Electronic Colloquium on Computational Complexity, Report No. 177 (2026)

Algorithms for Finite Group Epimorphism Testing*

Joshua A. Grochow
Department of Computer Science, University of Colorado Boulder
Department of Mathematics, University of Colorado Boulder
jgrochow@colorado.edu

Pranjal Srivastava
Department of Math and Computing
Indian Institute of Information Technology Vadodara
pranjal.srivastava194@gmail.com

Dhara Thakkar
Graduate School of Mathematics
Nagoya University
thakkar_dhara@math.nagoya-u.ac.jp

Abstract

The Group Epimorphism Problem (GpEpi) asks, given two finite groups G_1 and G_2, whether there exists a surjective group homomorphism, or *epimorphism*, from G_1 to G_2. When the input groups are given by their multiplication (Cayley) tables, the problem admits a quasipolynomial-time algorithm in general, but little is known about its complexity for structured classes of finite groups. In this paper, we study the computational complexity of GpEpi for several well-studied classes of finite groups.

Our main results are polynomial-time epimorphism tests for several classes of groups for which polynomial-time isomorphism testing was previously known:

- Groups with Abelian normal Hall subgroups with cyclic complement
- Groups with (product of) elementary Abelian normal Hall subgroup with elementary Abelian complement.
- Groups with some constraints on their Abelian chief factors.

1 Introduction

The study of computational problems in finite groups has a long history in both (computational) algebra and theoretical computer science. Among the most well-known is the Group Isomorphism problem (GpI), which asks whether two given groups are isomorphic. From the perspective of worst-case guarantees,[1] this problem has been extensively studied for various classes of groups, including

*A preliminary version of this article appeared in the proceedings of the 53rd EATCS International Colloquium on Automata, Languages, and Programming (ICALP 2026)

[1]In this paper we focus on algorithms with worst-case guarantees as a function of the order of the group, though we occasionally comment on heuristics that will likely improve performance in practice. Because of our focus, we can without loss of generality assume that the multiplication (Cayley) tables are given as input. We refer the reader to the Handbook of Computational Group Theory [HEO05], as well as, e. g., the works of Holt, Eick, O'Brien, Leedham-Green, and Hulpke [EHH17, BEO02, ELGO02, BE99, CH03, Hul22] for research into practical algorithms in more succinct input models.

ISSN 1433-8092

Abelian groups, groups with normal Hall subgroups, and groups without Abelian normal subgroups [BCQ12, BCGQ11, BMW17, BQ12a, GQ17a, GQ24, GQ23, LG09, LW12, QST12, Ros13, Sun23, IMQ+25]. Efficient algorithms in these settings often rely on exploiting the underlying algebraic structure, such as decompositions into simpler subgroups or the use of representation theory.

A related problem is the Group Epimorphism Problem (GpEpi), which, given two finite groups G_1 and G_2, asks to decide whether there exists an *epimorphism* (=surjective homomorphism)[2] from G_1 to G_2. When G_1 and G_2 are given by their Cayley tables, one can easily design an $n^{\log_p n+O(1)}$-time algorithm for the GpEpi problem, where $|G_1| = n$ and p is the smallest prime divisor of n. Unlike isomorphisms, epimorphisms allow the domain group to be larger and potentially more complex than the codomain, introducing new algorithmic and structural challenges.

The GpEpi problem has been studied previously, primarily in the setting of *finitely presented groups*, where the focus is often on decidability and hardness questions. In this context, Remeslennikov showed that the epimorphism problem is undecidable when both the source and target groups are non-Abelian nilpotent groups given by finite presentations [Rem79]. Subsequent work has identified classes of target groups for which epimorphism testing is decidable or computationally hard. Friedl and Löh proved decidability results when the target group is virtually cyclic or a direct product of an Abelian and a finite group [FL21], while Elder, Shen, and Weiss showed that the problem is NP-complete for similar classes of targets [ESW25]. Kuperberg and Samperton further established NP-hardness when the target is a fixed finite non-Abelian simple group [KS18].

In contrast, comparatively little is known about the computational complexity of GpEpi for *finite groups given by their Cayley tables*. While GpI and related problem have been extensively studied in this model, efficient algorithms for epimorphism testing remain largely unexplored. Understanding which classes of finite groups admit polynomial-time algorithms for GpEpi is a natural and significant open direction in computational group theory and complexity theory.

Motivated by this, in this paper, we investigate the computational complexity of GpEpi for several well-studied classes of groups. We focus on classes for which structural properties can be exploited algorithmically, and for which efficient isomorphism testing is known. In particular, we study GpEpi for groups with Abelian normal Hall subgroups and groups without Abelian composition factors. Our results build on and extend techniques from the literature on GpI, while also introducing a new representation-theoretic problem and developing algorithmic frameworks specific to epimorphism testing.

Before coming to our contributions we mention a few points on the general complexity of GpEpi, that also serve to motivate some of the classes of groups we consider. If $|G| = |H|$, then epimorphisms $G \to H$ and isomorphisms are the same thing, so GpI $\leq_m^p$ GpEpi. In particular, this means that for any class of groups we cannot put GpEpi for that class into P without doing the same for GpI, hence we focus on classes of groups for which GpI is already known to be in P. It is clear that the problem is in NP (the epimorphism serves as a witness), and the generator-enumerator technique gives an $|G|^{\log|G|+O(1)}$-time algorithm for GpEpi. Unlike isomorphism problems, we do not know whether GpEpi is in coAM (though the quasi-polynomial-time upper bound nonetheless implies that it is not NP-complete unless the Exponential Time Hypothesis is false). Just as GpI reduces to Graph Isomorphism, GpEpi reduces to Graph Epimorphism, but the latter is NP-complete, even for target graphs of size $O(1)$ (epimorphisms to the triangle graph are the same as proper 3-colorings that use all three colors) [Vik97, GFM+14]. It is a somewhat interesting question whether GpEpi is in P when the target group has size $O(1)$.

[2] In some concrete categories, such as the category of rings, the concepts of epimorphism and surjective homomorphism differ, but in the category of groups they are the same [Lin70], so we do not dwell on the two definitions.

1.1 Our Contributions

We study GpEpi for several well-studied classes of finite groups. For each such class, we design a deterministic polynomial-time algorithm for GpEpi. We now summarize our main results.

To put our results in context, we recall some of the significant progress on algorithms with worst-case guarantees for GpI, and use this opportunity to introduce some notation we will use throughout the paper. We begin with some notation: for two group classes X and Y, Coprime(X, Y) is the class of groups with a normal subgroup N from X and a complement H from Y, such that $|N|$ and $|H|$ are coprime. Let Ab be the class of Abelian groups and let Ab_p be the class of Abelian p-groups, where p is a prime. Let ElemAb be the class of elementary Abelian groups, and let Cyc be the class of cyclic groups.

Over the last two decades, two of the most general classes of groups for which polynomial-time algorithms for GpI have been developed fall into the following lines of work, and we make progress on solving GpEpi along these lines:

- **Coprime extensions.** Le Gall [LG09] solves GpI for groups in Coprime(Ab, Cyc). Qiao, Sarma, and Tang [QST12] extended this to Coprime(Ab, ElemAb). This was extended to groups with Abelian Sylow towers by Babai & Qiao [BQ12b], and to tame Sylow towers in Grochow & Qiao [GQ15]. We refer the reader to those papers for definitions as we do not yet handle GpEpi for such groups here.

  We do solve GpEpi for groups in Coprime(Ab, Cyc) (cf. Le Gall *ibid.*) and Coprime($\prod$ ElemAb, ElemAb), and discuss challenges to extending our results to Coprime(Ab, ElemAb) (cf. Qiao–Sarma–Tang, *ibid.*).

- **Fitting-free groups.** Isomorphism of groups without Abelian normal subgroups, a.k.a. semisimple or Fitting-free, was solved in [BCQ12] (building on [BCGQ11]). This was extended to more general classes of groups in [GQ17b].

  Although we do not yet solve GpEpi for arbitrary Fitting-free groups, we handle two classes of groups that are more restrictive, yet headed in this direction. Namely, we solve GpEpi (1) for groups with no Abelian composition factors, and (2) for pairs (G, H) where H is Fitting-free and the Abelian chief factors of G have limited multiplicity. We discuss some challenges in extending this to all Fitting-free groups in Sec. 7.

For all the aforementioned results except the last, the classes of groups involved are closed under homomorphic images, and membership in the class is recognizable in polynomial time. If $\mathcal{C}$ is any class of finite groups with these properties, then solving GpEpi for pairs (G, H) with $G, H \in \mathcal{C}$ is equivalent to solving GpEpi for pairs (G, H) where $G \in \mathcal{C}$ and H is arbitrary.

Efficient epimorphism testing of Coprime(Ab, Cyc)**.** We begin by considering the class Coprime(Ab, Cyc), consisting of groups that are extensions of an Abelian group by a cyclic group. This class serves as a first step beyond Abelian groups for GpEpi. Polynomial-time algorithms for GpI are known for this class due to Le Gall [LG09]. Theorem 1 shows that GpEpi can be solved efficiently for groups in Coprime(Ab, Cyc). Although we leverage some of the same algebraic structure used by Le Gall, we also use additional results from representation theory and combinatorial techniques (maximum matching in bipartite graphs).

Theorem 1. *There is a polynomial-time algorithm for* GpEpi*, restricted to pairs of groups* (G_1, G_2) *such that* G_1 *is in* Coprime(Ab, Cyc)*. If there is an epimorphism from* G_1 *to* G_2*, our algorithms computes one such.*

Efficient epimorphism testing of Coprime($\prod$ ElemAb, ElemAb)**.** Next, we study GpEpi, for groups in the class Coprime($\prod$ ElemAb, ElemAb), which consists of groups with a normal Hall subgroup that is a direct product of elementary Abelian groups, complemented by another elementary Abelian group. To develop an algorithm for this class, we first consider the subclass, Coprime(ElemAb, ElemAb).

To solve GpEpi for groups in Coprime(ElemAb, ElemAb), we reduce it to a problem in representation theory of finite groups. We now describe the specific formulation of this problem that captures the GpEpi.

A *representation* of a group G is a homomorphism from G to a general linear group. When the group G is a finite elementary Abelian normal subgroup of a larger group, the condition of epimorphism testing of large groups with respect to their component groups naturally translates into questions about representations (Theorem 6). This leads to an interesting algorithmic problem in representation theory that is of independent interest. We define this problem below after introducing the following definition.

Let V and W be two finite-dimensional vector spaces over a field $\mathbb{F}$ of dimension d and d', respectively. Let $\tau : G \to \mathrm{GL}(d, \mathbb{F})$ and $\gamma : G \to \mathrm{GL}(d', \mathbb{F})$ be two representations (see Section 2). We say that τ and γ are *epivalent* if there exists a surjective linear transformation $\rho : V \to W$ such that $\rho\tau(g) = \gamma(g)\rho$ for every $g \in G$.

Problem 1. *(*SInducedRepEpivalent*) Given two representations, $\tau : H_1 \to \mathrm{GL}(m_1, \mathbb{Z}_p) = \mathrm{Aut}(\mathbb{Z}_p^{m_1})$ and $\gamma : H_2 \to \mathrm{GL}(m_2, \mathbb{Z}_p) = \mathrm{Aut}(\mathbb{Z}_p^{m_2})$, such that H_i are elementary Abelian q-groups, and p, q are distinct primes, determine whether there exists a surjective homomorphism $\phi : H_1 \to H_2$ such that the induced representation τ and $\gamma \circ \phi$ are epivalent, i. e., there exists a surjective linear map $\rho : \mathbb{Z}_p^{m_1} \to \mathbb{Z}_p^{m_2}$ such that $\rho \circ \tau(h) = \gamma(\phi(h)) \circ \rho$, $\forall h \in H_1$.*

The following theorem shows that SInducedRepEpivalent captures the essential difficulty of epimorphism testing for groups in Coprime(ElemAb, ElemAb).

Theorem 2. *For groups $G_1, G_2 \in$ Coprime(ElemAb, ElemAb), GpEpi is polynomial-time many-one equivalent to* SInducedRepEpivalent*.*

To solve SInducedRepEpivalent in the above setting, we further reduce it to the well-known Code Isomorphism problem (Problem 2). This is similar to the technique used to solve GpI for this class of groups in polynomial time [QST12], but in our case reducing to Code Isomorphism requires additional work, since we start with an epimorphism problem and are reducing to an isomorphism problem (whereas in Qiao–Sarma–Tang [QST12] they were reducing from one isomorphism problem to another).

Theorem 3. *Using the notation of Problem 1, when H_i are elementary Abelian of rank d, and the representations have $m = \max\{m_1, m_2\}$, the problem* SInducedRepEpivalent *reduces to* CodeIso *for d-dimensional codes in $\mathbb{F}^m$.*

The above theorem enables us to derive the following result.

Corollary 1. *There is a polynomial-time algorithm for* GpEpi*, restricted to pairs of groups (G_1, G_2) such that $G_1 \in$ Coprime(ElemAb, ElemAb).*

We then extend this result to obtain an efficient algorithm for testing epimorphism between groups in Coprime($\prod$ ElemAb, ElemAb).

Theorem 4. *There is a polynomial-time algorithm for* GpEpi *restricted to pairs of groups (G_1, G_2) such that $G_1 \in$ Coprime($\prod$ ElemAb, ElemAb).*

Efficient epimorphism testing of groups with limited Abelian composition factors. We next study the GpEpi, for groups with no Abelian composition factors, that is, finite groups whose composition factors are all non-Abelian simple groups. This class includes two important classes of groups, namely the *direct product of non-Abelian simple groups*, and *almost simple groups*. It forms a well-structured subclass of *groups with no nontrivial Abelian normal subgroups* (a.k.a. Fitting-free groups). Groups with no nontrivial Abelian normal subgroups have been widely studied in various algorithmic contexts, including efficient isomorphism testing (see e.g., [CH03, BCGQ11, BCQ12]).

Groups with no Abelian composition factors has also been studied extensively in group theory, particularly in the context of structural classification, enumeration, and understanding their minimal faithful permutation degree (see, e.g., [Klo03, Ber67, Sab23, Cha20, LA22]). While algorithmic problems such as GpI and the Minimum Generating Set problem have been explored for various non-solvable group classes including Fitting-free groups, the computational complexity of GpEpi even for groups with no Abelian composition factors has not been addressed previously. Our main result for this class is the following.

Theorem 5. *There is a polynomial-time algorithm for* GpEpi*, restricted to pairs of groups* (G_1, G_2) *such that* G_1 *has no Abelian composition factors.*

We can extend this slightly in the direction of Fitting-free groups that allow Abelian composition factors of limited "multiplicity;" see Cor. 2 and the definitions preceding it.

Organization. The remainder of the paper is organized as follows. We begin with preliminaries in Section 2. In Section 3, we develop a criterion for epimorphism testing for large groups, reducing the problem to normal Hall subgroups and their complements. In Section 4, we prove Theorem 1. In Section 5, we establish Theorem 2, Theorem 3, and Theorem 4. Finally, in Section 6, we prove Theorem 5. In Section 7, we conclude with several open problems.

2 Preliminaries

In this section, we recall some relevant terminology required for the paper. An interested reader may refer to standard references such as [Rot95, Ser77] for more details.

Group theory. We consider groups with finitely many elements. The *order* of group G is the number of elements in a group G, denoted by $|G|$. The order of an element $g \in G$, denoted as $\mathrm{ord}(g)$, is the smallest positive integer m such that $g^m = 1$. The *exponent* of G is the smallest positive integer m such that $g^m = 1$ for all $g \in G$. Let H be a subgroup of G, if for all $a \in G$, $a^{-1}Ha = H$ then we say that H is a normal subgroup of G (denoted by $H \triangleleft G$). A *normal Hall* subgroup N is a normal subgroup of G with $\gcd(|N|, |G/N|) = 1$. For any subgroup H and any normal subgroup K of G we denote the subgroup $\{hk \,|h \in H, k \in K\} = \{kh \,|h \in H, k \in K\}$ by HK.

Let N be a normal subgroup of G. We say that G is *semidirect product* of N by a subgroup H of G, denoted as $G = N \rtimes H$ if $G = NH$ and $N \cap H = 1$. Since $N \triangleleft G$, this gives rise to a homomorphism $\tau : H \to \mathrm{Aut}(N)$ by $h \to \chi_h$, where $\chi_h : N \to N$ by $n \to h^{-1}nh$. In this case, we write $G = N \rtimes_\tau H$. We say N is a *normal subgroup* of this decomposition and H the *complement* of N in G. Conversely, given two groups N and H and a homomorphism $\tau : H \to \mathrm{Aut}(N)$, we can define a group $G := \{(n, h) \mid n \in N, h \in H\}$ with the product operation, $(n_1, h_1)(n_2, h_2) = (n_1\chi_{h_1}(n_2), h_1h_2)$, for all $(n_1, h_1), (n_2, h_2) \in G$. This gives a construction of

the outer semidirect product $G = N \rtimes_\tau H$. For a normal Hall subgroup N of G, the Schur–Zassenhaus theorem guarentees that a complement subgroup $H \leq G$ such that $\gcd(|H|, |N|) = 1$ and $G = N \rtimes_\tau H$ exists. Furthermore, if H and K are complements of N, then H and K are conjugate (see, e.g., [Rot95]).

Socle series and chief series. A *minimal normal subgroup of* G is a normal subgroup $N \trianglelefteq G$ with no nontrivial subgroups that are also normal in G; equivalently, if $M \trianglelefteq G$ and $M \leq N$, then $M \in \{1, N\}$. A standard exercise is that every minimal normal subgroup of a finite group is a direct power T^n of some finite simple group T. The *socle* of a group G, denoted $\mathrm{Soc}(G)$ is the (characteristic) subgroup generated by all minimal normal subgroups of G. The *socle series* of G is defined by $\mathrm{Soc}^1(G) := \mathrm{Soc}(G)$ and $\mathrm{Soc}^i(G)$ is the unique subgroup of G such that $\mathrm{Soc}^i(G)/\mathrm{Soc}^{i-1}(G) = \mathrm{Soc}(G/\mathrm{Soc}^{i-1}(G))$.

A *normal series* in G is a series $1 = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_k = G$ such that $N_i \trianglelefteq G$ for all i. A *chief series* is a normal series that cannot be further refined (a so-called "maximal" normal series). Equivalently, a chief series is a normal series such that N_i/N_{i-1} is a minimal normal subgroup of G/N_{i-1} for all i. If N_* is a chief series, then the factor groups N_i/N_{i-1} are called *chief factors* of G. Each chief factor is of the form T^n for some simple group T and some integer n, and the multiset of isomorphism types of chief factors is well-defined for G, independent of the chief series (see e.g., [Hal18, Theorem 8.4.4]).

The socle series can be refined to a chief series by taking the minimal normal subgroups $M_1, \ldots, M_k$ of $G/\mathrm{Soc}^i(G)$, taking their pre-images $\hat{M}_1, \ldots, \hat{M}_k$ in G, and then inserting them in between $\mathrm{Soc}^i(G)$ and $\mathrm{Soc}^{i+1}(G)$ in any order, viz. $\mathrm{Soc}^i(G) \trianglelefteq \mathrm{Soc}^i(G)M_1 \trianglelefteq \mathrm{Soc}^i(G)M_1M_2 \trianglelefteq \cdots \trianglelefteq \mathrm{Soc}^i(G)M_1M_2\cdots M_{k-1} \trianglelefteq \mathrm{Soc}^{i+1}(G)$. We say G has *socle length* ℓ if ℓ is the least integer such that $G = \mathrm{Soc}^\ell(G)$.

The Code Isomorphism problem. Let $\mathbb{F}$ be a field. A d-dimensional linear subspace $C \subseteq \mathbb{F}^n$ is called a *linear code* of dimension d. A generating matrix of a linear code C, of dimension d, is a $d \times n$ matrix with row vectors being a basis of C. We will also use C to denote the generating matrix of a linear code C.

Problem 2. *(*Code Isomorphism*) Given two generating matrices $C_{d\times n}$ and $D_{d\times n}$ over the field $\mathbb{F}$, the* Code Isomorphism *Problem asks to determine the existence of $T \in \mathrm{GL}(d, \mathbb{F})$ and a permutation matrix $P_{n\times n}$ such that $T_{d\times d}C_{d\times n}P_{n\times n} = D_{d\times n}$.*

Representation theory. Let V be a vector space of dimension d over $\mathbb{F}$. A *representation* of a group G is a homomorphism $\tau : G \to \mathrm{GL}(d, \mathbb{F})$. A subspace W of V is called *G-invariant* if for all $g \in G$ and $w \in W$, we have $\tau_g(w) \in W$. A representation $\tau : G \to \mathrm{GL}(d, \mathbb{F})$ is called *irreducible* if the only G-invariant subspaces of V are 0 and V.

Let V and W be two finite-dimensional vector spaces over a field $\mathbb{F}$ of dimension d and d', respectively. We say that two representations $\tau : G \to \mathrm{GL}(d, \mathbb{F})$ and $\gamma : G \to \mathrm{GL}(d', \mathbb{F})$ are *equivalent* if there is an invertible linear map $f : V \to W$ such that $f \circ \tau_g = \gamma_g \circ f$ for all $g \in G$.

Let N be an elementary abelian p-group and let $G = N \rtimes_\tau H$ be a group, where $\tau : H \to \mathrm{Aut}(N)$ is an action of H on N. Since N is an elementary abelian p-group, $N \cong \mathbb{Z}_p^d$, and $\mathrm{Aut}(N) = \mathrm{GL}(d, \mathbb{F}_p)$. Then the homomorphism τ can be seen as a representation of H given by $\tau : H \to \mathrm{Aut}(N) = \mathrm{GL}(d, \mathbb{F}_p)$.

Linear algebra and Modules. We say that matrix $A_{d\times n}$ of rank d is in standard form if $A = [I_d|A']$, i.e., the first d columns of A form the identity matrix. We can perform row operations

on A followed by a permutation of the columns to transform A to a standard form, i.e., we can find B and B' such that BAB' is in standard form.

Let R be a ring and M, N be R-modules. A map $\phi : M \to N$ is an *R-module homomorphism* if $\phi(\alpha x + y) = \alpha\phi(x) + \phi(y)$ for all $x, y \in M$ and $\alpha \in R$. A module M is *indecomposable* if $M = M_1 \oplus M_2$ implies $M_1 = 0$ or $M_2 = 0$.

Let G be a group. A (left) G-module is an abelian group A on which G acts by additive maps on the left, i.e., a left G-module consists of an abelian group A together with a left group action $\tau : G \times A \to A$ such that $g \cdot (a_1 + a_2) = g \cdot a_1 + g \cdot a_2$, for all $a_1, a_2 \in A$ and $g \in G$. Similarly, we can define right G-module. Unless explicitly mentioned otherwise the term "G-module" will always mean "left G-module". We refer reader to [Wei94, DF04] for more details on group modules.

3 Condition for epimorphism testing

In this section, prove that epimorphism testing for groups with normal Hall subgroups reduces to that for the normal Hall subgroups and their complements. Our proof is based on the ideas discovered by Taunt [Tau55, Theorem 3.3]. A similar result for isomorphism testing between groups was established using the same ideas (see e.g., [QST12, Theorem 3]).

Theorem 6. *Given $G_1 = N_1 \rtimes_\tau H_1$, $G_2 = N_2 \rtimes_\gamma H_2$, where N_1, N_2 are normal Hall subgroups. Then there is an epimorphism from G_1 to G_2 if and only if there exist an epimorphism $\rho : N_1 \to N_2$, and an epimorphism $\phi : H_1 \to H_2$, such that, $\forall h \in H_1$,*

$$\rho \circ \tau(h) = \gamma(\phi(h)) \circ \rho. \tag{1}$$

Proof. ($\implies$) Let $f : G_1 \to G_2$ be an epimorphism from G_1 to G_2 such that $G_1/\ker f \cong G_2$. Let $L = \ker f \cap N_1$ and $K = \ker f \cap H_1$. It is easy to see that $\ker f = L \rtimes_\tau K$.

We now show that the action of K on N_1/L, given by $(nL)^k = knk^{-1}L$ for $k \in K$, $n \in N_1$, is trivial. Since $f(k) = 1$ we have $f(knk^{-1}) = f(n)$, which implies that $n^{-1}knk^{-1} \in \ker f$. Clearly $n^{-1}knk^{-1} \in N_1$, therefore $n^{-1}knk^{-1} \in L$ and $knk^{-1}L = nL$. Define an action τ' of H_1/K on N_1/L given by $\tau'(hK) := \tau(h)L$. Since K acts on N_1/L trivially, τ' is well-defined. Indeed, if $hK = h'K$, then $h' = hk$ for some $k \in K$. $\tau'(h'K)(nL) = \tau(h')(n)L = \tau(hk)(n)L = (\tau(h)\tau(k))(n)L = \tau(h)(\tau(k)(n)L) = \tau(h)(n)L = \tau'(hK)(nL)$.

Consider a map $\pi : \frac{N_1 \rtimes_\tau H_1}{L \rtimes_\tau K} \to \frac{N_1}{L} \rtimes_{\tau'} \frac{H_1}{K}$ defined by $\pi(n_1, h_1) = (n_1L, h_1K)$. It is easy to see that π is an isomorphism. Moreover, $\frac{N_1}{L} \rtimes_{\tau'} \frac{H_1}{K} \cong N_2 \rtimes_\gamma H_2$, with $|N_1/L| = N_2$ and $|H_1/K| = H_2$. By [Tau55, Theorem 3.3], there exist an isomorphism $\overline{\rho} : N_1/L \to N_2$ and an isomorphism $\overline{\phi} : H_1/K \to H_2$ such that, $\forall hK \in H_1/K$, $\overline{\rho} \circ \tau'(hK) = \gamma(\overline{\phi}(hK)) \circ \overline{\rho}$. By lifting $\overline{\phi}, \overline{\rho}, \tau'$ to ϕ, ρ and τ respectively, via the canonical epimorphism we obtain $\rho \circ \tau(h) = \gamma(\phi(h)) \circ \rho$.

($\impliedby$) Consider a map $f : G_1 \to G_2$ defined by $f(n, h) = (\rho(n), \phi(h))$. It is clear that f is an epimorphism from G_1 to G_2. Now, consider

$$\begin{aligned}
f((n,h)(n',h')) &= f(n\tau_h(n'), hh') \\
&= (\rho(n\tau_h(n')), \phi(hh')) \\
&= (\rho(n)\rho(\tau_h(n'), \phi(h)\phi(h')) \\
&= (\rho(n)\gamma_{\phi(h)}(\rho(n')), \phi(h)\phi(h')) \\
&= (\rho(n), \phi(h))(\rho(n'), \phi(h')) \\
&= f(n,h)f(n',h').
\end{aligned}$$

Hence, f is an epimorphism from G_1 to G_2. □

4 Efficient epimorphism testing of Coprime(Ab, Cyc)

In this section, we design an algorithm for finding an epimorphism between two groups G_1 and G_2 such that $G_1 \in \text{Coprime}(\text{Ab}, \text{Cyc})$. Before we present our algorithm, we prove certain preliminary results which will be required in the algorithm.

Consider two groups $G_1, G_2 \in \text{Coprime}(\text{Ab}, \text{Cyc})$ defined as $G_1 = N_1 \rtimes_\tau H_1$ and $G_2 = N_2 \rtimes_\gamma H_2$, where N_1 and N_2 are Abelian, and H_1 and H_2 are cyclic. Moreover, $\gcd(|H_1|, |N_1|) = 1$ and $\gcd(|H_2|, |N_2|) = 1$. Suppose there exists an epimorphism $\rho : N_1 \to N_2$ that satisfies the condition of Equation (1) for some epimorphism $\phi : H_1 \to H_2$. Let $K = \ker(\phi)$ be the unique subgroup of H_1 whose order is $|H_1|/|H_2|$. Define a subgroup L of N_1 generated by the set $\{v^{\tau(k)} - v \mid v \in N_1, k \in K\}$. It is clear that $L \leq \ker(\rho)$.

The following observation on L is of independent interest, and we realized it in the course of coming up with the proofs below. Although it is ultimately not required for our proofs, as it may be of future use we include its proof in Appendix A.

Observation 1. *With the notations above, L is a direct sum of maximal indecomposable H_1-submodules of N_1.*

Let N be an Abelian group, but not necessary elementary Abelian. A $(\mathbb{Z}/p^k\mathbb{Z})[H]$-module is a $\mathbb{Z}H$-module N where the exponent of N (the LCM of the orders of the elements of N) divides p^k.

Lemma 1. *[Thé81, Corollary 1.2] Let H be a finite group. If p is coprime to $|H|$, then any indecomposable $(\mathbb{Z}/p^k\mathbb{Z})[H]$-module is generated (as an H-module) by a single element.*

Lemma 2. *Let N be an Abelian group (not necessarily elementary Abelian), and H a cyclic group acting on N by automorphisms. Moreover, suppose $\gcd(|N|, |H|) = 1$. Then a decomposition of N into its indecomposable H-submodules can be computed in polynomial time in $|N|, |H|$.*

Proof. For each $v \in N$, we compute the H-submodule $\langle v \rangle_H$ of N. For each such submodule, we then use the algorithm of Ciocănea-Teodorescu [CT15, Theorem 1.1] to test whether $\langle v \rangle_H$ appears as a direct summand in a direct sum decomposition of N as an H-module, and if so, to find a complement, that is, another H-submodule $U \leq N$ such that $N = \langle v \rangle_H \oplus U$. As soon as one such direct sum decomposition is found, the algorithm is then called recursively on $\langle v \rangle_H$ and U to see if they can be further decomposed. Furthermore, if N is decomposable, then there must exist a $v \in N$ such that $\langle v \rangle_H$ is a direct summand, for N must contain an indecomposable direct summand by induction on its size, and for a prime p dividing $|N|$, by Lemma 1, in this setting, indecomposable H-modules are generated by a single element. If no such direct sum decomposition is found, then N is an indecomposable H-module, and the recursion stops. □

In practice, some pre-processing can be done beforehand; for example, at the start, N can be split into a direct sum of its Sylow p-subgroups for different primes p. And within each Sylow p-subgroup, if $\langle v \rangle_H = p\langle u \rangle_H$ for some $u \in N$, then $\langle v \rangle_H$ is not a direct summand of N and can be excluded from the above search.

We are now ready to prove Theorem 1.

Proof of Theorem 1. First we check that G_2 is in $\text{Coprime}(\text{Ab}, \text{Cyc})$ (otherwise reject). In order to test whether there is an epimorphism between G_1 and G_2, we first run the algorithm from [QST12, Theorem 1] on the inputs G_1 and G_2 to obtain all normal Hall subgroups and their complements. We then select an arbitrary normal Hall subgroup N_1 of G_1 (respectively, N_2 of G_2) and its complement H_1 (respectively, H_2) such that $|N_1| \geq |N_2|$, $|H_1| \geq |H_2|$, N_1 and N_2 are Abelian, and H_1 and H_2 are cyclic. All these conditions can be verified in polynomial time for each

normal Hall subgroup and all of its complements. If no such pair of normal Hall subgroup and its complement exists, then by Theorem 6, we conclude that there is no epimorphism from G_1 to G_2. Otherwise, we proceed as follows.

Since every finite cyclic group has a unique subgroup of any given order dividing its order, there exists a unique subgroup $K \lhd H_1$ such that $|H_1/K| = |H_2|$. If no such K exists, then the algorithm will reject. Moreover, K can be computed in polynomial time. Let τ (respectively, γ) be a conjugation action of H_1 on N_1 (respectively, H_2 on N_2). We compute the normal subgroup $L = \langle \{v^{\tau(k)} - v \mid v \in N_1, k \in K\} \rangle \lhd N_1$, and determine its order in polynomial time.

If $|N_1/L| = |N_2|$ then there is an epimorphism from G_1 to G_2 if and only if the groups $N_1/L \rtimes_\tau H_1/K$ and $N_2 \rtimes_\gamma H_2$ are isomorphic[3] (see the proof of Theorem 6). There exists a polynomial-time algorithm to test whether these two groups are isomorphic and, if so, to compute an explicit isomorphism between them by Le Gall [LG09, Theorem 1.2]. If such an isomorphism exists, we can lift it to an epimorphism from G_1 to G_2 by composing the canonical epimorphism, $G_1 \to N_1/L \rtimes_\tau H_1/K$, with the computed isomorphism from $N_1/L \rtimes_\tau H_1/K$ to G_2.

Otherwise, we may assume $|N_1/L| > |N_2|$ (for if $|N_2| > |N_1/L|$ then the algorithm can simply return that there is no epimorphism). Since $L \lhd N_1$ and N_1 is an H_1-module, it follows that L and N_1/L both are an H_1-module. Let $\bigoplus V_i$ and $\bigoplus U_j$ denote the decomposition of N_1/L and N_2 into their indecomposable H_1-submodules and H_2-submodules, respectively. These decompositions can be computed in polynomial time by Lemma 2. Note that the underlying group of each V_i is $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^{d_i}$, for some p_i, and the exponent of V_i divides $p_i^{k_i}$ (see, e.g., [Thé81, GL26]). Moreover, the underlying group of the quotient V_i/p_iV_i is an elementary Abelian group $(\mathbb{Z}/p_i\mathbb{Z})^{d_i}$ [Thé81].

Let $\bar{\phi} : H_1/K \to H_2$ be an isomorphism. All such isomorphisms can be computed in polynomial time, as both H_1/K and H_2 are cyclic groups. Fix such an isomorphism $\bar{\phi}$. For each i, the module V_i inherits an H_2-module structure via $\bar{\phi}$, since K acts trivially on V_i.

We now construct a bipartite graph $\Gamma_{\bar{\phi}}$ as follows. The vertex set of $\Gamma_{\bar{\phi}}$ is the disjoint union of two sets, one containing a vertex labeled i for each V_i, and the other containing a vertex labeled j for each U_j. There is an edge (i, j) between vertices i and j if and only if there exists $l_{ij} \leq k_i$ such that there is an H_2-module isomorphism from $V_i/p_i^{l_{ij}}V_i$ to U_j.

Claim 1. *For some $l_{ij} \leq k_i$ there is an H_2-module isomorphism from $V_i/p_i^{l_{ij}}V_i$ to U_j if and only if there is an H_2-modules isomorphism from V_i/p_iV_i to U_j/p_iU_j, and exponent$(U_j) \leq$ exponent(V_i).*

Proof of Claim 1. Let $\rho_{ij} : V_i/p_i^{l_{ij}}V_i \to U_j$ be an H_2-module isomorphism. Note that $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^{d_i}$ and $(\mathbb{Z}/p_i^{k'_i}\mathbb{Z})^{d_j}$ are the underlying groups of V_i and U_j, respectively. Additionally, we have $(\mathbb{Z}/p_i^{l_{ij}}\mathbb{Z})^{d_i} \cong (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^{d_i}/p_i^{l_{ij}}(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^{d_i} = V_i/p_i^{l_{ij}}V_i \cong U_j = (\mathbb{Z}/p_i^{k'_i}\mathbb{Z})^{d_j}$ implies that $d_i = d_j$ and $k'_i = l_{ij}$. Define $f_{ij} : V_i/p_iV_i \to U_j/p_iU_j$ by $f_{ij}(\mathbf{v} + p_iV_i) = \rho_{ij}(\mathbf{v} \mod p_i^{l_{ij}}V_i) + p_iU_j$, where $\mathbf{v} = (v_1, \ldots, v_{d_i}) \in V_i$ and $V_i/p_iV_i \cong (\mathbb{Z}/p_i\mathbb{Z})^{d_i}$. It is easy to see that f_{ij} is an epimorphism. Moreover, $f_{ij}(\mathbf{v}^h + p_iV_i) = \rho_{ij}(\mathbf{v}^h \mod p_i^{l_{ij}}V_i) + p_iU_j = \rho_{ij}(\mathbf{v} \mod p_i^{l_{ij}}V_i)^h + p_iU_j = f_{ij}(\mathbf{v} + p_iV_i)^h$, where $h \in H_2$. Therefore, by Schur's lemma [Ser77, Proposition 4] we have f_{ij} is an H_2-module isomorphism.

Next, we have for each $v \in V_i/p_i^{l_{ij}}V_i$, there is $v' \in V_i$ such that $\text{ord}(v') = \text{ord}(v)m_v$ for some positive integer m_v. This implies exponent(U_j) = exponent$(V_i/p_i^{l_{ij}}V_i)$ = lcm$(\text{ord}(v) \mid v \in V_i/p_i^{l_{ij}}V_i)$ = lcm$(\text{ord}(v')/m_v \mid v' \in V_i) \leq$ lcm$(\text{ord}(v') \mid v' \in V_i)$ = exponent(V_i).

Conversely, let $f_{ij} : V_i/p_iV_i \to U_j/p_iU_j$ be an H_2-module isomorphism and let exponent$(U_j) \leq$ exponent(V_i). Let $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^{d_i}$ and $(\mathbb{Z}/p_i^{k'_i}\mathbb{Z})^{d_j}$ be the underlying groups of V_i and U_j, respectively.

[3]The quotient H_1/K naturally inherits the action τ since K acts trivially on N_1/L (see, e.g., proof of Theorem 6)

Since f_{ij} is an isomorphism, we have $d_i = d_j$. Take $l_{ij} = k'_i \leq k_i$. By [Thé81, Theorem 1.1], if modules $V_i/p_i^{l_{ij}}V_i$ and U_j are not isomorphic then so the modules $(V_i/p_i^{l_{ij}}V_i)/(p_iV_i/p_i^{l_{ij}}V_i)$ and U_j/p_iU_j. This completes the proof of the claim. □

First, we see that the graph $\Gamma_{\overline{\phi}}$ and the isomorphism ρ_{ij} can be constructed in deterministic polynomial time. By Claim 1, to test whether there is an H_2-module isomorphism from $V_i/p_i^{l_{ij}}V_i$ to U_j it is enough to test whether there is an H_2-modules isomorphism from V_i/p_iV_i to U_j/p_iU_j, and that exponent$(U_j) \leq$ exponent(V_i). Since the Cayley tables of the underlying groups of V_j and U_j can be constructed, we can compute exponent(U_j) and exponent(V_i) in polynomial time.

Both V_i/p_iV_i and U_j/p_iU_j are elementary Abelian p_i-groups. Let $M_{V_i}, M_{U_j} \in \mathrm{GL}(\mathbb{F}_{p_i}, d_i)$ be the matrices induced by an action of H_2 on V_i/p_iV_i and U_j/p_iU_j respectively. Testing whether there is an H_2-modules isomorphism between these modules is equivalent to testing whether M_{V_i} and M_{U_j} are conjugate in $\mathrm{GL}(\mathbb{F}_{p_i}, d_i)$. Since $\mathrm{GL}(\mathbb{F}_p, n)$ is an $\mathbb{F}_p$-algebra, this conjugacy problem can be solved in deterministic polynomial time as described in [CIK97, Theorem 2]. Moreover, this algorithm also compute a matrix T such that $T^{-1}M_{V_i}T = M_{U_j}$, if such a T exists. Then f_{ij} is the corresponding linear map. Moreover, we can compute a module isomorphism ρ_{ij} by [CT15, Corollary 1.2]. Therefore, the graph $\Gamma_{\overline{\phi}}$ and the isomorphism ρ_{ij} can be constructed in deterministic polynomial time.

Next, we compute a maximum matching in $\Gamma_{\overline{\phi}}$, which can be done in polynomial time. If the matching saturates all the vertices corresponding to the U_j's, i.e., if its size equals the number of indecomposable H_2-modules of N_2, then the matching defines the epimorphism from N_1/L to N_2, say $\overline{\rho}$ (otherwise, we conclude that no epimorphism from N_1/L to N_2 exists and hence there is also no epimorphism from G_1 to G_2). Moreover, since we have computed the homomorphism ρ_{ij} corresponding to the matched edges, we can explicitly construct $\overline{\rho}$ in polynomial time. Note that $(\overline{\rho}, \bar{\phi})$ gives an isomorphism from $N_1/L \rtimes_\tau H_1/K$ to G_2 since $\overline{\rho}$ and $\bar{\phi}$ satisfies Equation (1) by construction. Next, we lift this isomorphism to an epimorphism from G_1 to G_2 by composing the canonical epimorphism $G_1 \to N_1/L \rtimes_\tau H_1/K$ with the computed isomorphism. □

5 Efficient epimorphism testing of Coprime($\prod$ ElemAb, ElemAb)

In this section, we solve GpEpi for groups from Coprime($\prod$ ElemAb, ElemAb). We first prove Theorem 2 in Section 5.1. Then we further study SInducedRepEpivalent in Section 5.2 where we prove Theorem 3. We conclude this section by proving Theorem 4.

5.1 Proof of Theorem 2

Proof of Theorem 2. GpEpi *of Groups in* Coprime(ElemAb, ElemAb) *to* SInducedRepEpivalent. By listing all normal Hall subgroups and their complements, we can find a normal Hall subgroup N_1 of G_1 (resp. N_2 of G_2) with complement H_1 (resp. H_2), such that both N_1 and N_2 are elementary Abelian p-groups, both H_1 and H_2 are elementary Abelian q-groups. Thus, in order to test the epimorphism of the G_1 and G_2, we first solve the group epimorphism problem for the normal and complement parts. Since the normal and complement parts of G_1 and G_2 are both elementary abelian, their epimorphism problems can be solved in polynomial time by checking their orders. Given this, the only task left is to test whether there exist epimorphisms $\rho : N_1 \to N_2$ and $\phi : H_1 \to H_2$ satisfying *Equation* (1), which can be reduces to solving SInducedRepEpivalent by considering the representations τ and γ as an instance of the problem SInducedRepEpivalent.

SInducedRepEpivalent *to* GpEpi *of Groups from* Coprime(ElemAb, ElemAb). As discussed in Section 2, a representation $\tau : H \to \mathrm{Aut}(N)$, defines a group $G = N \rtimes_\tau H$. Given two representations, $\tau : H_1 \to \mathrm{Aut}(\mathbb{Z}_p^{m_1})$ and $\gamma : H_2 \to \mathrm{Aut}(\mathbb{Z}_p^{m_2})$, we can construct two groups $G_1 = \mathbb{Z}_p^{m_1} \rtimes_\tau H_1$ and $G_2 = \mathbb{Z}_p^{m_2} \rtimes_\gamma H_2$. Since H_i's are elementary Abelian q-groups, both $G_1, G_2 \in$ Coprime(ElemAb, ElemAb). Then we can call an oracle to test if there is an epimorphism from G_1 to G_2. By Theorem 6, the two representations are epivalent if and only if there is an epimorphism from G_1 to G_2, which gives the reduction. □

5.2 Proof of Theorem 3

Representations of $\mathbb{Z}_q^l$ over $\mathbb{Z}_p$. Before we proceed to prove Theorem 3, we recall some basic facts on representations of $\mathbb{Z}_q^l$ over $\mathbb{Z}_p$, where p and q are two different primes. The reader can refer to [QST12, Section A5] for details.

Let $\Phi_q(x)$ be the q^{th} cyclotomic polynomial. Let $h_1(x) \cdots h_r(x)$ are factors of $\Phi_q(x)$ over $\mathbb{Z}_p$ such that h_i's are monic polynomial of same degree $m = (q-1)/r$, where m is the order of p in the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$. Let $M \in \mathrm{GL}(\mathbb{Z}_p, d)$ be the companion matrix of $h_1(x)$. For each nonzero vector $v \in \mathbb{Z}_q^l$, define $v^\star : \mathbb{Z}_q^l \to \mathbb{Z}_q, v^\star(u) = (v, u)$ (inner product of u and v), and define a representation $f_v : \mathbb{Z}_q^l \to \mathrm{GL}(\mathbb{Z}_p, d), f_v(u) = M^{v^\star(u)}$. Then f_v is an irreducible representation of $\mathbb{Z}_q^l$ over $\mathbb{Z}_p$, and $\{f_v \mid v \in \mathbb{Z}_q^l\}$ is the set of all irreducible representations of $\mathbb{Z}_q^l$ over $\mathbb{Z}_p$.

Let $\tau : \mathbb{Z}_q^l \to \mathrm{GL}(\mathbb{Z}_p, m_1)$ and $\gamma : \mathbb{Z}_q^l \to \mathrm{GL}(\mathbb{Z}_p, m_2)$ be two representations of $\mathbb{Z}_q^l$ and let $m_2 \leq m_1$. By Maschke's theorem (see e.g., [Ser77, Theorem 1], both τ and γ can be written as direct sum of irreducible representations as follows, $\tau \cong f_{v_1}^{k_1} \oplus \cdots \oplus f_{v_t}^{k_t}, v_i \in \mathbb{Z}_q^l$ and $\gamma = f_{u_1}^{r_1} \oplus \cdots \oplus f_{u_{t'}}^{r_{t'}}, u_i \in \mathbb{Z}_q^l$.

Lemma 3. *With the notation above, τ and γ are epivalent if and only if for every irreducible representation f_{u_j} of γ with multiplicity r_j, there is an irreducible representation f_{v_i} of τ equivalent to f_{u_j} with multiplicity at least r_j .*

Proof. Assume that τ and γ are epivalent. Let $T : \mathbb{Z}_p^{m_1} \to \mathbb{Z}_p^{m_2}$ be a surjective linear map. Since both $\mathbb{Z}_p^{m_1}$ and $\mathbb{Z}_p^{m_2}$ are both $\mathbb{Z}_q^l$-modules, T is also a surjective $\mathbb{Z}_q^l$-module homomorphism. By fundamental theorem of module homomorphism, we have $\mathbb{Z}_p^{m_1}/\ker(T) \cong \mathbb{Z}_p^{m_2}$ which implies that $\mathbb{Z}_p^{m_1} \cong \ker(T) \oplus \mathbb{Z}_p^{m_2}$. Thus, each f_{u_j} appear in the decomposition of τ with multiplicity at least r_j for $1 \leq j \leq t'$. Conversely, if all irreducible constituents of γ appear in τ with the appropriate multiplicities, then we can define a surjective $\mathbb{Z}_q^l$-module homomorphism $T : \mathbb{Z}_p^{m_1} \to \mathbb{Z}_p^{m_2}$ by projecting onto the relevant direct summand. □

Let $\tau : \mathbb{Z}_q^{l_1} \to \mathrm{GL}(\mathbb{Z}_p, m_1)$ and $\gamma : \mathbb{Z}_q^{l_2} \to \mathrm{GL}(\mathbb{Z}_p, m_2)$ be two representations. Let f_u be an irreducible representation of $\mathbb{Z}_q^{l_2}$ over $\mathbb{Z}_p$, appears in the decomposition of γ. Let $\phi : \mathbb{Z}_q^{l_1} \to \mathbb{Z}_q^{l_2}$ be a surjective linear transformation. Then the induced representation of f_u by ϕ gives the representation $f_u \circ \phi$. Moreover, $(f_u \circ \phi)(v) = f_{\phi^T(u)}(v)$, for all $v \in \mathbb{Z}_q^{l_1}$ [QST12, Section 5.1].

We decompose $\tau = f_{v_1}^{k_1} \oplus \cdots \oplus f_{v_t}^{k_t}$, for $v_i \in \mathbb{Z}_q^{l_1}, i \in [t]$, and $\gamma = f_{u_1}^{r_1} \oplus \cdots \oplus f_{u_{t'}}^{r_{t'}}$, for $u_i \in \mathbb{Z}_q^{l_2}, i \in [t']$ into their irreducible representations such that $k_1 + \cdots + k_t = m_1$ and $r_1 + \cdots + r_{t'} = m_2$. This decomposition can be computed in polynomial time, as shown in [QST12, Proposition 2]. Consider a set $\mathcal{L}_1 = \{v_1, \ldots, v_1, \ldots, v_t, \ldots, v_t\}$ of vectors in $\mathbb{Z}_q^{l_1}$, where each v_i appears exactly k_i times in the set $\mathcal{L}_1$. Similarly, let $\mathcal{L}_2 = \{u_1, \ldots, u_1, \ldots, u_{t'}, \ldots, u_{t'}\}$ of vectors in $\mathbb{Z}_q^{l_2}$, where each u_j appears exactly r_j times in the set $\mathcal{L}_2$. Using $\mathcal{L}_1$ and $\mathcal{L}_2$, we construct two matrices, $M_1 = (v_1, \ldots, v_1, \ldots, v_t, \ldots, v_t)$ of order $l_1 \times m_1$, and $M_2 = (u_1, \ldots, u_1, \ldots, u'_t, \ldots, u'_{t'})$ of order $l_2 \times m_2$.

To test if there is an epimorphism from G_1 to G_2, where G_1 and G_2 identified as $G_1 = \mathbb{Z}_p^{m_1} \rtimes_\tau \mathbb{Z}_q^{l_1}$ and $G_2 = \mathbb{Z}_p^{m_2} \rtimes_\gamma \mathbb{Z}_q^{l_2}$, by Theorem 2 we can view τ (resp. γ) as representations of $\mathbb{Z}_q^{l_1}$ (resp. of

$\mathbb{Z}_q^{l_2}$) over $\mathbb{Z}_p$ of dimension m_1 (resp. m_2). We solve SInducedRepEpivalent problem for τ and γ.

Proof of Theorem 3. By Lemma 3, τ and $\gamma \circ \phi$ are epivalent if and only if for each $j \in [t']$, there exists $i \in [t]$ such that $f_{\phi^T(u_j)}$ is equivalent to f_{v_i} and $r_j \leq k_i$. This latter condition is equivalent to verifying that $\{\phi^T(u_1), \ldots, \phi^T(u_{r_{t'}})\} \subseteq \{v_1, \ldots, v_t\}$ as each irreducible representation of $\mathbb{Z}_q^{l_1}$ is of the form f_{v_i} for some $v_i \in \mathbb{Z}_q^{l_1}$. To test whether $\{\phi^T(u_1), \ldots, \phi^T(u_{r_{t'}})\} \subseteq \{v_1, \ldots, v_t\}$, it is enough to compute the linear transformation ϕ, a matrix $P_{m_1 \times m_2}$ such that each row and each column of P contains at most one entry equals to 1 (with all other entries being zero), and the equality $M_1 P = \phi^T M_2$ holds. We now prove that finding such ϕ and P can be reduced to an instance of Code Isomorphism.

Without loss of generality, we may assume that $\text{rank}(M_1) = l_1$ (resp. $\text{rank}(M_2) = l_2$). We can perform row operations on M_1 (resp. on M_2) followed by a permutation of the columns to transform M_1 (resp. M_2) to a standard form. Let $A_1 \in \text{GL}(\mathbb{Z}_q, l_1)$ (resp. $A_2 \in \text{GL}(\mathbb{Z}_q, l_2)$) and B_1 a permutation matrix in $\text{GL}(\mathbb{Z}_q, m_1)$ (similarly $B_2 \in \text{GL}(\mathbb{Z}_q, m_2)$) be such that $A_1 M_1 B_1 = [I_{l_1} | M_1']$ (resp. $A_2 M_2 B_2 = [I_{l_2} | M_2']$). Since P is an injection matrix, we can write $P = SQ$, where $S = \begin{bmatrix} I_{m_2} \\ \mathbf{0} \end{bmatrix}$ is of dimension $m_1 \times m_2$ and Q is a permutation matrix of dimension $m_2 \times m_2$.

Note that the number of zero columns of M_2 can be at most the number of zero columns of M_1, as otherwise, there can not exist P and ϕ^T satisfying $M_1 P = \phi^T M_2$ (in which case the algorithm immediately rejects). Therefore, once we get to this point, we can safely delete all the zero columns of M_1 and M_2. Now

$$\begin{aligned} M_1 P &= \phi^T M_2 \\ A_1^{-1}[I_{l_1} \mid M_1'] B_1^{-1} SQ &= \phi^T A_2^{-1}[I_{l_2} \mid M_2'] B_2^{-1} \\ [I_{l_1} \mid M_1'] B_1^{-1} SQ B_2 &= A_1 \phi^T A_2^{-1}[I_{l_2} \mid M_2'] \end{aligned} \tag{2}$$

Note that $\text{rank}([I_{l_1} \mid M_1'] B_1^{-1} S) = \text{rank}(M_1 P) = \text{rank}(\phi^T M_2) = l_2$. Let ψ be the matrix such that $\psi[I_{l_1} \mid M_1'] B_1^{-1} S = \begin{bmatrix} \tilde{M_1} \\ \mathbf{0} \end{bmatrix}$, where $\tilde{M_1}$ is of dimension $(l_2 \times m_2)$ and $\text{rank}(\tilde{M_1}) = l_2$. Let $\tilde{Q} = QB_2$. We have $\psi[I_{l_1} \mid M_1'] B_1^{-1} SQB_2 = \begin{bmatrix} \tilde{M_1}\tilde{Q} \\ \mathbf{0} \end{bmatrix}$. By Equation (2), there exists $\tilde{\phi^T}$ such that $\psi A_1 \phi^T A_2^{-1}[I_{l_2} \mid M_2'] = \begin{bmatrix} \tilde{\phi^T} \\ \mathbf{0} \end{bmatrix} [I_{l_2} \mid M_2']$, where $\tilde{\phi^T}_{(l_2 \times l_2)}$ is of rank l_2. It follows now from Equation (2) that

$$\tilde{M_1}\tilde{Q} = \tilde{\phi^T}[I_{l_2} \mid M_2'] \tag{3}$$

Equation (3) is an instance of the Code Isomorphism problem, completing the proof. □

Corollary 1 then follows from Theorem 2 and Theorem 3. At that point, Babai's algorithm for Code Isomorphism in singly exponential time [BCGQ11] gives a polynomial-time algorithm for SInducedRepEpivalent for elementary Abelian groups, finishing the proof of Corollary 1.

Next, we prove Theorem 4.

Proof of Theorem 4. The idea for Coprime(ElemAb, ElemAb) can be extended to Coprime($\prod$ ElemAb, ElemAb) as follows. First we check that G_2 is in Coprime($\prod$ ElemAb, ElemAb) (otherwise reject). For both G_1 and G_2, we compute all the normal Hall subgroups and their complements in polynomial time by [QST12, Theorem 1].

Additionally, we can identify G_1, G_2 as $G_1 = \prod_{i \in S_1} \mathbb{Z}_{p_i}^{k_i} \rtimes_\tau \mathbb{Z}_q^{l_1}$ and $G_2 = \prod_{i \in S_2} \mathbb{Z}_{p_i}^{k'_i} \rtimes_\gamma \mathbb{Z}_q^{l_2}$ with the associated actions as τ and γ, respectively.

Now we need to test if there exist an epimorphism $\psi : \prod_{i \in S_1} \mathbb{Z}_{p_i}^{k_i} \to \prod_{i \in S_2} \mathbb{Z}_{p_i}^{k'_i}$ and $\phi : \mathbb{Z}_q^{l_1} \to \mathbb{Z}_q^{l_2}$ such that $\psi \circ \tau(h_1) = \gamma(\phi(h_1)) \circ \psi, \forall h_1 \in \mathbb{Z}_q^{l_1}$. Let $\tau_i : \mathbb{Z}_q^{l_1} \to \mathrm{GL}(\mathbb{Z}_{p_i}, k_i)$ be the projection of τ into the i-th component for $i \in S_1$, and let $\gamma_i : \mathbb{Z}_q^{l_2} \to \mathrm{GL}(\mathbb{Z}_{p_i}, k'_i)$ be the projection of γ into the i-th component for $i \in S_2$. For each τ_i and γ_i, let M_i and $M_{i'}$ be the matrices arising from the irreducible representation τ_i and γ_i, respectively (see proof of Theorem 3). Define $M_1 := \mathrm{diag}(M_i)_{i \in S_1}, M_2 = \mathrm{diag}(M_{i'})_{i' \in S_2}$, i.e., M_1 (resp. M_2) is a block diagonal matrix with diagonal blocks M_i (resp. $M_{i'}$). Then it suffices to solve $M_1 P = \phi M_2$ as in Theorem 3. □

6 Efficient epimorphism testing in groups with limited Abelian composition factors

In this section, we prove Theorem 5. We first prove the following lemma.

Lemma 4. *Suppose H is a quotient of G, and let ℓ be the socle length of G. Then there exist integers $k_1, \ldots, k_\ell$ and groups M_{ij} for $i = 1, \ldots, \ell$ and $j = 1, \ldots, k_i$ for all i such that*

1. *M_{ij} is a minimal normal subgroup of $G/\operatorname{Soc}^{i-1}(G)$*
2. *There is a minimal normal subgroup $\widehat{M}_{ij}$ of $G_i := G/\langle \widehat{M}_{i'j'} : i' < i \text{ and } j' \in [k_{i'}] \rangle$ such that the natural quotient map $G_i \to G/\operatorname{Soc}^{i-1}(G)$ maps $\widehat{M}_{ij}$ isomorphically onto M_{ij}.*
3. *$H \cong G_{\ell+1}$.*

Proof. Let $K \trianglelefteq G$ be such that $G/K \cong H$. Let $M_{11}, \ldots, M_{1,k_1}$ be the minimal normal subgroups of G that are contained in K. Then we can define $\widehat{M}_{1j} = M_{1j}$ to satisfy the first two parts of the lemma. Define $K_1 = \langle M_{1j} | j \in [k_1] \rangle$.

Now let $i > 1$, and suppose inductively that $M_{i'j'}$, $\widehat{M}_{i'j'}$ have been defined for all $i' < i$ and all $j' \in [k_{i'}]$ that satisfy (1) and (2) and such that $M_{i',1}, \ldots, M_{i',k_{i'}}$ are all the minimal normal subgroups of $G/\operatorname{Soc}^{i'-1}(G)$ that are contained in $K/\operatorname{Soc}^{i'-1}(G)$. Define $K_{i-1} = \langle M_{i'j'} | i' < i; j' \in [k_{i'}] \rangle$, and let $\widehat{M}_{i1}, \ldots, \widehat{M}_{i,k_i}$ be the minimal normal subgroups of G/K_{i-1} that are contained in K/K_{i-1}. First, we claim that they are mapped isomorphically onto their images by the natural quotient map $G/K_{i-1} \to G/\operatorname{Soc}^{i-1}(G)$; call these images M_{ij}. For if some $\widehat{M}_{ij}$ is not mapped isomorphically onto its image by this map, then it must be contained in the kernel of the map, hence in $\operatorname{Soc}^{i-1}(G)$. But since $\widehat{M}_{ij}$ was contained in K/K_{i-1}, if it were also in $\operatorname{Soc}^{i-1}(G)$, then by construction $\widehat{M}_{ij}$ would have been contained in K_{i-1} (since the latter is equal to $K_i \cap \operatorname{Soc}^{i-1}(G)$), contradicting the fact that it was a minimal normal subgroup of G/K_{i-1}. Let M_{ij} be the image of $\widehat{M}_{ij}$ in $G/\operatorname{Soc}^{i-1}(G)$. Then M_{ij} is indeed a minimal normal subgroup of $G/\operatorname{Soc}^{i-1}(G)$.

The above induction continues until $K/K_i = 1$, at which point $K = K_i$. Since each time we progress up the socle series, this happens at some $i \leq \ell + 1$, and thus we satisfy part (3) of the lemma. □

Proof of Theorem 5. First, we check that G_2 has no Abelian composition factors (otherwise reject). Computing the composition factors in $\mathrm{poly}(|G_2|)$ time is easy (indeed, computing the composition factors of permutation groups can even be done in NC [BLS87]).

Next, we compute a chief series of G_1 that refines the socle series, which is again easy by standard techniques.

For all subsets of the chief factors in our computed chief series—note that the chief series has length at most $\log|G_1|$, hence that are at most $2^{\log|G_1|} \leq |G_1|$ many such subsets—we attempt to make those the kernel of an epimorphism $G_1 \to G_2$. Say the subset we pick has M_{ij} for $j = 1, \ldots, k_i$ that are among the minimal normal subgroups of $G_1/\operatorname{Soc}^{i-1}(G_1)$.

First, we check that the order is correct: if $|G_1|/\prod_{i,j}|M_{ij}| \neq |G_2|$, then skip this choice of subset of the chief factors.

Next, we check that this subset of chief factors is a valid kernel, in the sense of Lemma 4. That is, we check inductively that there are subgroups $\widehat{M}_{ij}$ corresponding to the chosen M_{ij} that satisfy parts (1) and (2) of Lemma 4. If so, then we finally we compute the quotient $G_1/\prod_{i,j}\widehat{M}_{ij}$, and test isomorphism between that group and G_2. The latter can be done in polynomial time since G_2 is Fitting-free [BCQ12]. □

We can make some progress towards extending Theorem 5 to Fitting-free groups, and in doing so, we highlight one of the remaining obstacles. The issue is that when $\operatorname{Soc}(G)$ contains Abelian minimal normal subgroups $T_1, \ldots, T_k$ such that the subgroup they generate is their direct product, and such that all T_i are pairwise isomorphic as G-modules, then $T_1T_2\cdots T_k \cong T_1 \times \cdots \times T_k$ contains $p^{\Theta(k^2)}$ many Abelian normal subgroups N (normal in G) that are isomorphic to $T_1^{k/2}$ as G-modules. (In the "extreme" case that the T_i are central, they are each 1-dimensional, trivial G-modules $\mathbb{Z}_p$, and the previous discussion is the same as saying that a k-dimensional vector space has a number of $k/2$-dimensional subspaces that is $p^{\Theta(k^2)}$.) Of course we have $k \leq \log_p|G|$, but if $k = \Theta(\log|G|)$, then $p^{\Theta(k^2)} = |G|^{O(\log|G|)}$, so there are too many choices to brute force over them all in polynomial time. And then this issue can arise at any layer of the socle series.

Towards this direction, we make the following definition. Given an Abelian minimal normal subgroup $T \trianglelefteq G$, we define its *multiplicity* in G as the largest k such that there exist $T_1 \times \cdots \times T_k \trianglelefteq G$ where all T_i are minimal normal subgroups of G such that they are all isomorphic to T as G-modules.

Definition 1. The *Abelian width* of a group G is the maximum k such that there is an $i \geq 0$ and an Abelian minimal normal subgroup $T \trianglelefteq G/\operatorname{Soc}^i(G)$ of multiplicity k.

We note that the Abelian width is always at most $O(\log|G|)$, and there are even Fitting-free groups that achieve this width, for example: $G = S_5^k$ has socle A_5^k, with quotient $\mathbb{Z}_2^k$, so its Abelian width is $k = \log_{120}|G|$.

However, we also note that the Abelian width can be quite a bit smaller than the dimension of any chief factor, as in the following example. For sufficiently large p, prime cyclic group C_p has p distinct irreducible representations over $\mathbb{F}_{3^{p-1}}$ (an extension of $\mathbb{F}_3$ that has p-th roots of unity), that are 1-dimensional over $\mathbb{F}_{3^{p-1}}$ (hence dimension $p-1$ over $\mathbb{F}_3$). If we let N be the direct sum of those irreps, then the group $G = N \rtimes C_p$ has order $3^{p(p-1)}p$, the socle is N which has dimension $\Theta(p^2)$ over $\mathbb{F}_3$, each irrep has dimension $p-1 = \Theta(\sqrt{\log|G|})$ over $\mathbb{F}_3$, but the Abelian width is only 1 since N is a direct sum of pairwise non-isomorphic, irreducible C_p-modules (hence, the same is true when viewed as G-modules).

The following is a corollary to the proof of Theorem 5 above.

Corollary 2. *There is a polynomial-time algorithm for* GpEpi*, restricted to pairs of groups (G_1, G_2) such that G_2 is Fitting-free and G_1 has Abelian width at most $O(\sqrt{\log|G_1|})$.*

Proof sketch. The idea is essentially the same as above, except we handle Abelian subgroups in each socle layer a little differently than the chief factors as in the proof of Theorem 5. If $\operatorname{Soc}(G/\operatorname{Soc}^{i-1}(G))$ contains an Abelian $G/\operatorname{Soc}^{i-1}(G)$-module T of multiplicity k, then instead of breaking T^k up into its chief factors (isomorphic copies of T), we brute force over all possible copies of T^j contained within T^k, for $j = 0, 1, \ldots, k$, of which there are at most $kp^{\Theta(k^2)} \leq |G|^{O(1)}$ by our

assumption that the Abelian width is $O(\sqrt{\log |G_1|})$. The rest of the algorithm and proof are then the same as that of Theorem 5. □

7 Conclusion and open problems

Of course the main question we leave open is whether GpEpi is in P (a positive answer would imply GpI is in P). Other basic questions about its complexity are:

Open Question 1. *Is* GpEpi *in* coAM*?*

Open Question 2. *What is the complexity of the counting problem* #GpEpi*?*

As stepping stones towards understanding the complexity of GpEpi in general, other classes of groups for which GpI is in P form natural targets for putting GpEpi into P:

Open Question 3. *Is* GpEpi *in* P *when the input groups are:*

1. *Fitting-free (cf. [BCQ12, BCGQ11])?*
2. *When the target group has size $O(1)$? Or is $O(1)$-generated?*
3. *Quotients of genus 1 (cf. [LW12])? Both are of genus 2 (cf. [BMW17])?*
4. *Groups with Abelian Sylow towers (cf. [BQ12b]) or tame towers (cf. [GQ15])?*
5. *Groups with central, elementary Abelian radicals such that $G/Rad(G)$ is a direct product of non-Abelian simple groups (cf. [GQ17b, Thm. C])?*

We comment on the Fitting-free question. If the target group H is Fitting-free, then there is an epimorphism $G \to H$ iff there is an epimorphism $G/Rad(G) \to H$ (since if any part of the radical is not in the kernel, then it would yield an Abelian normal subgroup in the image), so we immediately reduce to the case that both groups are Fitting-free. If G, H are Fitting-free, deciding whether H is a quotient of G by a subgroup of $\mathrm{Soc}(G)$ doesn't seem particularly hard; the difficulty arises when the socle of H may come from chief factors that are at many different layers of the socle series of G.

Acknowledgments

We thank the ICALP reviewers for their helpful comments on the submission. DT also thanks Armin Weiss for bringing the Group Epimorphism problem to her attention. Joshua A. Grochow was supported by NSF CAREER Award CCF-2047756. Dhara Thakkar was supported by JSPS KAKENHI Grant Numbers 24H00071 and 25K24674.

References

[BCGQ11] László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 1395–1408. SIAM, Philadelphia, PA, 2011.

[BCQ12] László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups. In *Automata, Languages, and Programming: 39th International Colloquium, ICALP 2012, Warwick, UK*, pages 51–62, 2012.

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

[BEO02] Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien. A millennium project: constructing small groups. *Internat. J. Algebra Comput.*, 12(5):623–644, 2002. doi:10.1142/S0218196702001115.

[Ber67] R. Bercov. On groups without Abelian composition factors. *J. Algebra*, 5:106–109, 1967. doi:10.1016/0021-8693(67)90029-4.

[BLS87] László Babai, Eugene Luks, and Ákos Seress. Permutation groups in NC. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 409–420, 1987.

[BMW17] Peter A. Brooksbank, Joshua Maglione, and James B. Wilson. A fast isomorphism test for groups whose Lie algebra has genus 2. *J. Algebra*, 473:545–590, 2017. doi:10.1016/j.jalgebra.2016.12.007.

[BQ12a] László Babai and Youming Qiao. Polynomial-time isomorphism test for groups with abelian Sylow towers. In *29th International Symposium on Theoretical Aspects of Computer Science*, volume 14 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 453–464. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2012.

[BQ12b] László Babai and Youming Qiao. Polynomial-time isomorphism test for groups with abelian sylow towers. In Christoph Dürr and Thomas Wilke, editors, *29th International Symposium on Theoretical Aspects of Computer Science, STACS 2012, Paris, France, February 29 - March 3, 2012*, volume 14 of *LIPIcs*, pages 453–464. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2012. URL: https://doi.org/10.4230/LIPIcs.STACS.2012.453, doi:10.4230/LIPICS.STACS.2012.453.

[CH03] John J. Cannon and Derek F. Holt. Automorphism group computation and isomorphism testing in finite groups. *J. Symbolic Comput.*, 35(3):241–267, 2003.

[Cha20] Robert Chamberlain. Subgroups with no abelian composition factors are not distinguished. *Bull. Aust. Math. Soc.*, 101(3):446–452, 2020. doi:10.1017/s0004972719001011.

[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 (Kihei, HI)*, pages 68–74. ACM, New York, 1997. doi:10.1145/258726.258751.

[CT15] Iuliana Ciocănea-Teodorescu. The module isomorphism problem for finite rings and related results. arXiv:1512.08365 [math.RA], 2015. Abstract appeared at ACM Communications in Computer Algebra, Vol. 49 Iss. 1.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[EHH17] Bettina Eick, Max Horn, and Alexander Hulpke. Constructing groups of 'small' order: recent results and open problems. In *Algorithmic and experimental methods in algebra, geometry, and number theory*, pages 199–211. Cham: Springer, 2017. doi:10.1007/978-3-319-70566-8_8.

[ELGO02] Bettina Eick, C. R. Leedham-Green, and E. A. O'Brien. Constructing automorphism groups of p-groups. *Comm. Algebra*, 30(5):2271–2295, 2002.

[ESW25] Murray Elder, Jerry Shen, and Armin Weiss. On the complexity of epimorphism testing with virtually abelian targets. *arXiv preprint arXiv:2501.05283*, 2025.

[FL21] Stefan Friedl and Clara Löh. Epimorphism testing with virtually Abelian targets. *Confluentes Math.*, 13(1):61–78, 2021.

[GFM+14] Steven Gay, François Fages, Thierry Martinez, Sylvain Soliman, and Christine Solnon. On the subgraph epimorphism problem. *Discrete Appl. Math.*, 162:214–228, 2014.

[GL26] Joshua A. Grochow and Michael Levet. On the parallel complexity of group isomorphism via Weisfeiler–Leman. *J. Comput. System Sci.*, 156, 2026.

[GQ15] Joshua A. Grochow and Youming Qiao. Polynomial-time isomorphism test of groups that are tame extensions. In *26th International Symposium on Algorithms and Computation (ISAAC) (Springer Lecture Notes in Computer Science 9472)*, pages 578–589, 2015. Full version available as arXiv:1507.01917 [cs.DS]. doi:10.1007/978-3-662-48971-0_49.

[GQ17a] Joshua A. Grochow and Youming Qiao. Algorithms for group isomorphism via group extensions and cohomology. *SIAM J. Comput.*, 46(4):1153–1216, 2017. doi:10.1137/15M1009767.

[GQ17b] Joshua A. Grochow and Youming Qiao. Algorithms for group isomorphism via group extensions and cohomology. *SIAM J. Comput.*, 46(4):1153–1216, 2017. Preliminary version in IEEE Conference on Computational Complexity (CCC) 2014 (DOI:10.1109/CCC.2014.19). Also available as arXiv:1309.1776 [cs.DS] and ECCC Technical Report TR13-123. doi:10.1137/15M1009767.

[GQ23] Joshua A. Grochow and Youming Qiao. On the complexity of isomorphism problems for tensors, groups, and polynomials I: Tensor isomorphism-completeness. *SIAM J. Comput.*, 52(2):568–617, 2023.

[GQ24] Joshua A. Grochow and Youming Qiao. On p-group isomorphism: search-to-decision, counting-to-decision, and nilpotency class reductions via tensors. *ACM Trans. Comput. Theory*, 16(1):Art. 2, 39, 2024.

[Hal18] Marshall Hall. *The theory of groups*. Courier Dover Publications, 2018.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[Hul22] Alexander Hulpke. The perfect groups of order up to two million. *Math. Comput.*, 91(334):1007–1017, 2022. Also arXiv:2104.10828. doi:10.1090/mcom/3684.

[IMQ+25] Gábor Ivanyos, Euan J. Mendoza, Youming Qiao, Xiaorui Sun, and Chuanqi Zhang. Faster isomorphism testing of p-groups of Frattini class 2. *SIAM Journal on Computing*, pages FOCS24–115, 2025.

[Klo03] Benjamin Klopsch. Enumerating finite groups without abelian composition factors. *Israel J. Math.*, 137:265–284, 2003. doi:10.1007/BF02785965.

[KS18] Greg Kuperberg and Eric Samperton. Computational complexity and 3-manifolds and zombies. *Geom. Topol.*, 22(6):3623–3670, 2018. doi:10.2140/gt.2018.22.3623.

[LA22] Giancarlo Lucchini Arteche. On homogeneous spaces with finite anti-solvable stabilizers. *C. R. Math. Acad. Sci. Paris*, 360:777–780, 2022. doi:10.5802/crmath.339.

[LG09] François Le Gall. Efficient isomorphism testing for a class of group extensions. In *STACS 2009: 26th International Symposium on Theoretical Aspects of Computer Science*, volume 3 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages 625–636. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2009.

[Lin70] C. E. Linderholm. A group epimorphism is surjective. *Am. Math. Mon.*, 77:176–177, 1970. doi:10.2307/2317336.

[LW12] Mark L. Lewis and James B. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups Complex. Cryptol.*, 4(1):73–110, 2012. doi:10.1515/gcc-2012-0008.

[QST12] Youming Qiao, Jayalal Sarma, and Bang-Sheng Tang. On isomorphism testing of groups with normal Hall subgroups. *Journal of Computer Science and Technology*, 27(4):687–701, 2012.

[Rem79] V. N. Remeslennikov. An algorithmic problem for nilpotent groups and rings. *Sibirsk. Mat. Zh.*, 20(5):1077–1081, 1167, 1979.

[Ros13] David J Rosenbaum. Bidirectional collision detection and faster deterministic isomorphism testing. *arXiv preprint arXiv:1304.3935*, 2013.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, fourth edition, 1995. doi:10.1007/978-1-4612-4176-8.

[Sab23] Luca Sabatini. The growth of abelian sections. *Ann. Mat. Pura Appl. (4)*, 202(3):1197–1216, 2023. doi:10.1007/s10231-022-01276-w.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*, volume Vol. 42 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, french edition, 1977.

[Sun23] Xiaorui Sun. Faster isomorphism for p-groups of class 2 and exponent p. In *STOC'23—Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 433–440. ACM, New York, [2023] ©2023. doi:10.1145/3564246.3585250.

[Tau55] D. R. Taunt. Remarks on the isomorphism problem in theories of construction of finite groups. *Proc. Cambridge Philos. Soc.*, 51:16–24, 1955. doi:10.1017/s030500410002987x.

[Thé81] Jacques Thévenaz. Representations of finite groups in characteristic p^r. *Journal of Algebra*, 72(2):478–500, 1981.

[uh] user2661923 (https://math.stackexchange.com/users/464411/user2661923). If 2^a is the highest power of 2 which divides $n!$, show that a lies between $n-1$ and $n-\lfloor \log_2(n+1)\rfloor$. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/4349429 (version: 2022-01-05). URL: https://math.stackexchange.com/q/4349429, arXiv: https://math.stackexchange.com/q/4349429.

[Vik97] Narayan Vikas. *Computational complexity of graph compaction*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–Simon Fraser University (Canada). URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:NQ24360.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.

A Deferred proofs

Below we give a proof of Observation 1. We recall the notation: N_1 is an Abelian group that is coprime to the cyclic group H_1, and $\tau\colon H_1 \to \mathrm{Aut}(N_1)$ is an action. $K \trianglelefteq H_1$, and $L = \{v^{\tau(k)} - v : v \in N_1, k \in K\}$. The observation to prove is that L is a direct sum of maximal indecomposable H_1-submodules of N_1.

Proof of Observation 1. Let $N_1 = \bigoplus_i V_i$ be a decomposition of N_1 into its indecomposable H_1-submodules, V_i. Let p_i be the prime such that V_i is a p_i-group. Define $V_i' := \{v^{\tau(k)} - v : v \in V_i, k \in K\}$. Then we immediately have $L = \bigoplus_i V_i'$. Then it is necessary and sufficient to show that $V_i^{'} = V_i$ whenever $V_i^{'} \neq 0$.

From [Thé81, Corollary 1.2] it follows that, since V_i is indecomposable and $|H_1|$ is coprime to $|N_1|$, the only submodules of V_i are of the form $p_i^l V_i$ for some $l \geq 0$.

Let p_i^b be the exponent of V_i: $p_i^b V_i = 0$ and $p_i^{b-1} V_i \neq 0$. Suppose that $V_i^{'} = p_i^l V_i$ for some $b > l \geq 1$ (in particular, we are assuming $V_i' \neq 0$, as that is the only case we need to handle). Then K acts trivially on $V_i \mod p_i^l$. For $k \in K$, we have $\tau(k) = \iota + p_i^l M_k$, where ι is an identity map and $M_k \in \mathrm{End}(V_i)$. We now prove that $\tau(k)^{p_i^{b-l}} = \iota$. We have $\tau(k)^{p_i^{b-l}} = (\iota + p_i^l M_k)^{p_i^{b-l}} = \sum_{j=0}^{p_i^{b-l}} \binom{p_i^{b-l}}{j} (p_i^l M_k)^j$. To show that $\tau(k)^{p_i^{b-l}} = \iota$, it is enough to show that p_i^b divides $\binom{p_i^{b-l}}{j}(p_i^l M_k)^j$ for all j. If $j \leq p_i$ then $p_i^b | \binom{p_i^{b-l}}{j}$. And if $j \geq b/l$ then $p_i^b | (p_i^l M_k)^j$. So now consider $p_i \leq j < b/l$. The power of p_i dividing $j!$ is $\leq \lfloor j/p_i \rfloor + \lfloor j/p_i^2 \rfloor + \lfloor j/p_i^3 \rfloor + \cdots \leq \frac{j}{p_i - 1}$. Thus, $p_i^{b-l-\frac{j}{p_i-1}} | \binom{p_i^{b-l}}{j}$.

Now suppose $p_i \neq 2$ or $l \neq 1$. Then, we have $l(p_i - 1) \geq \frac{j}{j-1}$, and therefore

$$\begin{aligned} b - l - \frac{j}{p_i - 1} + jl &= b + l(j-1) - \frac{j}{p_i - 1} \\ &\geq b. \end{aligned}$$

It follows that, $p_i^b | \binom{p_i^{b-l}}{j}(p_i^l M_k)^j$.

Finally, let us now consider the case when $p_i = 2$ and $l = 1$. It is standard that if $2^x | j!$, then $x \leq j - 1$ [uh]. Therefore, $2^b = 2^{(b-1)-(j-1)+j} | \binom{2^{b-1}}{j} (2M_k)^j$. Thus proves that $\tau(k)^{p_i^{b-l}} = \iota$. This implies that $\mathrm{ord}(\tau(k)) | p_i^{b-l}$. However, since $\tau : H_1 \to \mathrm{Aut}(N_1)$ is a homomorphism, $\mathrm{ord}(\tau(k)) | \mathrm{ord}(k)$, and $\mathrm{ord}(k) || H_1|$. Since $\gcd(|N_1|, |H_1|) = 1$, we get $\mathrm{ord}(\tau(k)) = 1$, hence $\tau(k) = \iota$. This implies that $V_i^{'} = 0$, which is a contradiction. Therefore, $V_i^{'} = V_i$. This completes the proof of Observation 1. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il