly fix arbitrary subsets of $\{S_1, \ldots, S_t\}$ setwise. □

Lemma 5.4.4. *Let G be semisimple, then we have* $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq \log\log|G| + 4$.

Proof. By Lemma 5.4.1, we may use individualizations, or equivalently, fixed pebbles in the bijective pebble game, to define an ordering of the simple direct factors of $\mathrm{Soc}(G)$. In the worst case we need $\log t$ pebble pairs for this, where t is the number of simple factors of $\mathrm{Soc}(G)$. In particular, $\log t$ is bounded by $\log\log|G|$. To see that the lemma is applicable to $\mathrm{Soc}(G)$, recall that $\mathrm{Soc}(G)$ is 5-$\mathrm{WL}_{\mathrm{implicit}}$-detectable by Lemma 4.2.32.

Relative to this fixed total ordering of the simple factors of $\mathrm{Soc}(G)$, Spoiler can use two more pebble pairs to fix an ordering of $\mathrm{Soc}(G)$. To see this, write $\mathrm{Soc}(G) = S_1 \times \cdots \times S_t$ and for each $i \in [t]$, let s_1^i and s_2^i be chosen such that $\langle s_1^i, s_2^i \rangle = S_i$ holds. Since the direct factors of $\mathrm{Soc}(G)$ are ordered, for each i, the element s_1^i can be recovered from $s_1 := \prod_i s_1^i$, and the analogous statement holds for s_2^i and $s_2 := \prod_i s_2^i$. Hence, Spoiler can fix a generating set of $\mathrm{Soc}(G)$, and thereby fix an ordering of $\mathrm{Soc}(G)$, by placing pebbles on s_1 and s_2. By semisimplicity, it holds that $C_G(\mathrm{Soc}(G))$ is trivial, so every element of G is uniquely determined by its conjugation action on the ordered set $\mathrm{Soc}(G)$. Since 2-$\mathrm{WL}_{\mathrm{implicit}}$ distinguishes elements based on this action, we obtain that the coloring computed by 2-$\mathrm{WL}_{\mathrm{implicit}}$ on G, relative to the fixed ordering of $\mathrm{Soc}(G)$, is discrete. In conclusion, $(\log\log|G| + 2 + 2)$-$\mathrm{WL}_{\mathrm{implicit}}$ identifies G up to isomorphism. □

As a corollary, we obtain a new proof for a well-known result of Babai et al, bounding the number of automorphisms of semi-simple groups [9]. In contrast to the original strategy, through the use of the Weisfeiler-Leman algorithm, we do not have to solve permutational isomorphism explicitly.

Corollary 5.4.5. *If G is a finite semisimple group, then we can list all automorphisms of G in time $|G|^{\mathcal{O}(\log\log|G|)}$.*

When more is known a priori about the permutational isomorphism type of the induced action on the socle factors, we can derive better bounds on the WL-dimension.

Lemma 5.4.6. *Let G be monolithic with non-abelian monolith M and assume that G/M is abelian. Then G is uniquely determined up to isomorphism by the isomorphism types of the characteristically simple group M and the abelian group G/M. In particular, the* $\mathrm{WL}_{\mathrm{explicit}}$*-dimension of G is at most* 4.

Proof. As G is semisimple, the isomorphism type of G is determined by the isomorphism type of M together with the permutational isomorphism type of the action of G induced on the set of simple factors of M. Since M is a the unique minimal normal subgroup of G, we have that G/M acts transitively and faithfully on the simple factors of M. Now G/M is abelian, hence the action of G/M is regular and permutationally isomorphic to the right-regular action of G/M, which is entirely determined by the isomorphism type of the abstract group G/M. The latter is identified by 4-$\mathrm{WL}_{\mathrm{explicit}}$ since G/M is abelian and 4-$\mathrm{WL}_{\mathrm{explicit}}$ is able to count the elements whose cosets modulo M have a given fixed order in the quotient group G/M by Lemma 4.1.9. □

We can partially generalize the bound on the WL-dimension of semisimple groups by parameterizing the WL-dimension of a finite group in terms of the rank of its solvable radical.

Lemma 5.4.7. *Let G be a finite group such that its solvable radical $\mathcal{R}(G)$ has a complement in G, so G is a semidirect product $\mathcal{R}(G) \rtimes G/\mathcal{R}(G)$. Let d be minimal such that $\mathcal{R}(G)$ is contained in some d-generated subgroup of G (so in particular we have $d \leq d(\mathcal{R}(G))$. Then*

$$\dim_{\mathrm{WL}_{\mathrm{explicit}}}(G) \leq \log\log|G| + d + 2.$$

Proof. Spoiler uses d pebble pairs to order $\mathcal{R}(G)$, since by assumption, there is a set of d group elements that generate an over-group of $\mathcal{R}(G)$, and after individualizing these d elements, the group they generate obtains a discrete coloring through 3-WL$_{\mathrm{implicit}}$ (we note that $\log\log|G| + d + 2$ is at least 4). Then Spoiler uses $\log\log|G| + 2$ pebble pairs to order $G/\mathcal{R}(G)$ (via Lemma 5.4.4 and Lemma 4.1.9). Relative to these orderings, G is completely ordered as it is a semidirect product of $\mathcal{R}(G)$ and $G/\mathcal{R}(G)$, so each element has a unique representation as a product of elements in ordered groups. □

5.5 Groups colored with a composition series

In view of a result by Luks [83], placing group isomorphism relative to fixed composition series in polynomial time, we investigate the Weisfeiler-Leman dimension of groups that are pre-colored in such a way, that the coloring encodes a fixed composition series. We make this precise in the following definition.

Definition 5.5.1. Let G be a group and χ a coloring of the elements of G. We say that χ *encodes a composition series of* G, if there is a composition series $1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ of G such that each G_i is a union of χ-color classes.

Consequently, all automorphisms of the colored group are contained in the stabilizer of the chosen composition series.

Lemma 5.5.2. *Let G be a direct product of non-abelian simple groups and let χ be a coloring that encodes a composition series of G. Then the stable coloring of* 4-WL$_{\mathrm{explicit}}$ *on (G, χ) assigns distinct colors to distinct simple normal subgroups of G, that is, it decomposes G into a direct product of detectable simple subgroups.*

Proof. We show the claim by induction on the number of simple direct factors of G, where the claim is fulfilled by definition if G is simple. So assume that G is not simple and let U be the maximal term of the composition series encoded by χ, that is not equal to G. In other words, χ restricted to U encodes a composition series of U, and U is a normal subgroup of G with G/U simple. By induction and Lemma 4.1.9, using the fact that U is a union of χ-color classes, it follows that the coloring computed by 4-WL$_{\mathrm{explicit}}$ on (G, χ) assigns distinct colors to distinct simple normal subgroups of U. Hence, we obtain a decomposition

$$G = U_1 \times \cdots \times U_m \times S,$$

where S is the unique simple normal subgroup of G not contained in U (here we use that G is a direct product of non-abelian simple groups, see also Lemma 4.2.29), each U_i is simple, and each U_i is a union of the color classes computed by 4-WL$_{\text{explicit}}$ on (G, χ). By definition of χ, it holds that the elements $1 \neq s \in S$ are characterized by the property that $\langle s^G \rangle$ is simple and $\chi(s)$ is not contained in $\chi(U)$. By Lemma 4.1.3, S too is then a union of color classes computed by 4-WL$_{\text{explicit}}$, proving the claim. □

In the case of semisimple groups, the previous result can be lifted to a bound on the WL-dimension of groups colored with a composition series.

Lemma 5.5.3. *Let G be a semisimple group and let χ be a coloring that encodes a composition series of G. Then* $\dim_{\text{WL}_{\text{explicit}}}(G, \chi) \leq 7$. *Moreover, with* 2 *individualizations,* 5-WL$_{\text{explicit}}$ *computes a discrete coloring on* (G, χ).

Proof. By Lemma 4.2.32, we have that $\text{Soc}(G)$ is a union of stable color classes with respect to 5-WL$_{\text{explicit}}$. If we run the WL-algorithm on (G, γ), then the stable coloring is also a refinement of γ. Hence, the stable coloring computed by 5-WL$_{\text{explicit}}$ on (G, γ), restricted to $\text{Soc}(G)$, encodes a composition series of $\text{Soc}(G)$. By Lemma 5.5.2, 5-WL$_{\text{explicit}}$ then iteratively detects each simple direct factor of $\text{Soc}(G)$, or in other words, the stable coloring induces an ordering of the simple direct factors.

Write $\text{Soc}(G) = S_1 \times \cdots \times S_t$ and let S_i be generated by $\{s_i, r_i\}$. Relative to the ordering of the simple direct factors of $\text{Soc}(G)$ induced by stable 5-WL$_{\text{implicit}}$-color classes, fixing the elements $s := s_1 \cdots s_t$ and $r := r_1 \cdots r_t$, i.e., individualizing them, fixes a linear order on the elements of $\text{Soc}(G)$. Relative to a linear order on $\text{Soc}(G)$, each element of the semisimple group G acts as an ordered permutation in a unique way, and this ordered permutation is 3-WL$_{\text{implicit}}$-detectable. That is, with two individualizations, 5-WL$_{\text{explicit}}$ discretizes G and in particular, G is identified up to isomorphism by 7-WL$_{\text{explicit}}$. □

In the next lemma we use similar arguments for groups that are not necessarily semisimple, but where conditions on the input group guarantee that its isomorphism type can be reconstructed from the induced action on the simple direct factors of $G/\mathcal{R}(G)$.

Lemma 5.5.4. *Assume that G is a perfect group with $\mathcal{R}(G) = Z(G)$, and let χ be a coloring that encodes a composition series of G. Then* $\dim_{\text{WL}_{\text{explicit}}}(G, \chi) \leq 7$.

Proof. By Lemma 5.5.3 together with Lemma 4.1.9, with 2 suitable individualizations, 5-WL$_{\text{explicit}}$ computes a coloring on G that induces a discrete coloring on the semisimple group $G/R(G)$. Now it holds $R(G) = Z(G)$, so for all $g, h \in G$, the commutator $[g, h]$ only depends on the color class of $gR(G)$ in $G/R(G)$. Thus, since $G/R(G)$ becomes discretely colored through 5-WL$_{\text{explicit}}$ after 2 individualizations, 5-WL$_{\text{explicit}}$ also subsequently assigns a discrete coloring to $\{[g, h] \mid g, h \in G\}$, and consequently, to G'. By assumption $G = G'$ holds, so G is discretized by 5-WL$_{\text{explicit}}$ after 2 appropriate individualizations. Then $\dim_{\text{WL}_{\text{explicit}}}(G, \chi) \leq 5 + 2 = 7$ by Lemma 3.4.7. □

5.6 Colored abelian groups

We showed earlier that the implicit 2-dimensional WL algorithm identifies abelian groups up to isomorphism. To prepare the investigation of group extensions by abelian normal subgroups, we now analyze the behavior of WL on abelian groups in greater detail.

5.6.1 Automorphisms of abelian groups

In the following we repeatedly identify the automorphism group of an abelian p-group A with a certain matrix group over the ring $\mathbb{Z}/\exp(A)\mathbb{Z}$, as described below. The material in this subsection is loosely based on [41] and [97].

Let A be an abelian p-group. Fix a homocyclic decomposition of A, that is a direct decomposition

$$A = A_1 \times \cdots \times A_m,$$

such that $A_i \cong C_{p^{f_i}}^{d_i}$ holds for increasing values $1 \leq f_1 < \cdots < f_m$ and $e_i \in \mathbb{N}$. Set $d := d(A) = d_1 + \cdots + d_m$. Consider the free $\mathbb{Z}/p\mathbb{Z}$-module $\left(\mathbb{Z}/p^{f_m}\mathbb{Z}\right)^d$ and denote its j-th standard basis vector with e_j. Then we can identify A with the submodule

$$\left\langle p^{f_m-f_1}e_1, \ldots, p^{f_m-f_1}e_{d_1}, p^{f_m-f_2}e_{d_1+1}, \ldots, p^{f_m-f_2}e_{d_1+d_2}, \ldots, e_{d-d_m+1}, \ldots, e_d \right\rangle$$

of $\left(\mathbb{Z}/p^{f_m}\mathbb{Z}\right)^d$. That is, we identify A_i with $\langle p^{f_m-f_i}e_{d_1+\cdots+d_{i-1}+1}, \ldots, p^{f_m-f_i}e_{d_1+\cdots+d_i}\rangle \cong \left(\mathbb{Z}/p^{f_i}\mathbb{Z}\right)^{d_i}$ as a submodule of $\left(\mathbb{Z}/p^{f_m}\mathbb{Z}\right)^d$. Let $\theta\colon A \to \left(p^{f_m-f_1}\mathbb{Z}/p^{f_m}\mathbb{Z}\right)^{d_1} \oplus \cdots \oplus \left(\mathbb{Z}/p^{f_m}\mathbb{Z}\right)^{d_m}$ denote a corresponding isomorphism, i.e., a choice of basis for each A_i.

Denote the setwise stabilizer of $\theta(A)$ in $\mathrm{GL}_d(\mathbb{Z}/p^{f_m}\mathbb{Z})$ by $\mathrm{GL}(A)$. Let $K(A)$ denote the set of matrices of the form $I_d + X$, where $X \in (\mathbb{Z}/p^{f_m}\mathbb{Z})^{d\times d}$ has the property that the first d_1 columns only contain entries from $p^{f_1}\mathbb{Z}/p^{f_m}\mathbb{Z}$, the next d_2 columns only contain entries from $p^{f_2}\mathbb{Z}/p^{f_m}\mathbb{Z}$, etc. (so the last d_m columns are zero columns). Then $K(A)$ is the pointwise stabilizer of $\theta(A)$ in $\mathrm{GL}_d(\mathbb{Z}/p^{f_m}\mathbb{Z})$, and $\mathrm{Aut}(A)$ can be naturally identified with $\mathrm{GL}(A)/K(A)$ (see also [97], which contains a version of this construction).

Given $M \in \mathrm{GL}(A)$, denote the $(d_i \times d_i)$-submatrix of M, where rows and columns are chosen by the index set $\{d_1 + \cdots + d_{i-1} + 1, \ldots, d_1 + \cdots + d_i\}$, by $D_i(M)$. Two important connections between $\mathrm{GL}(A)$ and $\mathrm{GL}_d(\mathbb{F}_p)$ are given by the following homomorphisms:

1. *reduction modulo p.* Define

$$\Psi_p\colon\ \mathrm{GL}(A) \to \mathrm{GL}_d(\mathbb{F}_p), (M_{i,j})_{i,j} \mapsto (M_{i,j} \bmod p\mathbb{Z}/p^{f_m}\mathbb{Z})_{i,j}.$$

2. *reduction to diagonal part.* Define

$$\Psi_{\mathrm{diag}}\colon\ \mathrm{GL}(A) \to \mathrm{GL}_d(\mathbb{F}_p), M \mapsto \mathrm{diag}(\Psi_p(D_1(M)), \ldots, \Psi_p(D_m(M))).$$

In both cases, $K(A)$ is contained in the kernel of these homomorphisms, and thus we obtain induced homomorphisms $\Psi_p\colon\ \mathrm{Aut}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$ and $\Psi_{\mathrm{diag}}\colon\ \mathrm{Aut}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$, by first factoring through $K(A)$.

We collect basic properties of these homomorphisms below.

Lemma 5.6.1 ([41, Prop. 4.1]). *The image of* Ψ_{diag} *is precisely given by the diagonal embedding of* $\mathrm{GL}_{d_1}(\mathbb{F}_p) \times \cdots \times \mathrm{GL}_{d_m}(\mathbb{F}_p)$ *into* $\mathrm{GL}_d(\mathbb{F}_p)$. *The kernel* $\ker(\Psi_{\mathrm{diag}})$ *is a* p*-group.*

Lemma 5.6.2. *The image of* Ψ_p *consists of all lower block-triangular matrices in* $\mathrm{GL}_d(\mathbb{F}_p)$ *(if we let our matrices act from the left, otherwise upper block-triangular), where the block-sizes are* $d_1, d_2, \ldots, d_m$. *The kernel* $\ker(\Psi_p)$ *is a* p*-group.*

Proof. The first claim is by definition of $\mathrm{GL}(A)$. For the second claim, we note that $\ker(\Psi_p)$ is contained in $\ker(\Psi_{\mathrm{diag}})$. The latter is a p-group by Lemma 5.6.1 so the former is also a p-group. $\square$

The two maps Ψ_p and Ψ_{diag} play a special role in our concrete applications to group extensions since they can be interpreted as induced actions. This is clarified in the following observation.

Observation 5.6.3. *The image of Ψ_p can be identified with the induced action of* $\mathrm{Aut}(A)$ *on $A/A^p \cong \mathbb{F}_p^d$ with respect to the basis $(\theta^{-1}(p^{f_1-f_m}e_1)A^p, \ldots, \theta^{-1}(e_d)A^p)$.*

Consider $\varphi \in \mathrm{Aut}(A)$, then the i-th diagonal block of $\Psi_{diag}(\theta\varphi\theta^{-1})$ describes the action of φ on the characteristic quotient

$$\{a \in A \mid |a| \leq p^{f_i}\}/\{ab \in A \mid |a| < p^{f_i},\ |b| \leq p^i,\ b \in A^p\},$$

which is isomorphic to A_i/A_i^p. Different choices of θ differ by conjugation in $\mathrm{GL}_{d_i}(\mathbb{F}_p)$.

For the remainder of the present subsection, we work with arbitrary homomorphisms $\Psi\colon\ \mathrm{GL}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$ that have the property that $\ker(\Psi)$ is a p-group. For subsequent applications we have Ψ_p and Ψ_{diag} in mind.

In the following three lemmas we establish the key connection between homomorphisms $H \to \mathrm{Aut}(A)$ and certain induced homomorphisms $H \to \mathrm{GL}_d(\mathbb{F}_p)$. The first result was proved by Le Gall for the special case $\Psi = \Psi_{\mathrm{diag}}$ (see [41, Prop. 4.2]). However, it turns out that Le Gall's proof only uses the fact that $\ker(\Psi)$ is a p-group. We repeat the arguments for the sake of clarity.

Lemma 5.6.4. *Let A be an abelian p-group and set $d := d(A)$, let $\Psi\colon\ \mathrm{GL}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$ be a homomorphism whose kernel is a p-group and let M_1 and M_2 be elements of* $\mathrm{GL}(A)$ *whose orders are not divisible by p. Then M_1 is conjugate to M_2 in* $\mathrm{GL}(A)$ *if and only if $\Psi(M_1)$ is conjugate to $\Psi(M_2)$ in* $\mathrm{Im}(\Psi)$. *Moreover, for each $X \in \mathrm{GL}(A)$ with $\Psi(X)\Psi(M_1)\Psi(X)^{-1} = \Psi(M_2)$, there exists $Y \in \ker(\Psi)$ with $XYM_1(XY)^{-1} = M_2$.*

Proof. If M_1 is conjugate to M_2 via $X \in \mathrm{GL}(A)$ then $\Psi(M_1)$ is conjugate to $\Psi(M_2)$ by $\Psi(X)$, since Ψ is a homomorphism. Conversely, assume that $\Psi(M_1)$ is conjugate to $\Psi(M_2)$ by some element in $\mathrm{Im}(\Psi)$, say $\Psi(X)$. Then it follows that $XM_1X^{-1}M_2^{-1}$ lies in $\ker(\Psi)$, so we have $\langle\ker(\Psi), M_2\rangle = \langle\ker(\Psi), XM_1X^{-1}\rangle$. By assumption p does not divide $|M_2|$, so the latter group is a coprime extension of both $\langle M_2\rangle$ and $\langle XM_1X^{-1}\rangle$, in each case extended by the p-group $\ker(\Psi)$. By the Schur-Zassenhaus Theorem 2.3.7, there is $Y \in \ker(\Psi)$ that conjugates $\langle XM_1X^{-1}\rangle$ to $\langle M_2\rangle$, so it holds $(YX)M_1(YX)^{-1} = M_2^m$ for some $m \in \mathbb{N}$. Applying Ψ again gives $\Psi(XM_1X^{-1}) = \Psi(M_2) = \Psi(M_2^m)$, so $M_2^{-1}M_2^m = M_2^{m-1}$ is in $\ker(\Psi)$ and thus a p-element. Since p does not divide the order of M_2, it follows that M_2 is equal to M_2^m. $\square$

In the next step we consider another well-known representation theoretic principle. Recall that, up to equivalence, $\mathbb{C}$-representations are uniquely determined by their characters. In other words, two complex representations $\Delta_1, \Delta_2\colon G \to \mathrm{GL}_n(\mathbb{C})$ of G are equivalent (i.e., equal up to conjugation with a fixed $X \in \mathrm{GL}_n(\mathbb{C})$) if and only if their characters agree element wise, i.e., for all $g \in G$ it holds $\chi_{\Delta_1}(g) = \chi_{\Delta_2}(g)$. In the following lemmas we prove an analogue, first for representations in coprime characteristic and then adapted to coprime extensions.

Lemma 5.6.5. *Let G be a group whose order is not divisible by p and let Δ_1 and Δ_2 be two representations of G over $V := \mathbb{F}_q^d$, where q is some power of p. If Δ_1 and Δ_2 are* element-conjugate*, i.e., for all $g \in G$ there is some $X_g \in \mathrm{GL}_d(q)$ such that $X_g\Delta_1(g)X_g^{-1} = \Delta_2(g)$ holds, then they are* conjugate*, i.e., there is a single matrix $X \in \mathrm{GL}_d(q)$ with $X\Delta_1(g)X^{-1} = \Delta_2(g)$ for all $g \in G$.*

Proof. We begin by decomposing V as $V_0^{\Delta_i} \oplus V_p^{\Delta_i}$ for $i \in \{1, 2\}$, such that the following property holds: With respect to Δ_i, each irreducible $\mathbb{F}_q$-representation of G occurs in $V_0^{\Delta_i}$ with a multiplicity m, such that $0 \leq m \leq p - 1$, and in $V_p^{\Delta_i}$ with a multiplicity m', such that m' is divisible by p. Since p does not divide $|G|$, we have that V is semi-simple as a $\mathbb{F}_qG$-module and thus, such decompositions can always be constructed by arranging the irreducible constituents of V in a suitable way.

Let χ_i be the character associated to Δ_i. By definition, χ_i is also the character associated to the representation induced on $V_0^{\Delta_i}$ by restriction. According to [68, Corollary 9.22], independent of the characteristic, irreducible characters of inequivalent irreducible representations are always linearly independent. Hence, by definition of $V_0^{\Delta_i}$, we obtain that the representations induced on $V_0^{\Delta_1}$ and $V_0^{\Delta_2}$ by restriction are equivalent, if and only if $\chi_1 = \chi_2$ holds. By assumption, Δ_1 and Δ_2 are element-conjugate, so in particular we have $\chi_1(g) = \mathrm{tr}(\Delta_1(g)) = \mathrm{tr}(\Delta_2(g)) = \chi_2(g)$ for all $g \in G$. In conclusion, $V_0^{\Delta_1}$ and $V_0^{\Delta_2}$ are isomorphic as $\mathbb{F}_qG$-modules.

Considering $V_p^{\Delta_i}$, by definition there exists a $\mathbb{F}_qG$-submodule $W^{\Delta_i} \leq V_p^{\Delta_i}$, such that $V_p^{\Delta_i}$ is equivalent to $\left(W^{\Delta_i}\right)^p$ and then $V_p^{\Delta_1}$ and $V_p^{\Delta_2}$ are equivalent if and only if W^{Δ_1} and W^{Δ_2} are. Furthermore, Δ_1 and Δ_2 being element-conjugate implies that the representations induced on W^{Δ_1} and W^{Δ_2} by restriction are element-conjugate too (this follows from the fact that, over any field, matrices are conjugate if and only if they have the same multi-set of elementary divisors). We may then inductively assume that they are even conjugate, i.e., W^{Δ_1} and W^{Δ_2} are equivalent as G-modules. In conclusion, Δ_1 and Δ_2 are equivalent representations, i.e., they are conjugate. □

Lemma 5.6.6. *Let G and A be finite groups, where A is abelian and $|G|$ and $|A|$ are coprime. Consider group homomorphisms $\Delta_i \colon G \to \mathrm{Aut}(A)$ for $i \in \{1, 2\}$. If Δ_1 and Δ_2 are element-conjugate in* Aut(A)*, then they are conjugate in* Aut(A).

Proof. If A is elementary abelian, that is, isomorphic to a finite vector space $\mathbb{F}_p^n$, then Δ_i is an $\mathbb{F}_p$-representation and the claim follows from Lemma 5.6.5.

Suppose next that A is an arbitrary abelian p-group. We decompose A into homocyclic components as $A = A_1 \times \cdots \times A_m$, where for each i it holds that $A_i \cong C_{p^{f_i}}^{d_i}$ with increasing values of f_i and with $d_i > 0$. Set $d := d(A)$. Recall that the homomorphism Ψ_{diag} defined at the beginning of the present section induces a hoomorphism $\Psi_{\mathrm{diag}} \colon \mathrm{Aut}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$.

By assumption, $\psi_1 := \Psi_{\mathrm{diag}} \circ \Delta_1$ and $\psi_2 := \Psi_{\mathrm{diag}} \circ \Delta_2$ are element-conjugate in $\mathrm{Im}(\Psi_{\mathrm{diag}})$, which means that for each $g \in G$ the corresponding i-th blocks of $\psi_1(g)$ and $\psi_2(g)$ are conjugate in $\mathrm{GL}_{d_i}(\mathbb{F}_p)$. By Lemma 5.6.5, element-conjugate representations over finite fields are conjugate. In this context, this means that there exist $X_i \in \mathrm{GL}_{d_i}(\mathbb{F}_p)$, for all $i \in [m]$, such that for all $g \in G$, the i-th block of $\psi_1(g)$ is conjugate onto the i-th block of $\psi_2(g)$ via X_i. So $X\psi_1(g)X^{-1} = \psi_2(g)$, where $X := \mathrm{diag}(X_1, \ldots, X_m) \in \mathrm{Im}(\Psi_{\mathrm{diag}})$. Let Y be a preimage of X under $\Psi_{\mathrm{diag}} \colon \mathrm{Aut}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$ and let K be the kernel of $\Psi_{\mathrm{diag}} \colon \mathrm{Aut}(A) \to \mathrm{GL}_d(\mathbb{F}_p)$.

Since p does not divide $|G|$, in particular, for $i \in \{1,2\}$, p does not divide $|\Delta_i(G)|$, so $K\Delta_i(G) = K \rtimes \Delta_i(G)$ forms a semidirect product by the Schur-Zassenhaus Theorem (Theorem 2.3.7). Now it holds that $YK\Delta_1(g)Y^{-1} = K\Delta_2(g)$ for all $g \in G$, i.e., $KY\Delta_1(G)Y^{-1} = K\Delta_2(G)$. In particular, the group $Y\Delta_1(G)Y^{-1}$ forms a complement of K in $K\Delta_2(G)$ and by the Schur-Zassenhaus Theorem, there is an element $k \in K$ that conjugates $Y\Delta_1(G)Y^{-1}$ onto $\Delta_2(G)$. Furthermore, by definition of Y, there exists an element $x \in K$ with $Y\Delta_1(g)Y^{-1} = x\Delta_2(g)$. This implies

$$(kY)\Delta_1(g)(kY)^{-1} = k(x\Delta_2(g))k^{-1} = kx(k^{-1})^{\Delta_2(g)}\Delta_2(g),$$

and this is an element of $\Delta_2(G)$, since k conjugates $Y\Delta_1(G)Y^{-1}$ onto $\Delta_2(G)$. Since K and $\Delta_2(G)$ intersect trivially, it follows that $kx(k^{-1})^{\Delta_2(g)} = 1$ holds, for all g and x as above, and then Δ_1 is globally conjugate to Δ_2 in $\mathrm{Aut}(A)$.

Finally, if A is an arbitrary abelian group, conjugacy in $\mathrm{Aut}(A)$ is equivalent to conjugacy in $\mathrm{Aut}(A_{p_1}) \times \cdots \times \mathrm{Aut}(A_{p_m})$ where $p_1, \ldots, p_m$ are precisely the prime divisors of $|A|$ and where A_{p_i} is the Sylow p_i-subgroup of A. This conjucagy problem problem can be solved for each prime independently. □

Lemma 5.6.7. *For $i \in \{1,2\}$, consider group homomorphisms $\Delta_i\colon G \to \mathrm{Aut}(A)$ with an abelian p-group A and a group G of order coprime to p. Let $\Psi\colon \mathrm{Aut}(A) \to \mathrm{GL}_{d(A)}(\mathbb{F}_p)$ be any homomorphism whose kernel is a p-group. Let δ_i denote the representation induced on $\mathbb{F}_p^{d(A)}$ by $\Psi \circ \Delta_i$. Then Δ_1 is conjugate to Δ_2 in $\mathrm{Aut}(A)$ if and only if δ_1 is conjugate to δ_2 in $\mathrm{Im}(\Psi)$.*

Proof. The "only if"-direction follows by taking a global conjugator in $\mathrm{Aut}(A)$ and mapping it through Ψ.

In the setting of the proof of Lemma 5.6.6, two automorphisms φ_1 and φ_2 of A of order coprime to p are conjugate in $\mathrm{Aut}(A)$ if and only if $\Psi(\varphi_1)$ and $\Psi(\varphi_2)$ are conjugate in $\mathrm{Im}(\Psi)$ by Lemma 5.6.4. Thus, for the "if"-direction, global conjugacy of δ_1 and δ_2 implies element-conjugacy of Δ_1 and Δ_2 via Lemma 5.6.4, which in turn implies global conjugacy by Lemma 5.6.6. □

5.6.2 WL-dimension of colored abelian groups

We now show that the WL-algorithm solves certain types of problems regarding the extendability of partial group isomorphisms. That is, an isomorphism between subgroups (or quotients) of abelian groups is given via colorings, and the question is whether it extends to a group isomorphism. It is unclear whether WL solves this problem in general.

We consider several specific cases. The first type of extendability question we consider is the case in which the given isomorphism is defined on a subgroup of full rank.

Definition 5.6.8. Consider finite abelian groups A and A^* with subgroups $U \leq A$ and $U^* \leq A^*$, and let $\varphi\colon U \to U^*$ be an isomorphism. Two colorings γ_U and γ_{U^*} on A and A^*, respectively, encode φ if

- $\gamma_U(u) = \gamma_{U^*}(u^*)$ is equivalent to $u^* = \varphi(u)$ for all $u \in U$, $u^* \in U^*$,
- $|\gamma_U(A \setminus U) \cup \gamma_{U^*}(A^* \setminus U^*)| = 1$, and

- $(\gamma_U(A \setminus U) \cup \gamma_{U^*}(A^* \setminus U^*)) \cap (\gamma_U(U) \cup \gamma_{U^*}(U^*)) = \emptyset$.

Thus if two colorings encode a partial isomorphism then all elements in the subgroups are singletons and whenever an element is mapped to another via φ, then the respective elements have the same color. Moreover, elements outside the subgroups all have the same color, which is distinct from the elements in the subgroups.

Lemma 5.6.9 (Extending isomorphisms of full rank subgroups of abelian groups)**.** *Let A and A^* be abelian groups with subgroups $A_0 \leq A$ and $A_0^* \leq A^*$. Assume that $d(A_0) = d(A)$ and that the colorings γ_{A_0} and $\gamma_{A_0^*}$ encode a partial isomorphism $\varphi\colon A_0 \to A_0^*$. Then isomorphism of the colored groups (A, γ_{A_0}) and $(A^*, \gamma_{A_0^*})$ is decided by 2-WL$_{\text{implicit}}$.*

Proof. Since 2-WL$_{\text{implicit}}$ identifies abelian groups up to isomorphism, we may assume that A and A^* are isomorphic as uncolored groups. Furthermore, since Sylow p-subgroups are 2-WL$_{\text{implicit}}$-detectable in abelian groups and decompose abelian groups into direct products of groups of prime power order, it is sufficient to consider the case where A and A^* are p-groups.

There exists a minimal generating set of A, say $\{a_1, \dots, a_d\}$, such that $A = \langle a_1 \rangle \times \dots \times \langle a_d \rangle$ is a cyclic decomposition of A. Then $\{a_1^{m_1}, \dots, a_d^{m_d}\}$ generates some subgroup $B_0 \leq A_0$, where m_i is the smallest natural number for which $a_i^{m_i} \in A_0$. Note that for all i we have $a_i^{m_i} \neq 1$ since otherwise $\langle a_i \rangle \cap A_0 = \{1\}$ for some $i \in [d]$ and thus $d(A_0) \leq d(A) - 1$ (the rank of a subgroup of an abelian group is always bounded by the rank of the parent group by the classification of finite abelian groups), a contradiction. Again by the structure theorem on finitely generated abelian groups it follows that $d(B_0) = d$. Since the colorings induce a partial isomorphism, for each i there is a unique $b_i^* \in A^*$ with $\gamma_{A_0}(a_i^{m_i}) = \gamma_{A_0^*}(b_i^*)$.

Then either there exist elements $a_i^* \in A^*$ with $(a_i^*)^{m_i} = b_i^*$ for all i, or otherwise Spoiler has a winning strategy in the implicit 3- pebble game on A and A^*. Indeed, Spoiler can place pebbles on (a_i, a^*) and on (b_i, b^*) (where a^* and b^* have been chosen by Duplicator's bijections). If this configuration is not winning for Spoiler, then $b^* = b_i^*$ and $(a^*)^{m_i} = b^*$ must hold. In particular, we can choose a_i^* such that $|a_i| = |a_i^*|$ holds as well.

Thus, if Spoiler has no winning strategy, we get a map $a_i \mapsto a_i^*$ that extends to an isomorphism between A and A^*, inducing φ on the respective subgroups by the choice of a_i and a_i^*: indeed, we get a homomorphism since $A = \langle a_1 \rangle \times \dots \times \langle a_d \rangle$ holds. Then $\langle b_1^*, \dots, b_d^* \rangle \cong B_0$ implies that $d(B_0) = d$ holds and $|a_i| = |a_i^*|$ for all i further implies that the homomorphism defined through $a_i \mapsto a_i^*$ is injective. Since $A \cong A^*$ holds, it is also surjective. □

In the second type of extendability problem that we consider, isomorphisms between cyclic subgroups are given. We recall our discussion of splitting elements (see 4.3.1) in the following lemma.

Lemma 5.6.10. *Let A be an abelian p-group and let $A = A_1 \times \dots \times A_m$ be a direct decomposition of A into cyclic factors. Write $x = (x_1, \dots, x_m)$, where x_i is the projection of x onto A_i with respect to the fixed decomposition. Then x splits from A if and only if for some $i \in [m]$ with $|x_i| = |x|$ the factor A_i is generated by x_i. Moreover, the set of elements that split is* 2-WL$_{\text{implicit}}$*-detectable.*

Lemma 5.6.11. *Let A be isomorphic to $C_{p^{e_1}} \times \cdots \times C_{p^{e_n}}$ with $1 \leq e_1 < \cdots < e_n$. For each i, let a_i be an element of A that splits from A and such that $|a_i| = p^{e_i}$ holds. Then $A = \langle a_1 \rangle \times \cdots \times \langle a_m \rangle$.*

Proof. Since the orders of $a_1, \ldots, a_n$ are strictly increasing, we have that a_1 is contained in $\langle a_2, \ldots, a_n \rangle$, only if a_1 is a p-th power in A. Since a_1 splits from A, we thus obtain $\langle a_1 \rangle \cap \langle a_2, \ldots, a_n \rangle = \{1\}$. By the Krull-Schmidt Theorem, $\langle a_2, \ldots, a_n \rangle$ is then isomorphic to $C_p^{e_2} \times \cdots \times C_p^{e_n}$, so the claim follows by induction (since the order of a_1 is minimal among $a_1, \ldots, a_n$, each a_i with $i > 1$ splits from A if and only if it splits from $\langle a_2, \ldots, a_n \rangle$). □

The next lemma provides a construction of splitting subgroups through sequences of elements with increasing orders.

Lemma 5.6.12. *Let A be an abelian p-group and let $x_1, \ldots, x_r$ be elements of strictly increasing orders (i.e., $|x_i| < |x_{i+1}|$ for all i), such that each x_i splits from A. Then $X := \langle x_1, \ldots, x_r \rangle$ splits from A.*

Proof. Suppose $A = A_1 \times \cdots \times A_m$ is a direct decomposition of A into cyclic groups. Fix generators e_i of A_i. Using Lemma 5.6.10, by possibly renaming indices, we can assume that A_1 be generated by the projection of x_1 onto A_1 and also that $|x_1| = |A_1|$ holds. Then one direct complement for $\langle x_1 \rangle$ is given by $K_1 := \langle e_2, \ldots, e_m \rangle$. We can multiply $x_2, \ldots, x_r$ with appropriate powers of x_1 to obtain new elements $x_2', \ldots, x_r'$ contained in K_1 (i.e., $x_i' \in K_1 \cap x_i \langle x_1 \rangle$). Since $|x_1|$ is strictly smaller than all $|x_j|$ with $j > 1$, the elements $x_2', \ldots, x_r'$ fulfill the assumptions of the lemma for K_1 in place of A, which can be seen as follows. Since $|x_1| < |x_i|$ holds, x_i' splits from A. To see that x_i' splits from K_1, consider Lemma 5.6.10 with a cyclic decomposition of K_1 extended by $\langle x_1 \rangle$, then the condition for x_i' to split from A is equivalent to the condition for x_i' to split from K_1. Thus the assumptions are fulfilled. The claim then follows inductively, since, by construction, it is enough to show the claim for $x_1, x_2', \ldots, x_r'$. □

We are now ready to treat the second extendability problem, where we need to decide if two fixed elements of abelian groups can be mapped to each other via some isomorphism. In other words, we show that, on an abelian group A, WL computes the orbit partition with respect to $\mathrm{Aut}(A)$. We point out that orbit partitions in abelian groups, without any reference to WL, have been previously studied in the literature. For example, a combinatorial characterization of orbits in abelian groups can be found in [33].

Lemma 5.6.13. *Let A and A^* be abelian groups with elements $a \in A$ and $a^* \in A^*$. Let χ_a and χ_{a^*} denote the colorings with $\chi_a(a) = \chi_{a^*}(a^*)$ and $\chi_a(x) = \chi_{a^*}(x^*) \neq \chi_a(a)$ for all $x \in A \setminus \{a\}$ and $x^* \in A^* \setminus \{a^*\}$. Then isomorphism of (A, χ_a) and (A^*, χ_{a^*}) can be decided with* 3-WL$_{\text{implicit}}$.

Proof. We may assume without loss of generality that A and A^* are isomorphic as uncolored groups, since otherwise they are distinguished by 2-WL$_{\text{implicit}}$.

We first argue that we can assume that A and A^* are p-groups. Indeed, we can reduce to the case of p-groups due to the WL-detectability of the Sylow decomposition. It is sufficient to argue the claim for each Sylow factor independently, where the respective colorings are induced by the unique projections of a and a^* onto the respective Sylow subgroups.

Assuming now A and A^* are p-groups, we construct a strategy for Spoiler to win the implicit 4-pebble game whenever a and a^* cannot be mapped to each other via isomorphisms. Fix homocyclic decompositions $A = A_1 \times \cdots \times A_t$ and $A^* = A_1^* \times \cdots \times A_t^*$, such that $A_i \cong C_{p^i}^{d_i} \cong A_i^*$ holds for all i and appropriate integers $d_i \geq 0$. Denote the projection of $x \in A$ onto A_i by $A_i(x)$ and similarly define $A_i^*(x^*)$.

Let I be the set of indices i such that $|A_i(a)| = |a|$ holds. Choose m to be minimal such that some $A_j(a)$ with $j \in I$ is a p^m-th power. Then there exists an element $x_1 \in A$ such that $|x_1| = p^j$ and $A_j(x_1)^{p^m} = A_j(a)$ hold (in particular, x_1 splits from A by Lemma 5.6.10). By minimality of m, we may further choose x_1 such that $A_i(x_1)^{p^m} = A_i(a)$ holds for all $i \in I$, while still having x_1 split from A (see Lemma 5.6.10).

By construction, the order of $ax_1^{-p^m}$ is strictly smaller than the order of $|a|$. Spoiler starts by placing a pebble pair on $(x_1, f(x_1))$, where $f\colon A \to A^*$ is a bijection chosen by Duplicator, and if Spoiler does not win from this configuration then, setting $x_1^* := f(x_1)$, it must be the case that $(a^*)(x_1^*)^{-p^m}$ has strictly smaller order than a^* and x_1^* also spits from A^*.

Spoiler places an additional pebble pair on $(ax_1^{-p^m}, a^*(x_1^*)^{-p^m})$, all other pebble pairs can be re-used from this point onward (Duplicator must map $ax_1^{-p^m}$ to $a^*(x_1^*)^{-p^m}$ due to the pebbles on the board or loses immediately). This strategy can be iterated with $(ax_1^{-p^m}, a^*(x_1^*)^{-p^m})$ in place of (a, a^*) until Spoiler wins or the configuration $(1, 1^*)$ is reached. We note that Spoiler uses one pebble pair to fix $(ax_1^{-p^m}, a^*(x_1^*)^{-p^m})$ and two more pebble pairs to iterate the strategy, placing at most three pebble pairs on the board at a time.

We claim that in case the configuration $(1, 1^*)$ is reached, there indeed exists an isomorphism $\psi\colon A \to A^*$ with $\psi(a) = a^*$. The fact that the strategy described above was not winning for Spoiler implies the existence of elements $x_1, \ldots, x_r \in A$ and $x_1^*, \ldots, x_r^* \in A^*$ with the following properties: by construction we have $|x_i| \neq |x_j|$ for all $i \neq j$ and furthermore, each x_i splits from A. The analogues properties hold for the x_i^* with respect to A^*. Therefore, by Lemma 5.6.12, there exists an isomorphism $\psi\colon A \to A^*$ with $\psi(x_i) = x_i^*$ (observe that splitting elements of a fixed order are permuted transitively by automorphisms). Moreover, by construction there are integers $m_1, \ldots, m_r$, such that $a = \prod_{i=1}^r x_i^{p^{m_i}}$ and $a^* = \prod_{i=1}^r (x_i^*)^{p^{m_i}}$ hold, so we obtain $\psi(a) = a^*$. □

The previous result contrasts the case of full rank subgroups in the following sense: for full rank subgroups we can check whether an isomorphism given on subgroups extends to the parent groups or not, by considering the structure of the respective roots, i.e., elements whose powers lie in the domain of the partial isomorphism or the image, respectively. The proof of the previous lemma suggests that, in the case of cyclic groups, this is not sufficient. As a concrete example, consider the group $A := C_{p^3} \times C_{p^2} \times C_p$, generated by an element a of order p^3, b of order p^2 and c of order p, say. Then both $a^p c$ and bc are elements of order p^2 without any non-trivial roots in A. However, they do not lie in the same $\mathrm{Aut}(A)$-orbit, since bc splits form A and $a^p c$ does not.

Corollary 5.6.14. *If A is a finite abelian group, then* 3-WL$_{\text{implicit}}$ *computes the orbit partition of* $\mathrm{Aut}(A)$ *acting on A.*

Proof. This follows from the previous lemma by noting that two elements g_1 and g_2 obtain distinct colors exactly if Spoiler wins the implicit 4-pebble game on (A, A) with one pebble pair initially placed on (g_1, g_2). This initial pebble pair then takes the role of the given coloring in Lemma 5.6.13. □

We move on to consider colorings that describe arbitrary group homomorphisms, in the following precise sense.

Definition 5.6.15. Let A and B be abelian groups and let $\psi\colon A \to B$ be a group homomorphism. We say that a coloring χ of A encodes ψ, if the color classes of χ partition the fibers of ψ.

Lemma 5.6.16. *Let (A, χ) be a colored abelian group such that χ encodes some group homomorphism $\psi\colon A \to B$.*

1. *The coloring induced on $A/\ker(\psi)$ by setting $\chi(a\ker(\psi)) := \{\{\chi(ak) \mid k \in \ker(\psi)\}\}$ for all $a \in A$ is discrete.*

2. *If (A^*, χ^*) is not distinguished from (A, χ) by 3-$\mathrm{WL}_{\mathrm{implicit}}$, then χ^* encodes a homomorphism $\psi^*\colon A^* \to B^*$ such that the subgroups $\ker(\chi) \leq A$ and $\ker(\psi^*) \leq A^*$ are indistinguishable via 3-$\mathrm{WL}_{\mathrm{implicit}}$. Moreover, $(A/\ker(\psi), \chi)$ is isomorphic to $(A^*/\ker(\psi^*), \chi^*)$ with respect to the respective induced colorings.*

3. *Let (A^*, χ^*) be another group not distinguished from (A, χ) by 3-$\mathrm{WL}_{\mathrm{implicit}}$ and assume that χ^* encodes a homomorphism ψ^*. Let $\phi\colon A \to A^*$ be an isomorphism of uncolored groups such that $\phi(\ker(\psi)) = \ker(\psi^*)$ holds and such that, for some generating set S of A, we have $\chi^*(\phi(a)) = \chi(a)$ for all $a \in S$. Then ϕ is an isomorphism of colored groups.*

Proof. 1. If χ encodes ψ, then the coloring induced on $A/\ker(\psi)$ is discrete by definition.

2. Let χ_ψ denote the coloring whose color classes are exactly those unions of χ-color classes, where each union is taken over a fixed coset of $ker(\psi)$ in A.

   Assume that (A^*, χ^*) is not distinguished from (A, χ) by 3-$\mathrm{WL}_{\mathrm{implicit}}$. Then we can define a coloring χ^*_ψ, by setting $\chi^*_\psi(a^*)$ to the unique color that is contained in $\chi_\psi(\chi^{-1}(\chi^*(a^*)))$. So the color classes of χ_ψ and χ^*_ψ are defined through χ and χ^*, respectively, by taking unions of the corresponding color classes. Then indistinguishability of (A, χ) and (A^*, χ^*) implies indistinguishability of (A, χ_ψ) and (A^*, χ^*_ψ). The color classes of χ_ψ are exactly the cosets of $K := \ker(\psi)$ in A, so by indistinguishability, there is a subgroup $K^* \leq A^*$ that is the color class of 1 under χ^*_ψ. Furthermore K and K^* are indistinguishable. by 3-$\mathrm{WL}_{\mathrm{implicit}}$ as subgroups of A and A^*, respectively, and the χ^*_ψ color classes are exactly the cosets of K^* in A^*.

   This means that mapping $a\ker(\psi)$ to $(\chi^*_\psi)^{-1}(\chi_\psi(a))$ defines a bijection between A/K and A^*/K^*. Either this is an isomorphism of colored groups, or otherwise there are three colors, i, j and k say, such that $\chi_\psi^{-1}(i) \cdot \chi_\psi^{-1}(j) = \chi_\psi^{-1}(k)$ holds but $(\chi^*_\psi)^{-1}(i) \cdot (\chi^*_\psi)^{-1}(j) \neq (\chi^*_\psi)^{-1}(k)$. But then (A, χ_ψ) and (A^*, χ^*_ψ) would be distinguishable due to this property, contradicting the assumptions. Hence, A/K and A^*/K^* are isomorphic as colored groups with respect to the colorings induced by χ_ψ and χ^*_ψ. By definition, the number of elements of each fixed color in any given χ_ψ-color class is the same as the number of elements of the corresponding color in the corresponding χ^*_ψ-color class, so A/K and A^*/K^* are also isomorphic with respect to the colorings induced by χ and χ^*.

3. Since ϕ maps $\ker(\psi)$ to $\ker(\psi^*)$ and since χ and χ^* encode ψ and ψ^*, respectively, it follows that ϕ maps χ-color classes to χ^*-color classes. Since ϕ maps the elements $a \in S$ to elements of the correct χ^*-color in A^*, actually each color class is mapped correctly by ϕ: By indistinguishability of (A, χ) and (A^*, χ^*), for any three colors, i, j and k say, such that $\chi^{-1}(i) \cdot \chi^{-1}(j) = \chi^{-1}(k)$ holds, the same relationship must hold in A^*, that is, $(\chi^*)^{-1}(i) \cdot (\chi^*)^{-1}(j) = (\chi^*)^{-1}(k)$. Hence, through the homomorphism property, ϕ must be an isomorphism between the colored groups (A, χ) and (A^*, χ^*). □

Let A be an abelian p-group. Recall that we set $\Omega_i(A) := \langle\{a \in A \mid |a| \leq p^i\}\rangle$ and that, in case that A is abelian, it holds $\Omega_i(A) = \{a \in A \mid |a| \leq p^i\}$.

Lemma 5.6.17. *Let A be an abelian q-group for a prime q. Let $a \in A$ be a splitting element of order q^i and decompose A as $A = \langle a\rangle \times K$. Then we have $A = \langle ab\rangle \times K$ for all $b \in \Omega_{i-1}(A)\Omega_{i+1}(A)^q$.*

Proof. By assumption it holds $a^{q^{i-1}} \notin K$ and $\Omega_{i-1}^{q^{i-1}}(A) = \{1\}$, so we may assume without loss of generality that b is contained in $\Omega_{i+1}(A)^q$ and that b has order q^i. With respect to the decomposition $A = \langle a\rangle \times K$, this means that b can be written as $b = (a^{q^j}, k^q)$ with $|k| = q^{i+1}$ and $j \geq 1$. But then $(ab)^{q^{i-1}} = (a^{q^{i-1}}, k^{q^i}) \notin K$ and $(ab)^{q^i} = 1$, so $\langle ab\rangle \cap K = \{1\}$. This implies the claim, since by assumption $|ab| = |a|$ holds (in particular, a is not contained in $\Omega_{i-1}(A)\Omega_{i+1}(A)^q$, or otherwise it would not split from A in the first place). □

Lemma 5.6.18. *Let A be an abelian q-group. For each $i \in \{1, \ldots, \log_q(\exp(A))\}$, let ψ_i be an automorphism of $A_i := \Omega_i(A)/(\Omega_{i-1}(A)\Omega_{i+1}(A)^q)$. Then there exists an automorphism $\psi \in \mathrm{Aut}(A)$ that induces ψ_i on A_i for all i.*

Proof. For each maximal homocyclic direct factor H of A, it holds that H/H^q is isomorphic to A_i, where $\exp(H) = q^i$ holds. Then the claim of the present lemma is just a reformulation of the fact that the image of Ψ_{diag} is a direct product over the groups $\mathrm{GL}_{d(A_i)}(\mathbb{F}_q)$, see Lemma 5.6.1 and Observation 5.6.3. □

Lemma 5.6.19. *Let A be an abelian q-group for a prime q, let K be any subgroup of A and let χ be a coloring of A, such that the color classes of χ are precisely the cosets of A modulo K. Then $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(A, \chi) \leq 4$.*

Proof. Let (A^*, χ^*) be another colored group not distinguished from (A, χ) by 4-$\mathrm{WL}_{\mathrm{implicit}}$. Since the (implicit) WL-dimension of abelian groups is bounded by 2, we have that A and A^* are isomorphic as abstract groups. Furthermore, the color classes of χ in A carry a natural group structure, which is isomorphic to A/K colored with the discrete coloring induced by χ. This group structure can be exploited by k-$\mathrm{WL}_{\mathrm{implicit}}$ for $k \geq 3$, since k-$\mathrm{WL}_{\mathrm{implicit}}$ can check which color class is the product of any two given color classes. Hence, we may assume that the same holds for A^* and $K^* := \{a^* \in A^* \mid \chi^*(a^*) \in \chi(K)\}$, and that K and K^* are isomorphic as abelian groups and A/K and A^*/K^* are isomorphic via the unique isomorphism prescribed by χ and χ^* on these quotients.

For each i, set $A_i := \Omega_i(A)/(\Omega_{i-1}(A)\Omega_{i+1}(A)^q)$ and define a coloring χ_i on A_i via $\chi_i(a\Omega_{i-1}(A)\Omega_{i+1}(A)^q) := \{\{\chi(a\omega) \mid \omega \in \Omega_{i-1}(A)\Omega_{i+1}(A)^q\}\}$. Analogously define A_i^* and χ_i^*.

We first show that (A_i, χ_i) is isomorphic to (A_i^*, χ_i^*) for all i. To prove this, we note that $\Omega_i(A)$ and $(\Omega_{i-1}(A)\Omega_{i+1}(A)^q)$ are detectable subgroups by 4.2.16 and Lemma 4.1.3. Since 4-$\mathrm{WL}_{\mathrm{implicit}}$ does not distinguish A from A^*, Lemma 4.1.9 implies that (A_i, χ_i) and (A_i^*, χ_i^*) are not distinguished by 4-$\mathrm{WL}_{\mathrm{explicit}}$. These groups are elementary abelian and the induced colorings fulfill the assumptions from the present lemma: if $k \in K$ then $\{\{\chi(k\omega) \mid \omega \in \Omega_{i-1}(A)\Omega_{i+1}(A)^q\}\} = \{\{\chi(\omega) \mid \omega \in \Omega_{i-1}(A)\Omega_{i+1}(A)^q\}\}$ is independent of k. On the other hand, if $a, a' \in \Omega_i(A) \setminus (\Omega_{i-1}(A)\Omega_{i+1}(A)^q)$ with $\chi(a) \neq \chi(a')$, then $\chi_i(a) \neq \chi_i(a')$. So we reduced to the case where A is elementary abelian, and then the isomorphism type of (A, χ) is uniquely determined by the isomorphism type of the discretely colored group $(A/K, \chi)$, where cosets are again colored with the multiset of χ-colors of their elements, together with the rank of K. This is identified by 4-$\mathrm{WL}_{\mathrm{explicit}}$, according to Lemma 4.1.9, since the induced coloring on A/K is discrete, together with the fact that 4-$\mathrm{WL}_{\mathrm{explicit}}$ identifies the isomorphism type of the subgroup K, since it is elementary abelian and a union of χ-color classes.

Now if (A_i, χ_i) is isomorphic to (A_i^*, χ_i^*) for all i, by Lemma 5.6.18, there exists an isomorphism $\phi\colon A \to A^*$ such that ϕ induces an isomorphism $(A_i, \chi_i) \to (A_i^*, \chi_i^*)$ for each $i \in \{1, \ldots, \exp(A)\}$. Let $a_1, \ldots, a_r \in A$ be chosen such that A is a direct product of the cyclic groups $\langle a_i \rangle$, and denote the order of a_j by q^{e_j}. Then, by choice of ϕ, we have

$$\chi_{e_j}(a_j\Omega_{e_j-1}(A)\Omega_{e_j+1}(A)^q) = \chi_{e_j}^*(\phi(a_j)\Omega_{e_j-1}(A^*)\Omega_{e_j+1}(A^*)^q)$$

for all j. By Lemma 5.6.17 and by definition of χ_i and χ_i^*, we may thus choose a different isomorphism $\phi'\colon A \to A^*$, such that $\chi^*(\phi'(a_j)) = \chi(a_j)$ holds for all j (that is, we may align the colors of a_j and $\phi(a_j)$ by replacing a_j with a suitable representative modulo $\Omega_{e_j-1}(A)\Omega_{e_j+1}(A)^q$). Since products of color classes are again color classes for both χ and χ^*, and A is generated by $a_1, \ldots, a_r$, this implies that $\chi^*(\phi'(a)) = \chi(a)$ holds for all $a \in A$. □

Lemma 5.6.20. *Let (A, χ) be a colored abelian group such that χ encodes some homomorphism $\psi : A \to B$. Then $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(A, \chi) \leq 4$.*

Proof. For each prime p dividing $|A|$, denote the Sylow p-subgroup of A by A_p. For each such p, we get an induced homomorphism $\psi_p : A_p \to B$.

Since χ encodes ψ, the restriction of χ to A_p, say χ_p, encodes ψ_p. Since A_p is 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable, Lemma 5.6.19 implies that 4-$\mathrm{WL}_{\mathrm{implicit}}$ identifies each (A_p, χ_p) up to isomorphism. But (A, χ) is uniquely defined up to isomorphism by the collection of isomorphism types of (A_p, χ_p), where p runs through all prime divisors of $|A|$, since ψ is the unique homomorphism that extends the homomorphisms ψ_p to A and analogously, up to renaming colors, χ is the unique coloring that encodes a homomorphism on A and restricts to χ_p for each p. □

5.7 Coprime extensions

Group cohomology allows for the study of general extensions of groups. Given groups G, N and Q, we say that G is an *extension of Q by N*, if there exists a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow Q \longrightarrow 1.$$

In other words, we can view N as a normal subgroup of G with quotient $G/N = Q$. Conjugation in G induces an action of Q on N, which is represented by a homomorphism $\Delta\colon Q \to \mathrm{Aut}(N)$. For a broad treatment of group extensions and group cohomology, we refer the reader to [100], in particular [100, Chapter 4].

A group extension is *split*, if the associated short exact sequence splits. This is the case if and only if there exists a choice of coset representatives modulo N, given as a map $s\colon Q \to G$, that is a group homomorphism and this is in turn equivalent to G being a semidirect product $G = N \rtimes_\Delta Q$. Here, Δ is the associated action homomorphism $\Delta : Q \to \mathrm{Aut}(N)$.

In many group theoretic contexts, split extensions are easier to understand than general extensions (after all, each finite group is an iterated extension of simple groups). However, from an algorithmic point of view, even split extensions are not fully under control. For example, there is currently no known efficient algorithm to compute the complement of a normal subgroup N in G, even if the complement is known to exist a priori (see [28, 63] for state of the art methods dealing with the cases where N or Q are solvable). We also currently do not know efficient algorithms to solve the isomorphism problem for split extensions in general, even if the normal subgroup and complement are explicitly given.

A special class of split extensions is given by *coprime* extensions, that is, extensions of Q by N where $\gcd(|N|, |Q|) = 1$ holds. Indeed, such extensions are always split according to the Schur-Zassenhaus Theorem (see Theorem 2.3.7).

The following well-known lemma shows that the isomorphism problem of coprime extensions reduces to isomorphism problems of smaller groups and a conjugacy problem for the respective associated actions.

Lemma 5.7.1 (see [104])**.** *Let $G = N \rtimes_\Delta H$ and $G^* = N^* \rtimes_{\Delta^*} H^*$ be coprime extensions with associated actions Δ and Δ^*. Then G and G^* are isomorphic if and only if there exist isomorphisms $\varphi\colon H \to H^*$ and $\psi\colon N \to N^*$ with $\Delta = (\Delta^* \circ \varphi)^{\psi^{-1}}$.*

In the present subsection, we explore to which extent the structure of a coprime extension is detectable and exploitable by the Weisfeiler-Leman algorithm. Our main focus lies on extensions where the normal subgroup is abelian and we give bounds for various classes of such extensions, parameterized in terms of natural representation theoretic properties of the induced action on the abelian normal subgroup.

In the following, we frequently need *combinatorial* versions of well-known representation theoretic results. A first example is covered by the following lemma.

Lemma 5.7.2. *Let V be a finite vector space over $\mathbb{F}$ and let G be a finite group whose order is not divisible by the characteristic of $\mathbb{F}$. Let $\Delta\colon G \to \mathrm{GL}(V)$ be a representation.*

1. *The equivalence type of Δ is uniquely determined by, and uniquely determines, the multiset of equivalence types of $\Delta_{V_1}, \dots, \Delta_{V_t}$, where $V = V_1 \oplus \dots \oplus V_t$ is an arbitrary direct sum decomposition of V into irreducible sub-representations.*

2. *The equivalence type of Δ is uniquely determined by the multiset of isomorphism types of Δ_U, where U runs through all irreducible sub-representations of V with respect to Δ.*

Proof. Part 1) is a standard result from representation theory, see for example [70]. Moreover, the claim certainly holds for homogeneous representations, that is, representations where all irreducible submodules are equivalent, as in this case we only have to compare pairs of representations where one is strictly contained in the other (up to equivalence).

For the general case of Part 2), decompose V as $V = W_1 \oplus \times \oplus W_m$, where each W_i is the sum over all irreducible Δ-submodules of W of a fixed equivlence type. Let U be any irreducible Δ-submodule of V, then, by Part 1), U is contained in some W_j. Now W_j is homogeneous, so the equivalence type of W_j is uniquely determnied by counting the total occurences of equivalence types of irreducible subrepresentations. This is true for eacj W_j, and hence, by Part 1), for V. □

5.7.1 Coprime extensions by abelian groups

We now analyze the Weisfeiler-Leman algorithm on coprime extensions. Through our results in Chapter 4, the basic structural aspects of coprime extensions can be recovered from WL-colorings.

Lemma 5.7.3. *Let $G = N \rtimes H$ be a coprime extension, then N is 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable. In particular, if G^* is an arbitrary group which is indistinguishable from G via k-$\mathrm{WL}_{\mathrm{explicit}}$ for some $k \geq 4$, then G^* is a coprime extension $G^* = N^* \rtimes H^*$, where N is indistinguishable from N^* and H is indistinguishable from H^* via k-$\mathrm{WL}_{\mathrm{explicit}}$. This implies $|N^*| = |N|$ and $|H^*| = |H|$, and if N is additionally abelian, we have $N^* \cong N$.*

Building on this, we show in the next lemma that, if N is elementary abelian, then the automorphism associated to $h \in H$ acting on N is identified by 3-WL up to conjugation.

Lemma 5.7.4. *Let $G = A \rtimes_\Delta H$ and $G^* = A^* \rtimes_{\Delta^*} H^*$ be coprime extensions with $A \cong A^* \cong C_p^d$. If $g \in G$ is not distinguished from $g^* \in G^*$ by k-$\mathrm{WL}_{\mathrm{implicit}}$ with $k \geq 3$, then there is an isomorphism $\psi\colon A \to A^*$ such that $\Delta(gA)$ is equal to $\psi\Delta^*(g^*A^*)\psi^{-1}$.*

Proof. We assume that Duplicator has a winning strategy in the implicit $(k+1)$-pebble game starting with a pebble pair on (g, g^*). Set $h := gA \in H$ and $h^* := g^*A^* \in H^*$. We identify A and A^* with $\mathbb{F}_p^d$. By Maschke's Theorem (2.3.15), there is a decomposition of $A \cong \mathbb{F}_p^d$ into irreducible $\langle\Delta(h)\rangle$-modules, say

$$A = N_1 \times \cdots \times N_t.$$

By irreducibility, each N_i is generated by a single element as a $\langle\Delta(h)\rangle$-module. Considering the N_i as subgroups of A, this means that each subgroup of the form $\langle N_i, g\rangle$ can be generated by g and one more element from N_i. Thus, since Duplicator has a winning strategy and $k \geq 3$, there are subgroups N_i^* of G^* such that for each i the number of minimal normal subgroups $N \subseteq A$ of G with $\langle N, g\rangle \cong \langle N_i, g\rangle$ is the same as the number of minimal normal subgroups $N^* \subseteq A^*$ of G^* with $\langle N^*, g^*\rangle \cong \langle N_i^*, g^*\rangle$. By Lemma 5.7.2 and Lemma 5.7.1, there must be a decomposition of A^* into irreducible $\langle\Delta^*(h^*)\rangle$-modules

M_i^* such that $\langle N_i, g\rangle$ is isomorphic to $\langle M_i^*, g^*\rangle$ for each i (we note that N_i^* can be regarded as a module for $\langle g\rangle$ through the isomorphism $\langle g\rangle \to \langle g^*\rangle, g \mapsto g^*$). Due to the pebble pair on (g, g^*), all those isomorphisms can be chosen such that g is mapped to g^*.

In representation theoretic terms this means that there exists isomorphisms $\psi_i : N_i \to M_i^*$ with

$$\forall n \in N_i : \psi_i(\Delta(h)n) = \Delta^*(h^*)\psi_i(n)$$

for each i, and we can obtain a suitable isomorphism ψ as claimed in the lemma by taking the unique group isomorphism $\psi : A \to A^*$ with $\psi_{|N_i} = \psi_i$. □

Through the machinery we developed in the previous section, Lemma 5.7.4 can now be generalized to conjugacy in $\mathrm{Aut}(A)$ for appropriate abelian groups A.

Lemma 5.7.5. *Let $G = A \rtimes_\Delta H$ and $G^* = A^* \rtimes_{\Delta^*} H^*$ be coprime extensions by abelian groups A and A^*. If $g \in G$ is not distinguished from $g^* \in G^*$ by k-$\mathrm{WL}_{\mathrm{explicit}}$ with $k \geq 4$, then there is an isomorphism $\psi\colon A \to A^*$ such that $\Delta(gA)$ is equal to $\psi\Delta^*(g^*A^*)\psi^{-1}$.*

Proof. We can assume without loss of generality that A is a p-group, since A is k-$\mathrm{WL}_{\mathrm{implicit}}$-detectable by 5.7.3 and the direct decomposition of A into its Sylow-subgroups is 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable. Furthermore, the conjugacy class of $\Delta(gA)$ can be recovered from the induced actions on Sylow-subgroups.

So assume that A and A^* are abelian p-groups. Set $A_i := \{a \in A \mid |a| \leq p^i|\}$ and $A_{i,p} := \{ab \in A \mid |a| < p^i,\ |b| \leq p^i,\ b \in A^p\}$. For all i, the subgroups A_i and $A_{i,p}$ are 3-$\mathrm{WL}_{\mathrm{implicit}}$-detectable, as a consequence of Lemma 4.1.3.

Analogously define A_i^* and $A_{i,p}^*$ as subgroups of A^*. By Observation 5.6.3, for each $h \in H$, we have that $\Psi_{\mathrm{diag}}(\Delta(h))$ is a block diagonal matrix, where each block is given by the action of h induced on $A_i/A_{i,p}$. By Lemma 5.6.1, the image of Ψ_{diag} is a direct product of the groups $\mathrm{GL}(A_i/A_{i,p})$.

Using Lemma 5.6.4 for Ψ_{diag}, it is hence sufficient to show that the induced action of g on $A_i/A_{i,p}$ is conjugate to the induced action of g^* on $A_i^*/A_{i,p}^*$, via some isomorphism $\psi_i\colon A_i/A_{i,p} \to A_i^*/A_{i,p}^*$, for all i. Now $A_i/A_{i,p} \rtimes H$ and $A_i^*/A_{i,p}^* \rtimes H^*$ are again indistinguishable by k-$\mathrm{WL}_{\mathrm{explicit}}$ (this follows from detectability of A_i and $A_{i,p}$ together with Lemma 4.1.9).

If g and g^* are indistinguishable by k-$\mathrm{WL}_{\mathrm{explicit}}$, then, by detectability of A_i, there must be some $a \in A$ and $a^* \in A^*$, such that ga is indistinguishable from g^*a^*, where additionally $ga \in A_i \rtimes H$ and $g^*a^* \in A_i^* \rtimes H^*$ hold.

We note that the induced action of g on $A_i/A_{i,p}$ is the same as the induced action of ga, and the same holds for g^* and g^*a^* with respect to $A_i^*/A_{i,p}^*$. It is hence sufficient to show that the induced action of ga on $A_i/A_{i,p}$ is conjugate to the action of g^*a^* on $A_i^*/A_{i,p}^*$ via some isomorphism $\psi\colon A_i/A_{i,p} \to A_i^*/A_{i,p}^*$. Since $A_i/A_{i,p}$ is elementary abelian and k is at least 4, the conjugacy of these induced actions follows from Lemma 5.7.4. □

Next, we recall that, for every abelian group A, the WL-dimension of a semidirect product of the form $A \rtimes H$ is bounded by the rank of H.

Lemma 5.7.6. *Let $G = A \rtimes_\Delta H$ be a coprime extension with an abelian group A and an arbitrary group H. Then $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq d(H) + 3$.*

Proof. This is [48, Theorem 3.6], but we additionally use the number of generators as an input variable. The proof goes through unchanged. □

In the following, we develop more concise bounds, quantified in terms of natural representation theoretic properties of the action associated to a coprime extension.

When the Sylow subgroups of A are elementary abelian We first consider the case of extensions $A \rtimes H$, where H is abelian and all Sylow subgroups of A are elementary abelian. In this case, the action of H on each Sylow subgroup of A can directly be interpreted as a linear representation.

From a representation theoretic point of view, one usually wants to reduce questions about representations to questions about their irreducible constituents, and understanding the irreducible building blocks is a fundamental first step.

Lemma 5.7.7. *Let $G = A \rtimes_\Delta H$ and $G^* = A^* \rtimes_{\Delta^*} H^*$ be coprime extensions over elementary abelian groups A and A^*. Assume that G is not distinguished from G^* by* 3-WL$_{\text{implicit}}$. *Then, Δ is irreducible as an H-representation, if and only if Δ^* is irreducible as an H^*-representation.*

Proof. Δ is irreducible if and only if A is a minimal normal subgroup of G and the same holds for Δ^* with respect to A^*. If G is not distinguished from G^* by 3-WL$_{\text{implicit}}$, then Corollary 4.1.4 implies that A is a minimal normal subgroup if and only if A^* is. □

We first devise two more technical lemmas to analyze the structure of irreducible representations of abelian groups.

Lemma 5.7.8. *Let H be abelian and assume that each Sylow subgroup of H is homocyclic. Let $\Delta\colon H \to C$ be a group homomorphism with cyclic image $C \neq 1$. Then, for each $h \in H$ with $\langle \Delta(h) \rangle = \Delta(H)$, there exists a subgroup $K \leq \ker(\Delta)$ with $H = \langle h \rangle \times K$.*

Proof. Let $h \in H$ be given such that $\Delta(h)$ generates the image of Δ. If some prime p divides $|h|$ but not $|\Delta(h)|$, then the Sylow p-subgroup of H is contained in $\ker(\Delta)$. In this case, we may replace h by an appropriate p-power of h, whose order is not divisible by p anymore and show the claim for the unique largest subgroup of H that is not divisible by p. So assume without loss of generality that no Sylow subgroup of H is fully contained in $\ker(\Delta)$.

Then, since $\Delta(h)$ generates the image of Δ, we observe that h has no proper roots in H. Since the Sylow subgroups of H are homocyclic, this means that h is an element of maximal order in H, so we can write H as $H = \langle h \rangle \times U$ for an appropriate subgroup $U \leq H$. Write $h = h_1 \cdots h_r$, such that each h_i has prime power order for a prime p_i and such that p_i and p_j are distinct for $i \neq j$. We can always reach such a decomposition of h by letting each h_i be an appropriate power of h. Denote the Sylow p_i-subgroups of H and U by H_i and U_i, respectively. Then we have $H_i = \langle h_i \rangle \times U_i$. Since H_i is homocyclic, we can write $U_i = \langle u_1 \rangle \times \cdots \times \langle u_m \rangle$ for appropriate elements $u_j \in U_i$ with $|u_j| = |h_i|$ for all $j \in [m]$. By choice of h, for all j, there is some $e_j \in \mathbb{N}$ with $h_i^{e_j} u_j \in \ker(\Delta)$.

Then, since we have $|u_j| = |h_i|$ for all j, it holds

$$H_i = \langle h_i \rangle \times U_i = \langle h_i \rangle \times \langle h_i^{e_1} u_1, \ldots, h_i^{e_m} u_m \rangle,$$

with $K_i := \langle h_i^{e_1} u_1, \ldots, h_i^{e_m} u_m \rangle \leq \ker(\Delta)$. Now this is true for each i, so by the Chinese Remainder Theorem, we obtain the claimed decomposition $H = \langle h \rangle \times (K_1 \times \cdots \times K_r)$. □

Lemma 5.7.9. *Let G be an extension of an abelian q-group H by $A \cong C_p^d$ for primes $p \neq q$, with action $\Delta\colon H \to \mathrm{Aut}(A) \cong \mathrm{GL}_d(\mathbb{F}_p)$. Assume that $\Delta(H)$ is cyclic. If H does not admit a cyclic direct factor that acts trivial on A, then H is isomorphic to $C_{p^{e_1}} \times \cdots \times C_{p^{e_n}}$ with $1 \leq e_1 < \cdots < e_n$. Moreover, $\Delta(H)$ is generated by $\Delta(h)$ for any $h \in H$ of maximal order, and for each i, if h of order p^{e_i} splits from H, then $\Delta(h) = \Delta(x)$ for $x \in H$ implies $|x| \geq |h|$, with equality if and only if x splits from H as well.*

Proof. Otherwise H has a direct factor isomorphic to $C_{p^e} \times C_{p^e}$ for some $e \in \mathbb{N}$, generated by elements x and y say. Since $\Delta(H)$ is cyclic, there is some integer i such that one of xy^i and x^iy acts trivially on A, so assume without loss of generality that xy^i lies in $\ker(\Delta)$. By choice of x and y, we have that xy^i splits from H. Hence, by identifying H with G/A, we can find some $g \in G$ such that g acts trivially on A, the order of g is a power of q, and gA splits from G/A. Write $G/A = \langle gA\rangle \times U/A$ for an appropriate subgroup $U \leq G$ with $A \leq U$. We claim that $G = \langle g\rangle \times U$ holds, contradicting the indecomposability of G. To this end, we observe that, since the order of g is a q-power, we have that $\langle g\rangle \cap U$ is a q-group, hence $\langle g\rangle \cap U$ is isomorphic to $\langle gA\rangle \cap U/A = \{1\}$.

For the final claim of the lemma, assume that some element h of order p_i^e splits from H, and that $\Delta(h) = \Delta(x)$ holds for some $x \in H$. If $|x| < |h|$ holds, then hx^{-1} is an element that splits from H and lies in the kernel of Δ, so we reach the same contradiction to the indistinguishability of G as before. If $|x| = |h|$ holds, but x does not split from H, then again $hx^{-1} \in \ker(\Delta)$ splits from H. □

Lemma 5.7.10. *Let G be a coprime extension of an abelian group H by $A \cong C_p^d$ with action $\Delta\colon H \to \mathrm{Aut}(A) \cong \mathrm{GL}_d(\mathbb{F}_p)$. If Δ is irreducible as an $\mathbb{F}_p$- representation, then the* $\mathrm{WL}_{\mathrm{explicit}}$*-dimension of G is at most* 7.

Proof. By Theorem 4.3.27, we may assume without loss of generality that G is directly indecomposable if we then show the claim for 6-$\mathrm{WL}_{\mathrm{explicit}}$.

First assume that H is a q-group for a prime $q \neq p$. By Lemma 5.7.9, we have that H is isomorphic to $C_{p^{e_1}} \times \cdots \times C_{p^{e_n}}$ with $1 \leq e_1 < \cdots < e_n$ and $\Delta(H)$ is generated by the elements of maximal order in H.

By Lemma 2.3.18, we may choose an element $a \in A$ and an element $h \in H$ of maximal order, such that $A \leq \langle a, h\rangle$ holds. We individualize a and h at the cost of increasing the WL-dimension by 2. With a and h individualized, 3-$\mathrm{WL}_{\mathrm{explicit}}$ subsequently discretizes A. Thus, 4-$\mathrm{WL}_{\mathrm{explicit}}$ subsequently colors each $g \in G$ with the permutation it induces on the linearly ordered set A. This implies that the color classes induced on $G/A \cong H$ are at least as fine as the fibers of Δ.

For $i \in [n]$, let h_i be an element of order p^{e_i} splitting from H. Then $H = \langle h_1\rangle \times \cdots \times \langle h_n\rangle$ by Lemma 5.6.11, and the induced 4-$\mathrm{WL}_{\mathrm{explicit}}$ colors of $h_1, \dots, h_n$ uniquely determine the action of $\Delta(h)$ on the discretely colored A, for each $h \in H$. Hence, relative to the individualized group elements, the isomorphism type of G is uniquely determined by the colors of $h_1, \dots, h_n$ according to Lemma 5.7.1 (we note that the h_i need not to be individualized for this argument, different choices of h_i may have different colors, but the exact choice does not matter). Since the splitting elements of a fixed order are 4-$\mathrm{WL}_{\mathrm{explicit}}$-detectable in any abelian group, the WL dimension of G is bounded by $4 + 2 = 6$.

Finally, if H is not a q-group, we can still choose the elements a and h to fix a linear ordering on A, possibly having to choose h of composite order. We can use the exact same strategy from above for each Sylow factor of H individually: Since $\Delta(H)$ is cyclic, so is $\Delta(U)$ for each Sylow subgroup of H, and if H does not admit a cyclic direct factor acting trivially on A, then the same holds for U, since any q-element that splits from the Sylow q-group of H splits from H. But then the preimage of U under $G \mapsto G/A$ fulfills the assumptions of Lemma 5.7.9. □

Lemma 5.7.11. *Let $G = A \rtimes_\Delta H$ and $G = A^* \rtimes_{\Delta^*} H^*$ be coprime extensions with elementary abelian A and A^*. Consider the implicit k-pebble game, $k \geq 3$, on (G, G^*) starting with pebble pairs on (a_1, a_1^*) and (a_2, a_2^*), such that $\langle a_i^G \rangle$ is a minimal normal subgroup of G and $\langle (a_i^*)^{G^*} \rangle$ is a minimal normal subgroup of G^* for each i.*

If $\langle a_1^G \rangle$ and $\langle a_2^G \rangle$ are equivalent as H-modules but $\langle (a_1^*)^{G^*} \rangle$ is not equivalent to $\langle (a_2^*)^{G^*} \rangle$ as an H^*-module, then Spoiler has a winning strategy

Proof. The irreducible $\Delta(H)$-submodules contained in $\langle a_1^G, a_2^G \rangle$ correspond one-to-one to the minimal normal subgroups of G contained in $\langle a_1^G, a_2^G \rangle$, and an analogous statement holds for G^*.

Consider any representation $\Delta\colon X \to \mathrm{GL}(V)$ such that V decomposes into two irreducible $\Delta(X)$-submodules $V = N_1 \oplus N_2$. Then the number of irreducible $\Delta(X)$-submodules contained in V is 2 whenever N_1 and N_2 are not equivalent. If they are not equivalent the number is strictly larger than 2 (see Lemma 5.7.2).

Under the given assumptions this means that the number of minimal normal subgroups of G contained in $\langle a_1^G, a_2^G \rangle$ is strictly larger than the number of minimal normal subgroups of G^* contained in $\langle (a_1^*)^{G^*}, (a_2^*)^{G^*} \rangle$ and then, by Corollary 4.1.4, Spoiler can win from the given initial configuration. □

Lemma 5.7.12. *Let $G = A \rtimes_\Delta H$ be a coprime extension with H abelian and $A \cong C_p^d$. Let $A = M_1 \oplus \dots \oplus M_r$ be the decomposition of A into maximal homogeneous H-submodules. For each i, choose some irreducible submodule $N_i \leq M_i$. Then N_i and N_j are inequivalent irreducible H-representations for $i \neq j$ and we have*

$$\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq \max\big(3, \dim_{\mathrm{WL}_{\mathrm{implicit}}}((N_1 \times \dots \times N_r) \rtimes_\Delta H, \chi) + 1\big),$$

and

$$\dim_{\mathrm{WL}_{\mathrm{explicit}}}(G) \leq \max\big(4, \dim_{\mathrm{WL}_{\mathrm{explicit}}}((N_1 \times \dots \times N_r) \rtimes_\Delta H, \chi) + 1\big),$$

where χ colors the elements of each N_i with the multiplicity of N_i in M_i. (here we denote the induced action of Δ on $N_1 \times \dots \times N_r$ again by Δ).

Proof. By Lemma 5.7.11, elements $a \in \bigcup_i M_i$ are distinguished from elements in $A \setminus \bigcup_i M_i$ by 3-$\mathrm{WL}_{\mathrm{implicit}}$, and furthermore, pairs (a, b) with $a, b \in M_i$ are distinguished from pairs (a', b') with $a' \in M_j$ and $b' \in M_{j'}$ for $j \neq j'$. Hence, in the implicit k-pebble game, Spoiler can use one pebble on $a := a_1 \cdots a_r$ with $a_i \in N_i$ to distinguish the submodule $N_1 \times \dots \times N_r \leq A$ once and for all, since this is just the normal closure of a in G.

Moreover, by counting the number of pairs (a, b) that fulfill $\langle a^H, b^H \rangle \cong N_i^2$, each homogeneous component M_i can be colored with the multiplicity of N_i in M_i. Since k-$\mathrm{WL}_{\mathrm{implicit}}$ is also able to count these pairs according to Lemma 5.7.11, coloring each M_i with the multiplicity of N_i does not change the WL-dimension. Now the isomorphism type of G is uniquely determined by the isomorphism type of $(N_1 \times \dots \times N_r) \rtimes_\Delta H$ together with these multiplicities, so the WL-dimension increases by at most 1 when going from G to $((N_1 \times \dots \times N_r) \rtimes_\Delta H, \chi)$. □

Lemma 5.7.13. *Let $G = A \rtimes_\Delta H$ be a coprime extension of an abelian group H by an abelian group A, such that each Sylow subgroup of A is elementary abelian. Let $N \leq A$ be a minimal normal subgroup of G. Then there exist $n_1, n_2 \in N$ such that, after individualizing n_1 and n_2, the coloring computed by* $2\text{-WL}_{\text{implicit}}$ *on G is discrete on N.*

Proof. Since N is a minimal normal subgroup, N is elementary abelian and irreducible regarded as an H-module. Let n_1 be any generator of N as an H-module. Since N is irreducible and H is abelian, Lemma 2.3.18 gives an element $g \in G$ such that $\langle n_1, g\rangle$ contains N.

Set $n_2 = n_1^g$, so $n_2 = \Delta(gA)n_1$. We show that, after individualizing n_1 and n_2, the set $M := \{x \in G \mid \Delta_N(xA) = \Delta_N(gA)\}$ is $2\text{-WL}_{\text{implicit}}$-detectable, where Δ_N denotes the representation induced on N by Δ. To this end, let $x \in G$ be any element, then $2\text{-WL}_{\text{implicit}}$ distinguishes x from g if $\Delta_N(xA)n_1$ is not equal to n_2. But otherwise, $\Delta(gx^{-1}A)$ fixes n_1, and since $\Delta_N(H)$ is cyclic, we have $\Delta(gx^{-1}A)(\Delta(gA)^i n_1) = \Delta(gA)^i n_1$ for each i, so $gx^{-1}A$ lies in the kernel of Δ_N.

By definition of M, for each i, the set $\{\Delta(mA)^i n_1 \mid m \in M\}$ is a singleton set, say $\{\Delta(mA)^i n_1 \mid m \in M\} = \{n_i'\}$. Since n_1 is individualized and M is a union of $2\text{-WL}_{\text{implicit}}$-color classes, each n_i' obtains a $2\text{-WL}_{\text{implicit}}$-color class of size 1. Now the claim follows since by definition, N is generated by $n_1', \dots, n_k'$ for some $k \in \mathbb{N}$. □

Lemma 5.7.14. *Let $G = A \rtimes_\Delta H$ be a coprime extension with an abelian group H and an abelian group A such that all Sylow-subgroups of A are elementary abelian. Let χ be a coloring on G such that* $k\text{-WL}_{\text{implicit}}$ *($k \geq 4$) computes a coloring on (G, χ) which induces a discrete coloring on A. Then it holds* $\dim_{\text{WL}_{\text{implicit}}}(G, \chi) \leq k$. *The same holds for* $\text{WL}_{\text{explicit}}$*, provided that k is at least* 5.

Proof. If the coloring computed by $k\text{-WL}_{\text{implicit}}$ on is discrete on A, then $k\text{-WL}_{\text{implicit}}$ distinguishes elements of g by their action on the discretely colored A. Hence, the coloring induced on $H/\ker(\Delta)$ by stable $k\text{-WL}_{\text{implicit}}$ colors is discrete as well (when testing isomorphism between G and another group, we can think of this as prescribing isomorphisms on A and $G/C_G(A)$, the latter of which is isomorphic to $H/\ker(\Delta)$).

The claim follows from Lemma 5.7.1, by lifting the isomorphism prescribed on $H/\ker(\Delta)$ to an isomorphism of H. The lifting is always possible by Lemma 5.6.19. □

Theorem 5.7.15. *Let $G = A \rtimes_\Delta H$ be a coprime extension, where each Sylow subgroup of A is elementary abelian and H is abelian. Let $A = N_1 \times \cdots \times N_r$ be a decomposition of A into subgroups N_i, such that each N_i is irreducible regarded as an H-module (so in particular, each N_i is elementary abelian). Then we have* $\dim_{\text{WL}_{\text{implicit}}}(G) \leq 2r' + 4$, *where r' is the number of distinct equivalence types of $N_1, \dots, N_r$.*

Proof. By Lemma 5.7.12, we may assume that N_i and N_j are inequivalent as H-modules whenever $i \neq j$ holds, if we then show a bound of $2r + 3$ for $\dim_{\text{WL}_{\text{implicit}}}(G)$.

By Lemma 5.7.13, we can individualize a total of $2r$ elements of G to fix a linear ordering of A. The coloring computed by $3\text{-WL}_{\text{implicit}}$ on G after these individualizations then induces linear orderings on A and $H/\ker(\Delta)$. This implies the claim by Lemma 5.7.14 . □

Lemma 5.7.16. *Let $G = A \rtimes_\Delta H$ be a coprime extension with H abelian and A elementary abelian. Let $U \subseteq A$ be the union over all minimal normal subgroups of G that are contained in A and consider the equivalence relation $\sim$ on $U \setminus \{1\}$ given by*

$$x \sim y \colon \Leftrightarrow \langle x^G \rangle \rtimes_\Delta H \cong \langle y^G \rangle \rtimes_\Delta H.$$

Let $U_1 \ldots, U_m$ denote the corresponding equivalence classes. Then we have a direct decomposition $A = \langle U_1 \rangle \times \cdots \times \langle U_m \rangle$ and each $\langle U_i \rangle$ is twisted-homogeneous regarded as a $\Delta(H)$-module. Moreover, each U_i is 7-$\mathrm{WL}_{\mathrm{explicit}}$-detectable.

Proof. By Lemma 5.7.10, it holds that 7-$\mathrm{WL}_{\mathrm{explicit}}$ distinguishes pairs of group elements that are equivalent with respect to $\sim$ from pairs that are not. It follows, since each U_i is an equivalence class with respect to $\sim$, that each U_i and hence each $\langle U_i \rangle$ is 7-$\mathrm{WL}_{\mathrm{explicit}}$-detectable (recall Lemma 4.1.3).

By definition, each $\langle U_i \rangle$ can be written as a sum of irreducible modules, all twisted equivalent to each other, so $\langle U_i \rangle$ is twisted-homogeneous. By construction of $\sim$, no irreducible submodule of U_i is equivalent to any irreducible submodule of $\sum_{j \neq i} U_j$, we obtain a direct decomposition $\langle U_1, \ldots, U_m \rangle = \langle U_1 \rangle \times \cdots \times \langle U_m \rangle$. Since each irreducible submodule of A is contained in some U_i, this is a decomposition of all of A. □

Theorem 5.7.17. *Let $G = A \rtimes_\Delta H$ be a coprime extension of an abelian group H by an elementary abelian p-group A and let $A = \langle U_1 \rangle \times \cdots \times \langle U_m \rangle$ be the decomposition from Lemma 5.7.16 and set $D := \max_i \big(\dim_{\mathbb{F}_p}(\langle U_i \rangle)\big)$. Then*

$$\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq \max\{7, D + 4\},$$

where $\dim_{\mathbb{F}_p}(\langle U_i \rangle)$ is the dimension of $\langle U_i \rangle$ regarded as a vector space over $\mathbb{F}_p$.

Proof. Since each U_i is 7-$\mathrm{WL}_{\mathrm{explicit}}$-detectable, Spoiler may use D pebble pairs on products of generators $u_1 \cdots u_m$, with $u_i \in U_i$ (see Lemma 3.4.8), to fix a linear ordering of the elements of A. Hence, the claim follows from Lemma 5.7.14. □

Dealing with the problem of non-canonical irreducible constituents, in the next lemma we assume that we are given an ordering of direct factors of A in terms of a pre-coloring on G, and then we construct a Spoiler-strategy to win the pebble game with $\mathcal{O}(1)$ pebble pairs.

Lemma 5.7.18. *Let $G = A \rtimes_\Delta H$ be a coprime extension with an abelian group H and an abelian group A, such that all Sylow-subgroups of A are elementary abelian. Fix a decomposition*

$$A = N_1 \oplus \cdots \oplus N_r$$

of A into irreducible $\Delta(H)$-modules N_i (so in particular each N_i is of prime-power order). Let χ be a coloring on G such that $G \setminus A$ is a χ-color class and each $N_i \subseteq A$ is a union of χ-color classes. Then we have $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G, \chi) \leq 6$.

Proof. By Lemma 5.7.13, for each i, we may individualize two elements $n_i, m_i \in N_i$, such that afterwards 2-$\mathrm{WL}_{\mathrm{implicit}}$ discretizes N_i.

Now, since the given pre-coloring χ distinguishes spaces N_i and N_j with $i \neq j$ into distinct color classes, we can individualize $n := \sum_i n_i$ and $m := \sum_i m_i$ instead of individualizing each n_i and m_i separately, and still obtain that 2-$\mathrm{WL}_{\mathrm{implicit}}$ discretizes each N_i

relative to this individualization, see Lemma 3.4.8. Thus, A is completely discretized by 2-$\mathrm{WL}_{\mathrm{implicit}}$ after individualizing n and m. Then the 6-$\mathrm{WL}_{\mathrm{implicit}}$ color classes computed on (G,χ) identify the isomorphism type of the uncolored group G by Lemma 5.7.14. Since the coloring induced on A after individualizing m and n is discrete and $G \setminus A$ is a single χ-color class, it follows $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G,\chi) \leq 6$. □

One natural example for the situation of the previous lemma is the case of an abelian group A, where each Sylow subgroup is a (elementary abelian) minimal normal subgroup of $A \rtimes H$, and the WL-algorithm automatically distinguishes the N_i into minimal normal subgroups, as Sylow subgroups of abelian groups are 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.

Corollary 5.7.19. *Let $G := A \rtimes_\Delta H$ be a coprime extension with abelian groups H and A and assume that each Sylow subgroup of A is elementary abelian and irreducible as a $\Delta(H)$-module. Then we have* $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq 6$.

Intuitively, through Lemma 5.7.16 and Lemma 5.7.18, the hardness of distinguishing groups of the form $C_p^d \rtimes_\Delta H$ up to isomorphism depends on the number of irreducible direct summands contained in the twisted-homogeneous components of C_p^d regarded as a $\Delta(H)$-module. This observation is captured in the next definition and theorem.

Definition 5.7.20. Let $\Delta : H \to \mathrm{GL}_d(\mathbb{F}_p)$ be a representation. For an irreducible $\Delta(H)$-submodule $N \leq \mathbb{F}_p^d$, let $\mathcal{H}(N)$ denote the maximal twisted-homogeneous $\Delta(H)$-submodule of $\mathbb{F}_p^d$ that contains N. The *twist ratio* of N is $\dim(\mathcal{H}(N))/\dim(N)$.

Theorem 5.7.21. *Let $G = A \rtimes_\Delta H$ be a coprime extension of abelian groups and assume that each Sylow subgroup of A is elementary abelian. Let t denote the maximal twist ratio among all irreducible $\Delta(H)$-submodules of A. Then we have*

$$\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq \lceil \log(t) \rceil + 7.$$

In particular, $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq \log\log|G| + \mathcal{O}(1)$.

Proof. By Lemma 5.7.12, we may assume without loss of generality that each irreducible constituent of A considered as an H-module occurs with multiplicity 1, at the cost of increasing the dimension by one. The Lemma formally provides a reduction to a colored group, where the irreducible constituents are colored with their multiplicity in A, and we call this coloring χ_{mult}. We should also note that the reduction to pair-wise inequivalent irreducible constituents can only decrease the twist ratio, as the twisted homogeneous components can only get smaller by omitting copies of irreducible constituents.

Let $A = \langle U_1\rangle \times \cdots \times \langle U_m\rangle$ be the decomposition into twisted-homogeneous components from Lemma 5.7.16. The Lemma also shows that each U_i is 7-$\mathrm{WL}_{\mathrm{implicit}}$-detectable.

Since the irreducible constituents of A are pair-wise inequivalent, we obtain that, if $A = \bigoplus_{i=1}^r N_i$ is a decomposition of A into irreducible H-modules, then each irreducible H-module contained in A is equal to some N_i (this follows from Part 1) of Lemma 5.7.2). Hence, for each i, by Lemma 3.5.2, in the implicit pebble game, Spoiler can use $\lceil \log(t) \rceil$ pebble pairs to fix an ordered direct decomposition $U_i = N_{i,1} \oplus \cdots \oplus N_{i,t}$ into irreducible $\Delta(H)$-modules $N_{i,j}$ (if the twist-ratio of some U_i is strictly smaller than t, we just use the remaining pebbles on one element repeatedly). Let $u_{i,1}, \ldots, u_{i,\lceil \log(t) \rceil}$ be the elements pebbled by Spoiler to fix this decomposition.

Since each U_i is detectable, Spoiler may instead place $\lceil\log(t)\rceil$ pebble pairs on products $u_{1,j}\cdots u_{m,j}$, instead of placing separate pebbles on $u_{1,j},\dots,u_{m,j}$, and thereby still implicitly fix images of $u_{i,1},\dots,u_{i,\lceil\log(t)\rceil}$ (see Lemma 3.4.8). In conclusion, Spoiler can fix an ordered decomposition of A into irreducible $\Delta(H)$-modules by using a total of $\lceil\log(t)\rceil$ pebble pairs. We can interpret this as a pre-coloring on A, say χ_0, that assigns a unique color to each irreducible constituent of A and places all elements not contained in an irreducible constituent in one additional color class. Let χ be the coloring obtained by combining χ_0 with χ_{mult}, so $\chi := (\chi_0, \chi_{\text{mult}})$ assigns a pair of colors to each group element.

The colored group (G,χ) then fulfills the assumptions of Lemma 5.7.18, so the implicit $\mathrm{WL}_{\text{implicit}}$-dimension of (G,χ) is bounded by 6. Hence, by what we argued above, the $\mathrm{WL}_{\text{implicit}}$-dimension of (G,χ_{mult}) is bounded by $\lceil\log(t)\rceil+6$ and finally the $\mathrm{WL}_{\text{implicit}}$-dimension of G is bounded by $\lceil\log(t)\rceil+7$. □

Arbitrary abelian normal subgroups

Our discussion of automorphisms of abelian groups yields more general versions of the theorems from the previous paragraph, allowing the normal subgroups of the extensions to be abelian, without any restrictions on the exponent.

Corollary 5.7.22. *Let G be an extension of an abelian group H by an abelian p-group A, where p does not divide $|H|$. If $\Omega_1(A)$ is a minimal normal subgroup of G (i.e., the representation induced by H acting on $\Omega_1(A)$ is irreducible), or if A/A^p is a minimal normal subgroup of G/A^p, then* $\dim_{\mathrm{WL}_{\text{explicit}}}(G)\le 7$.

Proof. If $\Omega_1(A)$ is a minimal normal subgroup of G, it follows that A is homocyclic (otherwise some but not all elements of order p are $p^{\exp(A)-1}$-th powers, and then these generate a strictly smaller normal subgroup). The same holds if A/A^p is a minimal normal subgroup of G/A^p, as otherwise there exist elements of distinct orders in $A\setminus A^p$, and elements of smaller orders would give rise to a non-trivial normal subgroup, strictly contained in A/A^p.

By Theorem 4.1.10, we may consider the coloring computed by 7-$\mathrm{WL}_{\text{explicit}}$ on the quotient group G/A^p, which identifies the quotient group up to isomorphism by Lemma 5.7.10. Now if A is homocyclic, the image of Ψ_p is all of $\mathrm{GL}(A/A^p)$, thus Lemma 5.6.7 applied to Ψ_p implies that G is identified as well. □

Lemma 5.7.23. *Let A be an abelian p-group. Define a coloring χ_{ord} on A/A^p via*

$$\chi_{\text{ord}}(aA^p) := \min_{b\in A}|ab^p|.$$

Then it holds $\mathrm{Im}(\Psi_p)=\mathrm{Aut}(A/A^p,\chi_{\text{ord}})$.

Proof. Decompose A into maximal homocyclic direct factors, say $A=A_1\times\cdots\times A_t$, where for each i we have $A_i\cong C_{p^{e_i}}^{d_i}$, with a sequence of strictly increasing exponents $1\le e_1<\cdots<e_t$. Let $\alpha\in\mathrm{Aut}(A)$ be any automorphism. Then it holds $(A_i)^\alpha\subseteq(A_1\cdots A_i)A^p$ for all i. So the automorphism induced on A/A^p by α respects the coloring χ_{ord}. On the other hand, the orbit of A_i under $\mathrm{Aut}(A)$ contains each element of order p^i in $A_1\cdots A_i$, for all i. Hence, $\mathrm{Aut}(A)$ acts transitively on the color classes of χ_{ord}. □

Corollary 5.7.24. *Let $G = A \rtimes_\Delta H$ be a coprime extension with abelian groups H and A. Then we have* $\dim_{\mathrm{WL}_{\mathrm{explicit}}}(G) \leq \log\log|G| + 8$.

Proof. We define a coloring χ on the elementary abelian group $A/\Phi(A)$ as follows: If a lies in the Sylow p-subgroup of $A/\Phi(A)$, then set $\chi(a) := \min_{b \in A}|ab^p|$. Extend this coloring to $Q := G/\Phi(A)$ by placing all elements that are not contained in a Sylow subgroup of $A/\Phi(A)$ in one additional color class $Q \setminus (A/\Phi(A))$, and call the resulting coloring χ again.

By Theorem 5.7.21, the $\mathrm{WL}_{\mathrm{implicit}}$-dimension of the colored group (Q, χ) is bounded by $\log\log|Q| + 7 \leq \log\log|G| + 7$. So if $G^* = A^* \rtimes_{\Delta^*} H^*$ is not distinguished from G by k-$\mathrm{WL}_{\mathrm{explicit}}$ for $k \geq (\log\log|G| + 7)$, then we can define a coloring χ^* on $Q^* := G^*/\Phi(A^*)$ in analogy to χ and we obtain an isomorphism of colored groups $\theta\colon (Q, \chi) \to (Q^*, \chi^*)$. By Lemma 5.7.1, this implies the existence of two isomorphisms $\psi\colon A/\Phi(A) \to A^*/\Phi(A^*)$ and $\varphi\colon H \to H^*$ such that the actions induced on $A/\Phi(A)$ by $(\Delta^* \circ \varphi)^\psi$ and Δ agree. Since θ is compatible with the colorings χ and χ^*, we can choose ψ as an isomorphism of colored groups $(A/\Phi(A), \chi) \to (A^*/\Phi(A^*), \chi^*)$.

By Lemma 5.7.23, for each prime p that divides $|A|$, the homomorphism induced by $(\Delta^* \circ \varphi)$ on the Sylow p-subgroup $(A/\Phi(A))_p$ is conjugate to the homomorphism induced by Δ on $(A/\Phi(A))_p$, via some conjugator in the image of Ψ_p (where Ψ_p is defined with respect to H acting on A). By Lemma 5.6.7, the restriction of $(\Delta^* \circ \varphi)$ to the Sylow p-subgroup A_p is hence conjugate to the restriction of Δ to A_p, via some conjugator in $\mathrm{Aut}(A_p)$. This is true for all primes p dividing $|A|$, with fixed Δ, and hence G is isomorphic to G^*. □

We end our investigation of coprime extensions with a brief discussion of arbitrary (non-abelian) quotient groups.

Definition 5.7.25. In view of Lemma 5.7.5, we define the following coloring for any coprime extension $G = A \rtimes_\Delta H$ with an abelian group A. For each $h \in H$, we set $\chi^\Delta(h)$ to be the $\mathrm{Aut}(A)$-conjugacy class of $\Delta(h)$.

Definition 5.7.26. Let Δ be an irreducible representation of a finite group G. We say that Δ is *non-twisting*, if every representation that is twisted-equivalent to Δ is already equivalent to Δ.

Theorem 5.7.27. *Let $G = A \rtimes_\Delta H$ be a coprime extension with an abelian group A.*

1. *We have*
$$\dim_{\mathrm{WL}_{\mathrm{explicit}}}(G) \leq \max\left(4, \dim_{\mathrm{WL}_{\mathrm{explicit}}}\left((H, \chi^\Delta)\right)\right).$$
2. *Let $p_1 < \cdots < p_s$ be the prime divisors of $|A|$. Denote the linear representation induced by the action of H on A/A^{p_i} by Δ_{p_i}. Assume that, for all i, each irreducible constituent of Δ_{p_i} is non-twisting. Then we have*
$$\dim_{\mathrm{WL}_{\mathrm{explicit}}}(G) \leq \max\left(4, \dim_{\mathrm{WL}_{\mathrm{explicit}}}(H) + \mathcal{O}(1)\right).$$

Before we move on to the proof, let us first give an example for the situation in Part 2). An irreducible representation is non-twisting, if the corresponding character is uniquely determined up to equivalence by its degree and the multiset of character values. For instance, the irreducible complex A_5-representation of degree 5 is realizable over any field of coprime charactristic, and uniquely determined by its degree.

Proof. We start by establishing some general observations and from these deduce the claims of the theorem. Throughout the proof, we consider the explicit $(k+1)$-pebble game on (G, G^*), where we assume that G^* is indistinguishable from G by k-$\mathrm{WL}_{\mathrm{explicit}}$ (i.e., Duplicator has a winning strategy by Lemma 3.2.13). The goal is to show that G and G^* are isomorphic, provided that k is large enough. By Lemma 5.7.3, we may assume that G^* is also a coprime extension $G^* = A^* \rtimes_{\Delta^*} H^*$ with $A^* \cong A$. Since k is at least 4, by Lemma 5.7.5, we may assume that each element of $g \in G$ is colored with the $\mathrm{Aut}(A)$-conjugacy class of the action induced by conjugation of $\Delta(gA)$. Call this coloring χ and choose any isomorphism $\alpha\colon A \to A^*$. Then we can analogously define a coloring χ^* on G^*, by coloring each $g^* \in G^*$ with $\alpha^{-1} \circ \Delta^*(g^*A^*) \circ \alpha$. The coloring χ^* does not depend on the choice of α and by Lemma 5.7.5, if Duplicator does not respect this coloring at any point, then Spoiler can win the pebble game. Hence, we may assume without loss of generality that the groups G and G^* are pre-colored with χ and χ^*.

Then, by Lemma 5.7.5, it is sufficient to show that G and G^* are isomorphic, provided that Duplicator has a winning strategy in the k-pebble game on (G, χ) and (G^*, χ^*), where our bound on k depends on which case of the present Theorem we are considering.

1. We note that the quotient coloring that χ induces on $H = G/A$ is precisely χ^{Δ}, and similarly, the quotient coloring induced on H^* by χ^* is χ^{Δ^*}. We assume that Duplicator has a winning strategy in the $(k+1)$-pebble game on (G, χ) and (G^*, χ^*), where k is at least $\dim_{\mathrm{WL}_{\mathrm{explicit}}}\big((H, \chi^{\Delta})\big)$. By Theorem 4.1.10, we then have that $\big(H, \chi^{\Delta}\big)$ and $\big(H^*, \chi^{\Delta^*}\big)$ are indistinguishable via k-$\mathrm{WL}_{\mathrm{explicit}}$. Since we may assume that k is at least $\dim_{\mathrm{WL}_{\mathrm{implicit}}}\big((H, \chi^{\Delta})\big)$, there must exist an isomorphism of colored groups $\varphi\colon \big(H, \chi^{\Delta}\big) \to \big(H^*, \chi^{\Delta^*}\big)$. By definition of χ^{Δ}_{H} and $\chi^{\Delta^*}_{H^*}$, this means that Δ and $\Delta^* \circ \varphi$ are element-conjugate, and due to Lemma 5.6.6, they are also globally conjugate, that is, there exists an isomorphism $\psi\colon A \to A^*$ such that $\Delta = (\Delta^* \circ \varphi)^{\psi}$. It follows from Lemma 5.7.1 that G is isomorphic to G^*.

2. Here we assume that k is at least as large as $\dim_{\mathrm{WL}_{\mathrm{explicit}}}(H)$, so we may additionally assume that H and H^* are isomorphic. Fix some isomorphism $\varphi\colon H \to H^*$. We first consider the case that each Sylow subgroup of A is elementary abelian. Assume that Spoiler places a pebble pair on (a, a^*), where the normal closure of $a \in A$ forms a minimal normal subgroup of G, and a^* is chosen by an appropriate winning move for Duplicator. In particular, $N := \langle a^G \rangle$ is elementary abelian and irreducible as an $\Delta(H)$-module, and via indistinguishability the same holds for $N^* := \langle a^* \rangle$ with respect to H^* and Δ^*. Then $N \rtimes H$ must be indistinguishable from $N^* \rtimes H^*$ via $(k-1)$-WL, or otherwise Spoiler would be able to win from the current configuration by Corollary 4.1.4. In particular, N and N^* are isomorphic as abstract groups by Lemma 5.7.3. Fix some isomorphism $\psi\colon N \to N^*$. By Lemma 5.7.5, the multisets of $\mathrm{GL}(N)$-conjugacy classes of the elements in $\Delta(H)$ and $\psi^{-1}\Delta^*(H^*)\psi$ in their induced actions on N agree. Hence, the characters associated to N and N^* regarded as representation modules for H and H^*, respectively, have the same multisets of character values. By our assumptions in Part 2) and by irreducibility of N and N^*, the representations induced on N by Δ and $\psi^{-1}(\Delta^* \circ \varphi)\psi$ are thus equivalent. If we let a vary in A, eventually N runs through the irreducible constituents of Δ. Since Duplicator has a winning strategy, each irreducible representation of H appears in

Δ and $(\Delta^* \circ \varphi)$ with the same multiplicity, i.e., Δ and $\Delta^* \circ \varphi$ are conjugate. By Lemma 5.7.1, G and G^* are isomorphic.

Now we consider the general case, where the Sylow subgroups of A are not necessarily elementary abelian. Since abelian groups have a canonical decomposition into their Sylow subgroups, we can apply Lemma 5.6.7 for each prime divisor of $|A|$ separately. Then Δ and $\Delta^* \circ \varphi$ are conjugate if and only if the induced homomorphisms obtained by restriction to a single Sylow-subgroup are conjugate for each prime. So let A be an abelian p-group. By Theorem 4.1.10, indistinguishability of G and G^* via k-$\mathrm{WL}_{\mathrm{implicit}}$ implies indistinguishability of G/A^p and $G^*/(A^*)^p$ via k-$\mathrm{WL}_{\mathrm{explicit}}$. By the elementary abelian case, and since we may assume k to be large enough, we obtain that Δ_p and $\Delta_p^* \circ \varphi$ are conjugate in $\mathrm{Aut}(A/A^p)$. By Lemma 5.6.7, Δ and $\Delta^* \circ \varphi$ are conjugate in $\mathrm{Aut}(A)$. □

5.7.2 On the expressiveness of coprime extension

Although the structure of coprime extensions is fairly restricted compared to arbitrary groups, coprime extensions make up for an asymptotically dense subset of group orders in the set of all natural numbers. This is formalized in the following theorem.

Theorem 5.7.28 (Dietrich-Wilson, [31, Theorem II.5])**.** *There is an asymptotically dense subset of the integers $\mathcal{Y} \subseteq \mathbb{N}$ and a constant c, such that for each group G of order $n \in \mathcal{Y}$ there exist subgroups B and H of G with the following properties:*

1. *the orders $|B|$ and $|H|$ are coprime,*
2. *G factors as $G = B \rtimes H$,*
3. *B is a cyclic group,*
4. *we have $|H| \in (\log n)^{\mathcal{O}((\log\log n)^c)}$.*

In the previous theorem, a decomposition $G = B \rtimes H$ and generators for $\mathrm{Aut}(B)$ and $\mathrm{Aut}(H)$ can be computed in polynomial time. In [31] this is leveraged to show that isomorphism between these groups can be tested in polynomial time.

In Theorem 4.3.27, we show that, given a class $\mathcal{C}$ of finite groups of Weisfeiler-Leman dimension c, the Weisfeiler-Leman dimension of groups, all whose direct factors are contained in $\mathcal{C}$, is bounded by $c + 1$. However, we also show that if the dimension of one of the factors is at least c then the dimension of the product is at least c (see Lemma 4.3.4). We can use this to show that we cannot expect a result analogous to the one by Dietrich-Wilson showing that for most group orders the Weisfeiler-Leman dimension is bounded, unless this is generally the case.

Observation 5.7.29. *If the Weisfeiler-Leman dimension is bounded for all groups in a dense subset of the integers $\mathcal{Y} \subseteq \mathbb{N}$ then the Weisfeiler-Leman dimension is bounded for all finite groups.*

Proof. If $\mathcal{Y} \subseteq \mathbb{N}$ is an asymptotically dense set and G is any group, then $\mathcal{Y}$ and $|G|\mathbb{N}$ have non-trivial intersection. Thus $|G| \cdot |H| = |G \times H| \in \mathcal{Y}$ for a suitable group H. From Theorem 4.3.27 it follows that $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G \times H) \geq \dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) + \dim_{\mathrm{WL}_{\mathrm{implicit}}}(H)$.

We conclude that the WL-dimension of groups with orders in $\mathcal{Y}$ is unbounded if there are groups of arbitrarily large WL-dimension. □

In contrast to this observation, we note that the groups G with $|G| \in \mathcal{Y}$ can be generated with at most $\log\log|G|$ elements.

Corollary 5.7.30. *There is an asymptotically dense set $\mathcal{Y} \subseteq \mathbb{N}$, such that the WL-dimension of groups of order $n \in \mathcal{Y}$ is bounded by a polynomial in $\log\log n$.*

5.8 Central extensions

In this section, we turn to another extremal case of group extensions. An extension of Q by N is called *central* if the normal subgroup N is contained in the center of the group extension. In particular, the associated action of Q on N is trivial, and N is always abelian in this situation.

While, from a structural perspective, we have a better understanding of central extensions compared to general extensions, when it comes to the isomorphism problem, they currently form the frontier of our understanding. For instance, groups with prime exponent and nilpotency class 2 are currently among the most investigated but also most challenging group classes in the area of group isomorphism. All of these groups are central extensions of abelian groups by abelian groups (such groups are called metabelian). More generally, the following well-known observation emphasizes the structural potential of central extensions.

Lemma 5.8.1. *The class of finite groups that can be formed via iterated central extensions, starting from an abelian group, are precisely the finite nilpotent groups.*

We recall the following well-known lemma that relates central product decompositions to isomorphism testing.

Lemma 5.8.2. *Assume we are given groups G and H with central product decompositions $G = G_1G_2$ and $H = H_1H_2$. Assume that $|G| = |H|$ holds. Let $\psi_i\colon G_i \to H_i$ be group isomorphisms for $i \in \{1,2\}$, then there exists a* gluing *$\psi := \psi_1 \odot \psi_2$, that is an isomorphism $G \to H$ with $\psi_{|G_i} = \psi_i$, if and only if $(\psi_1)_{|G_1\cap G_2} = (\psi_2)_{|G_1\cap G_2}$ holds.*

Proof. By assuption, if there is such a homomorphism ψ with $\psi_{|G_i} = \psi_i$, then $(\psi_1)_{|G_1\cap G_2} = (\psi_2)_{|G_1\cap G_2}$ holds. Assume now that $(\psi_1)_{|G_1\cap G_2} = (\psi_2)_{|G_1\cap G_2}$ holds. We can then define a map $\psi\colon G \to H, g = g_1g_2 \mapsto \psi_1(g_1)\psi_2(g_2)$, where the factorization $g = g_1g_2$ with $g_i \in G_i$ can be chosen arbitrarily. If $g = x_1x_2$ is another factorization, then we have $x_1^{-1}g_1 = x_2g_2^{-1} \in G_1 \cap G_2$. By assumption this implies

$$\begin{aligned}\psi_1(g_1)\psi_2(g_2) &= \psi_1(x_1x_2g_2^{-1})\psi_2(g_2) = \psi_1(x_1)\psi_1(x_2g_2^{-1})\psi_2(g_2)\\ &= \psi_1(x_1)\psi_2(x_2g_2^{-1})\psi_2(g_2) = \psi_1(x_1)\psi_2(x_2).\end{aligned}$$

So ψ is a well-defined map, a homomorphism, since G_1 and G_2 commute, it is surjective since ψ_1 and ψ_2 are hence bijective, since we assume that $|G| = |H|$ holds. □

5.8.1 $\mathcal{O}(1)$-generated quotients

Here we assume that G is a central extension of a group H by an abelian group A and that H can be generated with a constant number of elements, say d. Our aim is to show that the WL-dimension of the entire group G is bounded by d, up to some fixed constant, provided that G fulfills certain structural restrictions.

We start with a reformulation of the given assumptions on G, relating central extensions with central product decompositions.

Lemma 5.8.3. *If G is a central extension of a d-generated group, then G has a d-generated subgroup, say U, such that $G = UZ(G)$ holds, that is, G is a central product of U and $Z(G)$.*

Via this reformulation, the isomorphism problem for such groups reduces to a problem of extending partial isomorphisms on abelian groups, as follows.

Lemma 5.8.4. *Let G and G^* be central products of d-generated subgroups U and U^* with the respective centers $Z(G)$ and $Z(G^*)$. Let $\varphi\colon U \to U^*$ be a group isomorphism. Then G and G^* are isomorphic, if and only if there is an isomorphism $\psi\colon Z(G) \to Z(G^*)$ that restricts to $\varphi_{|U\cap Z(G)}$ on $U \cap Z(G)$.*

Proof. Since $G = UZ(G)$ holds, we have $Z(G) \cap U = Z(U)$, and analogously it holds $Z(G^*) \cap U^* = Z(U^*)$. Hence $\varphi(Z(G) \cap U) = \varphi(Z(U)) = Z(U^*) = Z(G^*) \cap U^*$. The claim now follows from Lemma 5.8.2. □

We devise another technical lemma on splitting elements in finite groups.

Lemma 5.8.5. *If A is abelian and $a \in A$ has prime order, then any maximal root of a in A, that is, an element $r \in A$ that has maximal order with respect to $a \in \langle r\rangle$, splits from A.*

Proof. Set $p := |a|$ and denote the unique Sylow p-subgroup of A by A_p. By definition of r, for any prime $q \neq p$, we have that $|r|$ is divisible by the exponent of the unique Sylow q-subgroup of A. Hence, r splits from A if and only if the projection of r onto A_p, say r_p, splits from A_p. Let $A_p = \langle x_1\rangle \times \ldots \langle x_m\rangle$ be a cyclic decomposition of A_p. With respect to this decomposition, write $a = (a_1, \ldots, a_m)$ and $r_p = (r_1, \ldots, r_m)$. Then r_p is a maximal root of a in A_p and hence, the components r_i with $|r_i| = |r|$ are exactly those for which a_i is non-trivial. Since there is no root of a in A_p of order strictly larger than $|r_p|$, there is some i such that $|r_i| = |r| = |a_i|$ holds. By Lemma 5.6.10, r_p splits from A_p. □

Lemma 5.8.6. *Let G be a central product of a d-generated group U by an abelian group A. Assume that $Z(U)$ has full rank in $Z(G)$. Then it holds $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq d+3$.*

Proof. By assumption, $G/Z(G)$ can be generated with at most d elements, so if G^* is another group then, in the implicit pebble game on (G, G^*), Spoiler can use d pebble pairs and place the corresponding pebbles in G on a generating set for $G/Z(G)$. This either fixes an explicit isomorphism $\phi\colon G/Z(G) \to G^*/Z(G^*)$, or such an isomorphism does not exist and then Spoiler wins the game by Lemma 4.1.9.

So we may assume that there are d pebble pairs on the board specifying an isomorphism of subgroups $\phi : U \to U^* \leq G^*$ such that $G = UA$ and $U/Z(U) \cong G/Z(G)$

hold. If Spoiler does not have a winning strategy, then the current pebble pairs induce isomorphisms $U/Z(U) \cong U^*/Z(U^*) \cong G^*/Z(G^*)$ and $Z(U) \cong Z(U^*)$ by Lemma 4.1.9 and detectability of the center.

Now $Z(U)$ has full rank in $Z(G)$, and $\phi_{|U}$ induces an isomorphism $Z(U) \to Z(U^*) \leq Z(G^*)$ that is fixed through the current pebble pairs on the board. We can interpret this as a pre-coloring of the given groups G and G^* and then, using Lemma 5.6.9, if G and G^* are indistinguishable via $d+3$-dimensional $\mathrm{WL}_{\mathrm{implicit}}$, then there must exist an isomorphism $\psi \colon Z(G) \to Z(G^*)$ that extends $\phi_{|U}$. But then we obtain an isomorphism $G \to G^*, ua \mapsto \phi(u)\psi(a)$, which is well-defined by Lemma 5.8.2, since ϕ and ψ agree on $U \cap A$. □

Corollary 5.8.7. *Let G be a central product of a d-generated group U by an abelian group A. If U is perfect, then it holds* $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq d+4$.

Proof. We may assume that G does not admit non-trivial direct decompositions, since according to Theorem 4.3.27, the WL-dimension of any class of groups $\mathcal{C}$ is at most one larger than the WL-dimension of directly indecomposable direct factors of groups in $\mathcal{C}$.

We show that then $Z(U)$ has full rank in $Z(G) = Z(U)A$. Since U is perfect, we have $G' = U' = U$. For the sake of contradiction, assume that $Z(U)$ does not have full rank in $Z(G)$. If $G' = U$ holds, then choose some $a \in A$ of prime order and such that a is not contained in U. Let r be a maximal root of a in $Z(G)$. Since a has prime order, r splits from U by Lemma 5.8.5, and by choice of a we have $\langle r \rangle \cap U = \{1\}$. Since $U = G'$ holds, G/G' is isomorphic to a factor group of A and thus, rG' also splits from G/G'. By Lemma 4.3.9, r splits from G, contradicting indecomposability. □

5.8.2 Schur-covers

Schur-covers are special central extensions that play a fundamental role in the theory of perfect groups. For more information on perfect groups, stem extensions and Schur-covers, we refere to [4, Section 33].

Definition 5.8.8. A stem extension of a group G is a central extension E of G by an abelian group N, such that $N \leq Z(E)$ and $N \leq E'$ hold. A Schur-cover ΓG of a group G is a maximal stem extension of G. The center of a Schur-cover is called a *Schur-multiplier* of G, denoted by $S(G) := Z(\Gamma G)$.

If G is perfect, then the Schur-cover of G is the unique up to isomorphism and it can be defined as the largest perfect central extension of G. Moreover, this extension is universal in the class of central extensions of G and unique up to isomorphism. Here, universal means that for each central extension E of G by some abelian group N, there exists a group homomorphism $\mu \colon \Gamma G \to E$ such that for each $x \in \Gamma G$ the equality $xS(G) = \mu(x)N$ holds in $G = \Gamma G/S(G) = E/N$, see [4, Section 33].

We show that the Weisfeiler-Leman dimension does not increase when going from a perfect group to ist Schur-cover.

Lemma 5.8.9. *If G is a perfect group then* $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(\Gamma G) \leq \max(\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G), 3)$.

Proof. Let Γ^* be another group that is indistinguishable from the Schur cover ΓG via the $\max(\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G), 3)$-dimensional Weisfeiler-Leman algorithm. By detectability of the center (see Lemma 4.1.3), we have that $Z(\Gamma^*)$ is isomorphic to $Z(\Gamma G) = S(G)$ and via Theorem 4.1.10, this implies that $G \cong \Gamma G/S(G)$ is isomorphic to $\Gamma^*/Z(\Gamma^*)$. So Γ^* is isomorphic to a central extension of G by $S(G)$. Furthermore, by Lemma 4.2.12, the commutator subgroups are 3-WL-detectable, and since $Z(\Gamma G) \leq (\Gamma G)'$ holds by definition of the Schur-cover, indistinguishability of ΓG from Γ^* then implies that $Z(\Gamma^*) \leq (\Gamma^*)'$ holds as well. But then Γ^* is isomorphic to a stem extension of G by $S(G)$, so Γ^* is isomorphic to the unique Schur-cover of G, that is $\Gamma^* \cong \Gamma G$. □

5.8.3 Direct products of perfect center-less groups

We move on to investigate quotients with an arbitrary number of generators. Instead of bounding the rank of the input group, we require a bound on the rank of the center of the group etensions we consider. A basic example are direct products of non-abelian simple groups, which are uniquely determined up to isomorphism by their order and the isomorphism types of their minimal normal subgroups (with multiplicities), see also Lemma 4.2.28. More generally, we allow the quotient groups to be direct products of perfect center-less groups. Recall that center-less groups admit a unique decomposition into directly indecomposable factors (up to re-ordering) by Corollary 4.3.26, which reveals the direct product structure in a way that is easy to exploit in Spoiler-strategies. Nonetheless, the class of perfect center-less groups is a natural starting point in the theory of central extensions (see also [4, Section 33]), containing the class of direct products of simple groups.

A similar class of groups is investigated in [49], where the authors devise polynomial-time isomorphism tests for several classes of group extensions, including central extensions where the quotient group is a direct product of perfect groups of constant order or a direct product of non-abelian simple groups.

Let G be a group such that $G/Z(G) = T_1 \times \cdots \times T_m$ is a direct product of perfect center-less groups T_i. By choosing this decomposition of maximal length, we may further assume that each T_i is directly indecomposable. Then G is a central product of central extensions of perfect, center-less groups: let U_i be the subgroup of G for which $Z(G) \leq U_i$ and $U_i/Z(G) = T_i$. Then $G = U_1 \cdots U_m$ is a central decomposition of G, i.e., we have $[U_i, U_j] = 1$ whenever $i \neq j$, and each U_i is a central extension of T_i by $Z(G)$.

We first show that the Weisfeiler-Leman algorithm can exploit such a decomposition of $G/Z(G)$.

Definition 5.8.10. Let G be a group such that $G/Z(G) = T_1 \times \cdots \times T_m$ is a direct product of directly indecomposable, center-less groups T_i. For $g \in G$ we get a unique representation $gZ(G) = (t_1, \ldots, t_m)$ with $t_i \in T_i$. Define the *weight* of g as $\mathrm{wt}(g) := |\{i \in [m] \mid t_i \neq 1\}|$.

Lemma 5.8.11. *Let $k \geq 7$ and consider the explicit k-pebble game on groups G and H. Assume that $G/Z(G)$ and $H/Z(H)$ are direct products of center-less groups. Then, independent of the current configuration, Spoiler has a winning strategy if Duplicator ever picks a bijection $f\colon G \to H$ with $\mathrm{wt}(g) \neq \mathrm{wt}(f(g))$ for some $g \in G$. If all direct factors of $G/Z(G)$ are simple, then $k \geq 5$ is sufficient.*

Proof. Since centers are 2-$\mathrm{WL}_{\mathrm{implicit}}$-detectable (see Lemma 4.2.15), by Lemma 4.1.9 and Corollary 4.3.26, the set of elements of weight 1 is 6-$\mathrm{WL}_{\mathrm{explicit}}$-detectable in the case of center-less direct factors, and by the first line of the proof of Lemma 4.2.32, it is 4-$\mathrm{WL}_{\mathrm{explicit}}$-detectable in the case of simple direct factors. By Lemma 4.1.3, the set of elements of weight m is then inductively k-$\mathrm{WL}_{\mathrm{explicit}}$-detectable for the respective k and for every $m \geq 1$, where the induction step only requires $k \geq 4$. Finally recall that k-$\mathrm{WL}_{\mathrm{explicit}}$ corresponds to the explicit pebble game with $k+1$ pebble pairs (see Lemma 3.2.13), hence the bounds in the Lemma's statement. □

If G is an extension of Q by N such that Q and N can be generated by d and s elements, respectively, then G can always be generated by at most $d+s$ elements, and so the WL-dimension of G is trivially bounded by $d+s$. If all direct factors of G/N are centerless and generated by at most d' elements, we can improve the bound to $d'+s+\mathcal{O}(1)$ via exploiting the weight function defined above.

Lemma 5.8.12. *Let G be a finite group and assume that $G/Z(G)$ is a direct product of d-generated, center-less groups. Then we have $\dim_{\mathrm{WL}_{\mathrm{implicit}}}(G) \leq d + d(Z(G)) + \mathcal{O}(1)$.*

Proof. Let G^* be another group of order $|G|$ and consider the implicit pebble game on (G, G^*). Spoiler starts by placing $s := d(Z(G))$ pebble pairs on $(n_1, n_1^*), \ldots, (n_s, n_s^*)$ for some generating set $\{n_1, \ldots, n_s\}$ of $Z(G)$, where the n_i^* are chosen by Duplicator's bijections. By assumption, if Spoiler does not have a winning strategy with $s + \mathcal{O}(1)$ pebble pairs, then $Z(G^*)$ is generated by the n_i^*, and the map $n_i \mapsto n_i^*$ extends to an isomorphism $Z(G) \cong Z(G^*)$. Write $G/Z(G) = G_1 \times \cdots \times G_t$. With a constant number of additional pebbles, if Spoiler cannot win then $G^*/Z(G^*)$ decomposes as $G_1^* \times \cdots \times G_t^*$ such that G_i is indistinguishable from G_i^* for all i. This can be seen as follows: by Theorem 4.1.10, if G is indistinguishable from G^* then $G/Z(G)$ is indistinguishable from $G^*/Z(G^*)$. So we can apply Theorem 4.3.27 to $G/Z(G)$ and $G^*/Z(G^*)$, which proves that indeed, G_i is indistinguishable from G_i^* since we assume $G/Z(G)$ to be center-less. For all i, let U_i be the pre-image of G_i with respect to reduction modulo $Z(G)$ and let U_i^* be the pre-image of G_i^* modulo $Z(G^*)$. Then we have $G = U_1 \cdots U_t$ and $G^* = U_1^* \cdots U_t^*$.

Spoiler places d additional pebble pairs on the elements $(g_1, g_1^*), \ldots, (g_d, g_d^*)$ so that $\langle g_1 Z(G), \ldots, g_d Z(G) \rangle = G_1$ holds. Thus $\langle g_1, \ldots, g_d, n_1, \ldots, n_s \rangle = U_1$.

The elements g_i^* are again chosen by Duplicator's bijection, without loss of generality let $\langle g_1^*, \ldots, g_d^*, Z(G^*) \rangle$ be equal to U_1^*. If the current configuration does not induce an isomorphism of subgroups $\varphi_1 : U_1 \to U_1^*$, Spoiler can win the game with one additional pebble pair. Otherwise, Spoiler uses one additional pebble pair on (x, x^*) so that $x \in U_2 \cdots U_t$ has weight $t-1$. By Lemma 5.8.11, x^* must be contained in $U_2^* \cdots U_t^*$ and be of weight $t-1$ or otherwise Spoiler can win with $\mathcal{O}(1)$ additional pebble pairs. Again by Lemma 5.8.11, Duplicator must now map $U_2 \cdots U_t$ to $U_2^* \cdots U_t^*$ as long as x is not picked up, so the game reduces to these smaller groups. The d pebbles on U_1 can be reused and we iterate the argument with U_2 and U_2^*.

If Spoiler does not eventually win the game via iterating the strategy described above, then for all i, there must be isomorphisms $\varphi_i : U_i \to U_i^*$ and since the $s = d(Z(G))$ pebble pairs on $(n_1, n_1^*), \ldots, (n_s, n_s^*)$ were never lifted, we have $(\varphi_i)_{|Z(G)} = (\varphi_j)_{|Z(G)}$ for all i and j. But then these local isomorphisms can be glued to a global isomorphism $G \to G^*$ by applying Lemma 5.8.2 inductively. □

Chapter 6

Lower bounds and reductions that preserve the WL-dimension

We now turn to lower bounds, where we either provide explicit examples that certify Weisfeiler-Leman indistinguishability for small dimensions, or we provide combinatorial reductions that (asymptotically) preserve the Weisfeiler-Leman dimension to obtain conditional lower bounds. For example, we show that the WL-dimension of semisimple groups, that is, groups without non-trivial abelian normal subgroups, is at least as high as the WL-dimension of set-extended permutation groups with respect to permutational isomorphism (recall the definition of set-extended structures from Section 3.5).

6.1 WL-dimension of monoids

We briefly consider inverse semigroups, i.e., semigroups with unique inverses (see Definiton 6.1.4), instead of groups and show unbounded Weisfeiler-Leman dimension for the class of inverse semigroups based on the CFI-construction.

We define "graph-capturing" semigroups and discuss their combinatorial properties.

Our results on semigroups also automatically hold for the class of monoids: given a semi-group S, we can always introduce a new symbol, e say, and augment the multiplication on S to $S \cup \{e\}$ making e the new (unique) identity of $S \cup \{e\}$. This does not significantly change the combinatorial properties of S, and the results of this subsection go through unchanged.

We recall a well-known construction of semigroups from graphs. Given a simple graph Γ we define a commutative semi-group S_Γ. We set $S_\Gamma := V(\Gamma) \cup \{E, N, D\}$ together with the following multiplication: For $v, w \in V(\Gamma)$ let $v \cdot w = w \cdot v \in \{E, N\}$ according to wether v and w are connected in Γ (then $vw = E$) or not (then $vw = N$). For all other pairs of elements over S_Γ, define their product as D.

Lemma 6.1.1. *S_Γ is a (commutative) semigroup.*

Proof. We need to show the associativity of multiplication in S_Γ. By definition each product of two elements yields an element from $\{E, N, D\}$ and $\{E, N, D\} \cdot D = \{D\}$, thus for all $a, b, c \in S_\Gamma$ we have $(ab)c = D = a(bc)$. □

Lemma 6.1.2. *If $S_\Gamma \cong S_\Lambda$ then $\Gamma \cong \Lambda$ or $\mathrm{co}(\Gamma) \cong \Lambda$, where $E \in S_\Gamma$ is mapped to $E \in S_\Lambda$ in the first case and $E \in S_\Gamma$ is mapped to $N \in S_\Lambda$ in the second case.*

Proof. We may assume without loss of generality that Γ has at least two distinct vertices. Then for each $v \in V(\Gamma)$, there is some $w \in V(\Gamma)$ with $vw \in \{E, N\}$. On the other hand, for each element x of S_Γ, we have $Ex = Nx = D$, and D is the only element of S_Γ that is idempotent. Hence, D and the set $\{E, N\}$ are both invariant under automorphisms.

Now the claim follows, since the multiplication table of S_Γ restricted to pairs of vertices precisely describes the adjacency matrix of Γ or $\mathrm{co}(\Gamma)$, depending on whether (E, N) is interpreted as $(0, 1)$ or $(1, 0)$. □

We now show that this correspondence between graphs and semigroups also preserves the asymptotic behavior of the WL-dimension.

Lemma 6.1.3. *The* WL*-dimension of semigroups of the form S_Γ, with a simple graph Γ, is unbounded. In particular, this is true with respect to each version of the* WL*-algorithm we introduced above.*

Proof. Since we are only interested in a non-constant bound, in view of Theorem 3.2.25, we can choose to work with the explicit version of the algorithm. Let Γ be a CFI-graph (see 2.2.4) and consider the semigroup S_Γ. Recall that the class of CFI-graphs has unbounded $\mathrm{WL}_{\mathrm{graphs}}$-dimension.

By construction, 2-$\mathrm{WL}_{\mathrm{explicit}}$ distinguishes the elements of $V(\Gamma)$ from the elements E, N and D. Furthermore, by the CFI-construction, we may assume that the number of edges of Γ is linear in the number of vertices. In particular, we may assume that there are more pairs $(x, y) \in V(\Gamma)^2$ with $xy = N$ than pairs with $xy = E$. Consequently, k-$\mathrm{WL}_{\mathrm{explicit}}$ places the elements E, N, and D in singleton color classes, for k large enough.

It is thus sufficient to show that the initial coloring computed by k-$\mathrm{WL}_{\mathrm{explicit}}$ has the same color classes on $V(\Gamma)^k$ as $\mathrm{WL}_{\mathrm{graphs}}$, since the refinement step of both algorithms is identical by definition.

Hence consider two k-tuples $v := (v_1, \ldots, v_k)$ and $w := (w_1, \ldots, w_k)$ over $V(\Gamma)$. Then they obtain the same initial coloring in k-$\mathrm{WL}_{\mathrm{explicit}}$ if and only if $v_iv_j = E$ is equivalent to $w_iw_j = E$ for all $i, j \in [k]$, which is equivalent to the fact that the ordered subgraphs induced on v and w are isomorphic, i.e., equivalent to v and w obtaining the same initial color in k-$\mathrm{WL}_{\mathrm{graphs}}$. □

However, not all semigroups of the from S_Γ do embed into inverse semigroups, and inverse semigroups are arguably more closely related to groups than arbitrary ones. See, for instance, [99] for more background on inverse semigroups and group embeddings.

Definition 6.1.4. A semigroup S is called *inverse* if every $x \in S$ has a unique *inverse* $y \in S$ that fulfills $xyx = x$ and $yxy = y$.

Inverse semigroup isomorphism is *GI-complete* (see [15]), which means that the graph isomorphism problem can be reduced to the isomorphism problem of inverse semigroups in polynomial time. Inspired by this, we can slightly change the construction of semigroups from graphs, as given above, to obtain inverse (idempotent) semi-groups. Towards this end, given a graph Γ, we define T_Γ as $V(\Gamma) \cup E(\Gamma) \cup \{0, 1\}$ together with the following multiplication: All elements are idempotent, for an edge e and a vertex v we have that $e \cdot v$ is v if $v \in e$ and for two edges e, e', their product is v if they intersect in v (then v is unique). Furthermore 1 is the identity and all products not defined thus far are 0. This is essentially the graph Γ regarded as a semi-lattice with 0 and 1 added as minimal and maximal element and then reinterpreted as a semi-group.

Lemma 6.1.5. *T_Γ is an inverse idempotent monoid.*

We highlight that while T_Γ is indeed a monoid with inverses, it is usually not a group, since the inverses are not compatible with the identity element.

Lemma 6.1.6. *The* WL*-dimension of inverse monoids of the form T_Γ, with a simple graph Γ, is unbounded.*

Proof. Let Γ be a simple, undirected graph and consider the inverse monoid T_Γ.

By definition of T_Γ, for a fixed vertex v, the information contained in products $v \cdot x$ with $x \in V(\Gamma) \cup E(\Gamma) \cup \{0, 1\}$ is non-trivial only if x is a vertex adjacent to v or an edge incident with v. In all other cases, either x is contained in $\{v, 1\}$, or $v \cdot x$ is 0, in which case the product does not distinguish between the different possible choices for x. Similar observations hold for all possible products on T_Γ. If we consider the bijective pebble game on monoids of the form T_Γ, this means that a configuration of pebbles can be directly interpreted as a configuration of pebbles on the graph Γ, with the additional possibility that pebbles can be placed, not only on vertices, but also on edges. In other words, the bijective k-pebble game on T_Γ and T_{Γ^*} can be interpreted as the bijective k-pebble game on Γ_E and Γ^*_E, where Γ_E is a simple graph obtained from Γ by subdividing each edge e with a new vertex v_e and giving the set $\{v_e \mid e \in E(\Gamma)\}$ a new color to distinguish these vertices from the old ones. Subdividing edges does not change the fact that the WL-dimension of graphs is unbounded: the CFI-construction still provides examples of unbounded dimension (this is a well-known observation from the theory of WL on graphs, it can be proved using similar arguments as in the proof of Lemma 3.2.20). In other words, the WL-dimension of graphs with edge subdivisions, and hence the WL-dimension of monoids of the form T_Γ, is unbounded. □

6.2 Groups of prime exponent and class 2

We return to groups of prime exponent, where we first devise a condition which guarantees that the 2-dimensional Weisfeiler-Leman algorithm (explicit or implicit) does not distinguish two groups of odd prime exponent and nilpotency class two. Afterwards, we investigate reductions from the isomorphism problem of such groups to an equivalence problem of bilinear maps in the context of the WL-dimension.

The following result explains how the 2-dimensional WL-algorithm essentially only distinguishes groups of prime exponent and class 2 according to their commuting graphs. Recall that the commuting graph $\mathrm{Com}(G)$ of a group G is the simple graph with vertex set G, where any two distinct elements g and h are joined via an edge, if and only if they commute.

Lemma 6.2.1. *Let G and H be groups of exponent p and nilpotency class 2, and assume that $\mathrm{Com}(G) \equiv^2_{\mathrm{graphs}} \mathrm{Com}(H)$ holds, so the commuting graphs are not distinguished by 2-$\mathrm{WL}_{\mathrm{graphs}}$. Then we have $G \equiv^2_{\mathrm{implicit}} H$, so the groups are not distinguished by 2-$\mathrm{WL}_{\mathrm{implicit}}$.*

Proof. The claim holds for groups of exponent 2, as these are the groups C_2^m with $m \in \mathbb{N}$. We thus assume now that p is odd.

Consider the implicit 3-pebble game on (G, H), and further consider a configuration $[(g_1, g_2, \bot), (h_1, h_2, \bot)]$ with the third pebble pair in Spoiler's hands. Assume that the configuration is winning for Duplicator in the pebble game on the commuting graphs and that the pebbled tuples agree with respect to marked isomorphism of generated subgroups. So there is a winning move $f : G \to H$ that Duplicator can play in the pebble game on the commuting graphs, in the given configuration. We claim that f can be chosen such that Spoiler cannot win the pebble game on the groups by placing the third pebble pair. Thus, we reach a new configuration that fulfills the same properties, and Duplicator wins the pebble game on the groups by induction.

Now, for $i \in [2]$, all elements $1 \neq g \in G$ with $g \in \langle g_i \rangle$ are twins with g_i, and due to the pebbles on the board, f has to map twins of g_i to twins of h_i. However, twins can be arbitrarily permuted by the graph's automorphism group, so without loss of generality, we may assume that f maps g_i^m to h_i^m for all $m \in \mathbb{Z}$. Here, we may inductively assume that, for each $m \in \mathbb{N}$, it holds $g_2 = g_1^m$ if and only if $h_2 = h_1^m$ holds: Since G and H have exponent p, any two distinct cyclic subgroups of G or H intersect in the trivial element only.

We now have to show that for all $g \in G$, the marked isomorphism types of (g_1, g) and $(h_1, f(g))$ agree, and the marked isomorphism types of (g, g_2) and $(f(g), h_2)$ agree. By our discussion of twins, we may assume that $g \notin \langle g_i \rangle$ holds. But then the marked isomorphism type of the tuple depends only on the subgraph it induces in the commuting graph: Since G and H have exponent p and class 2, up to isomorphism, there is a unique non-cyclic subgroup generated by two (non-)commuting elements (that is, either the abelian group $C_p \times C_p$ or the non-abelian group $\langle x, y \mid x^p, y^p, [[x, y], x], [[x, y], y] \rangle$ of order p^3). □

A classical tool that is frequently used to tackle the isomorphism problem of groups of class 2 is the concept of *isoclinism*, defined below. In the following, we relate this approach to the Weisfeiler-Leman dimension.

Definition 6.2.2. Two groups G and G^* are *isoclinic*, if there exist group isomorphisms $\alpha\colon G/Z(G) \to G^*/Z(G^*)$ and $\beta\colon G' \to (G^*)'$ such that

$$\forall g, h \in G\colon [\alpha(gZ(G)), \alpha(hZ(G))] = \beta\left([gZ(G), hZ(G)]\right).$$

For (non-abelian) groups of nilpotency class 2, we are in the special situation where isomorphism and isoclinism coincide. This following result is well-known and it can be derived from Baer's correspondence [12] for instance, which we discuss below.

Lemma 6.2.3. *Let G and G^* be non-abelian groups of exponent p and nilpotency class 2. Then G and G^* are isomorphic, if and only if they are isoclinic and of the same order.*

We first interpret the previous lemma in terms of bilinear maps, associating an alternating bilinear space to each group of exponent p and class 2.

Definition 6.2.4. A *(finite) bilinear space* is a finite vector space $V \cong \mathbb{F}_p^n$ together with a bilinear map $b\colon V \times V \to \mathbb{F}_p^m$. We say that (V, b) is alternating if $b(x, y) = -b(y, x)$ holds for all $x, y \in V$. We say that (V, b) as an m-bilinear space if $\mathrm{Im}(b) = \mathbb{F}_p^m$.

We can also interpret a bilinear space as a relational structure on the ground set $V \uplus \mathbb{F}_p^m$ together with a ternary relation $\mathcal{R}_b$ that encodes b, so $(x, y, z) \in \mathcal{R}_b$, if and only if $b(x, y) = z$.

Alternating bilinear spaces are closely related to groups of prime exponent. Through the work of Baer [12], there is a one-to-one correspondence between isoclinism classes of groups of class at most 2, pseudo-isometry classes of certain alternating bilinear spaces, and isomorphism classes of certain nilpotent Lie algebras over $\mathbb{F}_p$ of class 2. We now explore this correspondence for groups of exponent p and in the context of the WL-algorithm.

Definition 6.2.5. Let G be a group of exponent p and nilpotency class 2. Set $n := d(G/G')$ and $m := d(G')$ and let $\varphi\colon G/G' \to \mathbb{F}_p^n$ and $\psi\colon G' \mapsto \mathbb{F}_p^m$ be group isomorphisms. Then the bilinear space associated to G is $\mathcal{B}_G := (\mathbb{F}_p^n, b_G)$, where

$$b_G\colon \mathbb{F}_p^n \times \mathbb{F}_p^n \to \mathbb{F}_p^m, (x, y) \mapsto \psi\left([\varphi^{-1}(x), \varphi^{-1}(y)]\right)$$

is an alternating bilinear map. In the other direction, given an odd prime p and any alternating m-bilinear space $\mathcal{B} = (\mathbb{F}_p^n, b)$, we can construct the group

$$P_{\mathcal{B}} := (\mathbb{F}_p^n \times \mathbb{F}_p^m, *),$$

where $(x, a) * (y, b)$ is defined as $\big(x + y, a + b + \frac{1}{2}b(x, y)\big)$.

Bilinear spaces admit a natural notion of equivalence that generalizes isoclinism of groups of exponent p and class 2.

Definition 6.2.6. Two m-bilinear spaces $\mathcal{B} := (\mathbb{F}_p^n, b)$ and $\mathcal{B}^* := (\mathbb{F}_p^n, b^*)$ are *pseudo-isometric*, if and only if there exist linear automorphisms $\alpha \in \mathrm{GL}_n(\mathbb{F}_p)$ and $\beta \in \mathrm{GL}_m(\mathbb{F}_p)$ with

$$\forall x, y \in \mathbb{F}_p^n\colon b^*(\alpha(x), \alpha(y)) = \beta(b(x, y)).$$

Lemma 6.2.7 (see [12])**.** *Let p be an odd prime. Then the map $P \mapsto \mathcal{B}_p$ between the isomorphism types of groups of exponent p and nilpotency class 2 and the pseudo-isometry classes of alternating bilinear spaces over $\mathbb{F}_p$ is bijective, with inverse $\mathcal{B} \mapsto P_{\mathcal{B}}$. For a group P as above, we have $|P/P'| = p^n$ and $|P'| = p^m$, if and only if $\mathcal{B}_P$ is an m-bilinear space defined on $\mathbb{F}_p^n$.*

The same correspondence has been used in the context of p-groups and group isomorphism (without any relation to the WL-algorithm) in many recent publications, see for instance [109, 51].

We note that it is possible to state the correspondence for slightly different constructions of bilinear spaces from the given groups, where $P/Z(P)$ replaces P/P' and $Z(P)$ replaces P'. In this case, it is not necessarily the case that the resulting bilinear maps are surjective, while with our chosen conventions, the resulting bilinear maps may be degenerate. In fact, with the conventions from above, the center of P (which is isomorphic to the center of $P_{\mathcal{B}_P}$) corresponds to $\{x \in V \mid b(x, V) = 0\} \times \mathrm{Im}(b)$.

Moreover, the Bear correspondence also applies to generating sets of subgroups in the following sense.

Corollary 6.2.8. *Let P and P^* be groups of exponent p and class 2. Consider $g_1, \dots, g_t \in P$ and $g_1^*, \dots, g_t^* \in P^*$, and set $U := \langle g_1, \dots, g_t \rangle$ and $U^* := \langle g_1^*, \dots, g_t^* \rangle$. Let $z_1, \dots, z_m \in U'$ and $z_1^*, \dots, z_m^* \in (U^*)'$. If $g_1P', \dots, g_mP'$ are linearly independent in the elementary abelian group P/P', then the map $g_i \mapsto g_i^*$, $z_j \mapsto z_j^*$ extends to an isomorphism between U and U^*, if and only if there is a pseudo isometry between $\mathcal{B}_U$ and $\mathcal{B}_{U^*}$ that maps g_iP' to $g_i^*(P^*)'$ and z_j to z_j^* for all $i \in [t]$ and $j \in [m]$.*

We now use this to show that the connection between the isomorphism problem of bilinear spaces and the isomorphism problem of groups, as stated above, also holds in terms of the Weisfeiler-Leman dimension.

Lemma 6.2.9. *For an odd prime p, we have that the Weisfeiler-Leman dimension of finite groups of prime exponent and nilpotency class 2 is bounded, if and only if the Weisfeiler-Leman dimension of finite alternating bilinear spaces over $\mathbb{F}_p$ is bounded.*

Proof. Let P and P^* be groups of exponent p (with p odd) and class 2, with $P' \cong (P^*)'$ and $P/P' \cong P^*/(P^*)'$. Fix a system of coset representatives of P/P', say $g_1, \dots, g_t$, and a system of coset representatives of $P^*/(P^*)'$, say $g_1^*, \dots, g_t^*$. Let $\mathcal{B}_P$ and $\mathcal{B}_{P^*}$ the corresponding bilinear spaces from the Bear correspondence, as discussed above.

We now compare the implicit pebble game on (P, P^*) with the implicit pebble game on the bilinear spaces $(\mathcal{B}_P, \mathcal{B}_{P^*})$. Through the Bear correspondence, we identify $\mathcal{B}_P$ with $(P/P', P')$ and $\mathcal{B}_{P^*}$ with $(P^*/(P^*)', (P^*)')$.

Assume first that Spoiler has a winning strategy in the implicit k-pebble game on (P, P^*) for some natural number k. We describe a winning strategy for Spoiler in the implicit $\mathcal{O}(k)$-pebble game on the bilinear spaces. In the latter, in each move Duplicator chooses two bijections $f_1 \colon P/P' \to P^*/(P^*)'$ and $f_2 \colon P' \to (P^*)'$. This defines a bijection $f \colon P \to P^*$ via $f(g_iz) := f_1(g_i)f_2(z)$ for all $i \in [t]$ and $z \in P'$, which we use in the pebble game on the groups as to simulate Duplicator's move and extract a winnig strategy for Spoiler, as a response to Duplicator choosing f. In particular, f maps $\{g_i \mid i \in [t]\}$ to $\{g_i^* \mid i \in [t]\}$ and P' to $(P^*)'$, so we can use Lemma 3.4.5 to consider the restrcited pebble pame instead of the stadard pebble game on (P, P^*). This means that Spoiler can use at most $2k$ pebble pairs, but only ever places them on $\{g_i \mid i \in [t]\} \cup P'$, and Lemma 3.4.5 ensures that Spoiler still has a winning strategy. This stratgey can be copied and applied to the bilinear spaces, interpreting a pebble on g_i as a pebble on g_iP'. By Corollary 6.2.8, a configuration of the restricted pebble game fulfills the winning condition for Spoiler, if and only if the corresponding configuration of the bijective pebble game on the bilinear spaces does (note that here, if z_j is not contained in the derived subgroup of $U := \langle g_1, \dots, g_t \rangle$, then we have $\langle U, z_j \rangle = U \times \langle z_j \rangle$).

In conclusion, if the WL-dimension of finite groups of exponent p and class 2 is bounded, then so is the WL-dimension of the corresponding bilinear spaces, which is the WL-dimension of arbitrary finite alternating bilinear spaces over $\mathbb{F}_p$, thorugh the Bear correspondence.

In the other direction, if Spoiler has a winning strategy on the bilinear spaces, we can obtain a winning strategy for Spoiler on the groups as follows. By Lemma 4.2.12, Duplicator has to map P' to $(P^*)'$ or otherwise Spoiler can win immediately. Then, any Duplicator move $f \colon P \to P^*$ induces a bijection $f_1 \colon P/P' \to P^*/(P^*)'$ by Lemma 3.4.3, and another bijection $f_2 \colon P' \to (P^*)'$ by restriction. These bijections can be used in the game on bilinear spaces to query for Spoiler moves, where again pebbles on g_iP' are interpreted as pebbles on g_i. By Corollary 6.2.8, if a configuration over the bilinear spaces fulfills the winning condition for Spoiler, then so does the corresponding configuration over the groups. □

6.3 Reductions to set-extended pebble games

We recall that we introduced the notion of set-extended structures to deal with the fact that products of group elements over a detectable set X in a group G can, under certain circumstances, be individualized to implicitly fix subsets of X setwise. Here, we investigate some natural choices for G and X and derive algorithmic reductions from the isomorphism problem of G to the isomorphism problem of the set-extended structure formed over X.

For the sake of clarity, we first reiterate the description of the pebble game played on set-extended structures. The *set-extended k-pebble game* on relational structures $\mathfrak{X}$ and $\mathfrak{X}^*$ is the standard k-pebble game, but played on $\mathfrak{X}_{\text{set}-\text{exteded}}$ and $\mathfrak{X}^*_{\text{set}-\text{extended}}$. Here we allow for all versions of the pebble game we discussed in the course of this thesis, see Section 3.2.1. Compared with the pebble game on the original structures, set-extension gives Spoiler the option to fix images for arbitrarily large subsets of $V(\mathfrak{X})$ through pebble pairs on the corresponding set-vertices. We note however, that Duplicator does not have to map set-vertices and original vertices in a consistent way at all times: only *after* Spoiler places a pebble pair on set vertices $(v_S, v^*_{S^*})$, Duplicator has to actually map S to S^*.

6.3.1 Coprime extensions and code equivalence

In general, deciding isomorphism of coprime extensions of order n is at least as hard as code equivalence for binary codes of length $\mathcal{O}(\log n)$, as we recall in the lemma below. First we recall the basic definitions.

Definition 6.3.1. Given a natural number N, a *binary code (of length N)* is a subspace of $\mathbb{F}_2^N$. Two binary codes C and C' in $\mathbb{F}_2^N$ are called *equivalent*, denoted by $C \cong C'$, if there is a permutation $\pi \in \mathrm{Sym}(N)$ such that

$$C^\pi := \big\{ \big(c_{\pi(1)}, \dots, c_{\pi(N)}\big) \mid c \in C \big\} = C'$$

holds.

There are several well-known and important constructions that derive codes of smaller length from a given linear code and thereby inductively describe the code's structure. In the context of this thesis, we recall punctures of a code.

Definition 6.3.2. Let $C \leq \mathbb{F}_q^d$ be a linear code. The *i-th puncture* of C, denoted by $C^{(i)}$, is the code obtained from C by replacing the i-th coordinate of each codeword $c \in C$ with 0 (the resulting code is then the set of all resulting vectors). We say that C *admits reconstruction*, if C can be uniquely recovered from its punctures, that is, if C' is another code such that the multiset of equivalence types of punctures of C and C' agree, then we have $C \cong C'$.

We can now relate binary code equivalence to a special instance of group extension.

Lemma 6.3.3. *Let $C \leq \mathbb{F}_2^N$ be a binary code of size $|C| = 2^d$ and consider the coprime extension $G_C := C_3^N \rtimes_\Delta C_2^d$, where we choose some linear isomorphism $\gamma\colon \mathbb{F}_2^d \to C$ and set*

$$\Delta(x) := \operatorname{diag}\left((-1)^{\gamma(x)_1}, \ldots, (-1)^{\gamma(x)_N}\right) \in \mathrm{GL}_N(\mathbb{F}_3).$$

Then, if C' is another binary code, we have

$$G_C \cong G_{C'} \Leftrightarrow C \cong C'.$$

We point out that the normal copy of C_3^N in a group of the form G_C is twisted-homogeneous regarded as the space of a linear representation, where the representation is induced by the conjugation action in G_C.

The length of C is small compared to the order of G_C, which can generally be exploited by isomorphism algorithms: code equivalence for codes of length N can be solved in time $2^{\mathcal{O}(N)}$, which is polynomial in $|G_C|$. However, the Weisfeiler-Leman dimension of binary codes might still be unbounded.

Definition 6.3.4. Let $C \leq \mathbb{F}_2^n$ be a binary code. We interpret C as a relational structure on the vertex set $C \uplus [n]$, together with the relations

$$\mathcal{R}_{\text{code}} := \{(c, i) \mid c \in C, c_i = 1\}.$$

We explicitly refer to the relational structure as $(C, [n])$. We refer to the vertices in C as *codeword vertices* and to those in $[n]$ as *coordinate vertices.* Additionally, the coordinate vertices receive a special color to distinguish them from codeword vertices. We define the *coordinate-extended* version of a binary code C as the induced substructure of $(C, [n])_{\text{set-extended}}$ which includes exactly those set-vertices that are defined over the coordinate vertices.

So basically, we represent binary codes as bipartite graphs, where codewords are connected to their non-zero coordinates. Importantly, this gives Spoiler the chance to place pebbles on coordinates in the pebble game on codes.

We first derive a constant upper bound on the class of those binary codes that admit reconstruction.

Lemma 6.3.5. *Let $\mathcal{C}$ be a class of linear codes that is closed under punctures and assume that each code in $\mathcal{C}$ admits reconstruction. Let $\mathcal{C}^+$ denote the class of coordinate-extended structures formed over the codes in $\mathcal{C}$. Then the implicit Weisfeiler-Leman dimension of $\mathcal{C}^+$ bounded by* 3*.*

Proof. Let C and C' be two non-equivalent codes of length n from $\mathcal{C}$. To prove the bound on the WL-dimension, in view of Lemma 3.2.13, we consider the implicit 4-pebble game on $((C, [n])_{\text{coordinate-extended}}, (C', [n])_{\text{coordinate-extended}})$. We need to show that Spoiler has a winning strategy, starting from the empty initial configuration.

For every possible bijection $f\colon (C, [n])_{\text{coordinate-extended}} \to (C', [n])_{\text{coordinate-extended}}$ that Duplicator may choose throughout the game, f has to map the codewords of C to those of C' and f has to map coordinates of C to coordinates of C'. Otherwise, Spoiler can win, since by the definition of set-extended structures and codes as relational structures, codeword vertices, coordinate vertices and set-vertices are distinguishable from each other.

By assumption, there does not exist an equivalence-type preserving bijection between the punctures of C and C'. Thus, if f is any Duplicator move, then there is some coordinate, say i, such that $C^{(i)}$ is not equivalent to $(C')^{(f(i))}$. Spoiler can thus place a pebble pair on $(i, f(i))$. By assumption, $C^{(i)}$ and $(C')^{(f(i))}$ are again non-equivalent codes from $\mathcal{C}$, so we can iterate the argument: in the next round, Spoiler uses an additional pebble pair to place a pebble on $(j, f'(j))$ such that $(C^{(i)})^{(j)}$ is not equivalent to $(C^{(f(i))})^{(f'(j))}$, where j is chosen depending on Duplicator's bijection f', in the same way i was chosen depending on f. With the current pebbles on the board, Duplicator needs to map the set vertex $\{i, j\}$ to $\{f(i), f'(j)\}$, or otherwise Spoiler can easily win. But then Spoiler can use another additional pebble pair to place a pebble on $(\{i, j\}, \{f(i), f'(j))$, and subsequently lift and re-use the pebbles on i and j. Progress for Spoiler has now been achieved, since $(C^{(i)})^{(j)}$ is not equivalent to $(C^{(f(i))})^{(f'(j))}$, where the number of the non-zero coordinates in these punctures is one less compared to $C^{(i)}$ and $(C')^{(f(i))}$. Spoiler can iterate this strategy and eventually reach a configuration with a pebble pair on set-vertices (I, I'), such that $[n] \setminus I$ and $[n] \setminus I'$ are singleton sets, and the iterated punctures $C^{(I)}$ and $(C')^{(I')}$ are non-equivalent. That is, Duplicator loses if the next bijection does not map I to I', but otherwise Duplicator is forced to map a zero-coordinate of C to a non-zero coordinate of C' (or vice versa). In either case, Spoiler can easily use the additional pebble pairs to win the game. □

The argument of the previous lemma equally applies to graphs, as discussed in the following corollary.

Definition 6.3.6. A graph Γ *is reconstructible*, if it is uniquely defined, up to isomorphism, by the multiset of isomorphism types of its induced subgraphs with $|V(\Gamma)| - 1$ vertices.

The famous reconstruction conjecture states that all graphs admit reconstruction. In the general case, the conjecture is currently still open, while it has been proved for some special classes of graphs, such as regular graphs or graphs with up to 13 vertices [85], see also the survey [60].

Corollary 6.3.7. *Let $\mathcal{C}$ be a class of graphs that are reconstructible, such that all induced subgraphs of graphs in $\mathcal{C}$ are again reconstructible. Let $\mathcal{C}^+$ be the class of set-extended structures over graphs in $\mathcal{C}$. Then the implicit Weisfeiler-Leman dimension of $\mathcal{C}^+$ is bounded by* 3*.*

In other words, if the reconstruction conjecture holds, then the WL-dimension of set-extended graphs is bounded by a constant.

Returning to isomorphism of coprime extensions, we show that the construction of coprime extensions from binary codes does not only preserve isomorphism and non-isomorphism, but also the Weisfeiler-Leman dimension.

Lemma 6.3.8. *Let $C \leq \mathbb{F}_2^n$ be a binary code. Then we have*

$$\dim_{\mathrm{WL}}(G_C) \in \Theta\left(\dim_{\mathrm{WL}}((C, [n])_{\textit{coordinate-extended}})\right).$$

Proof. Consider two non-isomorphic binary codes C_1 and C_2 of length n, and set $G_i := G_{C_i}$. For $i \in [2]$, write $G_i := N_i \rtimes C_i$, with $N_i \cong \mathbb{F}_3^n$, so we identify the code C_i with a fixed semidirect complement of N_i in G_i. We can regard N_i as a representation module for C_i, where the representation induced by the conjugation action in G_i. Then, via Lemma 5.7.12, we may assume up to multiplication of the WL-dimension by a constant, that each irreducible constituent of N_i is unique up to equivalence. By construction of G_i, this is equivalent to C_i not having repeated coordinates. To prove the present lemma, we now show that Spoiler can construct a winning strategy in the pebble game on (G_1, G_2) from a winning strategy in the pebble game on the coordinate-extended versions of C_1 and C_2, and vice versa. In each direction, the number of pebble pairs used in the corresponding strategies will be related by a constant factor.

First assume that Spoiler has a winning strategy in the implicit k-pebble game on the coordinate-extended codes. Since each irreducible constituent of N_i is uniue up to equivalence, the generators for a fixed irreducible constituent of N_i correspond to one coordinate of the binary code C_i. Spoiler obtains a winning strategy in the implicit $(k + \mathcal{O}(1))$-pebble game on (G_1, G_2) by identifying coordinate vertices of the codes with the generators of the corresponding irreducible constituent and identifying each codeword $c \in C_i$ with the corresponding group element cN_i the quotient group G_i/N_i. Since the properties of the codeword only depend on the induced conjugation action on N_i, and thus only depend on the coset cN_i, winning configurations for Spoiler in the two different pebble games correspond to each other in this identification. It remains to be argued that Duplicator must map coordinates to coordinates in this identification, i.e, map elements in irreducible constituents of N_1 to elements in irreducible constituents of N_2. But since each irreducible constituent of N_i is unique up to equivalence, these elements are exactly those that generate subgroups of N_1 and N_2 that are minimal normal in G_1 and G_2, respectively. The set of such elements is $\mathcal{O}(1)$-$\mathrm{WL}_{\mathrm{implicit}}$-detectable as a consequence of Lemma 4.1.4.

In the other direction, assume that Spoiler has a winning strategy in the implicit k-pebble game on (G_1, G_2). Via Lemma 3.4.5, Spoiler then has a winning stratgey in the restricted $\mathcal{O}(k)$-pebble game with respect to the normal subgroups N_1 and N_2 and the fixed semidirect complements C_1 and C_2. As before, Duplicator has to map elements in minimal normal subgroups to elements in minimal normal subgroups to not lose immediately, and then we can again identify irreducible consitutents of N_i with coordinates of C_i. In this identification, the winning strategy for Spoiler in the restricted pebble game directly corresponds to a winning strategy in the pebble game on the domain extended codes (since the elements in minimal normal subgroups are $\mathcal{O}(1)$-$\mathrm{WL}_{\mathrm{implicit}}$-detetable, via Lemma 3.4.8, Spoiler can use pebbles on products of such elements as pebbles on sets of coordinates). □

6.3.2 Semisimple groups and permutational isomorphism

The ideas from the previous section on code equivalence can be used similarly in the context of semisimple groups and permutational isomorphism. In the case of semisimple groups, we are particularly concerned with groups of the form $A_5^n \rtimes Q$ for arbitrary permutation groups $Q \leq S_n$, permuting the different copies of A_5. We show that boundedness of the WL-dimension of domain-extended permutaton groups is equivalent to boundedness of the WL-dimension of this class of semisimple groups.

Before, we encoded a binary code through the conjugation action in a semidirect product of groups, whereas here, we encode the permutational equivalence type of Q in the induced conjugation action of the semidirect product $A_5^n \rtimes Q$. Since Q acts faithfully on the copies of A_5, the group $A_5^n \rtimes Q$ is indeed semisimple.

Lemma 6.3.9. *Let $Q \leq \mathrm{Sym}(\Omega)$ and $Q^* \leq \mathrm{Sym}(\Omega^*)$ be permutation groups. Consider the semisimple groups $G := S \rtimes Q$ and $G^* := S^* \rtimes Q^*$, whose socles are given by $S := \times_{\omega\in\Omega} A_5$ and $S^* := \times_{\omega^*\in\Omega^*} A_5$, repsectively. If $\mathcal{O}(k)$-$\mathrm{WL}_{\mathrm{explicit}}$ does not distinguish $(Q,\Omega)_{domain\text{-}extended}$ from $(Q^*,\Omega^*)_{domain\text{-}extended}$, then k-$\mathrm{WL}_{\mathrm{explicit}}$ does not distinguish G from G^*.*

Proof. By Lemma 3.4.5, we may consider the restricted pebble game, where Spoiler agrees to only ever place pebbles in $Q \cup S$ and $Q^* \cup S^*$ and Duplicator always maps Q to Q^* and S to S^* (so here we treat Q and Q^* as concrete subgroups of G and G^*, respectively, which is possible by the semidirect structure of G and G^*). So assume that Spoiler has a winning strategy in the restricted k-pebble game. We show how Spoiler can then win the explicit k-pebble game on $(Q,\Omega)_{\text{domain-extended}}$ and $(Q^*,\Omega^*)_{\text{domain-extended}}$. By definition of domain-extended permutation groups, domain-vertices, set-vertices and group elements are distinguishable from each other, so Duplicator has to respect these types of different vertices or otherwise Spoiler can win immediately. Thus, we may assume that any bijection f Duplicator chooses in the pebble game on the domain-extended permutation groups induces two bijections $f_1\colon \Omega \to \Omega^*$ and $f_2\colon Q \to Q^*$. We define a bijection $f\colon G \to G^*$ via

$$((a_\omega)_{\omega\in\Omega}, \pi) \mapsto ((a_{f_1(\omega)})_{\omega\in\Omega}, f_2(\pi)).$$

Spoiler can use this bijection to simulate one step of the winning strategy in the pebble game on (G, G^*) as a response to Duplicator choosing the bijetion f. Here, a pebble on $a_\omega \in S$ is interpreted as a pebble on $\omega \in \Omega$ and more generally, a pebble on $(a_\omega)_{\omega\in\Omega} \in S$ is interpreted as a pebble on the set-vertex $\{\omega \in \Omega \mid a_\omega \neq 1\}$. If Spoiler reaches a winning configuration in the game on (G, G^*), then there are two possibilities: Either there are pebble pairs on (π_1, π_1^*), (π_2, π_2^*), and (π_3, π_3^*), with $\pi_i \in Q$ and $\pi_i^* \in Q^*$, such that exactly one of $\pi_1\pi_2 = \pi_3$ and $\pi_1^*\pi_2^* = \pi_3^*$ holds. In this case the corresponding pebble pairs also fulfill the winning condition for Spoiler in the game on the domain-extended permutation groups. Or there are pebble pairs on (π, π^*), $((a_\omega)_{\omega\in\Omega}, (a^*_{\omega^*})_{\omega^*\in\Omega^*})$, and $((b_\omega)_{\omega\in\Omega}, (b^*_{\omega^*})_{\omega^*\in\Omega^*})$, with $\pi \in Q$, $\pi^* \in Q^*$, $(a_\omega)_{\omega\in\Omega}, (b_\omega)_{\omega\in\Omega} \in S$, and $(a^*_{\omega^*})_{\omega^*\in\Omega^*}), (b^*_{\omega^*})_{\omega^*\in\Omega^*}) \in S^*$, such that exactly one of $(a_\omega)_{\omega\in\Omega})^\pi = (b_\omega)_{\omega\in\Omega})$ and $(a^*_{\omega^*})_{\omega^*\in\Omega^*})^\pi = (b^*_{\omega^*})_{\omega^*\in\Omega^*})$ holds. Since we explicitly chose Duplicator's moves as above, this can only happen if $\{\omega \mid a_\omega \neq 1\}^\pi \neq \{\omega \mid b_\omega \neq 1\}$ or $\{\omega^* \mid a_{\omega^*} \neq 1\}^{\pi^*} \neq \{\omega \mid b_{\omega^*} \neq 1\}$ holds, in which case the corresponding configuration in the game on domain extended sructures again fulfills the winning condition for Spoiler. □

Together with Lemma 5.4.3, we obtain the follwoing asymptotic equivalence.

Corollary 6.3.10. *The* WL*-dimension of semisimple groups of the from $S^n \rtimes Q$ with S non-abelian simple and $Q \leq S_n$ is bounded, if and only if, the* WL*-dimension of domain-extended permutation groups is bounded.*

Appendix: overview

The appendix contains further referential information, namely parts of the GAP-code we utilized in the preparation of this thesis, including a (non-optimized) version of the 2-dimensional Weisfeiler-Leman algorithm for groups in Appendix A, as well as presentations of groups we explicitly use in the thesis. For reasons of simplicity, we only reference concrete groups in terms of their identifier in the Small Groups Library in GAP [43]. To ensure that the results presented here remain correct and comprehensible, independent of the Small Groups Library, we list presentations for all groups we explicitly reference in Appendix B.

An overview of our explicit computational results can be found in Section 5.1. Further, concrete groups are discussed as examples or to certify the necessity of certain assumptions in Chapter 4.

Appendix A

GAP implementation of 2-WL$_{\text{implicit}}$

```
OrderedGroupList := function(S)
 local orbit, g, s;
   orbit := [S[1]];
   for g in orbit do
        for s in S do
            if not g*s in orbit then
                Add(orbit,g*s);
            fi;
        od;
   od;
   return orbit;
end;
IsomorphismByImages := function(gen,im)
 local G1,G2,i,j,len;
   G1 := OrderedGroupList(gen);
   G2 := OrderedGroupList(im);
   len := Length(G1);
   if len <> Length(G2) then return false; fi;
   if len <> Order(Group(gen)) then return false; fi;
   if len <> Order(Group(im)) then return false; fi;
   for i in [ 1 .. Length(gen) ] do
      if Position(G1,gen[i]) <> Position(G2,im[i]) then return false; fi;
   od;
   for i in [ 1 .. len ] do
      for j in [ 1 .. len ] do
         if Position(G1,G1[i]*G1[j]) <> Position(G2,G2[i]*G2[j]) then
            return false;
         fi;
      od;
   od;
   return true;
end;
```

```
WeisfeilerLeman2 := function(G,colMat,initCol,precol)
 local c1,c2,M,l,i,j,k,m,n,Gij,gi,gj,c,iterateColourMat,colourMat,colours,
test,listG,newColour;
   l := Order(G);
   listG := Elements(G);
   colours := [];
   colourMat := [];
   for i in [ 1 ..  l ] do       colourMat[i] := [];
      for j in [ 1 ..  l ] do          colourMat[i][j] := [];
      od;
   od;
   if initCol then
      colourMat := MutableCopyMat(colMat);
   else
      for i in [ 1 ..  l ] do
         for j in [ 1 ..  l ] do
            gi := listG[i];
            gj := listG[j];
            newColour := true;
            for k in [1..Size(colours)] do
               c := colours[k];
               if not IsEmpty(precol) then
                  c1 := Position(listG,c.gen1);
                  c2 := Position(listG,c.gen2);
                  if not (precol[i]=precol[c1] and precol[j] = precol[c2])
then continue;
                  fi;
               fi;
               test := GroupHomomorphismByImages(Group(gi,gj),Group(c.gen1,c.gen2),
   [gi,gj],[c.gen1,c.gen2]);
               if not test=fail then
                  if IsBijective(test) then
                     if Image(test,gi) = c.gen1 and Image(test,gj)=c.gen2 then
                        colourMat[i][j] := k;
                        newColour := false;
                        break;
                     fi;
                  fi;
               fi;
            od;
            if newColour then
               test := rec(gen1:=gi,gen2:=gj);
               Add(colours,test);
               colourMat[i][j] := Size(colours);
            fi;
         od;
      od;
   fi;
   while true do
   iterateColourMat := NullMat(l,l);
   k := Size(colours);
   colours := [];
   for i in [ 1 ..  l ] do
      for j in [ 1 ..  l ] do
         test := [];
            for n in [ 1 ..  l ] do
               Add(test,[colourMat[i][n],colourMat[n][j]]);
            od;
            newColour :=[1..l];
            for n in [ 1 ..  Size(test) ] do
               newColour[n] := [test[n],Size(Positions(test,test[n]))];
            od;
            test := [colourMat[i][j],Set(newColour)];
            m := Position(colours,test);
            if m=fail then
               Add(colours,test);
               iterateColourMat[i][j] := Size(colours);
            else
               iterateColourMat[i][j] := m;
            fi;
         od;
      od;
      if Size(colours)=k then
         return colourMat;
      fi;
      colourMat:=MutableCopyMat(iterateColourMat);
   od;
end;
```

```
WeisfeilerLemanPairing := function(G,H)
 local colG,colH,tmp,hi,hj,c1,c2,M,l,i,j,k,m,n,Gij,gi,gj,c,iterateColourMatG,
iterateColourMatH,colourMatG,colourMatH,colours,test,listG,listH,newColour;
   l := Order(G);
   listG := Elements(G);
   listH := Elements(H);
   colours := [];
   colourMatG := [];
   colourMatH := [];
   for i in [ 1 ..  l ] do
      colourMatG[i] := [];
      colourMatH[i] := [];
      for j in [ 1 ..  l ] do
         colourMatG[i][j] := [];
         colourMatH[i][j] := [];
      od;
   od;
   for i in [ 1 ..  l ] do
      for j in [ 1 ..  l ] do
         gi := listG[i];
         gj := listG[j];
         newColour := true;
         for k in [1..Size(colours)] do
            c := colours[k];
            test := IsomorphismByImages([gi,gj],[c.gen1,c.gen2]);
            if test then
               colourMatG[i][j] := k;
               newColour := false;
               break;
            fi;
         od;
         if newColour then
            test := rec(gen1:=gi,gen2:=gj);
            Add(colours,test);
            colourMatG[i][j] := Size(colours);
         fi;
         newColour := true;
         hi := listH[i];
         hj := listH[j];
         for k in [1..Size(colours)] do
            c := colours[k];
            test := IsomorphismByImages([hi,hj],[c.gen1,c.gen2]);
            if test then
               colourMatH[i][j] := k;
               newColour := false;
               break;
         fi;
      od;
      if newColour then
         test := rec(gen1:=hi,gen2:=hj);
         Add(colours,test);
         colourMatH[i][j] := Size(colours);
      fi;
   od;
od;
while true do
   iterateColourMatG := NullMat(l,l);
   iterateColourMatH := NullMat(l,l);
   k := Size(colours);
   colG := [];
   for i in [ 1 ..  k ] do
      Add(colG,Size(Positions(Concatenation(colourMatG),i)));
   od;
   colH := [];
   for i in [ 1 ..  k ] do
      Add(colH,Size(Positions(Concatenation(colourMatH),i)));
   od;
   if not colG = colH then return [false,colourMatG,colourMatH]; fi;
   colours := [];
   for i in [ 1 ..  l ] do
      for j in [ 1 ..  l ] do
         test := [];
         for n in [ 1 ..  l ] do
            Add(test,[colourMatG[i][n],colourMatG[n][j]]);
         od;
         newColour :=[1..l];
         tmp := Set(test);
         for n in [ 1 ..  Size(tmp) ] do
            newColour[n] := [tmp[n],Size(Positions(test,tmp[n]))];
         od;
         test := [colourMatG[i][j],Set(newColour)];
         m := Position(colours,test);
         if m=fail then
            Add(colours,test);
            iterateColourMatG[i][j] := Size(colours);
         else
            iterateColourMatG[i][j] := m;
         fi;
         test := [];
         for n in [ 1 ..  l ] do
            Add(test,[colourMatH[i][n],colourMatH[n][j]]);
         od;
```

```
            newColour :=[1..l];
            tmp := Set(test);
            for n in [ 1 ..  Size(tmp) ] do
               newColour[n] := [tmp[n],Size(Positions(test,tmp[n]))];
            od;
            test := [colourMatH[i][j],Set(newColour)];
            m := Position(colours,test);
            if m=fail then
               Add(colours,test);
               iterateColourMatH[i][j] := Size(colours);
            else
               iterateColourMatH[i][j] := m;
            fi;
         od;
      od;
      if Size(colours)=k then
         return [true,colourMatG,colourMatH];
      fi;
      colourMatG:=MutableCopyMat(iterateColourMatG);
      colourMatH:=MutableCopyMat(iterateColourMatH);
   od;
end;
```

Appendix B

Presentations for selected groups

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,171))));
  [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F4^-1,
F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,1122))));
  [ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1*F6^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-
1*F2^-1*F3*F2*F7^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-
1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6,
F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,164))));
  [ F1^2*F5^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1, F4^-1*F1^-1*F4*F1,
F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F6^-1, F3^-1*F2^-
1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-
1*F7*F2, F3^2*F7^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,999))));
  [ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1, F4^-1*F1^-1*F4*F1,
F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F7^-1, F3^-1*F2^-
1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-
1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,165))));
  [ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F7^-1,
F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-
1*F2^-1*F7*F2, F3^2, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]

gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,1011))));
  [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1*F6^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-
1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-
1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]

gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,166))));
  [ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F7^-1,
F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-
1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]

gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,1014))));
  [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1*F6^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F6^-1*F5^-
1, F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-
1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6,
F7^2 ]

gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,167))));
  [ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F7^-1,
F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-
1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]

gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,1013))));
  [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1*F6^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F6^-1,
F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-
1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,171))));
   [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F4^-1,
F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3,
F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4,
F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,1122))));
   [ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1*F6^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-
1*F2^-1*F3*F2*F7^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-
1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6,
F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,173))));
   [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F4^-1,
F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-
1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6,
F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,1126))));
   [ F1^2*F5^-1, F2^-1*F1^-1*F2*F1*F5^-1, F3^-1*F1^-1*F3*F1*F6^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F6^-1*F5^-
1, F3^-1*F2^-1*F3*F2*F7^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-
1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6,
F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,174))));
   [ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F5^-1,
F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2,
F7^-1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-
1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6,
F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,177))));
[ F1^2*F7^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F5^-1*F4^-1, F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-1*F7*F2, F3^2*F5^-1*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,555))));
[ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-1*F4*F1, F5^-1*F1^-1*F5*F1*F7^-1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3*F7^-1, F6^-1*F3^-1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4, F5^2*F7^-1, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,556))));
[ F1^2*F6^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-1*F4*F1, F5^-1*F1^-1*F5*F1*F7^-1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-1*F7*F2, F3^2*F7^-1*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3*F7^-1, F6^-1*F3^-1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4, F5^2*F7^-1, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,807))));
[ F1^2*F5^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3*F7^-1, F6^-1*F3^-1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4, F5^2*F7^-1, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,808))));
[ F1^2*F5^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2, F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2, F7^-1*F2^-1*F7*F2, F3^2*F7^-1*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3*F7^-1, F6^-1*F3^-1*F6*F3, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4, F7^-1*F4^-1*F7*F4, F5^2*F7^-1, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,831))));
   [ F1^2*F4^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F5^-1*F4^-
1, F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-1*F6*F2*F7^-
1, F7^-1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3, F6^-1*F3^-
1*F6*F3*F7^-1, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-1*F6*F4,
F7^-1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2*F7^-1, F7^-
1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(128,832))));
   [ F1^2*F4^-1, F2^-1*F1^-1*F2*F1*F4^-1, F3^-1*F1^-1*F3*F1*F5^-1, F4^-1*F1^-
1*F4*F1, F5^-1*F1^-1*F5*F1, F6^-1*F1^-1*F6*F1, F7^-1*F1^-1*F7*F1, F2^2*F7^-1*F5^-
1*F4^-1, F3^-1*F2^-1*F3*F2*F6^-1, F4^-1*F2^-1*F4*F2, F5^-1*F2^-1*F5*F2, F6^-1*F2^-
1*F6*F2*F7^-1, F7^-1*F2^-1*F7*F2, F3^2*F4^-1, F4^-1*F3^-1*F4*F3, F5^-1*F3^-1*F5*F3,
F6^-1*F3^-1*F6*F3*F7^-1, F7^-1*F3^-1*F7*F3, F4^2, F5^-1*F4^-1*F5*F4, F6^-1*F4^-
1*F6*F4, F7^-1*F4^-1*F7*F4, F5^2, F6^-1*F5^-1*F6*F5, F7^-1*F5^-1*F7*F5, F6^2*F7^-
1, F7^-1*F6^-1*F7*F6, F7^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(36,3))));
   [ F1^3*F2^-1, F2^-1*F1^-1*F2*F1, F3^-1*F1^-1*F3*F1*F4^-1*F3^-1, F4^-1*F1^-
1*F4*F1*F3^-1, F2^3, F3^-1*F2^-1*F3*F2, F4^-1*F2^-1*F4*F2, F3^2, F4^-1*F3^-1*F4*F3,
F4^2 ]
```

```
gap> RelatorsOfFpGroup(Image(IsomorphismFpGroup(SmallGroup(72,3))));
   [ F1^3*F2^-1, F2^-1*F1^-1*F2*F1, F3^-1*F1^-1*F3*F1*F5^-1*F4^-1*F3^-1, F4^-
1*F1^-1*F4*F1*F5^-1*F3^-1, F5^-1*F1^-1*F5*F1, F2^3, F3^-1*F2^-1*F3*F2, F4^-1*F2^-
1*F4*F2, F5^-1*F2^-1*F5*F2, F3^2*F5^-1, F4^-1*F3^-1*F4*F3*F5^-1, F5^-1*F3^-1*F5*F3,
F4^2*F5^-1, F5^-1*F4^-1*F5*F4, F5^2 ]
```

Bibliography

[1] A. Abdollahi, S. Akbari, and H. R. Maimani. Non-commuting graph of a group. *Journal of Algebra*, 298(2):468–492, 2006.

[2] M. Anders. dejavu. `http://alg.cs.uni-kl.de/team/anders/dejavu/`. Accessed: 2023-07-10.

[3] M. Anders and P. Schweitzer. Engineering a fast probabilistic isomorphism test. In *Proceedings of the Symposium on Algorithm Engineering and Experiments (ALENEX 2021)*, pages 73–84. SIAM, 2021.

[4] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2nd edition, 2000.

[5] A. Atserias, A. Bulatov, and A. Dawar. Affine systems of equations and counting infinitary logic. *Theoretical Computer Science*, 410(18):1666–1683, 2009.

[6] L. Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In *Proceedings of the 48th Annual Symposium on Theory of Computing (STOC 2016)*, pages 684–697. ACM, 2016.

[7] L. Babai and R. Beals. A polynomial-time theory of black-box groups I. *London Mathematical Society Lecture Note Series*, volume 260:30–64, 1999.

[8] L. Babai, P. Codenotti, J. A. Grochow, and Y. Qiao. Code equivalence and group isomorphism. In *Proceedings of the 22nd Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2011)*, pages 1395–1408. SIAM, 2011.

[9] L. Babai, P. Codenotti, and Y. Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups. In *Proceedings of the 39th International Colloquium on Automata, Languages and Programming (ICALP 2012)*, pages 51–62. Springer Berlin Heidelberg, 2012.

[10] L. Babai, P. Erdős, and S. M. Selkow. Random graph isomorphism. *SIAM Journal on Computing*, 9(3):62—635, 1980.

[11] L. Babai and Y. Qiao. Polynomial-time isomorphism test for groups with abelian sylow towers. In *Proceedings of the 29th International Symposium on Theoretical Aspects of Computer Science (STACS 2012)*, volume 14 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 453–464. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2012.

[12] R. Baer. Groups with abelian central quotient group. *Transactions of the American Mathematical Society*, 44(3):357–386, 1938.

[13] H. A. Bender. A determination of the groups of order p^5. *Annals of Mathematics*, 29(1):61–72, 1927.

[14] H. U. Besche, B. Eick, and E. A. O'Brien. The groups of order at most 2000. *Electronic Research Announcements of The American Mathematical Society*, 7:1–4, 2001.

[15] K. S. Booth and S. J. Colbourn. Problems polynomially equivalent to graph isomorphism. *Technical Report CS-77-04*, 1977.

[16] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997.

[17] J. Brachter and P. Schweitzer. On the Weisfeiler-Leman Dimension of Finite Groups. In *Proceedings of the 35th Annual Symposium on Logic in Computer Science (LICS 2020)*, pages 287–300. ACM, 2020.

[18] J. Brachter and P. Schweitzer. A systematic study of isomorphism invariants of finite groups via the Weisfeiler-Leman dimension. In *Proceedings of the 30th Annual European Symposium on Algorithms (ESA 2022)*, volume 244 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 27:1–27:14. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2022.

[19] S. Brenner. Tuple regularity and k-ultrahomogeneity for finite groups. *Preprint, arXiv:2307.08298 [math.GR]*, 2023.

[20] J. Britton. Boone William W.. The word problem. Annals of mathematics, vol. 70 (1959), pp. 207–265. *The Journal of Symbolic Logic*, 27:238–241, 2014.

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

[22] P. A. Brooksbank, Y. Li, Y. Qiao, and J. B. Wilson. Improved algorithms for alternating matrix space isometry: From theory to practice. In *Proceedings of the 28th Annual European Symposium on Algorithms (ESA 2020)*, volume 173 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 26:1–26:15. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2020.

[23] P. A. Brooksbank, J. Maglione, and J. B. Wilson. A fast isomorphism test for groups whose Lie algebra has genus 2. *Journal of Algebra*, 473:545–590, 2017.

[24] J.-Y. Cai, M. Furer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS 1989)*, pages 612–617. IEEE, 1989.

[25] P. J. Cameron. 6-transitive graphs. *Journal of Combinatorial Theory. Series B*, 28(2):168–179, 1980.

[26] P. J. Cameron. *Projective and polar spaces*, volume 13 of *QMW Maths Notes.* Queen Mary and Westfield College, School of Mathematical Sciences, London, 1992.

[27] P. J. Cameron. *Strongly regular graphs*, volume 102 of *Encyclopedia of Mathematics and its Applications*, pages 203–221. Cambridge Univ Press, 2004.

[28] F. Celler, J. Neubüser, and C. R. B. Wright. *Some remarks on the computation of complements and normalizers in soluble groups*, pages 57–76. Springer Dordrecht, 1990.

[29] G. Chen, Q. Ren, and I. Ponomarenko. On multidimensional Schur rings of finite groups. *Preprint, arXiv:2302.01114 [math.GR]*, 2023.

[30] H. Dietrich and J. B. Wilson. Polynomial-time isomorphism testing of groups of most finite orders. *Preprint, arXiv:1806.08872 [CoRR]*, 2018.

[31] H. Dietrich and J. B. Wilson. Group isomorphism is nearly-linear time for most orders. In *Proceedings of the 62nd Annual Symposium on Foundations of Computer Science (FOCS 2021)*, pages 457–467. IEEE, 2021.

[32] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics.* Springer New York, 2012.

[33] K. Dutta and A. Prasad. Degenerations and orbits in finite abelian groups. *Journal of Combinatorial Theory. Series A*, 118(6):1685–1694, 2011.

[34] B. Eick and M. Horn. The construction of finite solvable groups revisited. *Journal of Algebra*, 408:166–182, 2014.

[35] B. Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Communications in Algebra*, 30(5):2271–2295, 2002.

[36] B. Eick and E. A. O'Brien. Enumerating p-groups. *Journal of the Australian Mathematical Society*, 67(2):191–205, 1999.

[37] S. Evdokimov and I. Ponomarenko. On highly closed cellular algebras and highly closed isomorphisms. *Electronic Journal of Combinatorics*, 6, 1999.

[38] F. Fuhlbrück, J. Köbler, I. Ponomarenko, and O. Verbitsky. The Weisfeiler-Leman algorithm and recognition of graph properties. *Theoretical Computer Science*, 895:96–114, 2021.

[39] F. Fuhlbrück, J. Köbler, and O. Verbitsky. Local WL invariance and hidden shades of regularity. *Discrete Applied Mathematics*, 305:191–198, 2021.

[40] M. Fürer. On the combinatorial power of the Weisfeiler-Lehman algorithm. In *Proceedings of the International Conference on Algrotihms and Complexity (CIAC 2017)*, volume 10236 of *Lecture Notes in Computer Science*, pages 260–271. Springer, 2017.

[41] F. Le Gall. Efficient isomorphism testing for a class of group extensions. In *Proceedings of the 26th International Symposium on Theoretical Aspects of Computer Science (STACS 2009)*, volume 3 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 625–636. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2009.

[42] F. Le Gall and D. J. Rosenbaum. On the group and color isomorphism problems. *Preprint, arXiv:1609.08253 [cs.CC]*, 2016.

[43] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.12.2*, 2022.

[44] G. Glauberman and L. Grabowski. Groups with identical k-profiles. *Theory of Computing*, 11(15):395–401, 2015.

[45] W. Gomaa. Descriptive complexity of finite abelian groups. *International Journal of Algebra and Computation*, 20(8):1087–1116, 2010.

[46] D. Gorenstein. *Finite groups*, volume 301 of *AMS Chelsea Publishing Series*. American Mathematical Society, 2007.

[47] T. Gowers. Comment on Dick Lipton's blog: The group isomorphism problem: A possible polymath problem? Blog entry: November 7, 2011, Comment: November 12, 2011. https://rjlipton.wordpress.com/2011/11/07/the-group-isomorphism-problem-a-possible-polymath-problem/.

[48] J. A. Grochow and M. Levet. Weisfeiler-Leman for group isomorphism: Action compatibility. *Preprint, arXiv:2112.11487 [CoRR]*, 2021.

[49] J. A. Grochow and Y. Qiao. Algorithms for group isomorphism via group extensions and cohomology. *Preprint, arXiv:1309.1776 [cs.DS]*, 2017.

[50] J. A. Grochow and Y. Qiao. Isomorphism problems for tensors, groups, and cubic forms: Completeness and reductions. *Preprint, arXiv:1907.00309 [cs.CC]*, 2019.

[51] J. A. Grochow and Y. Qiao. On p-group isomorphism: Search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. In *Proceedings of the 36th Computational Complexity Conference (CCC 2021)*, volume 200 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 16:1–16:38. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2021.

[52] J. A. Grochow and Y. Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: tensor isomorphism-completeness. In *Proceedings of the 12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, volume 185 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 31:1–31:19. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2021.

[53] J. A. Grochow and Y. Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials IV: linear-length reductions and their applications. *Preprint, arXiv:2306.16317 [cs.CC]*, 2023.

[54] M. Grohe. *Descriptive complexity, canonisation, and definable graph structure theory*, volume 47 of *Lecture Notes in Logic*. Cambridge University Press, 2017.

[55] M. Grohe and J. Mariño. Definability and descriptive complexity on databases of bounded tree-width. In *Proceedings of the 7th International Conference on Database Theory (ICDT 1999)*, volume 1540 of *Lecture Notes in Computer Science*, pages 70–82. Springer, 1999.

[56] M. Grohe and O. Verbitsky. Testing graph isomorphism in parallel by playing a game. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP 2006)*, pages 3–14. Springer Berlin Heidelberg, 2006.

[57] R. Guralnick, B. Kunyavskiĭ, E. Plotkin, and A. Shalev. Thompson-like characterizations of the solvable radical. *Journal of Algebra*, 300(1):363–375, 2006.

[58] R. M. Guralnick and W. M. Kantor. Probabilistic generation of finite simple groups. *Journal of Algebra*, 234(2):743–792, 2000.

[59] M. Hall. *The theory of groups*, volume 288 of *AMS Chelsea Publishing Series*. AMS, 1976.

[60] F. Harary. A survey of the reconstruction conjecture. In *Graphs and Combinatorics*, volume 406 of *Lecture Notes in Mathematics*, pages 18–28. Springer Berlin Heidelberg, 1974.

[61] L. Hella. Logical hierarchies in PTIME. *Information and Computation*, 129(1):1–19, 1996.

[62] D. G. Higman. Intersection matrices for finite permutation groups. *Journal of Algebra*, 6(1):22–42, 1967.

[63] A. Hulpke. Calculation of the subgroups of a trivial-Fitting group. In *Proceedings of the 38th International Symposium on Symbolic and Algebraic Computation (ISSAC 2013)*, pages 205–210. ACM, 2013.

[64] A. Hulpke. The perfect groups of order up to two million. *Mathematics of Computation*, 91(334):1007–1017, 2021.

[65] B. Huppert. *Endliche Gruppen I*, volume 134 of *Grundlehren der mathematischen Wissenschaften*. Springer Berlin, 1967.

[66] N. Immerman and E. Lander. *Describing graphs: A first-order approach to graph canonization*, pages 59–81. Complexity Theory Retrospective. Springer New York, 1990.

[67] N. Immerman and R. Sengupta. The k-dimensional Weisfeiler-Leman algorithm. *Preprint, arXiv:1907.09582 [cs.CC]*, 2019.

[68] I. M. Isaacs. *Character theory of finite groups*. Dover Books on Mathematics. Dover Publications, 1994.

[69] G. Ivanyos and Y. Qiao. Algorithms based on *-algebras, and their applications to isomorphism of polynomials with one secret, group isomorphism, and polynomial identity testing. *SIAM Journal on Computing*, 48(3):926–963, 2019.

[70] G. James and M. Liebeck. *Representations and characters of groups.* Cambridge University Press, 2nd edition, 2001.

[71] Z. Jiping. On finite groups all of whose elements of the same order are conjugate in their automorphism groups. *Journal of Algebra*, 153(1):22–36, 1992.

[72] T. Kavitha. Linear time algorithms for abelian group isomorphism and related problems. *Journal of Computer and System Sciences*, 73(6):986–996, 2007.

[73] N. Kayal and T. Nezhmetdinov. Factoring groups efficiently. In *Proceedings of the 36th International Colloquium on Automata, Languages and Programming (ICALP 2009)*, volume 5555 of *Lecture Notes in Computer Science*, pages 585–596. Springer, 2009.

[74] S. Kiefer and D. Neuen. The power of the Weisfeiler-Leman algorithm to decompose graphs. In *Proceedings of the 44th International Symposium on Mathematical Foundations of Computer Science (MFCS 2019)*, volume 138 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 45:1–45:15. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

[75] S. Kiefer, I. Ponomarenko, and P. Schweitzer. The Weisfeiler-Leman dimension of planar graphs is at most 3. *Journal of the ACM*, 66(6):1–31, 2019.

[76] L. G. Kovács and M. F. Newman. Minimal verbal subgroups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 62(3):347–350, 1966.

[77] R. E. Ladner. On the structure of polynomial time reducibility. *Journal of the ACM*, 22(1):155–171, 1975.

[78] J. S. Leon. Permutation group algorithms based on partitions, I: Theory and algorithms. *Journal of Symbolic Computation*, 12(4):533–583, 1991.

[79] J. S. Leon. *Partitions, refinements, and permutation group computation*, volume 28 of *DIMACS Seris in Discrete Mathematics and Theoretical Computer Science*, pages 123–157. AMS, 1997.

[80] C. Li. A complete classification of finite homogeneous groups. *Bulletin of the Australian Mathematical Society*, 60:331–334, 1999.

[81] M. Lichter. Separating rank logic from polynomial time. In *Proceedings of the 36th Annual Symposium on Logic in Computer Science (LICS 2021)*, pages 1–13. IEEE, 2021.

[82] E. M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, 25(1):42–65, 1982.

[83] E. M. Luks. Group isomorphism with fixed subnormal chains. *Preprint, arXiv:1511.00151 [CoRR]*, 2015.

[84] D. MacHale. Some finite groups which are rarely automorphism groups: II. *Proceedings of the Royal Irish Academy. Section A: Mathematical and Physical Sciences*, 83A(2):189–196, 1983.

[85] B. McKay. Reconstruction of small graphs and digraphs. *The Australasian Journal of Combinatorics*, 83(2):448–457, 2022.

[86] B. McKay and A. Piperno. nauty and traces. `https://pallini.di.uniroma1.it/`. Accessed: 2023-07-10.

[87] B. McKay and A. Piperno. Practical graph isomorphism, II. *Journal of Symbolic Computation*, 60:94–112, 2014.

[88] A. H. Mekler. Stability of nilpotent groups of class 2 and prime exponent. *Journal of Symbolic Logic*, 46(4):781–788, 1981.

[89] G. L. Miller. On the $n^{\log n}$ isomorphism technique: A preliminary report. In *Proceedings of the 10th Annual Symposium on Theory of Computing (STOC 1978)*, pages 51–58. ACM, 1978.

[90] L. Mirsky and H. Perfect. Systems of representatives. *Journal of Mathematical Analysis and Applications*, 15(3):520–568, 1966.

[91] C. Norman. *Finitely generated abelian groups and similarity of matrices over a field*. Springer Undergraduate Mathematics Series. Springer London, 2012.

[92] E. A. O'Brien. Isomorphism testing for p-groups. *Journal of Symbolic Computation*, 17(2):131, 133–147, 1994.

[93] E. A. O'Brien and M. R. Vaughan-Lee. The groups with order p^7 for odd prime p. *Journal of Algebra*, 292(1):243–258, 2005.

[94] M. Otto. *Bounded variable logics and counting: A study in finite models*, volume 9 of *Lecture Notes in Logic*. Cambridge University Press, 2017.

[95] A. Piperno. Search space contraction in canonical labeling of graphs (preliminary version). *Preprint, arXiv:0804.4881 [CoRR]*, 2008.

[96] I. Ponomarenko and G. Chen. *Coherent configurations*. Wuhan: Central China Normal University Press, 2019.

[97] A. Ranum. The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group. *Transactions of the American Mathematical Society*, 8(1):71–91, 1907.

[98] D. J. Rosenbaum and F. Wagner. Beating the generator-enumeration bound for p-group isomorphism. *Theoretical Computer Science*, 593:16–25, 2015.

[99] B. Schein. Subsemigroups of inverse semigroups. *Le Matematiche*, 51:205–227, 1997.

[100] J. Serre. *Finite groups: An introduction.* International Press, Somerville, MA, revised edition, 2022.

[101] M. J. Smith. Computing automorphisms of finite soluble groups. *Bulletin of the Australian Mathematical Society*, 53(1):169–171, 1996.

[102] X. Sun. Faster isomorphism for p-groups of class 2 and exponent p. In *Proceedings of the 55th Annual Symposium on Theory of Computing (STOC 2023)*, pages 433–440. ACM, 2023.

[103] F. Szechtman and A. Tushev. On infinite groups admitting a faithful irreducible representation. *Journal of Algebra and Its Applications*, 17(1), 2016.

[104] D. R. Taunt. Remarks on the isomorphism problem in theories of construction of finite groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 51(1):16–24, 1955.

[105] D. Vagnozzi. *Variations on the theme of higher dimensional Weisfeiler-Leman algorithms.* Ph.D. dissertation. Department of Computer Science and Technology at the University of Cambridge, 2023.

[106] A. V. Vasil'ev, M. A. Grechkoseeva, and V. D. Mazurov. Characterization of the finite simple groups by spectrum and order. *Algebra and Logic*, 48:385–409, 2009.

[107] F. Dalla Volta and A. Lucchini. Generation of almost simple groups. *Journal of Algebra*, 178(1):194–223, 1995.

[108] B. Weisfeiler. *On construction and identification of graphs*, volume 558 of *Lecture Notes in Mathematics.* Springer Berlin-New York, 1976.

[109] J. B. Wilson. Decomposing p-groups via Jordan algebras. *Journal of Algebra*, 322(8):2642–2679, 2009.

[110] J. B. Wilson. The threshold for subgroup profiles to agree is $\Omega(\log n)$. *Preprint, arXiv:1612.01444 [CoRR]*, 2016.

[111] H. J. Zassenhaus. *The theory of groups.* Chelsea Publishing Company, 2nd edition, 1958.

Academic Curriculum Vitae

2013-2016	B. Sc. Mathematics *RWTH Aachen University*
2016-2018	M. Sc. Mathematics *RWTH Aachen University*
2019-2021	Doctoral student and research assistant Supervisor: Prof. Dr. Pascal Schweitzer *TU Kaiserslautern*
2021-2023	Doctoral student and research assistant Supervisor: Prof. Dr. Pascal Schweitzer *TU Darmstadt*