Electronic Colloquium on Computational Complexity, Report No. 123 (2013)

Algorithms for group isomorphism via group extensions and cohomology [*]

Joshua A. Grochow [†] Youming Qiao [‡]

September 6, 2013

Abstract

The isomorphism problem for groups given by their multiplication tables (GpI) has long been known to be solvable in $n^{O(\log n)}$ time, but until the last few years little progress towards a polynomial-time algorithm had been achieved. Recently, Babai *et al.* (ICALP 2012) gave a polynomial-time algorithm for groups with no abelian normal subgroups. Thus, at present it is crucial to understand groups with abelian normal subgroups to develop $n^{o(\log n)}$-time algorithms.

Towards this goal we advocate a strategy via the extension theory of groups, which is concerned with how a normal subgroup N is related via G to the quotient group G/N. This strategy "splits" GpI into two subproblems: one related to group actions on other groups, and one related to group cohomology. Special cases of these problems reduce to GpI, and GpI reduces to a simultaneous solution of the two problems. Previous works on GpI are naturally connected to this viewpoint; in particular, most previous results in the Cayley table model have focused on the group action aspect. However, by the aforementioned reductions the group cohomology aspect is necessary to tackle the general case. In particular, for p-groups of class 2—believed to be the hardest case of GpI—group cohomology is necessary to decide isomorphism.

With an eye towards making progress on the group cohomology aspect of GpI, we consider *groups with central radicals*, proposed in Babai *et al.* (SODA 2011): the class of groups whose solvable normal subgroups are contained in the center. Recall that Babai *et al.* (ICALP 2012) consider the class of groups with *no* solvable normal subgroups. Following the above approach, we exhibit an $n^{O(\log \log n)}$-time algorithm for isomorphism of groups with central radicals, and polynomial-time algorithms for several prominent sub-classes of groups with central radicals. We also exhibit an $n^{O(\log \log n)}$-time algorithm for isomorphism of groups with elementary abelian, but not necessarily central, radicals. Prior to this work, nothing better than the trivial $n^{O(\log n)}$-time algorithm was known, even for groups with a central radical of constant size, such as $Z(G) = \mathbb{Z}_2$. To develop these algorithms we utilize several mathematical results on the detailed structure of cohomology classes, as well as algorithmic results for code equivalence, coset intersection and cyclicity test of modules over finite-dimensional associative algebras.

Additionally, the cohomological strategy helps to explain in a unified way the recent successes on other group classes such as coprime extensions, quotients of generalized Heisenberg groups, and groups with no solvable normal subgroups. It also suggests several promising directions for future work.

[*] The introduction may serve as an extended abstract: §1.1 contains an informal exposition of §2, §3 and §4; §1.4 gives a brief overview of §5, §6 and §7.

[†] Department of Computer Science, The University of Toronto. jgrochow@cs.toronto.edu

[‡] Centre for Quantum Technologies, National University of Singapore. cqtqy@nus.edu.sg

ISSN 1433-8092

Contents

1 Introduction

The group isomorphism problem GpI is to determine whether two finite groups, given by their multiplication tables ("Cayley tables"), are isomorphic. For groups of order n, the easy $n^{\log n+O(1)}$-time algorithm [FN70, Mil78][1] for the general case of GpI has barely been improved over the past four decades (it was improved recently to $n^{0.5\log n+o(\log n)}$ by Rosenbaum [Ros13a]). The past few years have witnessed a resurgence of activity on this problem [LG09, CTW10, BCGQ11, QST11, Wag11, BQ12, BCQ12, Ros13b, Ros13a]. Before introducing these works and our results, we recall why GpI is an intriguing problem from the complexity-theoretic perspective.

As GpI reduces to graph isomorphism (GraphI) (see, e. g.[KST93]), GpI currently has an intermediate status: it is not NP-complete unless PH collapses [BHZ87, BM88], and is not known to be in P. In addition to its intrinsic interest, resolving the exact complexity of GpI is a tantalizing question. Further, there is a surprising connection between GpI and the Geometric Complexity Theory program (see, e. g., [Mul11] and references therein): techniques from GpI were used to solve cases of Lie algebra isomorphism that have applications in Geometric Complexity Theory [Gro12].

In a survey article [Bab95] in 1995, after enumerating several isomorphism-type problems including GraphI and GpI, Babai expressed the belief that GpI might be the only one expected to be in P.[2] Indeed, in many ways GpI seems easier than GraphI: there is a simple $n^{\log n+O(1)}$-time algorithm for GpI, whereas the best known algorithm (see [BL83]) for GraphI takes time $2^{\tilde{O}(\sqrt{n})}$ and is quite complicated. There is a polynomial-time reduction from GpI to GraphI, yet there is provably no AC^0 reduction in the opposite direction [CTW10]. Further, GraphI is as hard as its counting version, whereas no such counting-to-decision reduction is known for GpI. Finally, whereas the smallest standard complexity class known to contain GraphI is $\mathsf{NP}\cap\mathsf{coAM}$, Arvind and Torán [AT11] showed that GpI for solvable groups[3] is in $\mathsf{NP}\cap\mathsf{coNP}$ under a plausible assumption, weaker than that needed to show GraphI $\in \mathsf{coNP}$.

Despite this situation and considerable attention to GpI, prior to 2009 the actual developments towards polynomial-time algorithms for GpI essentially stopped at abelian groups. For abelian groups, Kavitha exhibited an $O(n)$-time algorithm [Kav07], improving Savage's $O(n^2)$ [Sav80] and Vikas's $O(n\log n)$ [Vik96]. The next natural group class after abelian groups—class 2 nilpotent groups[4]—turns out to be formidable. On the other hand, there is a large body of work in the area referred to as computational group theory (CGT) on practical algorithms for group isomorphism testing. That line of research typically works on inputs much more succinct than the full Cayley table, while the algorithms are often heuristic. In the main text, we mostly restrict our attention to works explicitly on the Cayley table model with worst-case analysis. See Appendix F for a discussion of the relationship between these two lines of research, as well as works in CGT related to our results.

Beginning in 2009 there were several advances, starting with Le Gall [LG09]. In [BCQ12], following [BCGQ11], Babai *et al.* developed a polynomial-time algorithm for groups with no abelian

[1] Miller [Mil78] attributes this algorithm to Tarjan.

[2] The exact quotation from Babai's 1995 survey [Bab95] is: "None of the problems mentioned in this section, with the possible exception of isomorphism of groups given by a Cayley table, is expected to have polynomial time solution."

[3] A group is solvable if all its composition factors are abelian. Certain solvable groups are widely believed to be the hardest cases of GpI.

[4] A group G is nilpotent of class 2 if the quotient $G/Z(G)$ is abelian, where $Z(G)$ is the center of G.

normal subgroups. This suggests the presence of abelian normal subgroups as a bottleneck.[5] With this in mind, Babai and Qiao [BQ12] developed a polynomial-time algorithm for a special class of non-nilpotent solvable groups, building on [LG09, QST11]. In 2013, Rosenbaum [Ros13b] exhibited a deterministic $n^{0.5 \log n + o(\log n)}$-time algorithm for solvable groups, developing ideas of Wagner [Wag11]. Very recently, Rosenbaum developed a general algorithmic technique that brings the time complexity of GpI to $n^{0.5 \log n + o(\log n)}$. To summarize, at present it is crucial to understand indecomposable[5] groups with abelian normal subgroups to develop $n^{o(\log n)}$-time algorithms.

Our contributions in this paper are twofold: (1) we propose a general strategy for group isomorphism; and (2) using that strategy, we develop an $n^{O(\log \log n)}$-time algorithm for a group class proposed in [BCGQ11], and polynomial-time algorithms for some prominent subclasses. Our strategy also helps to explain in a unified way the recent successes on other group classes [LG09, QST11, BQ12, BCGQ11, BCQ12, LW12], which can be viewed as adding class-specific tactics to the strategy outlined here.

1.1 A strategy via group extensions and cohomology

In this paper we use the theory of group extensions (see, e. g., [Rob96, Chapter 11] and [Rot94, Chapter 7]) to show that the group isomorphism problem "splits" into two subproblems—one coming from actions of groups on other groups (Action Compatibility), and the other coming from group extensions and cohomology (Cohomology Class Isomorphism), which we explain below. We note that in [BE99] Besche and Eick have proposed this splitting in a slightly different setting, under the name "strong isomorphism." In the abstract theory of finite groups this splitting is standard material; the contribution here is the observation that this standard material can be made algorithmically effective, and that doing so is useful and even formally necessary to resolve the complexity of GpI. For the converse direction, we observe that special cases of these subproblems reduce to GpI under polynomial-time reductions (§4.3). We summarize these results in:

Facts 4.1, 4.2, and Lemms 3.2, 3.12 ("Splitting" GpI into actions and cohomology)**.**

- *For coprime extensions* Action Compatibility $\equiv_m^p$ GpI*.*
- *For p-groups of class 2, when* $p > 2$*,* Cohomology Class Isomorphism $\equiv_m^p$ GpI*.*
- GpI *reduces to simultaneously solving*[6] Action Compatibility *and* Cohomology Class Isomorphism*.*

Most previous complexity-theoretic results on GpI have focused on some combination of algorithmic techniques and Action Compatibility. In this paper, for the first time from the worst-case complexity perspective, we make progress on Cohomology Class Isomorphism.

We now explain this "splitting" and the problems mentioned above informally. Consider the following natural strategy for testing whether G is isomorphic to H. If G is simple, then isomorphism can be tested in polynomial time as G is generated by at most two elements (Fact 5.1). If G is not simple, then it has some normal subgroup $N \trianglelefteq G$, and we may try to use a divide-and-conquer

[5] Abelian direct factors, as in $H \times \mathbb{Z}_n$ are not a bottleneck however: Kayal and Nezhmetdinov [KN09] and Wilson [Wil10] gave polynomial-time algorithms to decompose a direct product into its direct factors. For polynomial-time algorithms, one may thus assume that the groups under consideration are *directly indecomposable*: they cannot be written as a direct product of two nontrivial groups.

[6] See §1.4 and Lemma 3.2 for the exact meaning of "simultaneously solving."

strategy by first solving the isomorphism problem for N and G/N. However, even if we find $M \trianglelefteq H$ such that $N \cong M$ and $G/N \cong H/M$, this is typically not sufficient to conclude that $G \cong H$ (e. g., $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$). We must then understand how the groups N and G/N "glue" back together to get G. G is called an *extension* of N by G/N;[7] given N and Q, understanding the collection of groups G which are extensions of N by Q—that is, where $N \trianglelefteq G$ and $G/N \cong Q$—is known as the *extension problem.* The extension problem is considered quite difficult in general, but the theory of group cohomology exactly captures this problem and provides useful tools for its study, including connections with other cohomology theories such as in algebraic topology. One of the main technical achievements of the present paper is to make some aspects of group cohomology effective in the setting of worst-case complexity.

When N is abelian the extension theory is conceptually easier and technically cleaner. Coincidentally, due to the polynomial-time algorithm for semisimple groups [BCQ12], abelian normal subgroups are exactly the subject of interest at present. So for the rest of this subsection, *we assume N is abelian*; the theory for the general case is similar, and is covered in Section 3.3.

The extensions of N by Q are governed by two pieces of data: (1) an action of Q on N and (2) a cohomology class. We explain each of these in turn.

The action. If G is an extension of N by Q, then $N \trianglelefteq G$, so G acts on N by conjugation, giving a homomorphism $\theta' \colon G \to \mathrm{Aut}(N)$. As we have assumed N is abelian, N lies in the kernel of θ', so the conjugation action of G on N induces an action θ of $G/N \cong Q$ on N. Two such actions are *compatible* if they become equal after applying some element of $\mathrm{Aut}(N) \times \mathrm{Aut}(Q)$, giving rise to the first problem Action Compatibility.

The cohomology class. Informally speaking, the simplest examples of extensions are when Q can be "lifted" to a subgroup of G that is compatible with the isomorphism $G/N \cong Q$. However, it is possible to have an extension G of N by Q in which this cannot happen. For example, consider the additive group of real numbers $\mathbb{R}$, and its normal subgroup $2\pi\mathbb{Z}$.[8] The quotient $\mathbb{R}/2\pi\mathbb{Z}$ is isomorphic to the "circle group" S^1 of unit complex numbers under multiplication, yet S^1 is not even a subgroup of $\mathbb{R}$, let alone "liftable to $\mathbb{R}$." Contrast with the group $G = 2\pi\mathbb{Z} \times S^1$, which also has $2\pi\mathbb{Z} \trianglelefteq G$ and $G/2\pi\mathbb{Z} \cong S^1$, yet S^1 is a subgroup of G. Note that as both $\mathbb{R}$ and G are abelian the conjugation action of $\mathbb{R}$ or G on any normal subgroup is trivial. So the actions cannot explain the fact that S^1 is not a subgroup of $\mathbb{R}$; instead, it is group cohomology that exactly captures this phenomenon.

Specifically, if G is an extension of N by Q, the failure of Q to be "liftable" to G is measured by a *cohomology class* as follows. Consider any set map $s \colon Q \to G$ such that $s(q)$ is in the coset of N corresponding to q under the identification $G/N \cong Q$. Q is "liftable" if and only if s is a group homomorphism. The failure of s to be a homomorphism is measured by the function $f_s(q,p) := s(q)s(p)s(qp)^{-1}$: s is a homomorphism if and only if $f_s(q,p) = 1$ for all $p, q \in Q$. The cohomology class corresponding to G, viewed as an extension of N by Q, is then $\{f_s | s \colon Q \to G \text{ as above}\}$. Two cohomology classes are *isomorphic* if they become equal after applying some element of $\mathrm{Aut}(N) \times \mathrm{Aut}(Q)$, giving rise to the second problem Cohomology Class Isomorphism.

[7] Some authors use the opposite nomenclature and call this an extension of G/N by N.

[8] There are similar examples in finite groups, but we believe this example has more intuitive appeal. For readers familiar with group extensions, the goal here is to exhibit a nonsplit extension; $\{0, 2\} \trianglelefteq \mathbb{Z}_4$ is a familiar example.

Towards a formal strategy. Having introduced the action and the cohomology class, let us see how they can be useful in isomorphism testing. We refer to the pair (θ, f) of the corresponding action and (a representative of) a cohomology class as the *extension data* of the extension. Suppose we are given two groups G_1 and G_2. We cleverly choose some $N_1 \trianglelefteq G_1$ and $N_2 \trianglelefteq G_2$, and (somehow we are lucky to find that) $N_1 \cong N_2$ and $G_1/N_1 \cong G_2/N_2$. Viewing G_i as extensions of N_i by G_i/N_i, we extract the action θ_i and cohomology classes f_i, for $i = 1, 2$. If there is a simultaneous solution (one single $(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(G/N)$) to Action Compatibility for θ_1, θ_2 and Cohomology Class Isomorphism for f_1, f_2, we say the extension data are *pseudo-congruent*.[9]

If the extension data are pseudo-congruent, then $G_1 \cong G_2$ and we are done. However, it is possible that $G_1 \cong G_2$ but the extension data are not pseudo-congruent (we thank Naik [Nai10] for providing Example E.2). The difficulty is that G may contain two normal subgroups $M, M' \trianglelefteq G$ such that $M \cong M'$ and $G/M \cong G/M'$, but no automorphism of G sends M to M'. To resolve this problem, our Main Lemma 3.2 shows that it is enough to take N_1 and N_2 to be the center or the radical, or more generally any characteristic subgroups that are preserved under isomorphisms.[10] Now we state the Main Lemma informally.

Lemma (Main Lemma 3.2, informal)**.** *Given two groups G_1 and G_2, let A_i be the abelian characteristic subgroup of G_i of a particular type (e. g., the center), θ_i the action of G_i/A_i on A_i, and f_i the cohomology class of the extension of A_i by G_i/A_i. Suppose $A_1 \cong A_2$ (identified as A) and $G_1/A_1 \cong G_2/A_2$ (identified as Q).*

Then $G_1 \cong G_2$ if and only if $\theta_1 \equiv \theta_2$, and $f_1 \equiv f_2$ up to the action of $\mathrm{Aut}(A) \times \mathrm{Aut}(Q)$*.*

As evidence of the usefulness of the Main Lemma beyond this paper, we note that the polynomial-time algorithms for a special class of solvable groups in [LG09, QST11, BQ12] follow this strategy: they use a theorem of Taunt [Tau55] to reduce isomorphism testing to a problem about linear representations of finite groups (see Problem 1 in [QST11]), and solve that problem with additional tactics. In retrospect, Taunt's Theorem is a special case of the Main Lemma[11], and Problem 1 in [QST11] is essentially Action Compatibility. Similarly, in retrospect the polynomial-time algorithm for semisimple groups [BCGQ11, BCQ12] can be viewed as taking advantage of the nonabelian Main Lemma 3.12. We cover these examples in more detail in Section 4.2.

Due to the structure of the group classes considered in [LG09, QST11, BQ12], group Cohomology Class Isomorphism does not appear in these works. On the other hand, for p-groups of class 2 (currently believed the bottleneck), Cohomology Class Isomorphism is well-known to be necessary (see Fact 4.2). We thus turn to study the Cohomology Class Isomorphism problem in the following. As far as we know, this is the first time group cohomology has been used for GpI in the Cayley table model.

[9] We take this terminology from Naik [Nai12], who gives a different definition of pseudo-congruence of extensions that is more standard from the group-theoretic point of view, but less well-adapted to the computational setting. We give the other definition and show that the two are formally equivalent in §3.2. Robinson [Rob96] uses the term "isomorphism" for this notion; we prefer "pseudo-congruence" to avoid confusion with the several other notions of isomorphism floating around. Theoretical investigations of some aspects of this concept can be found in Robinson [Rob82, Sec. 4].

[10] In the practical setting, Besche and Eick [BE99] got around the pitfall by introducing the related concept of "strong isomorphism," which is more natural for their purpose, namely the construction of finite groups.

[11] Taunt's Theorem applies regardless whether the normal subgroup N is abelian or not. The works [LG09, QST11, BQ12] only used the case when N is abelian. The general Main Lemma 3.12 additionally covers the nonabelian case of Taunt's Theorem.

1.2 Motivation for the classes of groups considered

The classes of groups we consider are natural extensions of the class of groups considered in [BCGQ11, BCQ12], and are additionally motivated by the Babai–Beals filtration [BB99], and the Cannon–Holt approach to group isomorphism in the practical setting [CH03]. We go into the details of the Babai–Beals filtration and the Cannon–Holt approach in §8. Here we merely give enough of a flavor to help motivate the classes of groups we consider.

Important in both the Babai–Beals filtration and the Cannon–Holt approach is the solvable radical. Recall that a group is solvable if it has a series of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$ such that each G_i is normal in the next and G_i/G_{i-1} is abelian for all i. The solvable radical $\mathrm{Rad}(G)$ of a group G is the unique maximum solvable normal subgroup of G. Note that the center $Z(G)$, as an abelian normal subgroup, is contained in $\mathrm{Rad}(G)$. $G/\mathrm{Rad}(G)$ contains no solvable normal subgroups, side-stepping the currently intractible obstacle of solvable groups. Babai *et al.* [BCQ12] give a polynomial-time algorithm for isomorphism of groups with no solvable normal subgroups; following them, we call such groups "semisimple."[12]

We mainly consider the class of groups whose solvable radical coincides with its center, that is, $\mathrm{Rad}(G) = Z(G)$ (in Section 6.2 we also consider groups whose solvable radical is abelian, but need not be contained in the center). This class, which we refer to as *groups with central radicals* or *central-radical groups*, is a natural extension of the class of semisimple groups and a natural stepping stone towards general groups. Note that for such groups the solvable radical is necessarily abelian. Besides the motivations mentioned above, central-radical groups also cover a class of groups that is well-studied in finite group theory (see §1.3 and Appendix D). In the theory of Lie groups, central-radical groups correspond to the well-studied and important class of reductive Lie groups, which are important mainly because of their nice representation-theoretic properties.

While this may seem only a slight extension, central-radical groups in fact differ significantly from previous classes of groups with $n^{o(\log n)}$-time isomorphism algorithms. In particular, previous $n^{o(\log n)}$-time algorithms for GpI of special group classes only consider one of the two main aspects of GpI, namely actions.[13] On the other hand, to work with groups with central radicals, we need to focus on the other main aspect of the problem, namely cohomology (see §1.1). Our results also suggest one more step towards a formal reduction from the general case to nilpotent groups of class 2 (see §8.3).

1.3 New algorithms using this strategy

We use the strategy outlined in §1.1 to achieve the following results. For groups with central radicals, we give an $n^{O(\log \log n)}$-time algorithm in general, and for several subclasses of groups with central radicals we give polynomial-time algorithms. We also give similarly efficient algorithms for groups with elementary abelian, but not necessarily central, radicals. Prior to this work, nothing better than the trivial $n^{\log n + O(1)}$-time algorithm was known, even for groups with a central radical of constant size, such as $Z(G) = \mathrm{Rad}(G) = \mathbb{Z}_2$.

Theorem 6.2. *Isomorphism of central-radical groups of order n can be decided in time $n^{c \log \log n + O(1)}$, for $c = 1/\log_2(60) \approx 0.169$.*

[12] If there is a solvable normal subgroup $S \trianglelefteq G$, there is an abelian normal subgroup of G, namely the last term in the derived series of S. Hence semisimple groups can be characterized either as having no solvable normal subgroups or as having no abelian normal subgroups.

[13] In §4.2, we briefly indicate how actions are used in [LG09, QST11, BQ12, BCGQ11, BCQ12].

The algorithm in the above theorem in fact runs in polynomial time when the order or structure of the semisimple quotient $G/\operatorname{Rad}(G)$ is bounded as follows. Recall that a normal subgroup of G is *minimal* if it is nontrivial and does not contain any smaller normal subgroups of G. The number of minimal normal subgroups of $G/\operatorname{Rad}(G)$ is always at most $\log_{60} n$; if it happens to be just slightly smaller, then we have:

Theorem 6.3. *Let G and H be central-radical groups of order n. If $G/\operatorname{Rad}(G)$ has $O(\frac{\log n}{\log\log n})$ minimal normal subgroups, isomorphism between G and H can be decided in polynomial time.*

In particular, this includes groups G satisfying $|G/\operatorname{Rad}(G)| \leq n^{O(1/\log\log n)}$, but also many groups where $G/\operatorname{Rad}(G)$ is much larger. Both of these theorems are in fact corollaries of our more general Theorem 6.1 together with previous results on semisimple groups [BCGQ11], but we defer the statement of Theorem 6.1 until §7, as the above results make its significance clearer.

For groups with elementary abelian, but not necessarily central, radicals we get the same conclusions. This requires us to simultaneously solve Action Compatibility and Cohomology Class Isomorphism. We combine the above techniques with a novel reduction to known representation-theoretic algorithms [CIK97] to get:

Theorems 6.11 and 6.12. *Isomorphism of groups of order n with elementary abelian radicals can be decided in time $n^{c\log\log n+O(1)}$, for $c = 1/\log_2(60) \approx 0.169$.*

If furthermore $G/\operatorname{Rad}(G)$ has $O(\frac{\log n}{\log\log n})$ minimal normal subgroups, isomorphism can be decided in polynomial time.

We then consider central-radical groups with $G/\operatorname{Rad}(G)$ a direct product of nonabelian simple groups. Although this may seem restrictive, this class of groups is quite natural. In group theory, this class is closely related to the generalized Fitting subgroups (see, e. g., [Suz86, Ch. 6, §6] and [Asc00, Ch. 11], as well as Appendix D). Also, within central-radical groups, this class has two characterizations: (1) the last two of the four levels of the Babai–Beals filtration are trivial (see §8.2); or (2) those groups that are equal to their generalized Fitting subgroup (see Appendix D). We give polynomial-time algorithms for this group class when certain parameters are fixed. This includes, for example, central extensions of $\mathbb{Z}_p^{\Theta(\log n)}$ by $A_5^{\Theta(\log n)}$, which do not satisfy the conditions of Theorem 6.3 nor 6.12.

More importantly, we believe the techniques in Theorem 7.1 are worth noting: we rely on a detailed analysis of the structure of the cohomology classes (see §1.1), specific to this group class and traced back to Suzuki [Suz86], to allow for the application of known algorithmic techniques, including singly-exponential-time algorithms for Linear Code Equivalence [Bab10] (see [BCGQ11, Thm. 7.1]) and Coset Intersection [Bab83, Luk99] (see also [Bab08, BKL83]).

Theorem 7.1. *Isomorphism of groups G_1 and G_2 with central radicals and $G_i/\operatorname{Rad}(G_i)$ a direct product of nonabelian simple groups can be decided in polynomial time if either:*

1. $|\operatorname{Aut}(\operatorname{Rad}(G_1))|$ *is bounded by a polynomial; or*

2. $\operatorname{Rad}(G_1)$ *is elementary abelian, and the simple direct factors of* $G_1/\operatorname{Rad}(G_1)$ *each have order* $O(1)$.

1.4 Overview of our algorithms

Here we give an overview of the structure of our algorithms, as well as some of the more salient details. We first consider the case when the solvable radical is abelian, to see how the strategy in the above section is applied. We then focus on central-radical groups to outline some key steps in the algorithms.

Given groups G_1, G_2, we first compute their solvable radicals $A_i = \mathrm{Rad}(G_i)$ and the corresponding semisimple quotients $Q_i = G_i / \mathrm{Rad}(G_i)$. Then apply the algorithm from [Kav07] to A_1 and A_2, and the algorithm from [BCQ12] to Q_1 and Q_2. If either of them returns non-isomorphic, $G_1 \not\cong G_2$. If both algorithms return isomorphic, they also yield isomorphisms. Thus, without loss of generality, for $i = 1, 2$, we use A to denote $\mathrm{Rad}(G_i)$ and Q to denote $G_i / \mathrm{Rad}(G_i)$, identifying G_i as an extension of A by Q.

Next, we compute the corresponding actions θ_1, θ_2 and representatives f_1, f_2 of the corresponding cohomology classes. As mentioned §1.1, our Main Lemma 3.2 says that G_1 and G_2 are isomorphic if and only if there is an element of $\mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ which simultaneously turns θ_1 into θ_2, and f_1 into f_2 (as cohomology classes).

For groups with central radicals, $A = Z(G_i)$, so the actions θ_i are trivial, and we only need to solve Cohomology Class Isomorphism. We denote the twist of f_i by $(\alpha, \beta) \in \mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ by $f_i^{(\alpha,\beta)}$, and the task is to determine whether there exists $\alpha \in \mathrm{Aut}(A)$, and $\beta \in \mathrm{Aut}(Q)$, such that f_1 and $f_2^{(\alpha,\beta)}$ are in the same cohomology class. We now present some of the key ideas in our algorithms.

For general central-radical groups. Babai *et al.* [BCGQ11] showed that all automorphisms of a semisimple group can be enumerated in time $n^{O(\log\log n)}$. So if $n^{O(\log\log n)}$ time is allowed, we can use that algorithm to enumerate $\beta \in \mathrm{Aut}(Q)$. Then for each such β, search for some $\alpha \in \mathrm{Aut}(A)$ such that f_1 and $f_2^{(\alpha,\beta)}$ are in the same cohomology class.

To tackle the latter problem, to ease the exposition let us assume $A = \mathbb{Z}_p^k$. Then we shall view any map $f : Q \times Q \to A$ as a $k \times |Q|^2$-size matrix over $\mathbb{Z}_p$, with $\alpha \in \mathrm{Aut}(A)$ acting on the rows, $\mathrm{Aut}(Q)$ inducing an action on the columns. The main difficulty at this point has to do with identifying which cohomology class f is in, preferably in a way that is $\mathrm{Aut}(A) \times \mathrm{Aut}(Q)$-invariant. Viewing f as a $\mathbb{Z}_p$-linear vector (of dimension $k \times |Q|^2$), by Proposition C.1 we can compute a projection π in this vector space such that $\pi(f)$ identifies the cohomology class of f—that is, $\pi(f) = \pi(f')$ if and only if f and f' are in the same cohomology class—and such that π commutes with every $\alpha \in \mathrm{Aut}(A)$. With fixed β, this allows us to compute $\pi(f_1)$ and $\pi(f_2^{(\mathrm{id},\beta)})$, and then determine whether, as $k \times |Q|^2$-size matrices, their row spans are the same, which is a standard task in linear algebra. Finally, to move from $A = \mathbb{Z}_p^k$ to general abelian A, we must consider the automorphism group of an arbitrary abelian group in some detail, which we do in Section 6.1.1.

For central-radical groups with $G/\mathrm{Rad}(G)$ a direct product of nonabelian simple groups. In this case $Q = \prod_{i \in [\ell]} T_i$, T_i nonabelian simple. To ease the exposition let us assume T_i's are all isomorphic to T and $A = \mathbb{Z}_p^k$. For a function $f : Q \times Q \to A$, a key fact is that the cohomology class of f is completely determined by the *restrictions* of f to the direct factors T_i (Lemma 7.3). Several group-theoretic facts lead to this cohomological proposition, including: (1) the direct product decomposition of Q into nonabelian simple factors is unique (not just up to isomorphism); (2) if U_i is the preimage of T_i under the projection $G \to G/Z(G)$, then $u_i u_j = u_j u_i$ whenever $u_i \in U_i$,

$u_j \in U_j$, and $i \neq j$ ([Suz86, Chapter 6, Proposition 6.5], see Proposition 7.2). Another useful fact is the well-known description of $\mathrm{Aut}(Q)$ as $\mathrm{Aut}(T) \wr S_\ell$.

When A is small enough that we can enumerate $\mathrm{Aut}(A)$ in polynomial time, this allows us, up to a polynomial overhead, to focus on the multiset of cohomology classes of the U_i's. This idea leads to the algorithm for Theorem 7.1 (1).

When A is not small enough for the above tactic, instead of considering $f : Q \times Q \to A$, we can consider $f_i : T_i \times T_i \to A$, $i \in [\ell]$; and instead of working with a $k \times |Q|^2$-size matrix, we can work with a $k \times (\sum_{i\in[\ell]} |T_i|^2)$-size matrix. This difference between $|Q|^2 = \prod_{i\in[\ell]} |T_i|^2$ and $\sum_{i\in[\ell]} |T_i|^2$ leads to major savings. To find the pair (α, β) simultaneously, we combine algorithms for Linear Code Equivalence and Coset Intersection. This is the basic idea for Theorem 7.1 (2). We need several technical ingredients (including Lemma 7.4) to make the above procedure work though.

1.5 Organization of the paper

In §2 we collect basic concepts from extension theory. The strategy is developed in §3, which expands the ideas in §1.1 into a formal framework. Appendix E contains some further related concepts and facts from extension theory. §5 contains preliminaries and previous algorithmic results to prepare for the algorithms for central-radical groups. In §6 we describe the $n^{O(\log\log n)}$-time algorithm for the general central-radical groups (Theorem 6.2); this is also the algorithm for Theorem 6.3. We also give the algorithms for groups with elementary abelian radicals that need not be central. In §7, we describe the fixed-parameter polynomial-time algorithms for central-radical groups with $G/\mathrm{Rad}(G)$ a direct product of nonabelian simple groups. Finally §8 contains future directions, some of which are motivated by the Cannon–Holt approach and the Babai–Beals filtration.

2 Preliminaries for the strategy

General notations. For $n \in \mathbb{N}$, $[n] = \{1, \ldots, n\}$. In this paper, all groups are finite. We use id to denote the identity element, or the group of order 1. For a group G, $|G|$ denotes the order of G. We write $H \leq G$ if H is a subgroup of G. The (right) coset of H in G containing $g \in G$ is $Hg = \{hg \mid h \in H\}$. Given two groups G_1 and G_2, $\mathrm{Iso}(G_1, G_2)$ denotes the set of $G_1 \to G_2$ isomorphisms. $\mathrm{Aut}(G) = \mathrm{Iso}(G, G)$ is the group of automorphisms of G. The set $\mathrm{Iso}(G_1, G_2)$ is either empty or a coset of $\mathrm{Aut}(G_1)$. For $g \in G$, conjugation by g is the automorphism $\theta_g : G \to G$ defined by $\theta_g(x) := gxg^{-1}$. For $g \in G$, the maps θ_g are the inner automorphisms of G, and they form a subgroup $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. A subgroup $N \leq G$ is normal if it is invariant under all inner automorphisms, and we write $N \trianglelefteq G$. $N \leq G$ is a characteristic subgroup of G if it is invariant under all automorphisms of G. $Z(G)$ denotes the center of G. For $K, L \leq G$, $[K, L]$ denotes the subgroup generated by all elements of the form $[x, y] := x^{-1}y^{-1}xy$, $x \in K$ and $y \in L$. $[G, G]$ is called the commutator subgroup of G.

Group extension data. Given a finite group G and an abelian normal subgroup $A \trianglelefteq G$, when we consider G as an extension of A by $Q := G/A$, we denote this by $A \overset{\iota}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} Q$, where ι is an injective homomorphism and π a surjective homomorphism, such that $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. In this paper, we mostly use the "inner" perspective, by identifying A with its image $\iota(A) \trianglelefteq G$. We sometimes refer to G as the "total group" of the extension.

We have already mentioned (§1.1) that extension data consists of an action of Q on A and (a representative of) a cohomology class. Here we define the extension data more formally.

The action. Given $g \in G$, $c_g \in \mathrm{Aut}(A)$ denotes the conjugation action $c_g(a) := gag^{-1}$, and $\theta' \colon G \to \mathrm{Aut}(A)$ is the corresponding homomorphism $\theta'(g) := c_g$. As A is abelian, $A \leq \mathrm{Ker}(\theta')$, so that θ' induces a homomorphism $\theta \colon Q \to \mathrm{Aut}(A)$. We refer to this θ as the action of the extension $A \hookrightarrow G \twoheadrightarrow Q$, and θ_p denotes the image of $p \in Q$ in $\mathrm{Aut}(A)$.

The cohomology class. As A is abelian, we write the group operation in A additively, despite the fact that when considering general elements of G we write the group operation in G multiplicatively (this mixed notation is fairly standard in this setting). Even though A is a subgroup of G, we tend to only use these notations in separate contexts and it should not cause confusion.

Let $\pi \colon G \to G/A \cong Q$ be the natural projection; then any set map $s \colon Q \to G$ such that $\pi(s(q)) = q$ for all $q \in Q$ is called a *section* of π. Any such section s gives rise to a function $f_s \colon Q \times Q \to A$ defined by $f_s(p,q) := s(p)s(q)s(pq)^{-1}$. To see that the image of f_s in fact lies in A and not merely in G, note that $\pi(f_s(p,q)) = \pi(s(p))\pi(s(q))\pi(s(pq)^{-1}) = 1$, so $\mathrm{Im}\, f_s \subseteq \mathrm{Ker}(\pi) = A$.

We are free to choose $s(1) = 1$, and then $f_s(1,q) = f_s(q,1) = 0$ for all $q \in Q$. Such f are called *normalized*. In the following all sections are normalized unless stated otherwise.

The fact that the group operation in G is associative implies that for all $p,q,r \in Q$,

$$f_s(p,q) + f_s(pq,r) = \theta_p(f_s(q,r)) + f_s(p,qr) \qquad \text{(the 2-cocycle identity)}$$

Any function $f \colon Q \times Q \to A$ is called a *2-cochain*; any 2-cochain satisfying the 2-cocycle identity is a *2-cocycle*. Given any homomorphism $\theta \colon Q \to \mathrm{Aut}(A)$, every 2-cocycle arises as f_s for some section s of some extension $A \hookrightarrow G \twoheadrightarrow Q$ with action θ.

When do two 2-cocycles f_s, $f_{s'}$ correspond to the same extension? Suppose we know the two sections $s, s' \colon Q \to G$. As $s(q), s'(q)$ lie in the same coset of A, there is a function $u \colon Q \to A$ such that $s(q) = u(q)s'(q)$ for all $q \in Q$. Then $f_s(p,q) = f_{s'}(p,q) + (u(p) + \theta_p(u(q)) - u(pq))$. A *2-coboundary* is a function of the form $f_u(p,q) := u(p) + \theta_p(u(q)) - u(pq)$ for any set map $u \colon Q \to A$. Hence, if two 2-cocycles come from the same extension, they differ by a 2-coboundary. Eilenberg and Maclane [EM47] proved the converse, for a suitable notion of two extensions being "the same," which we discuss in §3.2. Two 2-cocycles which differ by a 2-coboundary are said to be *cohomologous*.

The 2-cochains form an abelian group $C^2(Q,A)$ defined by pointwise addition: $(f+g)(p,q) := f(p,q) + g(p,q)$. It is readily visible that the 2-cocycle identity is $\mathbb{Z}$-linear, and hence the 2-cocycles form a subgroup of the 2-cochains, denoted by $Z^2(Q,A,\theta)$. It is similarly verified that the 2-coboundaries form a subgroup of the 2-cocycles, denoted $B^2(Q,A,\theta)$.

A *2-cohomology class* is a coset of $B^2(Q,A,\theta)$ in $Z^2(Q,A,\theta)$, and any element of this coset is a representative of the cohomology class. If $f \in Z^2(Q,A,\theta)$, we denote the corresponding cohomology class by $[f]$. The group of 2-cohomology classes is denoted $H^2(Q,A,\theta) := Z^2(Q,A,\theta)/B^2(Q,A,\theta)$. By the above discussion, each extension $A \hookrightarrow G \twoheadrightarrow Q$ corresponds to a unique cohomology class $[f] \in H^2(Q,A,\theta)$.

We thus arrive at one of the central notions in this paper:

Definition 2.1. For A an abelian group and Q any group, a pair (θ, f) of an action $\theta \colon Q \to \mathrm{Aut}(A)$ and a 2-cocycle $f \colon Q \times Q \to A$, $f \in Z^2(Q,A,\theta)$ is an *extension data*. Given an extension $A \hookrightarrow G \twoheadrightarrow Q$, the extension data for this particular extension are the action θ as defined above, and any 2-cocycle f_s for any section $s \colon Q \to G$.

Note that extension data are non-unique, as we may choose any representative of the corresponding 2-cohomology class. Two extension data for the pair (Q, A) are *equivalent* if they have the exact same action and if the two 2-cocycles are cohomologous (differ by a coboundary).

Two important special cases of extension data (θ, f) are as follows.

f **is trivial (as 2-cohomology class).** This implies that there exists $P \leq G$ such that $AP = G$ and $P \cap A = \mathrm{id}$. Such P is called the *complement* of A in G, and the extension is called a *split* extension. In this case only Equation 1 is present in the pseudo-congruence test, equivalently, Extension Data Pseudo-congruence becomes Action Compatibility.

θ **is trivial.** This implies that $A \subseteq Z(G)$, and the extension is called central. In this case, we only need to focus on Equation 2 in the pseudo-equivalence test, that is, Extension Data Pseudo-congruence becomes Cohomology Class Isomorphism.

Remark 2.2. It is not difficult to test whether an input satisfies one of the above conditions: it is trivial to test whether an extension is central; see Appendix A for an algorithm to test whether an extension is split.

3 The main lemma

3.1 For abelian characteristic subgroups

Recall that a characteristic subgroup is a subgroup invariant under all automorphisms. The analogous notion for isomorphisms (rather than automorphisms) is a function $\mathcal{S}$ that assigns to each group G a subgroup $\mathcal{S}(G) \leq G$ such that any isomorphism $\varphi\colon G_1 \to G_2$ restricts to an isomorphism $\varphi|_{\mathcal{S}(G_1)}\colon \mathcal{S}(G_1) \to \mathcal{S}(G_2)$. In line with other works in group theory, we call such a function a *characteristic subgroup functor.* Note that if $G_1 = G_2$, this says that $\mathcal{S}(G_1)$ is sent to itself by every automorphism of G_1, that is, $\mathcal{S}(G_1)$ is a characteristic subgroup of G_1. Most natural characteristic subgroups encountered are characteristic subgroup functors, for example the center $Z(G)$, the commutator subgroup $[G, G]$, or the radical $\mathrm{Rad}(G)$.

Let $\mathcal{S}$ denote a fixed characteristic subgroup functor, and suppose we are given two groups G_1, G_2 such that $\mathcal{S}(G_1)$ and $\mathcal{S}(G_2)$ are both abelian. We first examine the consequences of an isomorphism $G_1 \cong G_2$. Let $\gamma : G_1 \to G_2$ be an isomorphism. By the definition of characteristic subgroup functor, $\gamma(\mathcal{S}(G_1)) = \mathcal{S}(G_2)$, thus $\mathcal{S}(G_1) \cong \mathcal{S}(G_2)$ (identified as A) and $G_1/\mathcal{S}(G_1) \cong G_2/\mathcal{S}(G_2)$ (identified as Q). Let (θ_i, f_i) be the extension data of $A \hookrightarrow G_i \twoheadrightarrow Q$, where $\theta_i : Q \to \mathrm{Aut}(A)$ and $f_i \in Z^2(Q, A, \theta_i)$. As we've identified $A = \mathcal{S}(G_1) = \mathcal{S}(G_2)$ and $Q = G_1/\mathcal{S}(G_1) = G_2/\mathcal{S}(G_2)$, γ induces some $\alpha \in \mathrm{Aut}(A)$ and $\beta \in \mathrm{Aut}(Q)$. We write $\theta_{i,q}$ as the shorthand for $\theta_i(q)$ for $i = 1, 2$ and $q \in Q$. It can then be verified that for $q \in Q$ and $a \in A$,

$$\theta_1(q)(a) = \alpha^{-1}(\theta_{2,\beta(q)}(\alpha(a))) =: \theta_2^{(\alpha,\beta)}(q)(a), \tag{1}$$

and we record this as $\theta_1 = \theta_2^{(\alpha,\beta)}$, where $\theta_2^{(\alpha,\beta)}$ is defined as above.

It can be similarly verified that $[f_1] = [f_2^{(\alpha,\beta)}]$ as cohomology classes in $H^2(Q, A, \theta_1)$, where $f_2^{(\alpha,\beta)}(p, q) := \alpha^{-1}(f_2(\beta(p), \beta(q)))$ for all $p, q \in Q$. In other words, we have:

$$f_1(p, q) = \alpha^{-1}(f_2(\beta(p), \beta(q))) + f_u(p, q) \tag{2}$$

for some 2-coboundary $f_u \in B^2(Q, A, \theta_1)$. Note that Equation 1 ensures $f_2^{(\alpha,\beta)}$ is a 2-cocycle in $Z^2(Q, A, \theta_1)$. This discussion leads to the following definition:

Definition 3.1. Let A be an abelian group and Q any group, and let (θ_1, f_1) and (θ_2, f_2) be two extension data for A-by-Q. Then the extension data are *pseudo-congruent*[9] if there exists $(\alpha, \beta) \in \mathrm{Aut}(A) \times \mathrm{Aut}(Q)$, such that $\theta_1 = \theta_2^{(\alpha,\beta)}$ and $[f_1] = [f_2^{(\alpha,\beta)}]$, that is, Equations (1) and (2) hold. In this case we write $(\theta_1, f_1) \cong (\theta_2, f_2)$.

Lemma 3.2 (Main Lemma)**.** *Let $\mathcal{S}$ be a characteristic subgroup functor. Given two finite groups G_1 and G_2, suppose $\mathcal{S}(G_1)$ and $\mathcal{S}(G_2)$ are abelian. Then $G_1 \cong G_2$ if and only if both of the following conditions hold:*

1. *$\mathcal{S}(G_1) \cong \mathcal{S}(G_2)$ (which we denote by A) and $G_1/\mathcal{S}(G_1) \cong G_2/\mathcal{S}(G_2)$ (which we denote by Q);*
2. *$(\theta_1, f_1) \cong (\theta_2, f_2)$, where (θ_i, f_i) is the extension data of the extensions $A \hookrightarrow G_i \twoheadrightarrow Q$ (by (1)).*

Proof. The above discussion shows the only if direction. For the other direction, suppose we are given an abelian group A, a group Q, an action $\theta : Q \to \mathrm{Aut}(A)$, and a 2-cocyle $f : Q \times Q \to A$, $f \in Z^2(Q, A, \theta)$. We shall need the following procedure of Eilenberg and MacLane [EM47] that takes A, Q, θ and f as input, and outputs a group H as an extension of A by Q with extension data (θ, f). We refer to this as the *standard reconstruction procedure.* The set of group elements of H is $A \times Q$. For $(a, p), (b, q) \in A \times Q$, the group operation $\circ_H$ is defined as

$$(a, p) \circ_H (b, q) = (a + \theta_p(b) + f(p, q), pq).$$

A simple but tedious calculation verifies that $A \hookrightarrow H \twoheadrightarrow Q$ is an extension with extension data (θ, f).

Getting back to our problem, from $(\theta_1, f_1) \cong (\theta_2, f_2)$, we can choose appropriate sections $s_i \colon Q \to G_i$ such that the corresponding 2-cocycles satisfy $f_1 = f_2^{(\alpha,\beta)}$ in $Z^2(Q, A, \theta_1)$. Note that as $\theta_1 = \theta_2^{(\alpha,\beta)}$, $f_2^{(\alpha,\beta)} \in Z^2(Q, A, \theta_1)$. Now apply the standard reconstruction procedure to (θ_i, f_i) to get $H_i \cong G_i$. It is then straightforward to verify that the bijection $\gamma \colon H_1 \to H_2$ defined by $\gamma((a, p)) = (\alpha(a), \beta(p))$ is in fact an isomorphism. □

3.2 Pseudo-congruence of extensions and extension data

The standard concepts of pseudo-congruence and equivalence apply to group extensions themselves, rather than extension data as in our definitions. We use our definitions because the standard definitions seem to presuppose that the total groups are isomorphic, whereas in our setting the whole goal is to determine whether this is the case. However, we show below that the definitions are in fact equivalent (which is closely related to the Main Lemma 3.2). We present the standard definition here as it has more intuitive appeal and we believe it makes our subsequent discussions clearer, for example the proof of Theorem 7.1.

Definition 3.3. Two extensions $A \hookrightarrow G_i \twoheadrightarrow Q$ $(i = 1, 2)$ of A by Q are *pseudo-congruent* if there is an isomorphism $\gamma \colon G_1 \to G_2$ such that $\gamma(A) = A$. In particular, γ induces automorphisms $\alpha \in \mathrm{Aut}(A)$ and $\beta \in \mathrm{Aut}(Q)$.

Pictorially, G_1 and G_2 are pseudo-congruent as extensions if there exist $\alpha \in \mathrm{Aut}(A)$, $\beta \in \mathrm{Aut}(Q)$

and $\gamma \in \mathrm{Iso}(G_1, G_2)$ such that the following diagram commutes:[14]

$$\begin{tikzcd}
A \arrow[r, hook, "\iota_1"] \arrow[d, "\alpha", "\cong"'] & G_1 \arrow[r, two heads, "\pi_1"] \arrow[d, "\gamma", "\cong"'] & Q \arrow[d, "\beta", "\cong"'] \\
A \arrow[r, hook, "\iota_2"] & G_2 \arrow[r, two heads, "\pi_2"] & Q
\end{tikzcd}$$

where ι_i is the injective homomorphism from A to G_i and π_i is the surjective homomorphism from G_i to Q with $\mathrm{Ker}(\pi_i) = \mathrm{Im}(\iota_i)$. It is possible for the total groups G_1 and G_2 to be isomorphic without the extensions being pseudo-congruent (see Example E.2).

Despite the fact that the usual Definition 3.3 seems to presuppose that the total groups are isomorphic, in fact it is equivalent to our Definition 3.1. The isomorphism of the total groups follows for free from pseudo-congruence of the extension data:

Lemma 3.4. *Definitions 3.1 and 3.3 are equivalent. In detail: let $A \hookrightarrow G_i \twoheadrightarrow Q$ $(i = 1, 2)$ be extensions of A by Q, and let (θ_i, f_i) be the corresponding extension data. Then G_1 and G_2 are pseudo-congruent as extensions of A by Q if and only if $(\theta_1, f_1) \cong (\theta_2, f_2)$.*

Proof. Suppose that the extensions are pseudo-congruent (Definition 3.3), and let $\gamma \in \mathrm{Iso}(G_1, G_2)$, $\alpha \in \mathrm{Aut}(A)$, $\beta \in \mathrm{Aut}(Q)$ be as in Definition 3.3. It is readily verified that $\theta_1 = \theta_2^{(\alpha,\beta)}$ and $[f_1] = [f_2^{(\alpha,\beta)}]$, that is, that the extension data are pseudo-congruent under Definition 3.1.

Conversely, suppose the extension data are pseudo-congruent (Definition 3.1). Then the isomorphism γ constructed in the proof of the Main Lemma 3.2 satisfies the conditions of Definition 3.3. □

Recall that two extension data are equivalent if they have the same action, and cohomologous 2-cocycles. Eilenberg and MacLane [EM47] showed that two extensions have equivalent extension data if and only if the extensions satisfy a very strict form of pseudo-congruence:

Definition 3.5. Two extensions $A \hookrightarrow G_i \twoheadrightarrow Q$ $(i = 1, 2)$ are *equivalent* if there exists an isomorphism $\gamma : G_1 \to G_2$, such that $\gamma(A) = A$, and γ induces the identity automorphism on both A and Q.

Theorem 3.6 (Eilenberg-MacLane [EM47], see also [Rob96])**.** *There is a bijection between equivalence classes of extensions of A by Q with action θ, and elements of the group $H^2(Q, A, \theta)$.*

This theorem also shows that our definition of "equivalent extension data" is equivalent to Definition 3.5.

3.3 The main lemma for nonabelian normal subgroups

Here we consider extensions $N \hookrightarrow G \twoheadrightarrow Q$ where N need not be abelian, i. e., the general case. We show that our Main Lemma 3.2 extends to the case when N comes from a characteristic subgroup functor (not necessarily abelian), showing the usefulness of the extension theory perspective in its full generality. The results of this section will only be needed in the next section, to show that the polynomial-time algorithm for semisimple groups [BCQ12] fits into the framework of the Main

[14] Such a diagram *commutes* if for any two directed paths in the diagram from one group to another, the corresponding compositions are equal as maps.

Lemma. Throughout the rest of the paper we only consider extensions where N is abelian. Suzuki's book [Suz86] contains a nice introduction to the extension theory in the nonabelian case, while our contribution here is to adapt this theory explicitly to the setting of isomorphism testing.

The action. The first difference to notice when N is non-abelian is that the conjugation map $\theta' \colon G \to \mathrm{Aut}(N)$, defined by $\theta'(g) = c_g$ where $c_g(n) = gng^{-1}$, no longer contains N in its kernel, and hence no longer descends to a map $Q \to \mathrm{Aut}(N)$. However, the action of N on itself by conjugation is by inner automorphisms (by definition) so that we do get a well-defined map $G/N \to \mathrm{Aut}(N)/\mathrm{Inn}(N)$, that is, $Q \to \mathrm{Out}(N)$. For ease of reference, we give a name to such maps:

Definition 3.7. An *outer action* of a group Q on a group N is a group homomorphism $Q \to \mathrm{Out}(N) = \mathrm{Aut}(N)/\mathrm{Inn}(N)$.

In computations, rather than represent an outer automorphism as a coset of $\mathrm{Inn}(N)$ in $\mathrm{Aut}(N)$, we simply give it by a representative automorphism, and must remember when we may need to multiply by an arbitrary element of $\mathrm{Inn}(N)$. Throughout this section we use T to denote an action rather than θ, to remind the reader that the essential object here is the outer action represented by T, despite the fact that we work directly with actions $T \colon Q \to \mathrm{Aut}(N)$.

Correspondingly, in the setting of general N, the problem Action Compatibility must be generalized to Outer Action Compatibility, which is defined as follows. Two actions $T_1, T_2 \colon Q \to \mathrm{Aut}(N)$ are said to be "outer equivalent" if there is a set map $t' \colon Q \to \mathrm{Inn}(N)$ and an automorphism $\alpha \in \mathrm{Aut}(N)$ such that $T_1(q) = \alpha^{-1} \circ t'(q) \circ T_2(q) \circ \alpha$ for all $q \in Q$. The Outer Action Compatibility problem is then: given two actions $T_1, T_2 \colon Q \to \mathrm{Aut}(N)$, determine whether there an element $\beta \in \mathrm{Aut}(Q)$ such that T_1 and $T_2 \circ \beta$ are outer equivalent. Putting these two definitions together, we see that Outer Action Compatibility is the question of whether there exists $(\beta, \alpha, t') \in \mathrm{Aut}(Q) \times (\mathrm{Aut}(N) \ltimes \mathrm{Inn}(N)^Q)$ such that $T_1(q) = \alpha^{-1} \circ t'(\beta(q)) \circ T_2(\beta(q)) \circ \alpha$ for all $q \in Q$.

Although this formulation of Outer Action Compatibility is more complicated than if we had represented an outer automorphism as a full coset $\theta\mathrm{Inn}(N)$, it will be useful when we formulate Extension Data Pseudo-congruence below.

Note that when N is abelian there are no inner automorphisms, so $\mathrm{Out}(N) = \mathrm{Aut}(N)$, the only choice for t' above is trivial, and Outer Action Compatibility then becomes Action Compatibility.

Remark 3.8. We note that, unlike the case of N abelian, when N is nonabelian it is possible that some outer actions $\theta \colon Q \to \mathrm{Out}(N)$ may not be induced by *any* extension of N by Q. When there *is* such an extension, the outer action θ is called *extendible*. Eilenberg and MacLane [EM47, Sec. 7–9] characterize which outer actions are extendible in terms of the third cohomology group $H^3(Q, Z(N))$. As our interest is primarily in GpI, whenever it matters (e. g., in the definition of Outer Action Compatibility) we happily restrict our attention to extendible outer actions. Note that the characterization in terms of cohomology with coefficients in $Z(N)$ allows one to use linear algebra over the abelian group $Z(N)$ to test in polynomial time whether a given outer action is extendible.

The cohomology class. As in the case of N abelian, one may still choose a set-theoretic section $s \colon Q \to G$ and get a 2-cocycle $f_s \colon Q \times Q \to N$. This section s gives an action (not just outer action) $T_s\colon Q \to \mathrm{Aut}(N)$ as above, namely $T_s(q)(n) = s(q)ns(q)^{-1}$. Starting from associativity in G, one may then work out, as in the abelian case, the 2-cocycle condition: $f_s(q_1,q_2)f_s(q_1q_2,q_3) = T_s(q_1)(f_s(q_2,q_3))f_s(q_1,q_2q_3)$. However, this condition depends not just on the action T_s and the 2-cochain f_s, but also on some relationship between T_s and f_s (in this case, that they come from the *same* section s). We would much prefer a condition that does not depend on the ambient extension group G. To get this condition, note that the action satisfies $T_s(q_1)T_s(q_2) = c_{f_s(q_1,q_2)}T_s(q_1q_2)$, where $c_n\colon N \to N$ denotes the inner automorphism given by conjugation by $n \in N$: $c_n(m) = nmn^{-1}$. This leads us to our definition of extension data for general N:

Definition 3.9 (Extension data for general Q, N)**.** Let Q and N be groups. We say that a pair (T, f) of an action $T\colon Q \to \mathrm{Aut}(N)$ and a set map $f\colon Q \times Q \to N$ is *extension data* if, for all $q_i \in Q$,

$$T(q_1)T(q_2) = c_{f(q_1,q_2)}T(q_1q_2) \tag{3}$$

and

$$f(q_1,q_2)f(q_1q_2,q_3) = T(q_1)\left(f(q_2,q_3)\right)f(q_1,q_2q_3). \tag{4}$$

In this case, we refer to f as a 2-cocycle with respect to the action T.

Note that condition (3) very nearly determines f: it determines $f(q_1,q_2)$ up to an element of $Z(N)$. In particular, when $Z(N) = 1$ condition (3) actually does determine f completely, a fact we will take advantage of when discussing the polynomial-time algorithm for groups with no abelian normal subgroups [BCQ12].

Another difference in the case of N nonabelian is that, although we might denote the set of 2-cocycles by $Z^2(Q,N,T)$, this set will not in general be a group in any natural way, let alone an abelian group. (Also note that it depends on the action T, whereas we know that the action is not intrinsic to the extension but only the corresponding outer action is.) However, the difference of two 2-cocycles with respect to the same action T will land in the center $Z(N)$, allowing us to reduce part of the question back to the case of N abelian. To see this, let f_1, f_2 be two 2-cocycles with respect to an action $T\colon Q \to \mathrm{Aut}(N)$, and consider their difference $f_1(q_1,q_2)f_2(q_1,q_2)^{-1}$:

$$c_{f_1(q_1,q_2)f_2(q_1,q_2)^{-1}} = T(q_1)T(q_2)T(q_1q_2)^{-1}T(q_1q_2)T(q_2)^{-1}T(q_1) = \mathrm{id}_N.$$

As the center $Z(N)$ consists exactly of those $n \in N$ such that $c_n = \mathrm{id}_N$, we find that $f_1(q_1,q_2)f_2(q_1,q_2)^{-1} \in Z(N)$. So although there isn't really a cohomology group "$H^2(Q,N,T)$," we will see that we can nonetheless reduce to questions about cohomology classes in $H^2(Q, Z(N), T|_{Z(N)})$.

Equivalence. As in the case of N abelian, two extensions $N \hookrightarrow G_i \twoheadrightarrow Q$ are said to be *equivalent* if there is an isomorphism $\gamma\colon G_1 \to G_2$ such that γ induces the identity map on both N and Q. However, since $Z^2(Q,N,T)$ is no longer a group and $B^2(Q,N,T)$ no longer its subgroup, the notion of equivalent extensions doesn't translate so easily to a notion of equivalence for extension data. Hence we derive this condition more or less from scratch. That is, we derive what it means for two extension data to be equivalent by analyzing how two extension data coming from the same extension may differ, when a different choice of section $s\colon Q \to G$ is made.

Fix an extension $N \hookrightarrow G \twoheadrightarrow Q$ and two sections $s_1, s_2\colon Q \to G$. Let $t(q) := s_1(q)s_2(q)^{-1}$; as the s_i are both sections, $s_1(q)$ and $s_2(q)$ are in the same coset of N, so that $t(q) \in N$ for all $q \in Q$.

Then the actions $T_1 = \theta_{s_1}$ and $T_2 = \theta_{s_2}$ differ by the inner automorphism $c_{t(q)}\colon T_1(q) = c_{t(q)} \circ T_2(q)$. Recall that we set $f_i(q_1, q_2) := s_i(q_1)s_i(q_2)s_i(q_1q_2)^{-1}$. Then we have that

$$\begin{aligned}
f_1(q_1, q_2) &= s_1(q_1)s_1(q_2)s_1(q_1q_2)^{-1} \\
&= t(q_1)s_2(q_1)t(q_2)s_2(q_2)s_2(q_1q_2)^{-1}t(q_1q_2)^{-1} \\
&= t(q_1)T_2(q_1)(t(q_2))s_2(q_1)s_2(q_2)s_2(q_1q_2)^{-1}t(q_1q_2)^{-1} \\
&= t(q_1)T_2(q_1)(t(q_2))f_2(q_1, q_2)t(q_1q_2)^{-1} \\
&= t(q_1)T_2(q_1)(t(q_2))c_{f_2(q_1,q_2)}(t(q_1q_2)^{-1})f_2(q_1, q_2) =: f_2^t(q_1, q_2)
\end{aligned}$$

For future reference, we denote this final expression by $f_2^t(q_1, q_2)$. Note that f_2^t in fact also depends on the action T_2, but this action will always be clear from context.

Definition 3.10. Two extension data (T_i, f_i) are *equivalent* if there is a map $t\colon Q \to N$ such that $T_1(q) = c_{t(q)} \circ T_2(q)$ for all $q \in q$ and $f_1 = f_2^t$.

There are several aspects of this definition to take note of:

- By definition, two extension data can be equivalent only if $T_1(q)$ and $T_2(q)$ represent the same outer automorphism of N, in accord with our discussion above.
- This definition agrees with the definition of equivalent extensions for N abelian. For when N is abelian, $c_{t(q)} = \mathrm{id}_N$ and the condition $f_1 = f_2^t$ exactly says that f_1 and f_2 differ by the 2-coboundary f_t defined by t.
- $T_1 = T_2$ if and only if $s_1(q)$ and $s_2(q)$ differ by an element of the center $Z(N)$, that is, t is a map $Q \to Z(N)$. In this case, let $T = T_1 = T_2$; then (T, f_1) and (T, f_2) are equivalent if and only if f_1 and f_2 differ by the coboundary $f_t \in B^2(Q, Z(N), T)$. Again, this will be relevant for our discussion below of the polynomial-time algorithm for semisimple groups [BCQ12].

Pseudo-congruence. As before, pseudo-congruence is defined as "equivalence up to twisting by $\mathrm{Aut}(N) \times \mathrm{Aut}(Q)$:"

Definition 3.11 (Pseudo-congruence of extension data for general Q, N)**.** Let Q and N be two groups. Two extension data $(T_i, f_i) \in (Q \to \mathrm{Aut}(N), Q \times Q \to N)$ are *pseudo-congruent* if there exists $(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(Q)$ such that (T_1, f_1) and $(T_2^{(\alpha,\beta)}, f_2^{(\alpha,\beta)})$ are equivalent.

In more detail, the extension data are pseudo-congruent if there exists $(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(Q)$ and $t\colon Q \to N$ such that, for all $q \in Q$ and all $n \in N$:

$$T_1(q)(n) = (\alpha^{-1} \circ c_{t(\beta(q))} \circ T_2(\beta(q)) \circ \alpha)(n) \tag{5}$$

and

$$f_1(q_1, q_2) = \alpha^{-1}\left[f_2^t(\beta(q_1), \beta(q_2))\right] =: f_2^{(\alpha,\beta,t)}(q_1, q_2). \tag{6}$$

Lemma 3.12 (Main Lemma for general Q, N)**.** *Let $\mathcal{S}$ be a characteristic subgroup functor. Given two finite groups G_1 and G_2, $G_1 \cong G_2$ if and only if both of the following conditions hold:*

1. *$\mathcal{S}(G_1) \cong \mathcal{S}(G_2)$ (which we denote by N) and $G_1/\mathcal{S}(G_1) \cong G_2/\mathcal{S}(G_2)$ (which we denote by Q);*

2. $(T_1, f_1) \cong (T_2, f_2)$*, where* (T_i, f_i) *is the extension data of the extensions* $N \hookrightarrow G_i \twoheadrightarrow Q$ *(by (1)).*

Proof. First suppose that $\gamma\colon G_1 \to G_2$ is an isomorphism. Since $\mathcal{S}$ is a characteristic subgroup functor, γ restricts to an isomorphism between the copy $\mathcal{S}(G_1)$ of N in G_1 and the copy $\mathcal{S}(G_2)$ of N in G_2, i. e., an automorphism $\alpha \in \operatorname{Aut}(N)$. Consequently, γ induces an automorphism $\beta := \overline{\gamma} \in \operatorname{Aut}(Q)$. After twisting by these automorphisms, the discussion preceding Definition 3.10 shows that the extension data become equivalent.

Conversely, suppose $(T_1, f_1) \cong (T_2, f_2)$, via $(\alpha, \beta, t) \in \operatorname{Aut}(N) \times \operatorname{Aut}(Q) \times (Q \to N)$. As in the abelian case we have a standard reconstruction procedure; we construct groups H_i from (T_i, f_i) such that $H_i \cong G_i$, and then we show how the pseudo-congruence of the extension data easily yields an isomorphism $H_1 \cong H_2$.

The underlying set of H_i will be $N \times Q$, with multiplication defined by

$$(n, p) \circ_{H_i} (m, q) = (nT_i(p)(m)f_i(p, q), pq).$$

Let $s_i\colon Q \to G_i$ denote the sections used to construct the extension data (T_i, f_i). Then it is readily verified that the map $(n, q) \mapsto ns_i(q)$ gives an isomorphism $H_i \overset{\cong}{\to} G_i$.

Finally, we claim that the map $\varphi(n, p) := (\alpha(n)t(\beta(p)), \beta(p))$ is an isomorphism from H_1 to H_2. The main fact to check is that this is even a homomorphism. Consider (n, p) and $(m, q) \in H_1$. On the one hand, we have

$$\begin{aligned}
\varphi((n, p) \circ_{H_1} (m, q)) &= \varphi(nT_1(p)(m)f_1(p, q), pq) \\
&= (\alpha(nT_1(p)(m)f_1(p, q))t(\beta(pq)), \beta(pq)) \\
&= (\alpha(n)\alpha(T_1(p)(m))\alpha(f_1(p, q))t(\beta(pq)), \beta(pq))
\end{aligned}$$

On the other hand, we have (here we'll sometimes use square brackets [] to denote application of an automorphism to help keep all the parentheses straight):

$$\begin{aligned}
\varphi(n, p) \circ_{H_2} \varphi(m, q) &= (\alpha(n)t(\beta(p)), \beta(p)) \circ_{H_2} (\alpha(m)t(\beta(q)), \beta(q)) \\
&= (\alpha(n)t(\beta(p))T_2(\beta(p))\,[\alpha(m)t(\beta(q))]\,f_2(\beta(p), \beta(q)), \beta(p)\beta(q) \\
&= (\alpha(n)t(\beta(p))T_2(\beta(p))[\alpha(m)]T_2(\beta(p))[t(\beta(q))]f_2(\beta(p), \beta(q)), \beta(pq)) \\
&= (\alpha(n)(c_{t(\beta(p))} \circ T_2(\beta(p)))[\alpha(m)]t(\beta(p))T_2(\beta(p))[t(\beta(q))]f_2(\beta(p), \beta(q)), \beta(pq))
\end{aligned}$$

Let's work through these two expressions bit by bit. We can dispense easily with the second coordinate, as $\beta(pq) = \beta(p)\beta(q)$ since $\beta \in \operatorname{Aut}(Q)$. Both of the first coordinates begin with $\alpha(n)$. Next we have $\alpha(T_1(p)(m))$ on the one hand and $(c_{t(\beta(p))} \circ T_2(\beta(p)))[\alpha(m)]$ on the other. From the definition of pseudo-congruence, we have that $T_1(p)(m) = \alpha^{-1}(c_{t(\beta(p)} \circ T_2(\beta(p)))[\alpha(m)]$. Applying α to both sides of this equation we see that these two terms are equal.

The remainder of the first coordinate is then $\alpha(f_1(p, q))t(\beta(pq))$ in the first case. From the definition of pseudo-congruence we have:

$$\begin{aligned}
\alpha(f_1(p, q))t(\beta(pq)) &= f_2^t(\beta(p), \beta(q))t(\beta(pq)) \\
&= t(\beta(p))T_2(\beta(p))[t(\beta(q))]f_2(\beta(p), \beta(q))t(\beta(pq))^{-1}t(\beta(pq)) \\
&= t(\beta(p))T_2(\beta(p))[t(\beta(q))]f_2(\beta(p), \beta(q),
\end{aligned}$$

which is exactly the remainder of the first coordinate in the second case, as desired. Hence φ is a homomorphism.

Finally, it suffices to show that φ is injective, for as $|H_1| = |N||Q| = |H_2|$, it will then follow that φ is bijective and hence an isomorphism. Consider the kernel of φ: $\varphi(n,p) = (1,1)$. As the second coordinate is 1, we have $\beta(p) = 1$ and hence $p = 1$. As the first coordinate is 1, we have $\alpha(n)t(\beta(p)) = \alpha(n) = 1$, so we also have $n = 1$. (In the first equality we use the fact that $t(1) = 1$, which follows from $T_i(1_Q) = \mathrm{id}_N$.) Hence φ is injective, and thus an isomorphism. □

Extensions with trivial outer action. We did not define Cohomology Class Isomorphism for general N and then proceed to pseudo-congruence, as in the abelian case, because it turns out that when the outer action is trivial, Cohomology Class Isomorphism for action-trivial extensions of N by Q reduces to Cohomology Class Isomorphism for extensions of $Z(N)$ by Q. To prove this we use one additional concept, that of a central product. A *central product* of two groups G_1 and G_2 is essentially the direct product $G_1 \times G_2$ with some subgroup of $Z(G_1)$ identified with an isomorphic subgroup of $Z(G_2)$. If $\varphi\colon Y_1 \to Y_2$ is an isomorphism between subgroups $Y_i \leq Z(G_i)$, then the central product $G_1 \times_Y G_2$ is defined to be the quotient of $G_1 \times G_2$ by the subgroup $\{(y^{-1}, \varphi(y)) : y \in Y_1\}$. Central products are characterized by the property that they contain a copy of each G_i (these copies may overlap nontrivially, viz. Y), and that these copies commute with one another.

Lemma 3.13. *Let $N \hookrightarrow G \twoheadrightarrow Q$ be an extension of N by Q which induces the trivial outer action $\theta(q) = \mathrm{id}_N\mathrm{Inn}(N)$ for all $q \in Q$. Then there is an extension $Z(N) \hookrightarrow H \twoheadrightarrow Q$ such that $G \cong N \times_{Z(N)} H$ (in fact, the two are even equivalent as extensions of N by Q). We denote the extension H by $G|_{Z(N)}$.*

Proof. There is a section $s\colon Q \to G$ such that $c_{s(q)} = \mathrm{id}_N$ for all $q \in Q$. Let $f(p,q) = f_s(p,q) = s(p)s(q)s(pq)^{-1}$ be the 2-cocycle corresponding to s. As $c_{s(q)} = \mathrm{id}_N$ for all $q \in Q$, we also have that $c_{f(p,q)} = \mathrm{id}_N$ for all $p, q \in Q$. As $f(p,q) \in N$, this implies that $f(p,q) \in Z(N)$. Hence f is a 2-cocycle in $H^2(Q, Z(N))$ (for the trivial action of Q on $Z(N)$). The standard reconstruction procedure (see the proof of the Main Lemma 3.2) then yields an extension $Z(N) \hookrightarrow G|_{Z(N)} \twoheadrightarrow Q$ which is a subgroup of G that contains $Z(N)$ and surjects onto Q.

The central product $N \times_{Z(N)} G|_{Z(N)}$ is readily seen to be an extension of N by Q, as $N \cap G|_{Z(N)} = Z(N)$ in this group. Next, as $G|_{Z(N)}$ commutes with N in $N \times_{Z(N)} G|_{Z(N)}$, the outer action of Q on N induced by the extension $N \hookrightarrow N \times_{Z(N)} G|_{Z(N)} \twoheadrightarrow Q$ is trivial. Finally, we have already seen that the f from above is also a 2-cocycle corresponding to the extension $N \hookrightarrow N \times_{Z(N)} G|_{Z(N)} \twoheadrightarrow Q$. Hence the extension data for $N \times_{Z(N)} G|_{Z(N)}$ is identical to that for G (not even just equivalent). From the discussion of equivalence above, it follows that G is equivalent to $N \times_{Z(N)} G|_{Z(N)}$ as extensions of N by Q, and in particular that $G \cong N \times_{Z(N)} G|_{Z(N)}$. □

Proposition 3.14. *Let $\mathcal{S}$ be a polynomial-time computable characteristic subgroup functor. Suppose that G_1, G_2 are two groups for which the induced outer action of $G_i/\mathcal{S}(G_i)$ on $\mathcal{S}(G_i)$ by conjugation is trivial (equivalently: the induced action is by inner automorphisms of $\mathcal{S}(G_i)$). Then the group isomorphism problem for (G_1, G_2) Cook-reduces to the two instances of* GpI *given by $(\mathcal{S}(G_1), \mathcal{S}(G_2))$ and $(G_1|_{Z(\mathcal{S}(G_1))}, G_2|_{Z(\mathcal{S}(G_2))})$.*

In particular, group isomorphism for groups for which the outer action of $G/\mathrm{Rad}(G)$ on $\mathrm{Rad}(G)$ is trivial reduces to isomorphism of central radical groups and isomorphism of solvable groups.

Proof. If $\mathcal{S}(G_1) \cong \mathcal{S}(G_2)$, then Lemma 3.13 implies that $G_1 \cong G_2$ if and only if $G_1|_{Z(\mathcal{S}(G_1))} \cong G_2|_{Z(\mathcal{S}(G_2))}$, so all that remains to show is that $G_i|_{Z(\mathcal{S}(G_i)}$ can be constructed in polynomial time. We do this for G_1, the proof for G_2 being identical. Let $N = \mathcal{S}(G_i)$ and $Q = G_1/N$. By assumption, the subset $N = \mathcal{S}(G_i)$ can be identified from the Cayley table of G_1 in polynomial time.

Next, choose any section $s\colon Q \to G$. It may be that some $s(q)$ acts nontrivially on N via conjugation. However, by the assumption that the outer action is trivial, $c_{s(q)}$ must be some inner automorphism of N, say $c_{n(q)}$ for some $n(q) \in N$. To find this $n(q)$, we may search through N exhaustively in at most $O(|N|^2) \leq O(|G_1|^2)$ time: essentially $|N|$ steps to check the action of a given n on N by conjugation, and there are $|N|$ possible n's to check. Then let $s'(q) = s(q)n(q)^{-1}$; as $n(q) \in N$, s' is another section, and by construction $c_{s'(q)} = \mathrm{id}_N$ for all N.

Finally, let $f(p, q) = s'(p)s'(q)s'(pq)^{-1}$. Computing all the values of f takes essentially $O(|Q|^2) \leq O(|G_1|^2)$ time, and then the standard reconstruction procedure lets us construct the Cayley table of $G_1|_{Z(\mathcal{S}(G_1)}$ in polynomial time. □

Extensions of centerless groups. We have already mentioned a few useful properties of extensions of centerless groups, that is, when $Z(N) = 1$. One that is implicit in what we've already said is that every outer action $Q \to \mathrm{Out}(N)$ is extendible, that is, it is induced from some extension of N by Q. These properties culminate in the following very useful theorem:

Theorem 3.15 (see, e. g., [Suz86, Thm. 2.7.11])**.** *Let N be a centerless group, Q any group, and G an extension of N by Q. Then G is determined up to isomorphism by the induced outer action of Q on N.*

Furthermore, every such extension is equivalent to a subgroup $\Gamma \leq Q \times \mathrm{Aut}(N)$ satisfying $\Gamma \cap \mathrm{Aut}(N) = \mathrm{Inn}(N)$ and $\pi_Q(U) = Q$, where $\pi_Q\colon Q \times \mathrm{Aut}(N) \to Q$ is the projection onto the first factor.

In particular, if $\mathcal{S}$ is a characteristic subgroup functor computable in polynomial time, and $\mathfrak{C}$ is a class of groups for which $\mathcal{S}(G)$ is centerless for every $G \in \mathfrak{C}$, then isomorphism of groups in $\mathfrak{C}$ reduces to isomorphism of groups of the type $G/\mathcal{S}(G)$ for $G \in \mathfrak{C}$, groups of the type $\mathcal{S}(G)$ for $G \in \mathfrak{C}$, and Outer Action Compatibility.

4 The strategy

Suppose we are given two groups G_1 and G_2 from some class of groups $\mathfrak{C}$. Our Main Lemma 3.12 suggests (and indeed was motivated by) a divide-and-conquer strategy to test isomorphism (Section 4.1). This strategy highlights important structural features of GpI, which we show are formally necessary in Section 4.3. It also naturally suggests new group classes for which polynomial-time isomorphism tests might be within reach, and also suggests *a priori* many group classes for which polynomial-time algorithms have previously been achieved. In Section 4.2 we show how essentially all previous polynomial-time algorithms for special classes of groups (with the easy exceptions of abelian groups and groups generated by $O(1)$ elements, such as simple groups) can be viewed as special cases of this strategy.

4.1 A recipe for group isomorphism

1. Choose wisely a polynomial-time computable characteristic subgroup functor $\mathcal{S}$. Note that if $\mathcal{S}(G)$ is always abelian, then the technically simpler abelian Main Lemma 3.2 can be applied.

2. Test whether $\mathcal{S}(G_1) \cong \mathcal{S}(G_2)$ (which we henceforth refer to as N) and $G_1/\mathcal{S}(G_1) \cong G_2/\mathcal{S}(G_2)$ (which we refer to as Q). If either of these fails, then $G_1 \ncong G_2$.

3. Extract the extension data (T_i, f_i) from the extension $N \hookrightarrow G_i \twoheadrightarrow Q$ for $i = 1, 2$ by picking arbitrary sections $s\colon Q \to G_i$ and computing the action and cohomology class.

4. Test pseudo-congruence of the two extension data. That is, find $(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(Q)$, and a map $t : Q \to N$ such that $T_1(q) = c_{t(q)} \circ T_2^{(\alpha,\beta)}(q)$ and $f_1 = (f_2^{(\alpha,\beta)})^t$. If the abelian Main Lemma 3.2 applies, then t is unnecessary.

Some general remarks are due for each of these steps:

1. A seemingly obvious requirement would be that $\mathcal{S}(G)$ should not be trivial for any $G \in \mathfrak{C}$. However, even if this is not the case, it may be fruitful to consider separately the class of groups for which $\mathcal{S}(G)$ is trivial. For example, semisimple groups arise this way, as those groups for which $\mathrm{Rad}(G)$ is trivial.

2. Due to the nature of the divide and conquer strategy, $\mathcal{S}(G)$ and $G/\mathcal{S}(G)$ should be from group classes with known efficient isomorphism tests. Alternatively, if, say, $\mathcal{S}(G)$ is not from such a class, it may be possible to use this strategy to reduce isomorphism of groups in $\mathfrak{C}$ to isomorphism of groups of the form $\mathcal{S}(G)$ for $G \in \mathfrak{C}$ (or similarly for $G/\mathcal{S}(G)$).

3. This step is easy in the Cayley table model. Based on the group class $\mathfrak{C}$ the extension data usually turn out to have nice mathematical structure;

4. This pseudo-congruence test is the main bottleneck. Choosing $\mathcal{S}$ so that this step can take advantage of known cohomological results may be helpful. For example, if $\mathcal{S}(G) \leq Z(G)$ then Extension Data Pseudo-congruence simplifies to Cohomology Class Isomorphism; at the opposite end of the spectrum, if $G = \mathcal{S}(G) \rtimes (G/\mathcal{S}(G))$ then Extension Data Pseudo-congruence simplifies to Action Compatibility. As another example, if $\mathcal{S}(G)$ is centerless, one may take advantage of Theorem 3.15, as in the case of semisimple groups (see below).

4.2 Previous results from the point of view of the main lemma

As mentioned in the introduction, there have been polynomial-time algorithms for several group classes: semisimple groups, generalized Heisenberg groups, groups with abelian Sylow towers, and (in Section 7) $n^{o(\log n)}$-time algorithms for central-radical groups. However, the definitions of these group classes may at first seem obscure, and it is not *a priori* clear why we should have found efficient algorithms for these particular classes of groups, as opposed to others. We believe that the viewpoint of extensions and cohomology, especially in light of the Main Lemma, gives a unifying perspective to these works which helps to explain the progress on these group classes.

In the following, we first summarize some basic information about these works, and then explain in detail how previous works on GpI fit into the general strategy described as above.

References	Group class	Characteristic subgroup functor	Extension type
[BCGQ11, BCQ12]	Semisimple groups	Socle	Extension of a centerless group
[LW12]	Quotients of generalized Heisenberg groups	Center	Special type of central extension of $\mathbb{Z}_p^k$ by $\mathbb{Z}_p^\ell$
[LG09, QST11, BQ12]	Groups with abelian Sylow towers	Normal Hall subgroups	Split extension of A by Q with $(\|A\|, \|Q\|) = 1$
This work	Central-radical groups	Solvable radical	Central extension of abelian groups by semisimple groups

Semisimple groups (groups with no abelian normal subgroups). In the polynomial-time algorithm for semisimple groups [BCQ12] we take $\mathcal{S} = \mathrm{Soc}$, i. e., $N = \mathrm{Soc}(G)$, which is a polynomial-time characteristic subgroup functor. Hence the general Main Lemma 3.12 applies and isomorphism of semisimple groups reduces to Extension Data Pseudo-congruence. When G is semisimple, its socle is a direct product of nonabelian simple groups, so $Z(N) = 1$. N being centerless simplifies some of the results in the previous section (as captured in Theorem 3.15) and leads to the problems considered by Babai *et al.* [BCGQ11, BCQ12].

Note that in the definition of pseudo-congruence for nonabelian N, after twisting by $(\alpha, \beta) \in \mathrm{Aut}(N) \times \mathrm{Aut}(Q)$ to make the actions T_1, T_2 become equivalent as outer actions, the condition on the 2-cocycles is simply that they differ by a 2-coboundary in $B^2(Q, Z(N), T)$. In particular, when N is centerless $B^2(Q, Z(N), T)$ is trivial, so Extension Data Pseudo-congruence reduces to Outer Action Compatibility.

In the case of semisimple groups, using the structure of these groups, one sees quickly that Outer Action Compatibility reduces to the problem of twisted code equivalence (introduced in [BCQ12]), where the "twisting" groups correspond to the action of $\mathrm{Out}(N) = \mathrm{Out}(\mathrm{Soc}(G))$ in the definition of Outer Action Compatibility, and the choice of $t\colon Q \to N$ is handled by considering codes whose codewords correspond to elements of G rather than just elements of Q.

Nilpotent groups, esp. quotients of generalized Heisenberg groups. For p-groups of class 2 and exponent p with odd p, Baer's correspondence [Bae38] suggests considering the alternating bilinear maps defined by the commutator bracket: isomorphism of p-groups corresponds to pseudo-isometry of these bilinear maps. These bilinear maps are 2-cocycles, and two such cocycles are isomorphic as cohomology classes if and only if the bilinear maps are pseudo-isometric, so we see that this is a particular instance of Cohomology Class Isomorphism and Baer's correspondence can be viewed as a special case of the abelian Main Lemma 3.2.

Lewis and Wilson [LW12] studied a large class of p-groups—quotients of generalized Heisenberg groups—which are indistinguishable to classical invariants but for which they nonetheless present a polynomial-time isomorphism test. These groups can alternatively be characterized as those for which the centroid of the above bilinear map is a field (see [LW12, Theorem 3.1]). Their polynomial-time isomorphism test for these groups takes advantage of the special structure of the bilinear maps corresponding to these groups ([LW12, Theorem 4.1]).

Groups with abelian Sylow towers. Though claiming to solve GpI for the seemingly obscure group class "groups with abelian Sylow towers", the core of [BQ12] (following [LG09, QST11]) deals with the case of *coprime extensions*, namely extension of an abelian A by Q where $(|A|, |Q|) = 1$. The Schur–Zassenhaus Theorem guarantees that coprime extensions split, thus reducing Extension Data Pseudo-congruence to Action Compatibility for such groups. Assuming $\mathrm{Aut}(Q)$ is known (via recursive divide-and-conquer), [BQ12] views the actions of Q on A as linear representations and utilizes the completely reduciblility of these representation by Maschke's Theorem. Thus viewing the induced action of $\mathrm{Aut}(Q)$ on the irreducible constituents as a permutation group action, [BQ12] develops some parameterized permutation group algorithm to finally solve Action Compatibility in this case.

Central-radical groups. Similarly, by considering cohomology rather than actions we will see in the following how to handle central-radical groups. An elementary way of manipulating the 2-cohomology classes yields an $n^{O(\log\log n)}$-time algorithm for groups with central radicals. For a subclass of groups with central radicals, a more detailed understanding of 2-cohomology classes (Lemma 7.3) helps establish two polynomial-time algorithms under (natural) fixed parameters in Theorem 7.1. In particular, singly exponential algorithms for Linear Code Equivalence and for Coset Intersection enter inevitably in the algorithm for Theorem 7.1 (2).

4.3 Necessity of pseudo-congruence and cohomology

Lemma 3.2 suggests studying Extension Data Pseudo-congruence to make progress towards GpI for groups with abelian normal subgroups. In this section, we shall see that pseudo-congruence tests for certain classes of extension data are exactly isomorphism tests for certain interesting group classes. While Lemma 3.2 almost implies so, a pitfall is that in the reconstruction procedure we need the normal copy of A in H to be the image of a characteristic subgroup functor.[15] This leads us to look at some concrete classes of extension data, for which this property holds.

For split extensions, a well-known example is the case when $|A|$ and $|Q|$ are coprime, as ensured by the Schur–Zassenhaus Theorem. In this case G is said to be a coprime extension of A by Q, and A is a normal Hall subgroup in G.[16] Noting that taking a normal Hall subgroup of a specific order is a characteristic subgroup functor, with the standard reconstruction procedure we have:

Fact 4.1. There is a polynomial-time function r which takes any group action $\theta\colon G \to \mathrm{Aut}(B)$ (for any groups B, G) to a group $r(\theta)$ with the following property. When A is abelian, Q is a group of order coprime to $|A|$, and $\theta_i\colon Q \to \mathrm{Aut}(A)$ $(i = 1, 2)$ are group actions, then $(\theta_1, \theta_2) \mapsto (r(\theta_1), r(\theta_2))$ is a Karp reduction from these instances of Action Compatibility to GpI.

A polynomial-time algorithm for Action Compatibility for the case in Fact 4.1 was given in [BQ12], yielding a polynomial-time time algorithm for "groups with abelian Sylow towers" as phrased in [BQ12].

For central extensions, let $p \neq 2$ be a prime. For $A = \mathbb{Z}_p^k$ and $Q = \mathbb{Z}_p^\ell$, a bilinear map $f : Q \times Q \to A$ is a 2-cocycle, as the cocycle identity follows directly from bilinearity. Note that the

[15] In the setting of Lemma 3.2 the standard reconstruction procedure does return groups H_i with the copy of $A = \mathcal{S}(H_i)$, but this is because of the conditions of that lemma.

[16] The Schur–Zassenahus Theorem states that a coprime extension is split, regardless of whether A is abelian or not. When A is abelian the proof is straightforward. The bulk of the proof of the Schur–Zassenhaus Theorem is devoted to the case when A is nonabelian.

action of $\mathrm{Aut}(A)\times\mathrm{Aut}(Q)$ preserves bilinearity. The following proposition is known ([Bae38, Laz54], see also [War76, Section 5] and [Wil09a]); the standard reconstruction procedure is altered to make the image of A the commutator subgroup.

Fact 4.2. Given a prime $p \neq 2$, $A = \mathbb{Z}_p^k$ and $Q = \mathbb{Z}_p^\ell$, let $f_i : Q \times Q \to A$ be an alternating $\mathbb{Z}_p$-bilinear map. Then Cohomology Class Isomorphism for f_1, f_2 Karp-reduces to GpI.

Proof. Given f_i for $i = 1, 2$, alter the standard construction as follows. For $a, b \in A$ and $q, q' \in Q$, we define the group G_i with operation $\circ$ over the set $A\times Q$ as $(a, q)\circ(b, q') = (a+b+\frac{1}{2}f_i(q, q'), q+q')$. It is known that G_i's are p-groups of class 2, the copy of A in G_i is the commutator subgroup, and $f_1 \cong f_2$ if and only if $G_1 \cong G_2$ [Wil09a]. □

Finally let us examine groups whose solvable radicals are abelian, a super-class of central-radical groups. When Q is semisimple, the standard reconstruction procedure sends A to the solvable radical. (A solvable normal subgroup N is the solvable radical if and only if G/N is semisimple.) This hints at the fact that for central-radical groups, group isomorphism is equivalent to Cohomology Class Isomorphism.

Fact 4.3. Let A be abelian and Q semisimple. For $i = 1, 2$, let $\theta_i : Q \to \mathrm{Aut}(A)$ be a homomorphism, and $f_i : Q \times Q \to A$ be a 2-cocycle in $Z^2(Q, A, \theta_i)$. Then Extension Data Pseudo-congruence for (θ_1, f_1) and (θ_2, f_2) Karp-reduces to GpI.

5 Preliminaries for the algorithms

Some general notations are described at the beginning of §2.

Further notations and some group-theoretic facts. Given a finite set Ω, $\mathrm{Sym}(\Omega)$ denotes the symmetric group consisting of all permutations of Ω. A permutation group acting on Ω is a subgroup of $\mathrm{Sym}(\Omega)$. Given $\pi \in \mathrm{Sym}(\Omega)$ and $a \in \Omega$, the image of a under π is denoted by a^π. If $\Omega = [n]$, $n \in \mathbb{N}$, we use S_n to denote $\mathrm{Sym}(\Omega)$, and $A_n \leq S_n$ consists of permutations of even signs. For a vector space V over a field $\mathbb{F}$, the general linear group $\mathrm{GL}(V)$ consists of all non-singular linear transformations of V. If $V = \mathbb{F}_q^n$, q is a prime power, we may write $\mathrm{GL}(n, q)$ for $\mathrm{GL}(V)$.

By the Fundamental Theorem of Finite Abelian Groups, a finite abelian group is isomorphic to a direct product of cyclic groups of prime power orders. Formally, let A be an abelian group, then there exists a direct product decomposition of A as $A = \langle e_1\rangle \times \langle e_2\rangle \times \cdots \times \langle e_n\rangle$, where $e_i \in A$ has order $p_i^{k_i}$, such that $p_1 \leq p_2 \leq \cdots \leq p_n$, and if $p_i = p_{i+1}$, then $k_i \leq k_{i+1}$, for all i. This decomposition is called the primary decomposition of A, and the tuple $(e_1, \ldots, e_n)$ forms a basis of A. The elementary abelian groups are those groups of the form $\mathbb{Z}_p^n$ for some prime p and any n. Note that $\mathrm{Aut}(\mathbb{Z}_p^n) \cong \mathrm{GL}(n, p)$.

A group G is *simple* if $|G| > 1$ and G has no proper nontrivial normal subgroups. The celebrated Classification of Finite Simple Groups lists all finite simple groups explicitly [CCN$^+$85]. The only abelian simple groups are the cyclic groups of prime order. We use the following fact, which (currently) depends on the Classification for its proof:

Fact 5.1 ([Ste62, AG84])**.** Every nonabelian simple group can be generated by 2 elements.

Let T be a nonabelian simple group, it is easily shown that $\mathrm{Aut}(T^k) \cong \mathrm{Aut}(T) \wr S_k$ where $\wr$ denotes the wreath product. If a group G is a direct product of nonabelian simple groups, then this direct product decomposition is unique, not just up to isomorphism: if $G = T_1 \times \cdots \times T_k = S_1 \times \cdots \times S_\ell$, T_i, S_j nonabelian simple, then $k = \ell$ and $\exists \sigma \in S_k$, $\forall i \in [k]$, $T_i = S_{i^\sigma}$ as subsets of G.

Useful algorithms. We shall need two known algorithmic results, which were also useful for previous results on group isomorphism such as [BCGQ11, QST11]. Recall that in permutation group algorithms (see [Luk91, Ser03]), a coset $P\sigma \subseteq S_n$ is represented by a set of generators for $P \leq S_n$ and a coset representative σ. A particularly relevant problem on permutation groups is the Coset Intersection problem: given two cosets of subgroups of $\mathrm{Sym}(A)$, find their intersection. GraphI can be Karp-reduced to Coset Intersection [Luk82]. The Coset Intersection problem for permutation groups of degree n can be solved in $\exp(\tilde{O}(\sqrt{n}))$ time [Bab83] (see also [Bab08, BKL83]), while a relatively easier singly exponential ($\exp(O(n))$) algorithm has been obtained by Luks [Luk99]. Algorithms over finite-dimensional algebras have been considered in e. g. [CIK97, BL08]. Over finite fields, polynomial-time algorithms for isomorphism testing and Module Cyclicity are devised in [CIK97].

A linear code of length n is a linear subspace $V \leq \mathbb{F}^n$, represented by a $d \times n$ matrix where $d = \dim(V)$, and the rows form a linear basis of V. S_n acts on a linear code by permuting the coordinates (that is the columns of the matrices). Two linear codes $V, U \leq \mathbb{F}^n$ are equivalent if there exists a permutation $\sigma \in S_n$ such that $V^\sigma = U$ as linear subspaces. Such a σ is called an equivalence between V and U, and the set of all equivalences, denoted as $\mathrm{CodeEq}(V, U)$ is either empty or a coset in S_n. This problem is GraphI-hard in general [PR97] while Babai presents a singly exponential time algorithm:

Theorem 5.2 (Babai, [Bab10], cf. [BCGQ11])**.** *The set of equivalences of two linear codes of length n (over any field) given by generator matrices can be found in $(2 + o(1))^n$ time, assuming field operations at unit cost.*

We will also need the following results of Babai *et al.* [BCGQ11]:

Theorem 5.3 ([BCGQ11, Thm. 1.1])**.** *All isomorphisms between two semisimple groups Q_1 and Q_2 of order n, can be listed in time $n^{c \log \log n + O(1)}$, where $c = 1/\log(60) \approx 0.16929$.*

It is also noted in [BCGQ11] that there exist semisimple groups G of order n with $|\mathrm{Aut}(G)| \geq n^{c \log \log n}$, namely $G = A_5^k$. Hence, for listing all isomorphims this result is essentially optimal.

The number of minimal normal subgroups of any group of order n is at most $O(\log n)$. If it happens to be $O(\log n / \log \log n)$, they show:

Theorem 5.4 ([BCGQ11, Cor. 4.4])**.** *Suppose Q_1 and Q_2 are semisimple groups of order n with at most $O(\log n / \log \log n)$ minimal normal subgroups. Then all isomorphisms between Q_1 and Q_2 can be listed in polynomial time.*

In §7 we extend both of these results to decision algorithms for isomorphism of groups with central radicals, with the same time bounds as above.

We also mention a useful result for groups in the Cayley table model is by Kayal and Nezhmetdinov [KN09], though it is not strictly required in the following. They show that decomposing a group G into indecomposable direct factors can be done in polynomial time. Even in the stronger setting of permutation groups Wilson showed [Wil10] that this task can be performed in polynomial time.

6 When enumerating $\mathrm{Aut}(Q)$ is allowed

Our main results in this section are $n^{O(\log\log n)}$-time algorithms to test isomorphism of (1) groups with central radicals (Corollary 6.2) and (2) groups with elementary abelian radicals (Corollary 6.11). These follow from our more general Theorems 6.1 and 6.10, respectively, and a theorem on semisimple groups from [BCGQ11] (reproduced above as Theorem 5.3).

6.1 For central extensions of general abelian groups

We first consider the case when both extensions G and H are central.

Theorem 6.1. *Let $\mathcal{S}$ be a polynomial-time-computable characteristic subgroup functor. For two groups G, H of order n, if (1) $\mathcal{S}(G) \leq Z(G)$, and (2) $\mathrm{Aut}(G/\mathcal{S}(G))$ can be listed in time $t(n)$, then isomorphism of G and H can be decided in time $t(n)n^{O(1)}$.*

Before proving Theorem 6.1, let us see how it is applied to groups with central radicals. Combining Theorem 6.1 with Theorem 5.3, respectively Theorem 5.4 we have our first two main results:

Corollary 6.2. *Isomorphism of central-radical groups of order n can be decided in time $n^{c\log\log n+O(1)}$, for $c = 1/\log_2(60) \approx 0.169$.*

Corollary 6.3. *Let G and H be central-radical groups of order n. If $G/\mathrm{Rad}(G)$ has $O(\log n/\log\log n)$ minimal normal subgroups, isomorphism between G and H can be decided in polynomial time.*

For the proof of Theorem 6.1, for clarity we first deal with the elementary abelian case, i. e., when $A = \mathbb{Z}_p^k$; the general abelian case will be handled in Section 6.1.1.

Let us consider how to work with 2-cohomology classes in algorithms. Let G be a central extension of $A = \mathbb{Z}_p^k$ by Q (thinking of $A = \mathcal{S}(G)$ and $Q = G/\mathcal{S}(G)$). As the action is trivial in central extensions, we drop it from the notation, as in $Z^2(Q, A)$, $B^2(Q, A)$ and $H^2(Q, A)$. By choosing an arbitrary section, we get a 2-cocycle $f : Q \times Q \to A$. Let $e_1, \dots, e_k$ be the standard basis of $\mathbb{Z}_p^k$. We may view f as a $k \times |Q|^2$-size $\mathbb{Z}_p$-matrix, which we denote by M_f. The rows are indexed by the set $[k]$ and the columns are indexed by $Q \times Q$. For $i \in [k]$ and $(q, q') \in Q \times Q$, $M_f[i, (q, q')]$ is the ith coordinate of $f(q, q')$ relative to the basis $\{e_1, \dots, e_k\}$. Note that the actions of $\mathrm{Aut}(A)$ and $\mathrm{Aut}(Q)$ commute,

Under the above identification, the set $C^2(Q, A)$ of 2-cochains is identified with the set of all $k \times |Q|^2$ matrices over $\mathbb{Z}_p$. Then $Z^2(Q, A)$ is not just a subgroup, but also a $\mathbb{Z}_p$-linear subspace of $C^2(Q, A)$, and similarly $B^2(Q, A)$ is a $\mathbb{Z}_p$-linear subspace of $Z^2(Q, A)$. $\mathrm{Aut}(A) \cong \mathrm{GL}(k, p)$ acts on $C^2(Q, A)$ by left multiplication, and $\mathrm{Aut}(Q)$ acts on $C^2(Q, A)$ by permuting the columns according to the diagonal action of $\mathrm{Aut}(Q)$ on $Q \times Q$.

Proposition 6.4. *A basis of $B^2(Q, \mathbb{Z}_p)$ can be computed in time $O(|Q|^3(\log |Q| + \log p))$.*

Note that the running time here is $O(|G|^3 \log |G|)$ in the larger context of GpI.

Proof. For $q \in Q$, $q \neq \mathrm{id}$, let $u_q : Q \to \mathbb{Z}_p$ be $u_q(q') = \delta(q, q')$ where δ is the Kronecker delta. Let $f_q : Q \times Q \to \mathbb{Z}_p$ be the 2-coboundary based on u_q. $V := \{f_q \mid q \in Q\}$ then forms a basis of $B^2(Q, \mathbb{Z}_p)$. There are $|Q|$ basis elements, each of which is constructed by computing its $|Q|^2$ values; each value can be computed by a constant number of additions in $\mathbb{Z}_p$ (taking $O(\log p)$ steps) and one table lookup to compute a single product in Q (taking $O(\log |Q|)$ steps). □

As we identified $C^2(Q,A)$ as $k \times |Q|^2$ matrices over $\mathbb{Z}_p$, let $E_{i,j}$, $i \in [k]$, $j \in Q \times Q$ be a $k \times |Q|^2$ matrix such that $E_{i,j}(i',j') = 1$ if $i' = i, j' = j$, and 0 otherwise. Then $\{E_{i,j} \mid i \in [k], j \in Q \times Q\}$ is a basis of $C^2(Q,A)$. Let U_i be the subspace of $C^2(Q,A)$, spanned by $\{E_{i,j} \mid j \in Q \times Q\}$, corresponding to matrices whose only nonzero entries are in the i-th row. Then $C^2(Q,A) = \oplus_{i\in[k]} U_i$. The following proposition says that not only does $C^2(Q,A)$ split as a direct sum over the rows, but $B^2(Q,A)$ does as well. It follows directly from the fact that the condition to be a 2-coboundary in $B^2(Q,\mathbb{Z}_p^k)$ only depends on the columns ($Q \times Q$) and not on the rows ($[k]$).

Proposition 6.5. *Let V be the basis of $B^2(Q,\mathbb{Z}_p)$ from Proposition 6.4, and let $V_i \leq C^2(Q,A)$ be a copy of V in U_i. Then $\sqcup_{i\in[k]} V_i$ (disjoint union) is a basis of $B^2(Q,\mathbb{Z}_p^k)$.*

Given two 2-cocycles f_1 and f_2, let M_i be the matrix representation of f_i, $i = 1,2$, and $R_i \subseteq \mathbb{Z}_p^{|Q|^2}$ be the set of rows in M_i. Recall that $\alpha \in \mathrm{GL}(k,p)$ acts on the rows of M_i.

Proposition 6.6. *With notation as above, there exists $\alpha \in \mathrm{GL}(k,p)$ such that f_1 and f_2^α are cohomologous if and only if $\langle R_1, B^2(Q,\mathbb{Z}_p)\rangle = \langle R_2, B^2(Q,\mathbb{Z}_p)\rangle$, where $\langle\cdot\rangle$ denotes the linear span.*

Proof. Let $r_{i,j} \in \mathbb{Z}_p^{|Q|^2}$ be the jth row in M_i, $j \in [k]$, $i = 1,2$. Let B denote $B^2(Q,\mathbb{Z}_p)$. Note that Proposition 6.5 says that $B^2(Q,\mathbb{Z}_p^k) = B \oplus B \oplus \cdots \oplus B$ (k summands).

($\Rightarrow$) f_1 and f_2^α are cohomologous if and only if $f_1 - f_2^\alpha \in B^2(Q,\mathbb{Z}_p^k)$. Let $r_{2,j}^\alpha$ be the jth row in the matrix representation of f_2^α. By Proposition 6.5, for every $i \in [k]$, $r_{1,i} - r_{2,i}^\alpha \in \langle V_i\rangle = B^2(Q,\mathbb{Z}_p) = B$. That is $r_{1,i} \in \langle R_2, B\rangle$ as $r_{2,j}^\alpha \in \langle R_2\rangle$ (note that the linear span of R_2, i. e., the rowspan of M_2, is left unchanged by the action of α). Similarly we have $r_{2,i} \in \langle R_1, B\rangle$, $\forall i \in [k]$. This shows $\langle R_1, B\rangle = \langle R_2, B\rangle$.

($\Leftarrow$) For $\alpha \in \mathrm{GL}(k,p)$, again let $r_{2,j}^\alpha$ be the jth row of f_2^α. Given $\langle R_1, B\rangle = \langle R_2, B\rangle$, we have $\langle R_1, B\rangle/B$ and $\langle R_2, B\rangle/B$ are the same as subspaces of $\mathbb{Z}_p^{|Q|^2}/B$. That means that we can choose $\alpha \in \mathrm{GL}(k,p)$ such that $r_{1,i} + B = r_{2,i}^\alpha + B$, $\forall i \in [k]$. This gives $f_1 - f_2^\alpha \in B^2(Q,A)$. □

Proof of Theorem 6.1 when $\mathcal{S}(G)$ is elementary abelian. We list $\mathrm{Aut}(Q)$ in time $t(n)$. For $i = 1,2$, choose an arbitrary section of Q in G_i to get a 2-cocycle f_i. By the Main Lemma 3.2, it is necessary and sufficient to test whether there exists an $(\alpha,\beta) \in \mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ such that f_1 and $f_2^{(\alpha,\beta)}$ are cohomologous.

For each $\beta \in \mathrm{Aut}(Q)$ we get $f_2' = f_2^{(\mathrm{id},\beta)}$. We first use Proposition 6.4 to get a basis V of $B^2(Q,\mathbb{Z}_p)$. Let M_1 be the matrix representation of f_1, and M_2 for f_2'. We now need to determine whether there exists α such that f_1 and f_2' are cohomologous. By Proposition 6.6 it is enough to decide whether the linear span of the rows of f_1 with V, and the linear span of the rows of f_2 with V, are the same. This is a standard task in linear algebra and can be determined in time polynomial in $|Q|$ and $\dim_{\mathbb{Z}_p} |A| = k$.

The Main Lemma 3.2 implies that $G_1 \cong G_2$ if and only if the above test succeeds for some $\beta \in \mathrm{Aut}(Q)$. □

6.1.1 From elementary abelian to general abelian

The proof here follows the same steps as in the elementary abelian case. As each abelian group A is the direct product of its Sylow p-subgroups A_p, we essentially treat the case of a single Sylow p-subgroup, that is, when A is an abelian p-group $\mathbb{Z}_{p^{\mu_1}} \times \cdots \times \mathbb{Z}_{p^{\mu_k}}$ (not necessarily elementary). We begin by extending Propositions 6.4–6.6 to the case of abelian p-groups.

As such groups are no longer just vector spaces over $\mathbb{Z}_p$, we must speak of subgroups of A rather than subspaces, and generating sets rather than $\mathbb{Z}_p$-bases. To emphasize the similarities, we use the terminology "$\mathbb{Z}$-basis" for "irredundant generating set." Similarly for $C^2(Q, A)$, $Z^2(Q, A)$, and $B^2(Q, A)$. We represent a 2-cochain $f \colon Q \times Q \to A$ by a $k \times |Q|^2$ integer matrix, where we consider the entries in the i-th row modulo p^{μ_i}, that is, as elements of $\mathbb{Z}_{p^{\mu_i}}$. As before, we use U_i to denote the subgroup of $C^2(Q, A)$ consisting of matrices whose only nonzero entries are in the i-th row (in particular, $U_i \cong \mathbb{Z}_{p^{\mu_i}}^{|Q|^2}$).

For these first two propositions, the proofs are the same as the analogous propositions above for elementary abelian A.

Proposition 6.7. *A $\mathbb{Z}$-basis of $B^2(Q, \mathbb{Z}_{p^\mu})$ can be computed in time $O(|Q|^3(\log |Q| + \mu \log p))$.*

Proposition 6.8. *Let $V^{(\mu)}$ denote the $\mathbb{Z}$-basis of $B^2(Q, \mathbb{Z}_{p^\mu})$ from Proposition 6.7, and let $V_i^{(\mu_i)} \leq C^2(Q, A)$ be a copy of $V^{(\mu)}$ in U_i. Then $\sqcup_{i \in [k]} V_i^{(\mu_i)}$ (disjoint union) is a $\mathbb{Z}$-basis of $B^2(Q, \mathbb{Z}_{p^{\mu_1}} \times \cdots \times \mathbb{Z}_{p^{\mu_k}})$.*

Before giving the analog of Proposition 6.6 for general abelian A, we recall the structure of $\mathrm{Aut}(A)$ (see, e. g., the exposition in [HR07]); it is only slightly more complicated than the fact that $\mathrm{Aut}(\mathbb{Z}_p^k) = \mathrm{GL}(k, p)$. First, if A_p is the p-Sylow subgroup of A, then $\mathrm{Aut}(A) = \mathrm{Aut}(A_{p_1} \times \cdots A_{p_d}) = \mathrm{Aut}(A_{p_1}) \times \cdots \times \mathrm{Aut}(A_{p_d})$ where $p_1, \ldots, p_d$ are the distinct primes dividing $|A|$. So we reduce to the case where A is an abelian p-group $\mathbb{Z}_{p^{\mu_1}} \times \cdots \times \mathbb{Z}_{p^{\mu_k}}$ with $1 \leq \mu_1 \leq \mu_2 \leq \cdots \leq \mu_k$. Think of elements of A as integer column vectors of length k, where the i-th entry is considered modulo p^{μ_i}. As in the elementary abelian case (where $\mu_1 = \cdots = \mu_k = 1$), an automorphism may replace each entry with a $\mathbb{Z}$-linear combination of the entries, as follows. For $i < j$, the i-th coordinate can contribute to the j-th coordinate by multiplying by $p^{\mu_j - \mu_i}$—in other words, by using the unique inclusion $\mathbb{Z}_{p^{\mu_i}} \hookrightarrow \mathbb{Z}_{p^{\mu_j}}$. In the opposite direction, the j-th coordinate can contribute to the i-th coordinate by taking the j-th coordinate modulo p^{μ_i}—in other words, using the natural surjection $\mathbb{Z}_{p^{\mu_j}} \twoheadrightarrow \mathbb{Z}_{p^{\mu_i}}$. (Note that when $\mu_i = \mu_j$ these two operations are the same, corresponding to the identity map on $\mathbb{Z}_{p^{\mu_i}}$.)

More symbolically, we may consider each element of $\mathrm{Aut}(A)$ as an integer $k \times k$ matrix α such that: (1) for $i > j$, $p^{\mu_j - \mu_i}$ divides the (i, j) entry, (2) the entries in row i are considered modulo p^{μ_i}, and (3) α is invertible when taken modulo p.

Finally, consider (row) subgroups $R \leq \mathbb{Z}_{p^{\mu_i}}^{|Q|^2}$. In accord with the above description of the automorphisms of A, for $\mu < \mu_i$ let $R^{(\mu)}$ denote the subgroup of $\mathbb{Z}_{p^\mu}^{|Q|^2}$ that is given by taking R modulo p^μ; for $\mu > \mu_i$, let $R^{(\mu)}$ denote the subgroup of $\mathbb{Z}_{p^\mu}^{|Q|^2}$ that is given by multiplying every element of R by $p^{\mu - \mu_i}$. For any prime q, let $R^{(q,\mu)}$ denote $R^{(\mu)}$ if $q = p$ and the trivial subgroup 0 otherwise.

Now, return to A being an arbitrary abelian group. For a 2-cochain $f_1 \in C^2(Q, A)$ with corresponding $k \times |Q|^2$ matrix M with i-th row $R_{1,i} \leq \mathbb{Z}_{p_i^{\mu_i}}^{|Q|^2}$, let $R_1^{(p,\mu)}$ denote the subgroup of $\mathbb{Z}_{p^\mu}^{|Q|^2}$ generated by all the $R_{1,i}^{(p,\mu)}$; we write $R_1^{(p,\mu)} = \langle R_{1,1}^{(p,\mu)}, \ldots, R_{1,k}^{(p,\mu)} \rangle$.

Proposition 6.9. *Let $A = \mathbb{Z}_{p_1^{\mu_1}} \times \cdots \mathbb{Z}_{p_k^{\mu_k}}$ be an arbitrary abelian group (the p_i are primes, not necessarily distinct). With other notation as above, there exists $\alpha \in \mathrm{Aut}(A)$ such that f_1 and f_2^α are cohomologous if and only if $\langle R_1^{(p_i,\mu_i)}, B^2(Q, \mathbb{Z}_{p_i^{\mu_i}}) \rangle = \langle R_2^{(p_i,\mu_i)}, B^2(Q, \mathbb{Z}_{p_i^{\mu_i}}) \rangle$ for each $1 \leq i \leq k$, where $\langle \cdot \rangle$ denotes the $\mathbb{Z}$-span (=group generated by).*

Proof. Let $r_{i,j} \in \mathbb{Z}_{p_j^{\mu_j}}^{|Q|^2}$ be the j-th row in M_i, $j \in [k]$, $i = 1, 2$. Let $B^{(p,\mu)}$ denote $B^2(Q, \mathbb{Z}_{p^\mu})$. Note that Proposition 6.5 says that $B^2(Q, \mathbb{Z}_{p_1^{\mu_1}} \times \cdots \mathbb{Z}_{p_k^{\mu_k}}) = B^{(p_1,\mu_1)} \oplus \cdots \oplus B^{(p_k,\mu_k)}$.

($\Rightarrow$) f_1 and f_2^α are cohomologous if and only if $f_1 - f_2^\alpha \in B^2(Q, A)$. Let $r_{2,j}^\alpha$ be the j-th row in the matrix representation of f_2^α. By Proposition 6.7, for every $i \in [k]$, $r_{1,i} - r_{2,i}^\alpha \in \langle V_i^{(p,\mu_i)} \rangle = B^2(Q, \mathbb{Z}_{p_i^{\mu_i}}) = B^{(p_i,\mu_i)}$. That is $r_{1,i} \in \langle R_2^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle$ as $r_{2,j}^\alpha \in \langle R_2^{(p_i,\mu_i)} \rangle$ (note that the subgroup generated by of $R_2^{(p_i,\mu_i)}$ is, by definition, left unchanged by the action of α). Similarly we have $r_{2,i} \in \langle R_1^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle$, $\forall i \in [k]$. This shows $\langle R_1^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle = \langle R_2^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle$ for each i.

($\Leftarrow$) For $\alpha \in \mathrm{Aut}(A)$, again let $r_{2,j}^\alpha$ be the jth row of f_2^α. Given $\langle R_1^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle = \langle R_2^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle$ for each i, we have $\langle R_1^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle / B^{(p_i,\mu_i)}$ and $\langle R_2^{(p_i,\mu_i)}, B^{(p_i,\mu_i)} \rangle / B^{(p_i,\mu_i)}$ are the same as subgroups of $\mathbb{Z}_{p_i^{\mu_i}}^{|Q|^2} / B^{(p_i,\mu_i)}$. That means that we can choose $\alpha \in \mathrm{Aut}(A)$ such that $r_{1,i} + B^{(p_i,\mu_i)} = r_{2,i}^\alpha + B^{(p_i,\mu_i)}$, $\forall i \in [k]$. This gives $f_1 - f_2^\alpha \in B^2(Q, A)$. □

Finally, we come to the proof of Theorem 6.1 for general abelian A:

Proof of Theorem 6.1 for general abelian $\mathcal{S}(G)$. The proof is the same as for the elementary abelian case, but using Propositions 6.8 and 6.9 instead of Propositions 6.4 and 6.6, respectively. Checking the condition of Proposition 6.9 amounts to solving a system of equations over the abelian group A ("linear algebra over A"), which can be done in polynomial time (see, e. g., [GR02]). □

6.2 For general extensions of elementary abelian groups

Theorem 6.10. *Let $\mathcal{S}$ be a polynomial-time-computable characteristic subgroup functor. For two groups G, H of order n, if $\mathcal{S}(G) \cong \mathbb{Z}_p^k$ and $\mathrm{Aut}(G/\mathcal{S}(G))$ can be listed in time $t(n)$, then isomorphism of G and H can be decided in time $t(n)n^{O(1)}$.*

As before, let us first see how this is applied to groups with elementary abelian radicals. Combining Theorem 6.10 with Theorem 5.3, respectively Theorem 5.4, we have:

Corollary 6.11. *Isomorphism of elementary abelian radical groups of order n can be decided in time $n^{c \log\log n + O(1)}$, for $c = 1/\log_2(60) \approx 0.169$.*

Corollary 6.12. *Let G and H be elementary abelian radical groups of order n. If $G/\mathrm{Rad}(G)$ has $O(\log n/\log\log n)$ minimal normal subgroups, isomorphism between G and H can be decided in polynomial time.*

The proof of Theorem 6.10 is a reduction to module cyclicity testing, for which a deterministic polynomial-time algorithm over finite fields is provided by Chistov, Ivanyos and Karpinski [CIK97]. Before the reduction it might be helpful to see this problem in a special case, when the extensions are split.

Remark 6.13. If the algorithm for cyclicity test of modules [CIK97] can be generalized to the case when the underlying module is an abelian group (rather than a vector space), then the above three results can be generalized to groups with arbitrary abelian radicals. See also Section 8.1.

For split extensions: a.k.a. module isomorphism problem. Recall that G_1 and G_2 are extensions of $A = \mathbb{Z}_p^k$ by Q. Furthermore suppose both extensions split. Then to test isomorphism we are left with the ACTION COMPATIBILITY, that is, we extract the actions of Q on A in G_i as $\theta_i : Q \to \mathrm{Aut}(A) = \mathrm{GL}(k, p)$, and the goal is to find $(\alpha, \beta) \in \mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ such that $\theta_1 = \theta_2^{(\alpha,\beta)}$. As $\mathrm{Aut}(Q)$ is enumerable, we fix a β and all that remains is to test whether there exists $\alpha \in \mathrm{GL}(k, p)$ such that $\forall q \in Q$ $\theta_1(q) = \alpha^{-1}\theta_2(q)\alpha$. In other words, viewing θ_i as linear representations of Q over the field $\mathbb{F}_p$, the problem is to test whether these two representations are equivalent. This can also be formulated as finding a nonsingular matrix α such that $\alpha\theta_1(q) = \theta_2(q)\alpha$, $\forall q \in Q$, namely the module isomorphism problem. Over finite fields this problem admits deterministic polynomial-time algorithms [CIK97, BL08].

Now we present the reduction for the general case.

The general case: reduction to cyclicity test of modules. Let G_1 and G_2 be extensions of $A = \mathbb{Z}_p^k$ by Q, and (θ_i, f_i) the extension data of $A \hookrightarrow G_i \twoheadrightarrow Q$. It can be verified that if (α, β) satisfies $\theta_1 = \theta_2^{(\alpha,\beta)}$, then (α, β) sends $Z^2(Q, A, \theta_2)$ to $Z^2(Q, A, \theta_1)$ and sends $B^2(Q, A, \theta_2)$ to $B^2(Q, A, \theta_1)$. As $\mathrm{Aut}(Q)$ is enumerable, the problem is to find $\alpha \in \mathrm{GL}(k, p)$ such that (1) $\forall q \in Q$, $\alpha\theta_1(q) = \theta_2(q)\alpha$; (2) $\alpha f_1 = f_2$ as cohomology classes in $Z^2(Q, A, \theta_2)$ (that is $[\alpha f_1] = [f_2]$).

This task can be reduced to cyclicity test of modules over finite-dimensional algebras, in almost the same way as the reduction from module isomorphism problem to module cyclicity test [CIK97]. We include a sketch here for completeness. Let $M(k, p)$ be the linear space of $k \times k$ matrices over $\mathbb{Z}_p$. Consider a linear subspace of $M(k, p)$, $V = \{\alpha \in M(k, p) \mid \forall q \in Q, \alpha\theta_1(q) = \theta_2(q)\alpha, \text{ and } \exists a \in \mathbb{Z}_p, [\alpha f_1] = [af_2]\}$. Also consider $U = \{\gamma \in M(k, p) \mid \forall q \in Q, \gamma\theta_2(q) = \theta_2(q)\gamma, \text{ and } \exists a \in \mathbb{Z}_p, [\gamma f_2] = [af_2]\}$. It can be verified that U is an associative algebra over $\mathbb{Z}_p$ with identity. Then V is a left U-module: for $\alpha \in V$, $\gamma \in U$ and $q \in Q$, $\gamma\alpha\theta_1(q) = \gamma\theta_2(q)\alpha = \theta_2(q)\gamma\alpha$. To show that $[\gamma\alpha f_1] = [af_2]$ is a little subtle, and for this we need to recall the fact that, if $\gamma\theta_2(q) = \theta_2(q)\gamma$ for every $q \in Q$, then γ preserves $B^2(Q, A, \theta_2)$. That is, $\alpha f_1 = af_2 + g$ for some $a \in \mathbb{Z}_p$ and $g \in B^2(Q, A, \theta_2)$, and $\gamma\alpha f_1 = \gamma(af_2 + g) = a\gamma f_2 + \gamma g = a'f_2 + g' + g''$ where $a' \in \mathbb{Z}_p$, $\gamma f_2 = f_2 + b'$ and $\gamma b = b''$. Now we claim that if V contains invertible elements, then (1) it is cyclic, and (2) every generator is invertible. To show (1), let $\alpha' \in V$ be invertible, and form $\phi : U \to V$ by sending $\gamma \to \gamma\alpha'$. Then ϕ is an U-module isomorphism between U and V, whose inverse is $V \to U$ by $\alpha \to \alpha\alpha'^{-1}$; $\alpha\alpha'^{-1} \in U$ again follows from that α and α' can be shown to send $B^2(Q, A, \theta_2)$ to $B^2(Q, A, \theta_1)$ as a consequence of $\alpha\theta_1(q) = \theta_2(q)\alpha$. For (2), if α'' generates V, then $\alpha''\alpha'^{-1}$ generates U as a left U-module, and thus $\alpha''\alpha'^{-1}$ is invertible, showing that α'' is invertible. Finally we note that if some invertible $\alpha' \in V$ sends $[f_1]$ to $[af_2]$ for some $a \in \mathbb{Z}_p$, then $a^{-1}\alpha' \in V$ is also invertible and sends $[f_1]$ to $[f_2]$.

Given the above reduction, here is an algorithm for the general case: we still represent 2-cocycles by $k \times |Q|^2$ matrices over $\mathbb{Z}_p$. We first compute a $\mathbb{Z}_p$-basis of $B^2(Q, A, \theta_2)$ using the following functions from $Q \to A$: for $q \in Q$, $i \in [k]$, $u_{q,i}(q') = \delta(q, q')e_i$ where δ is the Kronecker delta and e_i is the ith standard basis. Using these 2-cocycles we can represent V and U as solution spaces of homogeneous linear equations. Finally we apply the module cyclicity test algorithm from [CIK97], either to get that V is not cyclic, thus does not contain invertible elements, or to get a generator $\alpha' \in V$. In the latter case we conclude based on whether α' is invertible or not.

7 When $\mathrm{Aut}(Q)$ is too big

In this section we present polynomial-time algorithms for certain central-radical groups even when $\mathrm{Aut}(Q)$ cannot be enumerated in polynomial time. In particular, we present two fixed-parameter polynomial-time algorithms for central radical groups with $G/\mathrm{Rad}(G)$ a direct product of non-abelian simple groups:

Theorem 7.1. *Isomorphism of groups G_1 and G_2 with central radicals and $G_i/\mathrm{Rad}(G_i)$ a direct product of nonabelian simple groups can be decided in polynomial time if either:*

1. $|\mathrm{Aut}(\mathrm{Rad}(G_1))|$ *is bounded by a polynomial; or*
2. $\mathrm{Rad}(G_1)$ *is elementary abelian, and the simple direct factors of $G_1/\mathrm{Rad}(G_1)$ each have order $O(1)$.*

Note that Theorem 7.1 yields polynomial-time algorithms for the following concrete cases: (1) covers the case when $|\mathrm{Rad}(G)| \leq 2^{\sqrt{\log n}}$; (2) covers groups G with $\mathrm{Rad}(G) = Z(G) \cong \mathbb{Z}_5^k$ and $G/Z(G) \cong A_5^k$. We remind the reader that, singly exponential algorithms for Linear Code Equivalence and Coset Intersection play an important role in Theorem 7.1 (2).

For Theorem 7.1 (1), we also give the proof for the case when $A = Z(G) = \mathrm{Rad}(G)$ is the elementary abelian p-group $\mathbb{Z}_p^k$; the general case of $Z(G) = \mathrm{Rad}(G)$ can be obtained following the idea in Appendix 6.1.1.

For Theorem 7.1 (2), currently we can only work with elementary abelian groups; an open problem posed in [BCGQ11, Section 7.7], namely the group code equivalence problem, seems to be the current obstacle.

As remarked before, for Theorem 7.1 we need more detailed (while not difficult) understanding of central extensions in this special group class.

7.1 Preparations from cohomology

Let A be an abelian group, and $T_1, \dots, T_\ell$ be nonabelian simple groups. For an extension G of A by $Q = \prod_{i\in[\ell]} T_i$, let U_i be the inverse image of T_i in G under the natural projection from G to Q. The following proposition adapted from from Suzuki [Suz86] is crucial; cf. Appendix B for its proof.

Proposition 7.2 (Cf. [Suz86, Chapter 6, Proposition 6.5])**.** *Let notations be as above. For $i, j \in [\ell]$, $i \neq j$, $[U_i, U_j] = 1$. That is, $\forall x \in U_i$, $\forall y \in U_j$, $xy = yx$.*

We now consider the U_i not just as subgroups of G, but as extensions $A \hookrightarrow U_i \twoheadrightarrow T_i$. As Proposition 7.2 shows that $[U_i, U_j] = \mathrm{id}$ for $i \neq j$, these extensions determine the extension G as follows.

Lemma 7.3. *Given two central extensions $A \hookrightarrow G_j \twoheadrightarrow Q$ ($j = 1, 2$) with $A = Z(G_i)$ and $Q = \prod_{i=1}^{\ell} T_i$, let $U_{j,i}$ be the inverse image of T_i under the natural projection $G_j \to G_j/A$. The extensions $A \hookrightarrow G_j \twoheadrightarrow Q$ ($j = 1, 2$) are equivalent if and only if for every $i \in [\ell]$, the extensions $A \hookrightarrow U_{j,i} \twoheadrightarrow T_i$ ($j = 1, 2$) are equivalent.*

Proof. The only if direction is trivial. For the other direction, for $j = 1, 2$ and $i \in [\ell]$, let $f_{j,i}$ be the 2-cocycle of the extension $A \hookrightarrow U_{j,i} \twoheadrightarrow T_i$ induced by some section $s_{j,i} : T_i \to U_i$. By Eilenberg–MacLane, as $U_{1,i}$ and $U_{2,i}$ are equivalent extensions for each i, $f_{1,i} - f_{2,i}$ is some 2-coboundary $b_i \in B^2(T_i, A)$. Again by Eilenberg–MacLane, to show the equivalence of $A \hookrightarrow G_j \twoheadrightarrow \prod_{i\in[\ell]} T_i$, we only need to exhibit two 2-cocycles f_j for $A \hookrightarrow G_j \twoheadrightarrow Q$ that differ by a 2-coboundary.

As Q is decomposed uniquely as $\prod_i T_i$, we can identify elements in Q as from $\prod_i T_i$ without ambiguity. Let $(p_1, \dots, p_\ell)$ and $(q_1, \dots, q_\ell)$ be two elements in Q, $p_i, q_i \in T_i$ for $i \in [\ell]$. Then define $b : Q \times Q \to A$ as

$$b((p_1, \dots, p_\ell), (q_1, \dots, q_\ell)) = \sum_{i\in[\ell]} b_i(p_i, q_i). \tag{7}$$

It can be verified that b is a 2-coboundary in $B^2(Q, A)$.

Recall that the 2-cocycle $f_{j,i}$ is induced by the section $s_{j,i} : T_i \to U_i$. We define a section $s_j : Q \to G_j$, as $s_j((p_1, \dots, p_\ell)) = s_{j,1}(p_1) \dots s_{j,\ell}(p_\ell)$. Let f_j be the 2-cocycle induced by s_j, then—noting that for $i_1 \neq i_2$, $s_{j,i_1}(p_{i_1})$ and $s_{j,i_2}(p_{i_2})$ commute by Proposition 7.2—it can be verified that

$$f_j((p_1, \dots, p_\ell), (q_1, \dots, q_\ell)) = \sum_{i\in[\ell]} f_{j,i}(p_i, q_i). \tag{8}$$

Thus $f_1 - f_2 = b \in B^2(Q, A)$, finishing the proof. □

For convenience, in the following we shall call $U_{j,i}$ the *restriction of* G_j *to* T_i and use $G_j|_{T_i}$ to denote it. The next lemma concerns the direct product structure of the normal part; its proof is put in Appendix B for completeness.

Lemma 7.4. *Let $A' \times A'' \hookrightarrow G \twoheadrightarrow Q$ be a central extension of $A' \times A''$ by Q. Let $p_{A'} \colon A' \times A'' \to A'$ be the projection onto A' along A''. If there is a 2-cocycle $f \colon Q \times Q \to A' \times A''$ such that $p_{A'} \circ f \colon Q \times Q \to A'$ is a 2-coboundary, then G is isomorphic (even equivalent) to the direct product $A' \times (G/A')$.*

Furthermore, given the Cayley table of G, A' can be computed in polynomial time using linear algebra over abelian groups.

Using general algorithms for decomposing direct products [KN09, Wil10], we could compute A' in polynomial time without the "furthermore." However, in the setting of Lemma 7.4, we give a much simpler algorithm to compute A' using linear algebra over abelian groups.

7.2 Proof of Theorem 7.1

Proof of Theorem 7.1. For G_j, $j = 1, 2$, we decompose it as an extension of $A = \mathbb{Z}_p^k$ by $Q = \prod_{i\in[\ell]} T_i$, where T_i is a nonabelian simple group. To decompose Q into T_i's is straightforward by [BCGQ11, Proposition 2.1]. As T_i's can be generated by 2 elements, we classify T_i's according to their isomorphism types and group them together, identifying $Q = \prod_{i\in[r]} Q_i^{\ell_i}$, where r is the number of isomorphism types in T_i's, each Q_i is isomorphic to some T_i, and the Q_i's are pairwise nonisomorphic. Then $\mathrm{Aut}(Q) \cong \prod_{i\in[r]} \mathrm{Aut}(Q_i) \wr S_{\ell_i} \cong \prod_{i\in[r]} (\mathrm{Aut}(Q_i)^{\ell_i} \rtimes S_{\ell_i})$. A *diagonal* of $\mathrm{Aut}(Q)$ is an element in $\prod_{i\in[r]} \mathrm{Aut}(Q_i)^{\ell_i}$. All diagonals are enumerable in polynomial time by the $n^{\#\text{ generators}}$ technique; note that $|\prod_{i\in[r]} \mathrm{Aut}(Q_i)^{\ell_i}| \leq (\prod_{i\in[r]} |Q_i|^2)^{\ell_i}) \leq |G_j|^2$, by Fact 5.1.

By Lemma 3.2, $G_1 \cong G_2$ if and only if they are pseudo-congruent extensions of A by Q. The extensions are pseudo-congruent if and only if there is an element of $\mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ such that, after twisting by this element, the resulting extensions are equivalent. Once an element of $\mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ is fixed, by Lemma 7.3, the latter problem is reduced to determining the equivalence of $G_1|_{T_i}$ and $G_2|_{T_i}$ for each $i \in [\ell]$.

(1) Note that the equivalence type of $G_j|_{T_i}$ can be computed by Theorem 6.1 as each T_i is generated by 2 elements so $\mathrm{Aut}(T_i)$ can be listed in polynomial time. Then the algorithm works as follows.

For every $\alpha \in \mathrm{Aut}(A)$, and every diagonal $\prod_{i\in[\ell]} \delta_i$ of $\prod_{i\in[\ell]} \mathrm{Aut}(T_i)$, do the following. Apply α^{-1} and δ_i to each restricted extension $G_2|_{T_i}$. Now compute the equivalence types of $G_2|_{T_i}$. If the multiset of equivalence types coming from $G_1|_{T_i}$ is equal to the multiset of equivalence types from the $(\alpha, \prod_i \delta_i)$-twisted $G_2|_{T_i}$, then G_1 and G_2 are pseudo-congruent as extensions, and the algorithm reports "isomorphic." On the other hand, if the equivalence of multisets is not detected for any $(\alpha, \prod_i \delta_i)$ then the algorithm returns "not isomorphic."

It is obvious that the above procedure runs in polynomial time in n and $|\mathrm{Aut}(A)|$. We remark that if $T_{i_1} \not\cong T_{i_2}$ then $G_1|_{T_{i_1}}$ and the (α, δ_{i_2})-twisted $G_2|_{T_{i_2}}$ cannot be equivalent. Thus the multiset of equivalence types distinguishes the isomorphism types of T_i's automatically. Finally, it is enough to compare the multisets because we have full symmetric groups S_{ℓ_i} acting on the isomorphic factors.

(2) Before presenting the algorithm we need some consequences of Lemma 7.3. For G_j, $j = 1, 2$, we say a 2-cocycle $f_j : Q \times Q \to A$ respects the direct factors if there exist $f_{j,i} : T_i \times T_i \to A$, $i \in [\ell]$ such that Equation 8 holds. Let $Z^2_{\mathrm{prod}}(Q, A)$ denote the set of 2-cocycles respecting the direct factors. The proof of Lemma 7.3 shows that $Z^2_{\mathrm{prod}}(Q, A) \neq \emptyset$. Similarly we can define 2-coboundaries that respect the direct factors $B^2_{\mathrm{prod}}(Q, A)$ using Equation 7). For two cohomologous 2-cocycles from $Z^2_{\mathrm{prod}}(Q, A)$, their difference is in $B^2_{\mathrm{prod}}(Q, A)$. Recall that M_{f_j} denotes the matrix representation of f_j with row index set $[k]$ and column index set $Q \times Q$. As f_j is completely determined by the direct factors, we can focus on M_{f_j} with row indices from $\cup_{i\in[\ell]} T_i \times T_i$. Thus for $f_j \in Z^2_{\mathrm{prod}}(Q, A)$ the size of M_{f_j} is assumed to be $k \times (\sum_{i\in[\ell]} |T_i|^2)$.

We will need the following analogue of Proposition 6.6. Let $\widetilde{M_{f_j}}$ denote the matrix with $(\sum_{i\in[\ell]} |T_i|^2$ columns, and whose first rows are just M_{f_j}. The remaining rows will be the union of bases for $B^2(T_i, \mathbb{Z}_p)$ for each i (see Proposition 6.4).

Proposition 7.5. *Suppose that $\widetilde{M_{f_j}}$ has full rank for $j = 1, 2$. Fix some diagonal $\delta \in \prod_i \mathrm{Aut}(T_i)$ and let $\widetilde{M_{f_1}}' = \widetilde{M_{f_1}}^{(\mathrm{id},\delta,\mathrm{id})}$. Then the intersection $\mathrm{CodeEq}(\widetilde{M_{f_1}}', \widetilde{M_{f_2}}) \cap \prod_i S_{\ell_i}$ is non-empty if and only if there exists $(\alpha, \sigma) \in \mathrm{Aut}(A) \times \prod_i S_{\ell_i}$ such that (α, δ, σ) is an isomorphism of f_1 and f_2 as cohomology classes.*

Proof. Let N be the number of rows of $\widetilde{M_{f_j}}$, and let $b = N - k$ be the number of rows of $\widetilde{M_{f_j}}$ that were added to $\widetilde{M_{f_j}}$ compared to M_{f_j}.

($\Rightarrow$) Suppose $\mathrm{CodeEq}(\widetilde{M_{f_1}}', \widetilde{M_{f_2}}) \cap \prod_i S_{\ell_i}$ is non-empty. Then there is some permutation $\sigma \in \prod_i S_{\ell_i}$ and some $\Lambda \in \mathrm{GL}(N, p)$ such that $\Lambda \widetilde{M_{f_1}}^{(\delta,\sigma)} = \widetilde{M_{f_2}}$. As the last b rows of $\widetilde{M_{f_1}}$ and $\widetilde{M_{f_2}}$ have the same rowspan (namely, $B^2_{prod}(Q, A)$) and this rowspan is preserved by all permutations of the columns, we may assume without loss of generality that Λ has the following block form:

$$\Lambda = \begin{pmatrix} \alpha & \gamma \\ 0 & \eta \end{pmatrix}.$$

In other words, to make the row spans of the bottom b rows equal, it is never necessary to add any multiples of the top k rows to the bottom b rows, as the bottom b rows already have equal row spans that are preserved by all permutations.

The sub-matrix γ contributes by adding elements of $B^2_{prod}(Q, A)$ to M_{f_1}, so that $\begin{pmatrix} \mathrm{id} & \gamma \\ 0 & \eta \end{pmatrix} M_{f_1}$ corresponds to a cocycle that is cohomologous to f_1. Finally, the contribution of the sub-matrix α is to send f_1 to a pseudo-congruent cocycle, since $\alpha \in \mathrm{Aut}(A)$. Therefore we have shown that (α, δ, σ) is an isomorphism of the cohomology classes f_1, f_2.

($\Leftarrow$) Suppose that $f_1^{(\alpha,\delta,\sigma)}$ is cohomologous to f_2 for some $\alpha \in \mathrm{Aut}(A)$ and $\sigma \in \prod S_{\ell_i}$. Then some matrix $\Lambda' = \begin{pmatrix} \alpha & \gamma \\ 0 & \mathrm{id} \end{pmatrix}$ will make the first k rows of $\Lambda' \widetilde{M_{f_1}}^{(\delta,\sigma)}$ equal to the first k rows of $\widetilde{M_{f_2}}$. The last b rows of $\Lambda' \widetilde{M_{f_1}}^{(\delta,\sigma)}$ and $\widetilde{M_{f_2}}$ have the same row span, so there is some η such that $\Lambda = \begin{pmatrix} \alpha & \gamma \\ 0 & \eta \end{pmatrix}$ makes the two matrices equal. (In fact, η will be a block-permutation matrix, which permutes the blocks in the same way that δ permutes the factors.) In particular, this shows that σ is a code equivalence, and hence that $\mathrm{CodeEq}(\widetilde{M_{f_1}}', \widetilde{M_{f_2}}) \cap \prod_i S_{\ell_i}$ is nonempty. □

To finish the proof of Theorem 7.1(2), we proceed as follows. First, find a direct decomposition of G_j [KN09]. If any direct factor is contained in $Z(G_j)$, set this direct factor aside. Then by Lemma 7.4, the matrices M_{f_j} will be full rank, *even after modding out by coboundaries.* The latter fact implies that the rank of $\widetilde{M_{f_j}}$ is then the rank of M_{f_j} plus the dimension of $B^2_{prod}(Q, A)$, in other words, the $\widetilde{M_{f_j}}$ are also of full rank.

Finally, we compute the coset of equivalences $\mathrm{CodeEq}(\widetilde{M}_1, \widetilde{M}_2) \subseteq S_m$ using Theorem 5.2. On the other hand $\prod_i S_{\ell_i}$ induces an action on $[m]$, which contains the permutations we want. Thus we need to intersect $\mathrm{CodeEq}(M_1, M_2)$ with $\prod_i S_{\ell_i}$. By Proposition 7.5, if this intersection is nonempty, the algorithm returns "isomorphic." If the intersection is empty for all diagonals δ, the algorithm returns "non-isomorphic."

To analyze the running time, the outer loop depending on the diagonals is polynomially related to n. Both the applications of the LINEAR CODE EQUIVALENCE algorithm (Theorem 5.2), and the singly-exponential time algorithm for COSET INTERSECTION ([Luk99]), take time $c^m \leq c^{\ell D^2}$ for some absolute constant c, where $D \leq \log_{60} |Q|$ is the maximum size of any of the T_i. □

Remark 7.6. Some parts of the results here can be generalized as follows. Consider the class of perfect groups; recall that a group G is perfect if $G = [G, G]$. By Grün's lemma, $G/Z(G)$ is centerless, thus its direct product decomposition is unique. Suppose $G/Z(G) = G_1/Z(G) \times \cdots \times G_\ell/Z(G)$, where $G_i/Z(G)$ is indecomposable with respect to direct product, and G_i is the full preimage of $G_i/Z(G)$ in $G \to G/Z(G)$. Lemma 7.3 can be generalized to show that $[G_i, G_j] = 1$. This implies that if we have efficient algorithms to test isomorphism of indecomposable and centerless perfect groups, then following the same strategy for central radical groups with $G/\mathrm{Rad}(G)$ a direct product of nonabelian simple groups we can handle general perfect groups. (For central radical groups with

$G/\operatorname{Rad}(G)$ a direct product of nonabelian simple groups the correspondents of "indecomposable and centerless perfect groups" are nonabelian simple groups, which can be handled by Fact 5.1.)

8 Future directions

In this paper we made significant progress on group isomorphism for groups with central radicals, extending the results of [BCQ12] and beginning to resolve an open problem from [BCGQ11]. We achieved an $n^{O(\log\log n)}$ algorithm for this class of groups, and polynomial-time algorithms for several prominent subclasses. The difficult cases seem to be when the radical $\operatorname{Rad}(G)$ and the semisimple quotient $G/\operatorname{Rad}(G)$ are roughly of the same size—say both are of order $\sqrt{n}$—and $G/\operatorname{Rad}(G)$ is complicated (without this last condition, we handle such groups in Theorem 7.1). Although the general case of central radicals remains open, we propose three directions for extending our work which we believe may now be within reach.

8.1 Abelian radical

A natural next step is to combine the essentially cohomological algorithms of our paper with algorithms to determine Action Compatibility. The simplest such open case is the case of abelian radicals (which need not be central).

Open Problem 8.1. Extend Theorems 6.1 and 7.1 to groups whose solvable radicals $\operatorname{Rad}(G)$ are abelian, but not necessarily central. Ultimately, decide isomorphism of groups with abelian radicals in polynomial time.

Note that the previous results that solve Action Compatibility, such as for groups with abelian Sylow towers [BQ12] (which subsumes [LG09, QST11]), only seem to work when the corresponding representations are completely reducible. However, when $|\operatorname{Rad}(G)|$ and $|G/\operatorname{Rad}(G)|$ are not coprime, the representation of $G/\operatorname{Rad}(G)$ on $\operatorname{Rad}(G)$ need not be completely reducible.

Chistov–Ivanyos–Karpinski [CIK97] and Brooksbank–Luks [BL08] have solved a closely related problem in algorithmic representation theory, even for representations that are not completely reducible. In Theorem 6.10 we have already taken the first step by combining these algorithms with the techniques of our paper to solve Problem 8.1 in $n^{O(\log\log n)}$ time when the radical is *elementary* abelian. After that, we believe that a key step towards resolving Problem 8.1 in full will be to extend the algorithms of Chistov–Ivanyos–Karpinski and Brooksbank–Luks from representations over fields to actions on finite abelian groups (which might be thought of as, by abuse of terminology, "finite representations over $\mathbb{Z}$").

8.2 The Babai–Beals filtration

The Babai–Beals filtration was defined and used in the context of algorithms for matrix groups [BB99, BBS09]—where the groups are given by a generating set of matrices, and the goal is algorithms which run in time polynomial in the input size, which can be polylogarithmic in $|G|$. In the context of GpI, it has also been used successfully in the polynomial-time algorithm for semisimple groups [BCGQ11, BCQ12].

The Babai–Beals filtration is the following chain of characteristic subgroups:

$$1 \leq \operatorname{Rad}(G) \leq \operatorname{Soc}^*(G) \leq \operatorname{Pker}(G) \leq G, \tag{9}$$

where $\operatorname{Rad}(G)$ is the solvable radical of G and $\operatorname{Soc}^*(G)$ is the subgroup such that $\operatorname{Soc}^*(G)/\operatorname{Rad}(G) = \operatorname{Soc}(G/\operatorname{Rad}(G))$. Note that the socle of the semisimple group $G/\operatorname{Rad}(G)$ is a direct product of non-abelian simple groups. G then acts on this direct product by, amongst other things, permuting the factors. The final subgroup in the Babai–Beals filtration, $\operatorname{Pker}(G)$, consists of those $g \in G$ which do not permute the direct factors of $\operatorname{Soc}^*(G)/\operatorname{Rad}(G)$.

In Theorem 7.1 we make progress on the case of groups G with central radical which further satisfy $G = \operatorname{Soc}^*(G)$. It is then natural to consider groups with the next step of the Babai–Beals filtration, $G = \operatorname{Pker}(G)$. As a polynomial-time algorithm for isomorphism of *semisimple* groups G satisfying $G = \operatorname{Pker}(G)$ [BCGQ11] was significantly simpler than the polynomial-time algorithm for general semisimple groups [BCQ12], we have hope that the following is achievable:

Open Problem 8.2. Extend Theorem 7.1 to groups with central radical which satisfy $G = \operatorname{Pker}(G)$.

8.3 The Cannon–Holt strategy

Cannon and Holt [CH03] suggest the following strategy for computing $\operatorname{Aut}(G)$ for a finite group G, as well as for isomorphism testing. They consider the following chain of characteristic subgroups:

$$1 = N_r \trianglelefteq N_{r-1} \trianglelefteq \cdots \trianglelefteq N_1 = \operatorname{Rad}(G) \trianglelefteq G, \tag{10}$$

where the N_i refine the derived series of $\operatorname{Rad}(G)$ and each N_i/N_{i+1} is elementary abelian. The algorithm proceeds by first computing $\operatorname{Aut}(G/N_1) = \operatorname{Aut}(G/\operatorname{Rad}(G))$, and then iteratively computing $\operatorname{Aut}(G/N_{i+1})$ from $\operatorname{Aut}(G/N_i)$.

This chain is convenient for describing known results in the Cayley table model: the case when $\operatorname{Rad}(G) = 1$ (equivalently $r = 1$) corresponds to the semisimple case, which can be solved in polynomial time [BCQ12]. When $G = \operatorname{Rad}(G)$ and $r = 2$, the case of $|N_2|$ and $|N_1/N_2|$ being coprime can be solved in polynomial time [BQ12]. When $|N_2|$ and $|N_1/N_2|$ are not coprime, this includes the notorious case of p-groups of class 2. Finally, the present work considers a special case of $r = 2$, namely when $\operatorname{Rad}(G) = Z(G)$.

In light of [BCQ12], in the Cayley table model the second step in the Cannon–Holt strategy—to compute $\operatorname{Aut}(G/N_2)$ from $\operatorname{Aut}(G/\operatorname{Rad}(G))$—is equivalent to the special case of Problem 8.1 in which $\operatorname{Rad}(G)$ is elementary abelian, which we have solved in $n^{O(\log\log n)}$ time in Theorem 6.10.

However, even before Problem 8.1 is completely resolved, it may be possible to give a reduction from the third step of the Cannon–Holt strategy to listing isomorphisms of two-step solvable groups. This is headed in the direction of a formal reduction from general group isomorphism to the solvable case. In a related vein, in Proposition 3.14 we showed how isomorphism of groups whose outer action on $\operatorname{Rad}(G)$ is trivial reduces to isomorphism of central-radical groups and isomorphism of solvable groups.

Open Problem 8.3. Extend Theorems 6.1 and 7.1 to groups whose radicals are two-step solvable, allowing access to an oracle for listing $\operatorname{Aut}(\operatorname{Rad}(G))$.

References

[AG84] M. Aschbacher and R. Guralnick. Some applications of the first cohomology group. *Journal of Algebra*, 90(2):446–460, 1984.

[Asc00] M. Aschbacher. *Finite group theory*, volume 10 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2000.

[AT11] Vikraman Arvind and Jacobo Torán. Solvable group isomorphism is (almost) in $\mathsf{NP} \cap \mathsf{coNP}$. *TOCT*, 2(2):4, 2011.

[Bab83] László Babai. Permutation groups, coherent configurations, and graph isomorphism, April 1983. D.Sc. Thesis, Hungarian Academy of Sci. (Hungarian).

[Bab95] László Babai. Automorphism groups, isomorphism, reconstruction. In R. L. Graham, M. Grötschel, and L. Lovász, editors, *Handbook of combinatorics (vol. 2)*, pages 1447–1540. MIT Press, Cambridge, MA, USA, 1995.

[Bab08] László Babai. Coset intersection in moderately exponential time. *Chicago J. Theoret. Comp. Sci.*, 2008. To appear.

[Bab10] László Babai. Equivalence of linear codes, 2010. Unpublished manuscript.

[Bae38] Reinhold Baer. Groups with abelian central quotient group. *Trans. Amer. Math. Soc.*, 44:357–386, 1938.

[BB99] László Babai and Robert Beals. A polynomial-time theory of black-box groups I. In C. M. Campbell, E. F. Robertson, N. Ruskuc, and G. C. Smith, editors, *Groups St Andrews 1997 in Bath, I*, volume 260 of *London Math. Soc. Lect. Notes*, pages 30–64. Cambr. U. Press, 1999.

[BBS09] László Babai, Robert Beals, and Ákos Seress. Polynomial-time theory of matrix groups. In *Proc. 41st ACM STOC*, pages 55–64. ACM Press, 2009.

[BCGQ11] László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *Proc. 22nd SODA*, pages 1395–1408, 2011.

[BCQ12] László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups - (extended abstract). In *ICALP*, pages 51–62, 2012.

[BE99] Hans Ulrich Besche and Bettina Eick. Construction of finite groups. *J. Symb. Comput.*, 27(4):387–404, 1999.

[BEO02] Hans Ulrich Besche, Bettina Eick, and E.A. O'Brien. A millennium project: Constructing small groups. *Intern. J. Alg. and Comput*, 12:623–644, 2002.

[BHZ87] Ravi Boppana, Johan Håstad, and Stathis Zachos. Does co-NP have short interactive proofs? *Inform. Process. Lett.*, 25:27–32, 1987.

[BJP97] W. Bosma, J. J. Cannon, and C. Playoust. The Magma algebra system I: the user language. *J. Symb. Comput.*, pages 235–265, 1997.

[BKL83] László Babai, William M. Kantor, and Eugene M. Luks. Computational complexity and the classification of finite simple groups. In *Proc. 24th IEEE FOCS*, pages 162–171. IEEE Comp. Soc., 1983.

[BL83] László Babai and Eugene M. Luks. Canonical labeling of graphs. In *Proc. 15th ACM STOC*, pages 171–183. ACM Press, 1983.

[BL08] Peter A. Brooksbank and Eugene M. Luks. Testing isomorphism of modules. *Journal of Algebra*, 320(11):4020 – 4029, 2008.

[BM88] László Babai and Shlomo Moran. Arthur–Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Computer and Sys. Sci.*, 36:254–276, 1988.

[BQ12] László Babai and Youming Qiao. Polynomial-time isomorphism test for groups with Abelian Sylow towers. In *29th STACS*, pages 453 – 464. Springer LNCS 6651, 2012.

[BW12] Peter A. Brooksbank and James B. Wilson. Computing isometry groups of hermitian maps. *Trans. Amer. Math. Soc.*, 364:1975–1996, 2012.

[CCN$^+$85] John Horton Conway, Robert Turner Curtis, Simon Phillips Norton, Richard A. Parker, and Robert Arnott Wilson. *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups.* Oxford University Press, 1985.

[CH03] John J. Cannon and Derek F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symb. Comput.*, 35:241–267, March 2003.

[CIK97] Alexander Chistov, Gábor Ivanyos, and Marek Karpinski. Polynomial time algorithms for modules over finite dimensional algebras. In *Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, ISSAC '97, pages 68–74, New York, NY, USA, 1997. ACM.

[CTW10] Arkadev Chattopadhyay, Jacobo Torán, and Fabian Wagner. Graph isomorphism is not AC^0 reducible to group isomorphism. In *FSTTCS*, pages 317–326, 2010.

[EM47] Samuel Eilenberg and Saunders MacLane. Cohomology theory in abstract groups. II: Group extensions with a non-abelian kernel. *Annals of Mathematics*, 48(2):pp. 326–341, 1947.

[FN70] V. Felsch and J. Neubüser. On a programme for the determination of the automorphism group of a finite group. In Pergamon J. Leech, editor, *Computational Problems in Abstract Algebra (Proceedings of a Conference on Computational Problems in Algebra, Oxford, 1967)*, pages 59–60, Oxford, 1970.

[GG13] The GAP Group. `GAP`—groups, algorithms, and programming, version 4.6.5, 2013. `http://www.gap-system.org/`.

[GR02] Mikael Goldmann and Alexander Russell. The complexity of solving equations over finite groups. *Inf. Comput.*, 178(1):253–262, October 2002.

[Gro12] Joshua A. Grochow. Matrix isomorphism of matrix Lie algebras. In *IEEE Conference on Computational Complexity*, pages 203–213, 2012. Also available as arXiv:1112.2012 and ECCC TR11-168.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory.* Chapman and Hall/CRC, London, 2005.

[HR07] Christopher J. Hillar and Darren L. Rhea. Automorphisms of finite abelian groups. *Amer. Math. Monthly*, 114(10):917–923, 2007. Available as arXiv:math/0605185 [math.GR].

[IKS10] Gábor Ivanyos, Marek Karpinski, and Nitin Saxena. Deterministic polynomial time algorithms for matrix completion problems. *SIAM J. Comput.*, 39(8):3736–3751, 2010.

[Isa08] I.M. Isaacs. *Finite group theory.* Graduate Studies in Mathematics Series. American Mathematical Society, 2008.

[Kav07] Telikepalli Kavitha. Linear time algorithms for Abelian group isomorphism and related problems. *J. Comput. Syst. Sci.*, 73(6):986–996, 2007.

[KN09] Neeraj Kayal and Timur Nezhmetdinov. Factoring groups efficiently. In *ICALP '09: Proceedings of the 36th International Colloquium on Automata, Languages and Programming*, pages 585–596. Springer-Verlag, 2009. Also availabe as ECCC Tech Report TR08-074.

[KST93] Johannes Köbler, Uwe Schöning, and Jacobo Torán. *The graph isomorphism problem: its structural complexity.* Birkhauser Verlag, Basel, Switzerland, Switzerland, 1993.

[Laz54] M. Lazard. *Sur les groupes nilpotents et les anneaux de lie.* Gauthier-Villars, 1954.

[LG09] François Le Gall. Efficient isomorphism testing for a class of group extensions. In *Proc. 26th STACS*, pages 625–636, 2009.

[Luk82] Eugene M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comp. Sys. Sci.*, 25:42–65, 1982.

[Luk91] Eugene M. Luks. Permutation groups and polynomial-time computation. In *Proc. Workshop on Groups and Computation*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 1991.

[Luk99] Eugene M. Luks. Hypergraph isomorphism and structural equivalence of boolean functions. In *Proc. 31st ACM STOC*, pages 652–658. ACM Press, 1999.

[LW12] Mark L. Lewis and James B. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups - Complexity - Cryptology*, 4(1):73–110, 2012.

[Mil78] Gary L. Miller. On the $n^{\log n}$ isomorphism technique (a preliminary report). In *Proc. 10th ACM STOC*, pages 51–58, New York, NY, USA, 1978. ACM Press.

[Mul11] Ketan Mulmuley. On P vs. NP and geometric complexity theory. *J. ACM*, 58(2):5, 2011.

[Nai10] Vipul Naik. Isomorphic extensions that are not pseudo-congruent. Personal communication, 2010.

[Nai12] Vipul Naik. Group extension problem. `http://groupprops.subwiki.org/wiki/Group_extension_problem`, December 2012.

[O'B94] E.A. O'Brien. Isomorphism testing for p-groups. *Journal of Symbolic Computation*, 17(2):133 – 147, 1994.

[PR97] Erez Petrank and Ron M. Roth. Is code equivalence easy to decide? *IEEE Transactions on Information Theory*, 43:1602–1604, 1997.

[QST11] Youming Qiao, Jayalal M. N. Sarma, and Bangsheng Tang. On isomorphism testing of groups with normal Hall subgroups. In *Proc. 28th STACS*, pages 567–578, 2011.

[Ran07] 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.

[Rob82] D.J.S. Robinson. Applications of cohomology to the theory of groups. In *Groups – St Andrews 1981*, volume 71 of *London Math. Soc. Lect. Notes*, pages 46–80. Cambridge University Press, 1982.

[Rob96] Derek J.S. Robinson. *A Course in the Theory of Groups.* Springer, 2nd edition, 1996.

[Ros13a] David Rosenbaum. Bidirectional collision detection and faster algorithms for isomorphism problems. arXiv:1304.3935 [cs.DS], 2013.

[Ros13b] David Rosenbaum. Breaking the $n^{\log n}$ barrier for solvable-group isomorphism. In *Proc. 24nd SODA*, 2013.

[Rot94] J.J. Rotman. *An Introduction to the Theory of Groups.* Graduate Texts in Mathematics. Springer, 1994.

[Sav80] Carla Savage. An $O(n^2)$ algorithm for Abelian group isomorphism. Technical report, North Carolina State University, 1980.

[Ser03] Ákos Seress. *Permutation Group Algorithms.* Cambridge University Press, 2003.

[Ste62] Robert Steinberg. Generators for simple groups. *Canadian Journal of Mathematics*, 14:277–283, 1962.

[Suz86] M. Suzuki. *Group Theory II.* Springer, 1986.

[Tau55] D. R. Taunt. Remarks on the isomorphism problem in theories of construction of finite groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 51:16–24, 1955.

[Vik96] Narayan Vikas. An $O(n)$ algorithm for Abelian p-group isomorphism and an $O(n \log n)$ algorithm for abelian group isomorphism. *J. Comput. Syst. Sci.*, 53(1):1–9, 1996.

[Wag11] Fabian Wagner. On the complexity of group isomorphism. Technical Report TR11-052, Electronic Colloquium on Computational Complexity (ECCC), 2011.

[War76] R.B. Warfield. *Nilpotent Groups.* Number 513 in Lecture Notes in Mathematics; 513. Springer-Verlag, 1976.

[Wil09a] James B. Wilson. Decomposing p-groups via Jordan algebras. *J. Algebra*, 322:2642–2679, 2009.

[Wil09b] James B. Wilson. Finding central decompositions of p-groups. *J. Group Theory*, 12:813–830, 2009.

[Wil10] James B. Wilson. Finding direct product decompositions in polynomial time, 2010. arXiv:1005.0548 [math.GR].

A An algorithm to decide whether an extension splits

The following method is straightforward and well-known, but we could not find a description in the Cayley table model, so include a sketch here. Cf. [HEO05, Section 7.6.2] for an algorithm in practical setting.

Proposition A.1. *There is a polynomial-time algorithm that takes the Cayley table of a finite group G and an abelian normal subgroup $A \lhd G$ as the input, and decides whether there is a complement of A in G. If there exists, it computes one such complement.*

Proof. Let $n = |G|$, $m = |A|$ and $\ell = n/m$. Take a set of coset representatives $S = \{s_1, \dots, s_\ell\}$ of A in G, then every set of coset representatives can be expressed as $\{a_1 s_1, \dots, a_\ell s_\ell\}$, where $a_i \in A$.

The question then is whether there exists $(a_1, \dots, a_\ell) \in A^\ell$ such that $T = \{t_1, \dots, t_\ell\}$ where $t_i = a_i s_i$ forms a subgroup of G. This can be reduced to solving a system of linear Diophantine equations as follows.

Note that T can be endowed with the group operation of G/A. Thus if $At_iAt_j = At_k$, for T to be a subgroup we need $t_it_j = t_k$. Expand $t_it_j = t_k$ as $a_is_ia_js_j = a_ks_k$, which yields

$$a_i + \theta_{s_i}(a_j) + b_{ijk} = a_k,$$

where θ_{s_i} denotes the conjugation action of s_i, $b_{ijk} := s_is_js_k^{-1} \in A$, and we use $+$ for the case as the summands are from A.

Now take a direct product decomposition of the abelian group $A = \mathbb{Z}_{q_1} \times \dots \mathbb{Z}_{q_d}$, where q_i is a prime power. Given this basis the conjugation action of s_i can be written as a $d \times d$ matrix, and we set $a_i = (x_{i1}, \dots, x_{id})$ where x_{ij} is an indeterminant over $\mathbb{Z}_{q_j}$. Then $a_i + a_j^{s_i} + b_{ijk} = a_k$ yields d linear equations, possibly modulo different integers. Collect all such linear equations arising from the group operation of G/A; then A has a complement if and only if this system of linear equations has a solution. To solve this system, use the standard trick to reduce this system of linear equations with different modulo numbers, to a system of linear Diophantine equations. The solvability of a system of linear Diophantine equations, as well as a solution if there exists, can be computed in time polynomial in the number of variables ($\ell \cdot d$), the number of equations ($\ell^2 \cdot d$) and $\log N$ where N is the largest coefficient ($\leq \log m$). If there are no solutions the algorithm returns "no complement." Otherwise the solution gives an assignment a_i' to the a_i's, such that $\{a_1' s_1, \dots, a_\ell' s_\ell\}$ is a complement. □

B Cohomological lemmas

Suppose $T_1, \dots, T_\ell$ are nonabelian simple groups. Let A be an abelian group, and $Q = \prod_{i \in [\ell]} T_i$. Let G be a group with $Z(G) = A$ and $G/Z(G) = Q$. Denote $U_i = AT_i$.

Proposition 7.2, restated. Let notations be as above. For $i, j \in [\ell]$, $i \neq j$, $[U_i, U_j] = 1$.

Proof. Let $\pi : G \to G/Z(G)$ be the natural projection. Note that $Q = G/Z(G)$ and T_i's are direct factors of Q. For $i \in [\ell]$, define V_i to be the smallest normal subgroup of G s.t. $\pi(V_i) = T_i$. Then $U_i = V_i Z(G)$, and for $i \neq j$, $[U_i, U_j] = \mathrm{id}$ if and only if $[V_i, V_j] = \mathrm{id}$.

As T_i is nonabelian simple, $\pi([V_i, V_i]) = \pi(V_i)$. Because of minimality of V_i, $V_i = [V_i, V_i]$. For $i \neq j$, $T_i \cap T_j = \mathrm{id}$, thus $[\pi(V_i), \pi(V_j)] = [T_i, T_j] = \mathrm{id}$ in Q, which implies that $[V_i, V_j] \subseteq Z(G)$. Now we have: (1) $[[V_i, V_j], V_j] \subseteq [Z(G), V_j] = \mathrm{id}$; (2) $[[V_j, V_i], V_j] = \mathrm{id}$ as $[V_i, V_j] = [V_j, V_i]$. Then Hall's three subgroup lemma [Suz86, Chapter 4, Proposition 1.9] gives that $[[V_j, V_j], V_i] = \mathrm{id}$. Finally noting that $V_j = [V_j, V_j]$ we have $[V_j, V_i] = \mathrm{id}$. □

Lemma 7.4. *Let $A' \times A'' \hookrightarrow G \twoheadrightarrow Q$ be a central extension of $A' \times A''$ by Q. Let $p_{A'} \colon A' \times A'' \to A'$ be the projection onto A' along A''. If there is a 2-cocycle $f \colon Q \times Q \to A' \times A''$ such that $p_{A'} \circ f \colon Q \times Q \to A'$ is a 2-coboundary, then G is isomorphic (even congruent) to the direct product $A' \times (G/A')$.*

Furthermore, given the Cayley table of G, A' can be computed in polynomial time using linear algebra over abelian groups.

Proof. We prove directly that $A' \trianglelefteq G$, exhibit a complement of A' in G and show that this complement is normal. At the end we show how to compute A' using linear algebra.

We may assume without loss of generality that the image of f lies entirely within A''. For if not, then we may add the 2-coboundary $p_{A'} \circ f \colon Q \times Q \to A' \hookrightarrow A' \times A''$ to f to get an equivalent 2-cocycle satisfying this condition. Similarly, we may assume that f is normalized so that $f(1, q) = f(q, 1) = 0$ for all $q \in Q$.

We construct a group congruent to G from the cocycle f in the usual way: the elements are $A' \times A'' \times Q$ as a set, with multiplication given by (writing A' and A'' additively):

$$(a_1, a'_1, q_1)(a_2, a'_2, q_2) = (a_1 + a_2, a'_1 + a'_2 + f(q_1, q_2), q_1 q_2)$$

since the image of f lies entirely in A''. We also have $(a, a', q)^{-1} = (-a, -a' - f(q, q^{-1}), q^{-1})$.

A' is normal:

$$\begin{aligned} (a, a', q)^{-1}(a_0, 1, 1)(a, a', q) &= (-a, -a' - f(q, q^{-1}), q^{-1})(a_0 + a, a', q) \quad (\text{since } f(1, q) = 0) \\ &= (-a + a_0 + a, -a' - f(q, q^{-1}) + a' + f(q, q^{-1}, qq^{-1}) \\ &= (a_0, 0, \mathrm{id}_Q). \end{aligned}$$

A' has a normal complement: as the image of f lies entirely in A'', it is readily verified that elements of the form $(0, a', q)$ are closed under product, hence form a subgroup of G which is isomorphic to G/A' and intersects A' only in the identity. Moreover, this subgroup is normal. For consider conjugating one of its elements by an arbitrary element of G: $(-a, -a' - f(q, q^{-1}), q^{-1})(0, a'_0, q_0)(a, a', q)$. From the multiplication rule above, it is clear that the first coordinate of this product is just the sum of the first coordinates of the three factors—namely, zero—whatever the second and third coordinates are.

Finally, we show how to compute A' from the Cayley table for G using linear algebra over abelian groups. We give the proof in the case that $Z(G) = \mathbb{Z}_p^k$ is elementary abelian; the general case uses the same ideas as in Section 6.1.1. First compute $Z(G)$ (which is $A' \times A''$, but we do not yet know this decomposition of $Z(G)$, we are only promised it exists) and $Q = G/Z(G)$. Choose any set-theoretic setction $s\colon Q \to G$ and compute the corresponding cocycle $f := f_s$. Let M_f be the $k \times |Q|^2$ $\mathbb{Z}_p$-matrix corresponding to f as in §7. We may view M_f as a $\mathbb{Z}_p$-linear map from $Z(G) = \mathbb{Z}_p^k$ to $\mathbb{Z}_p^{Q\times Q}$. As in §7, we may compute a basis of $B^2(Q, Z(G))$ that is a direct sum of bases for $B^2(Q, \mathbb{Z}_p)$, one copy for each row of M_f. The maximal A' satisfying the conditions of the theorem is then the inverse image of $B^2(Q, \mathbb{Z}_p)$ under this map. Computing the inverse image of $B^2(Q, \mathbb{Z}_p)$ under the map $M_f^T\colon Z(G) \to \mathbb{Z}_p^{Q\times Q}$ is then just linear algebra over $\mathbb{Z}_p$. □

C Alternative proofs for Theorem 6.1 and Theorem 7.1 (2)

C.1 Proof of Theorem 6.1

Proposition C.1. *For $A = \mathbb{Z}_p^k$ and a group Q, let $n = |A| \cdot |Q|$. In time $O(n^2 \log n)$ one can compute: a complement W of $B^2(Q, A)$ in $C^2(Q, A)$, and $\mathbb{Z}_p$-linear projection π from $C^2(Q, A)$ to W. Furthermore, W is an invariant subspace of α, and for any $\alpha \in \mathrm{Aut}(A)$, $\alpha\pi = \pi\alpha$ as linear maps on $C^2(Q, A)$.*

Proof. Under the above identification, the set $C^2(Q, A)$ of 2-cochains is identified with the set of all $k \times |Q|^2$ matrices over $\mathbb{Z}_p$. Then $Z^2(Q, A)$ is not just a subgroup, but also a $\mathbb{Z}_p$-linear subspace of $C^2(Q, A)$, and similarly $B^2(Q, A)$ is a $\mathbb{Z}_p$-linear subspace of $Z^2(Q, A)$. $\mathrm{Aut}(A) \cong \mathrm{GL}(k, p)$ acts on $C^2(Q, A)$ by left multiplication, and $\mathrm{Aut}(Q)$ acts on $C^2(Q, A)$ by permuting the columns according to the diagonal action of $\mathrm{Aut}(Q)$ on $Q \times Q$.

Let us then explicitly specify a basis of $B^2(Q, A)$. First for $i \in [k]$ let U_i be the linear subspace of $C^2(Q, A)$ where entries outside the ith row are all 0. For $q \in Q$, $q \neq \mathrm{id}$, $i \in [k]$, let $u_{q,i} : Q \to A$ be $u_{q,i}(q') = \delta(q, q')e_i$ where δ is the Kronecker delta. Let $f_{q,i} : Q \times Q \to A$ be the 2-coboundary based on $u_{q,i}$. Then $\{f_{q,i} | q \in Q, q \neq \mathrm{id}, 1 \leq i \leq n\}$ is a basis for $B^2(Q, A)$. Let $V_i = \{f_{q,i} \mid q \in Q, q \neq \mathrm{id}\}$, then $V_i \leq U_i$ and $B^2(Q, A) = \oplus_{i\in[k]} V_i$. In fact, when restricted to the subspace of the ith row, the V_i's are the same.

Now let us choose complements of W_i of V_i in U_i for $i \in [k]$, s.t. $W_i = W_j$ for every $i, j \in [k]$; let π_i be the projection to W_i along V_i in U_i. π_i's collectively define a projection π to $\oplus_i W_i$ along $\oplus_i V_i$ in $\oplus_i U_i = C^2(Q, A)$.

Given this π, it is not hard to identify the 2-cohomology class of $f \in Z^2(Q, A) \leq C^2(Q, A)$: $f, g \in Z^2(Q, A)$ are cohomologous, if and only if $\pi(f) = \pi(g)$. Furthermore, it is easy to see, but important to note that for any $\alpha \in \mathrm{Aut}(A)$, $\alpha\pi = \pi\alpha$. Also the above procedure involves only standard linear algebra tasks, and such π can be constructed in time $O(n^2 \log n)$. □

To summarize, consider $\alpha \in \mathrm{Aut}(A)$, $\beta \in \mathrm{Aut}(Q)$, and π just introduced. All of them can be viewed as linear maps on $C^2(Q, A)$, while α, β are nonsingular. We then note: (1) α and β commute; (2) α and π commute.

Proof of Theorem 6.1. We list $\mathrm{Aut}(Q)$ in time $t(n)$. For $i = 1, 2$, choose an arbitrary section of Q in G_i to get a 2-cocycle f_i. Use Proposition C.1 to get the projection $\pi : C^2(Q, A) \to W$ for some complement W of $B^2(Q, A)$ such that W is invariant under α and $\alpha\pi = \pi\alpha$ for every $\alpha \in \mathrm{Aut}(A)$. By the main Lemma 3.2, it is necessary and sufficient to test whether there exists an $(\alpha, \beta) \in \mathrm{Aut}(A) \times \mathrm{Aut}(Q)$ s.t. $\pi(f_1) = \pi(f_2^{(\alpha,\beta)})$. As every α commutes with both π and β, this condition is equivalent to $\pi(f_1) = (\pi(f_2^{(\mathrm{id},\beta)}))^{(\alpha,\mathrm{id})}$. In other words, we may leave α unspecified until the final step.

For each $\beta \in \mathrm{Aut}(Q)$, we compute $f_1' = \pi(f_1)$, and $f_2' = \pi(f_2^{(\mathrm{id},\beta)})$. Note that f_i' are in $W \leq C^2(Q,A)$. The task then reduces to compute $\alpha \in \mathrm{Aut}(A)$ s.t. $f_1' = \alpha^{-1}(f_2')$. This is because $\alpha\pi = \pi\alpha$ allows us to apply π to $f_2^{(\mathrm{id},\beta)}$ first, and leave α to be determined later. $f_1' = \alpha^{-1} f_2'$ for some $\alpha \in \mathrm{Aut}(A)$, if and only if the row spans of $M_{f_1'}$ and $M_{f_2'}$ are the same in $\mathbb{Z}_p^{|Q|^2}$. The latter task is standard in linear algebra and can be checked in time $O(|Q|^6)$.

The main Lemma 3.2 implies that $G_1 \cong G_2$ if and only if the above test succeeds for some $\beta \in \mathrm{Aut}(Q)$. □

C.2 Proof of Theorem 7.1 (2)

Proof. Before presenting the algorithm we need some consequences of Lemma 7.3. For G_j, $j = 1, 2$, we say a 2-cocycle $f_j : Q \times Q \to A$ respects the direct factors if there exist $f_{j,i} : T_i \times T_i \to A$, $i \in [\ell]$ s.t. Equation 8 holds. Let $Z^2_{\mathrm{prod}}(Q,A)$ denote the set of 2-cocycles respecting the direct factors. The proof of Lemma 7.3 suggests that $Z^2_{\mathrm{prod}}(Q,A) \neq \emptyset$. Similarly we can define 2-coboundaries that respect the direct factors (cf. Equation 7), and $B^2_{\mathrm{prod}}(Q,A)$. For two 2-cocycles from $Z^2_{\mathrm{prod}}(Q,A)$, their difference is in $B^2_{\mathrm{prod}}(Q,A)$. Recall that M_{f_j} denotes the matrix representation of f_j with row index set $[k]$ and column index set $Q \times Q$. As f_j is completely determined by the direct factors, we can focus on M_{f_j} with row indices from $\cup_{i\in[\ell]} T_i \times T_i$. Thus for $f_j \in Z^2_{\mathrm{prod}}(Q,A)$ the size of M_{f_j} is assumed to be $k \times (\sum_{i\in[\ell]} |T_i|^2)$.

As every $\beta \in \mathrm{Aut}(Q)$ can be represented as $(\delta, \sigma) \in (\prod_i \mathrm{Aut}(Q)^{\ell_i}) \times (\prod_i S_{\ell_i})$, thus $Z^2_{\mathrm{prod}}(Q,A)$ (resp. $B^2_{\mathrm{prod}}(Q,A)$) is an invariant subset in $Z^2(Q,A)$ under the actions of $\mathrm{Aut}(A)$ and $\mathrm{Aut}(Q)$. Following the proof of Proposition C.1, we can get a projection $\pi : C^2(Q,A) \to W$ for some $W \leq C^2(Q,A)$ s.t. (1) W is a complement of $B^2_{\mathrm{prod}}(Q,A)$ in $C^2(Q,A)$; (2) W is an invariant subspace of α and σ; (3) $\alpha\pi = \pi\alpha$ for $\alpha \in \mathrm{Aut}(A)$, and $\sigma\pi = \pi\sigma$ for $\sigma \in \prod_i S_{\ell_i}$. The relation with σ is ensured if for isomorphic factors $T_i \cong T_j$ we choose the same complement for $B^2(T_i,A)$ and $B^2(T_j,A)$ (in $C^2(T_i,A)$ and $C^2(T_j,A)$, respectively). The question then is to decide the existence of $(\alpha,\delta,\sigma) \in \mathrm{Aut}(A) \times (\prod_i \mathrm{Aut}(Q)^{\ell_i}) \times (\prod_i S_{\ell_i})$, making $\pi(f_1) = \pi(f_2^{(\mathrm{id},\delta,\mathrm{id})})^{(\alpha,\mathrm{id},\sigma)}$.

Note that $\pi(f_1) \in W \leq Z^2_{\mathrm{prod}}(Q,A)$ can be expressed as a $k \times (\sum_{i\in[\ell]} |T_i|^2)$-size matrix over $\mathbb{Z}_p$. Let $M_1 = M_{\pi(f_1)}$. By Lemma 7.4, wlog we assume M_1 is of rank k. Otherwise Lemma 7.4 splits a direct factor out of the center as $A' \times G_j/A'$.[17] By the Remak-Krull-Schmidt theorem, we are reduced to test isomorphism between G_1/A' and G_2/A', where the desired condition holds. To compute such $A' \in Z(G_j)$ s.t. A' is a direct factor is straightforward as discussed in Lemma 7.4. By assumption we have $|T_i| \leq D$ for some constant D. Given these preparations the algorithm works as follows.

For every diagonal $\prod_{j\in[\ell]} \alpha_j$ of $\prod_j T_j$, do the following. Compute $\pi(f_1)$ and $\pi(f_2^{(\mathrm{id},\delta,\mathrm{id})})$, and let $M_1 = M_{\pi(f_1)}$ and $M_2 = M_{\pi(f_2^{(\mathrm{id},\delta,\mathrm{id})})}$. Recall that M_j is the matrix of size $k \times (\sum_{i\in[\ell]} |T_i|^2)$ corresponding to f_j as described in §7. Let $m := \sum_i |T_i|^2 \leq \ell \cdot D^2$. Viewing M_j as two linear codes of dimension k in $\mathbb{Z}_p^m$, we compute the coset of equivalences $\mathrm{CodeEq}(M_1, M_2) \subseteq S_m$ using Theorem 5.2. On the other hand $\prod_i S_{\ell_i}$ induces an action on $[m]$, which consists the permutations we want. Thus we need to intersect $\mathrm{CodeEq}(M_1, M_2)$ with $\prod_i S_{\ell_i}$. If the intersection is nonempty, the algorithm reports "isomorphic." On the other hand, if for all $(\alpha, \prod_i \delta_i)$ we get empty intersection, then the algorithm returns "not isomorphic."

[17] Lemma 7.4 is concerned with general $Z^2(Q,A)$ and $B^2(Q,A)$ while it can be adapted easily to deal with $Z^2_{\mathrm{prod}}(Q,A)$ and $B^2_{\mathrm{prod}}(Q,A)$.

To analyze the running time, the outer loop depending on the diagonals is polynomially related to n. Both the applications of the Linear Code Equivalence algorithm (Theorem 5.2), and the singly-exponential time algorithm for Coset Intersection ([Luk99]), take time $c^{\ell \cdot D^2}$ for some absolute constant c. □

D Generalized Fitting subgroups of groups with central radical

Definition D.1. A group G is quasisimple if $G = [G, G]$ and $G/Z(G)$ is a nonabelian simple group. G is m-quasisimple if $G = [G, G]$ and $G/Z(G)$ is a direct product of nonabelian simple groups.

Our m-quasisimple groups are Suzuki's "semisimple groups" [Suz86, Page 446]; we cannot use Suzuki's terminology as we have used "semisimple" for groups with no abelian normal subgroups. Note that central-radical groups with $G/Z(G)$ a direct product of nonabelian simple groups need not be m-quasisimple groups, as the former need not be perfect. However, the difference is not much:

Proposition D.2 ([Suz86, Ch. 6, corollary to Theorem 6.4])**.** *Let G be a group such that $G/Z(G)$ is a direct product of nonabelian simple groups. Then $G = Z(G)[G, G]$, and $[G, G]$ is an m-quasisimple group.*

M-quasisimple groups are crucial for defining the generalized Fitting subgroups.

Proposition D.3 ([Suz86])**.** *Let H and K be m-quasisimple normal subgroups of G, then HK is m-quasisimple.*

This motivates the following definition. Recall that the Fitting subgroup $F(G)$ of G is the maximal nilpotent normal subgroup of G.

Definition D.4. Let G be a group. The *layer* $E(G)$ of a group G, is the maximal m-quasisimple normal subgroup of G. The *generalized Fitting subgroup* $F^*(G)$ of G is $E(G)F(G)$.

Proposition D.5. *Let G be a group with central radical.* $\mathrm{Soc}^*(G) = F^*(G)$.

Proof. As $\mathrm{Rad}(G) = Z(G)$, $F(G) = Z(G)$. Let $D = [\mathrm{Soc}^*(G), \mathrm{Soc}^*(G)]$. So D is m-quasisimple and $\mathrm{Soc}^*(G) = Z(G)D = F(G)D$ ([Suz86, Ch. 6, corollary to Theorem 6.4]). Thus $D \subseteq E(G)$ and $\mathrm{Soc}^*(G) \subseteq F^*(G)$.

To show $\mathrm{Soc}^*(G) \supseteq F^*(G)$, for the purpose of contradiction, suppose $Z(G)D = \mathrm{Soc}^*(G) \subsetneq F^*(G) = Z(G)E(G)$. Consider the decomposition of $E(G)$ into quasisimple groups ([Suz86, Ch. 6, Definition 6.8]) as $Q_1 \cdot \ldots \cdot Q_d$, where $\cdot$ denotes central product, and Q_i is subnormal in G. Wlog assume $Z(G)Q_1 \not\subseteq Z(G)D$. As Q_1 is subnormal in G, $G/Z(G)$ necessarily has $Q_1Z(G)/Z(G)$ as a subnormal group, contained in some minimal normal group $N/Z(G) \lhd G/Z(G)$ ([Isa08, Lemma 9.17]). By assumption, $Q_1Z(G)/Z(G)$ is not contained in $DZ(G)/Z(G) = \mathrm{Soc}^*(G)/Z(G) = \mathrm{Soc}(G/Z(G))$, so $N/Z(G)$ is a minimal normal subgroup not contained in $\mathrm{Soc}(G/Z(G))$, contradicting the definition of the socle. □

E Discussion of pseudo-congruence and its variants

Recall that two groups G_1 and G_2 as extensions of A by Q are equivalent if there exists an isomorphism $\gamma : G_1 \to G_2$ s.t. the following diagram commutes:

$$\begin{tikzcd}
A \arrow[r, hook, "\iota_1"] \arrow[d, equal] & G_1 \arrow[r, two heads, "\pi_1"] \arrow[d, "\gamma", "\cong"'] & Q \arrow[d, equal] \\
A \arrow[r, hook, "\iota_2"] & G_2 \arrow[r, two heads, "\pi_2"] & Q
\end{tikzcd}$$

It is possible for two extensions G_i of N by Q to be isomorphic as groups without being congruent, as the next example shows:

Example E.1 (Isomorphic groups from non-equivalent extensions)**.** $\mathbb{Z}_9$ can be viewed as an extension of $\mathbb{Z}_3$ by $\mathbb{Z}_3$ in two ways. Firstly $\mathbb{Z}_3 \hookrightarrow \mathbb{Z}_9$ by sending 1 to 3. Then define $\pi_i(1) = i$ for $i \in [2]$. To see π_1 and π_2 yield non-equivalent extensions, consider $\phi \in \mathrm{Aut}(\mathbb{Z}_9)$, suppose $\phi(1) = k$, $k \in \{1, 2, 4, 5, 7, 8\}$. ϕ induces identity on $\langle 3 \rangle$, thus $3 = \phi(3) = 3\phi(1) = 3k \mod 9$, thus $k = 1 \mod 3$. On the other hand, $1 = \pi_1(1) = \pi_2(\phi(1)) = \pi_2(k) = 2k \mod 3$, that is $k = 2 \mod 3$. We then arrive at a contradiction.

Recall that two extensions $A \hookrightarrow G_j \twoheadrightarrow Q$, $j = 1, 2$ are pseudo-congruent if there exist $\alpha \in \mathrm{Aut}(A)$, $\beta \in \mathrm{Aut}(Q)$ and $\gamma \in \mathrm{Iso}(G_1, G_2)$ such that the following diagram commute:

$$\begin{tikzcd}
A \arrow[r, hook, "\iota_1"] \arrow[d, "\alpha", "\cong"'] & G_1 \arrow[r, two heads, "\pi_1"] \arrow[d, "\gamma", "\cong"'] & Q \arrow[d, "\beta", "\cong"'] \\
A \arrow[r, hook, "\iota_2"] & G_2 \arrow[r, two heads, "\pi_2"] & Q
\end{tikzcd}$$

That is, if there exists an isomorphism $\gamma : G_1 \to G_2$ such that $\gamma(A) = A$ and it induces α on A and β on Q. Also recall that if γ induces the identity maps on A and Q the extensions are called equivalent.

It is also possible for two extensions G_1, G_2 of N by Q to have isomorphic total groups but not even be pseudo-congruent. The following example was provided by Vipul Naik [Nai10]:

Example E.2 (Isomorphic groups from non-pseudo-congruent extensions)**.** $N = \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$, $Q = \mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $G = \mathbb{Z}_{p^3} \times \mathbb{Z}_{p^2} \times \mathbb{Z}_p \times \mathbb{Z}_p$. In one extension, $\iota_1(a, b, c) = (pa, 0, b, c)$ and in the other $\iota_2(a, b, c) = (pa, pb, a \pmod{p}, c)$. To see that there is no automorphism of G sending $\mathrm{Im}\,\iota_1$ to $\mathrm{Im}\,\iota_2$, note that $\mathrm{Im}\,\iota_1$ contains elements that are p times an element of order p^3 in G, but $\mathrm{Im}\,\iota_2$ contains no such elements.

We describe two special cases of pseudo-congruence of extensions, explain the algorithmic problems corresponding to them, and indicate some of the solutions. The first one was discussed in [Rob82]. Consider the following case when γ only induces the identity map on A as follows:

$$\begin{tikzcd}
A \arrow[r, hook, "\iota_1"] \arrow[d, "\alpha", "\cong"'] & G_1 \arrow[r, two heads, "\pi_1"] \arrow[d, "\gamma", "\cong"'] & Q \arrow[d, equal] \\
A \arrow[r, hook, "\iota_2"] & G_2 \arrow[r, two heads, "\pi_2"] & Q
\end{tikzcd}$$

This corresponds to the algorithmic setting when enumerating $\mathrm{Aut}(Q)$ is allowed, as after fixing some $\beta \in \mathrm{Aut}(Q)$ we are reduced to looking for α such that G_1 and G_2 are pseudo-congruent by (α, β). If the extension is split and $A \in \mathbb{Z}_p^k$ is elementary abelian, this problem reduces to the module isomorphism problem: the action of each $q \in Q$ can be expressed as a nonsingular matrix in $\mathrm{GL}(k, p)$. So suppose $Q = \{q_1, \dots, q_s\}$, and in G_j the conjugation action of Q is written as $\{M(j, i) \mid M(j, i) \in \mathrm{GL}(k, p)\}$ where $M(j, i)$ denotes the action of q_i on A in G_j. The problem of compatibility of actions then reduces to determine whether there exists $T \in \mathrm{GL}(k, p)$ s.t. $TM(1, i) = M(2, i)T$ for every $i \in [\ell]$. This is a special case of the module isomorphism problem, which admits deterministic polynomial-time algorithms by [CIK97, BL08, IKS10]. On the other extreme when the extension is central, Theorem 6.1 solves the cohomology class isomorphism problem. At present it is not clear to us how concatenate the two procedures to solve the pseudo-congruent problem as a whole.

On the other hand, if γ only induces the identity map on A:

$$\begin{tikzcd}
A \arrow[r, hook, "\iota_1"] \arrow[d, equal] & G_1 \arrow[r, two heads, "\pi_1"] \arrow[d, "\gamma", "\cong"'] & Q \arrow[d, "\beta", "\cong"'] \\
A \arrow[r, hook, "\iota_2"] & G_2 \arrow[r, two heads, "\pi_2"] & Q
\end{tikzcd}$$

This corresponds to the algorithmic setting when $\mathrm{Aut}(A)$ is enumerable, and our goal is to find β such that G_1 and G_2 are pseudo-congruent. Note that Theorem 7.1 (1) falls into this setting. Also in this setting is the important work by Brooksbank and Wilson [BW12]. They presented an efficient algorithm to compute the isometry group of a Hermitian bilinear map in a model stronger than Cayley table model; given the connections between p-groups of class 2 and exponent p and alternating bilinear maps (cf. [Wil09a, Section 3.4]), this amounts to solve the problem of finding β as above. It would be very interesting to see whether following the approach in [BW12] will shed light on p-groups of class 2.

F Relationship with results on practical algorithms

It is not surprising that the complexity-theoretic results and practical results from the computational group theory (CGT) community often leverage the same underlying structure of the groups. Here we discuss the relationship between these two sets of results. A general reference for CGT is the handbook [HEO05]; algorithms in CGT are often implemented in Magma [BJP97] and/or GAP [GG13].

The goal in CGT is to get practical algorithms, so the groups are typically given as input by generating sets of permutations or matrices, or by poly-cyclic presentations (for solvable groups). In general, these encodings are of size poly-logarithmic in $|G|$, so for them even a provable worst-case guaranteed running time of $O(|G|)$ is usually impractical. However, in order to achieve better running times, they frequently use heuristic methods without provable guarantees. In contrast, we are interested in provable worst-case guarantees, but our input is the entire Cayley table and we allow ourselves running time polynomial in $|G|$.

Regarding isomorphism testing algorithms in CGT, besides [CH03] mentioned above, some notable works include [O'B94, BE99, LW12]. Very often isomorphism testing arises for them as a subroutine for the construction of all finite groups up to a certain order (up to isomorphism), as in [Tau55, BE99, BEO02]. Recently, Wilson *et al.* have produced several results related to isomorphism of p-groups (sometimes reformulated in the context of Hermitian bilinear maps) in

[Wil09a, Wil09b, LW12, BW12], some of which include worst-case guarantees. The structure they are uncovering in p-groups is also notable from the Cayley table perspective, and there is likely more to be discovered in this direction.

The two communities often leverage the same structure that is present in various classes of groups, though the complexity results often require further structural results on the group classes considered, in addition to further algorithmic results. For example, Besche and Eick had already considered the group classes in Le Gall's work [LG09] (the algorithm in Figure 4 in [BE99]), but Le Gall's work was the first to give a provably polynomial-time algorithm for groups of the form $A \rtimes \mathbb{Z}_p$ with A abelian and $p \nmid |A|$. A necessary ingredient in Le Gall's work is a detailed understanding of automorphism groups of abelian groups traced back to Ranum [Ran07], which was not needed in the practical setting of Besche and Eick. Another example is the polynomial-time algorithm for semisimple groups [BCQ12], where a similar situation is described at the end of that paper, comparing it with the practical work of Cannon and Holt [CH03]. For example, the algorithm in [BCQ12] required bounds on the orders of the transitive permutation groups other than S_n and A_n.

Relations to the present work. As mentioned above, our choice to focus on groups with central radicals is partially motivated by the strategy of Cannon and Holt [CH03]. Another work of particular relevance is [BE99]. There Besche and Eick considered construction of finite groups, and proposed three heuristics. To support one heuristic, they proposed the concept of "strong isomorphism" of groups, which can be viewed as a special case of our Lemma 3.2 in their setting. We use the same structural results to support the approach, but as we work in the Cayley table setting, we have much more freedom to handle the 2-cohomology classes directly, as in Theorem 6.1; we also need Lemma 7.3 which in turn allows us to apply algorithms for Linear Code Equivalence and Coset Intersection as in Theorem 7.1. These ingredients are not present in [CH03] nor [BE99], which is natural as in their setting these ingredients would not be practical.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de