Polynomial-time Isomorphism Test for Groups with Abelian Sylow Towers

László Babai[1] and Youming Qiao[2]

1 **Department of Computer Science, the University of Chicago**
laci@cs.uchicago.edu
2 **Institute for Interdisciplinary Information Sciences, Tsinghua University**
jimmyqiao86@gmail.com

Abstract

We consider the problem of testing isomorphism of groups of order n given by Cayley tables. The trivial $n^{\log n}$ bound on the time complexity for the general case has not been improved over the past four decades. Recently, Babai et al. (following Babai et al. in SODA 2011) presented a polynomial-time algorithm for groups without abelian normal subgroups, which suggests solvable groups as the hard case for group isomorphism problem. Extending recent work by Le Gall (STACS 2009) and Qiao et al. (STACS 2011), in this paper we design a polynomial-time algorithm to test isomorphism for the largest class of solvable groups yet, namely *groups with abelian Sylow towers*, defined as follows. A group G is said to possess a Sylow tower, if there exists a normal series where each quotient is isomorphic to a Sylow subgroup of G. A group has an abelian Sylow tower if it has a Sylow tower and all its Sylow subgroups are abelian. In fact, we are able to compute the coset of isomorphisms of groups formed as coprime extensions of an abelian group, by a group whose automorphism group is known. The mathematical tools required include representation theory, Wedderburn's theorem on semisimple algebras, and M. E. Harris's 1980 work on p'-automorphisms of abelian p-groups. We use tools from the theory of permutation group algorithms, and develop an algorithm for a parameterized version of the graph-isomorphism-hard setwise stabilizer problem, which may be of independent interest.

1998 ACM Subject Classification I.1.2 Algorithms

Keywords and phrases polynomial-time algorithm, group isomorphism, solvable group

Digital Object Identifier 10.4230/LIPIcs.STACS.2012.453

1 Introduction

We consider the Group Isomorphism problem when groups are given by their Cayley tables. We design a polynomial-time algorithm to test isomorphism for the largest class of solvable groups yet, namely *groups with abelian Sylow towers*, defined as follows. A group G is said to possess a Sylow tower, if there exists a normal series where each quotient is isomorphic to a Sylow subgroup of G. A group has an abelian Sylow tower if it has a Sylow tower and all its Sylow subgroups are abelian. If two groups G and G^* are isomorphic, the set of isomorphisms is a coset of $\mathrm{Aut}(G)$ in $\mathrm{Sym}(G \cup G^*)$, thus can be represented by a set of generators of $\mathrm{Aut}(G)$ and an isomorphism between G and G^*.

▶ **Theorem 1.1.** *There is a polynomial-time algorithm that decides isomorphisms between two groups with abelian Sylow towers, when the groups are given by Cayley tables. If the groups are isomorphic, the algorithm computes the coset of their isomorphisms.*

Let us sketch the current state of the Group Isomorphism problem. For the general case, a straightforward $n^{\log n + O(1)}$ algorithm has been known for about four decades (cf. [25]) and

29th Symposium on Theoretical Aspects of Computer Science (STACS'12).
Editors: Christoph Dürr, Thomas Wilke; pp. 453–464
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

has not been improved. While isomorphism of abelian groups can be tested in linear time according to Kavitha [21] (improving Savage's $O(n^2)$ [29] and Vikas's $O(n \log n)$ [33]), the next natural target to consider, p-groups of class 2, turns out to be currently intractable; nothing significantly better than the trivial $n^{\log n}$ bound is known. We note that p-groups are solvable. Partly for this reason, Babai et al. consider semisimple groups, i.e, groups without abelian normal subgroups (in certain sense the opposite of solvable groups), and present a polynomial-time algorithm for this class in [6] (building on [5]). This work thus amplifies the significance of the solvable case; every group has a solvable normal subgroup such that the quotient is semisimple.

Recently, some progress has been made for some classes of solvable groups, notably for those with at least one abelian normal Hall subgroup.

To explain, let us recall some definitions. For a group G, let N be a normal subgroup, and H a subgroup of G. We say that G is a *semidirect product* of N and H, denoted as $G = N \rtimes H$, if $NH = G$ and $N \cap H = \{\mathrm{id}\}$. H is called a *complement* of N in G. A subgroup is a *Hall subgroup* if its order is coprime to its index. The Schur-Zassenhaus theorem states that a normal Hall subgroup always has a complement. In [26], Qiao, Sarma and Tang present efficient algorithms for groups with an abelian normal Hall subgroup, assuming the complement is either a group with a bounded number of generators, or an elementary abelian group. [26] builds on a technique by Le Gall [13] which allows the normal Hall subgroup to go from elementary abelian to abelian, and an algorithmic result by Babai [4] to test equivalence of linear codes.

In [26], linear representation theory of finite groups was brought to bear on the Group Isomorphism problem, and the reason that the case when the complement is elementary abelian can be solved is mainly because the representations of elementary abelian groups is well-known and can be combined with the algorithmic result on code equivalence. Even the case when the complement is abelian, was not known. The main contribution of this paper is to combine ideas from permutation group algorithms with several mathematical results to compute in polynomial time the automorphism group of the semidirect product $G = A \rtimes H$, where A is an abelian normal Hall subgroup, assuming $\mathrm{Aut}(H)$ is known. The following result is an inductive tool used to prove Theorem 1.1. It can also be interpreted that we are able to test isomorphism of groups formed as coprime extensions of an abelian group, by a group whose automorphism group is known.

▶ **Theorem 1.2.** *Let A be an abelian group, and H a group of order coprime to $|A|$. Suppose two groups G and G^* both can be decomposed as $A \rtimes H$. Then there is a polynomial-time algorithm that computes the coset of isomorphisms between G and G^*, when the groups are given by Cayley tables, and $\mathrm{Aut}(H)$ is given by a list of generators.*

Successive applications of Theorem 1.2 along the Sylow tower gives our main result (Section 3.1).

We briefly indicate the techniques involved. The main object of study is the action of the automorphism group of H on the set of all linear representations of H up to equivalence of representations. Basic facts of representation theory allow us to interpret this action as a parameterized version of the *string G-isomorphism problem* (G a permutation group acting on the set of indices), the starting point of Luks' polynomial-time algorithm to test isomorphism of graphs with bounded degree [22]. Thus we introduce the following parameterized version of the setwise stabilizer problem: given $P \leq \mathrm{Sym}(\Omega)$ and $\Delta \subseteq \Omega$, compute $P_{\{\Delta\}} = \{\pi \in P \mid \Delta^\pi = \Delta\}$ in time $2^{|\Delta|} \cdot \mathrm{poly}(|\Omega|)$. We solve this problem by adapting Luks's dynamic programming technique for hypergraph isomorphism [24]. Finally, we need to generalize an argument by Le Gall [13] which reduces the case of abelian normal Hall

subgroups to elementary abelian. The generalization allows the complement to be an arbitrary group, rather than just a cyclic group. Of particular relevance is the work by M. E. Harris on p'-automorphisms of abelian p-groups ([15], [16]). We also need an old result by A. Ranum [27] on matrix representations of the automorphisms of abelian groups, and Wedderburn's classical theory of semisimple algebras (cf. Chapter 5 in [1]).

It has long been believed that p-groups or equivalently, nilpotent groups (as they are direct product of p-groups) represent the hard cases for Group Isomorphism problem. Our results do not change this perception since all nilpotent groups with abelian Sylow subgroups are abelian.

1.1 Related work and the organization of the paper

We mention some group theory literature related to groups with abelian Sylow towers. A Sylow tower of a group has been used in Chapter 7.6 in Gorenstein's Finite Groups [14]. A group is called an A-group if all its Sylow subgroups are abelian. An A-group is not necessarily solvable, e.g. A_5, while a group with an abelian Sylow tower is solvable. Properties of A-groups have been studied, cf. e.g. [31], [20], and Chapter 12 in [9]. In particular, in [9], the number of non-isomorphic solvable A-groups of order $\leq n$ is proved to be $n^{O(\log n)}$. On the other hand, in [26], the number of non-isomorphic groups with abelian Sylow towers of order $\leq n$ is shown to be $n^{\Omega(\log n)}$. Both Sylow towers and A-groups are discussed at length in Huppert's classical monograph [19].

The construction of finite groups of a given order has been studied by group theorists. To achieve this goal, criteria of isomorphism have been developed. The content of Section 4.2 is adapted from Taunt's work on constructing A-groups [32]. In [8], Besche, Eick and O'Brien surveyed the construction of finite groups of order at most 2000. In particular, in [8, Section 3.3], coprime split extensions are considered, and a practical algorithm, due to Eick, for listing all groups formed by coprime split extensions is presented. Work along these lines often reflects brilliant insights and can be a potential guidance to polynomial-time algorithms (as Taunt's work in our case), but they do not (at least not directly) address the time complexity of isomorphism testing, since their concern is to list all groups of certain order up to isomorphism in practice.

Several recent papers are related to or motivated by the group isomorphism problem. The works on groups without abelian normal subgroups ([5] and [6]), and groups with abelian normal Hall subgroups ([13] and [26]) have been mentioned in the introduction. p-groups of class 2 are generally believed to be the barrier for group isomorphism problem, and in this regard, recent work by Wilson [34, 35] on the structure of p-groups is noteworthy. From the complexity-theoretic perspective, we note that in [11], Chattopadhyay, Torán, and Wagner show that graph isomorphism has no AC^0-reduction to group isomorphism.

Given a permutation group $P \leq \mathrm{Sym}(\Omega)$ and a subset $\Delta \subseteq \Omega$ of the permutation domain, the setwise stabilizer problem asks to compute $P_{\{\Delta\}} = \{\pi \in P \mid \Delta^\pi = \Delta\}$. Our algorithm runs in $2^{|\Delta|} \cdot \mathrm{poly}(|\Omega|)$. It is inspired by Luks's simply-exponential time algorithm for hypergraph isomorphism [24]. Generalizing the special case of the graph isomorphism problem introduced by Babai in 1979 [3] to hypergraphs, Arvind et al. [2] consider the vertex-colored hypergraph isomorphism problem, where isomorphisms are required to preserve the colors and the color-classes have bounded size. They give a polynomial-time algorithm for this case. As a tool, they consider another parameterized version of the setwise stabilizer problem; the parameter is the size t of some P-stable set containing Δ. They presented an algorithm with the same running time as ours, with t in the place of $|\Delta|$. Our parameter "subsumes" theirs (as in our case Δ is not required to be contained in some small P-stable set), and the algorithms are different.

The rest of the paper is organized as follows. We present the preliminaries in Section 2. In Section 3, we explain the reduction of Theorem 1.1 to Theorem 1.2, and give an outline of the proof of Theorem 1.2. In particular, in Section 3.2, we first reduce the original problem of isomorphism computation (Problem 1) to Problems 2 and 3. This reduction is detailed in Section 4. In Section 5, we present solutions to Problems 2 and 3 for the special case when the normal group is elementary abelian; in this section, we establish new connections to permutation group algorithms. Finally in Section 6 we indicate how general case of Problems 2 and 3 reduces to elementary abelian case.

2 Preliminaries

2.1 General group theory

Groups are finite in this paper. Here we present a brief account of the concepts used, and introduce notation. For a group G, if $T \subseteq G$ generates G we write $G = \langle T \rangle$. We write $H \leq G$ for H being a subgroup of G. An *inner automorphism* of a group G is the *conjugation* by an element $g \in G$, i. e., the map $\iota_g : x \mapsto x^g : g^{-1}xg$ $(x \in G)$. A subgroup $N \leq G$ is normal if it is invariant under all inner automorphisms of G, and N is a characteristic subgroup of G if it is invariant under all automorphisms of G. A subgroup is a *Hall subgroup* if its order and its index are coprime. Given a group G and $N \lhd G$, G is the group extension of N by G/N. If N is a normal Hall subgroup, then G is the coprime extension of N by G/N. Given a semidirect product decomposition $G = N \rtimes H$, the conjugation action of H on N gives a homomorphism $\alpha : H \to \mathrm{Aut}(N)$. We denote this situation by $G = N \rtimes_\alpha H$. In the language of extension theory of groups, G is called the split extension of N by H. The well-known Schur-Zassenhaus theorem asserts that a normal Hall subgroup always has a complement. That is, all coprime extensions split. In [26] it is observed that its proof (e.g. Section 9 in [1]) is constructive, giving an efficient algorithm to compute a specific complement.

▶ **Theorem 2.1** (Algorithmic Schur-Zassenhaus theorem, cf. [26]). *Let G be a finite group. Given a normal Hall subgroup $N \lhd G$, there exists $H \leq G$ such that $G = N \rtimes H$, and such an H can be computed in polynomial time. If H and H^* are two complements of N, then H and H^* are conjugates.*

A (right) coset of H in G containing $g \in G$ is $Hg = \{hg \mid h \in H\}$. Given two groups G and G^*, the set of their isomorphisms is denoted by $\mathrm{Iso}(G, G^*)$. Given a group G and $\phi \in \mathrm{Aut}(G)$, we write the action of ϕ in the exponent, that is for $g \in G$, g^ϕ is the image of g under ϕ.

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. For $A \subseteq \Omega$, $A^\pi = \{a^\pi \mid a \in A\}$. Given a permutation group $P \leq \mathrm{Sym}(\Omega)$ and $x, y \in \Omega$, denote $P_{x \to y} = \{\pi \in P \mid x^\pi = y\}$. For a pair of subsets A, $B \subseteq \Omega$ of the same size, denote $P_{A \to B} = \{\pi \in P \mid A^\pi = B\}$. Let $\mathbb{F}$ be a field. Given a vector space V over $\mathbb{F}$, the general linear group $\mathrm{GL}(V)$ consists of all non-singular linear transformations of 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 $p_i^{k_i}$, s.t. $p_1 \leq p_2 \leq \cdots \leq p_n$, 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. An elementary abelian group is $\mathbb{Z}_p^n$, where p is a prime. Its automorphism group is isomorphic to $\mathrm{GL}(n,p)$. The set of generators of $\mathrm{GL}(n,p)$ described in Theorem 4.12 from [1] suffices for our use, and a suitable generalization can give a set of generators for $\mathrm{Aut}(A_p)$ where A_p is an abelian p-group.

2.2 Linear representations of finite groups

A (linear) representation of a finite group G over a field $\mathbb{F}$ is a homomorphism $G \to \mathrm{GL}(V)$ where V is a vector space over $\mathbb{F}$. In this paper, a representation of a group is over the field $\mathbb{F}_p$ of prime order p which is coprime to the order of the group. Given representations $\alpha, \beta : G \to \mathrm{GL}(n,p)$, $\hom(\alpha,\beta) := \{\phi \in M(\mathbb{F}_p, n) \mid \alpha(g)\phi = \phi\beta(g), \forall g \in G\}$, and $\mathrm{Iso}(\alpha,\beta) = \{\phi \in \hom(\alpha,\beta), \phi \text{ non-singular}\}$. If $\psi, \psi' \in \hom(\alpha,\beta)$, then $\psi + \psi' \in \hom(\alpha,\beta)$. This shows that $\hom(\alpha,\beta)$ is an algebra. α and β are *equivalent*, denoted as $\alpha \sim \beta$, if $\mathrm{Iso}(\alpha,\beta)$ is not empty. An invariant subspace U of $\alpha : G \to \mathrm{GL}(V)$ is a subspace of V such that $\forall g \in G$, $\alpha(g)(U) = U$. The restriction of α to U, $\alpha|_U$ is called a sub-representation of α. $\vec{0}$ and V are called trivial invariant subspaces. A representation without non-trivial invariant subspaces is an *irreducible representation*.

Schur's lemma states that for two irreducible representations α and β, if they are not equivalent, then $\hom(\alpha,\beta) = \{0\}$. If they are equivalent, then $\hom(\alpha,\beta)$ is a skew field. In the equivalence case, if α, β are over $\mathbb{F}_p$, Wedderburn's "little" theorem ensures $\hom(\alpha,\beta)$ to be a field, and thus $\mathrm{Iso}(\alpha,\beta) = \hom(\alpha,\beta)^\times$. Given a representation $\phi : G \to \mathrm{GL}(V)$, if $V = U \oplus W$, where U and W are invariant subspaces, then ϕ is called the direct sum of $\phi|_U$ and $\phi|_W$. A representation is completely reducible, if it is a direct sum of irreducible sub-representations. Maschke's theorem states that any representation $\phi : G \to \mathrm{GL}(n,\mathbb{F})$ where $\mathrm{char}(\mathbb{F}) \nmid |G|$ is completely reducible.

Let $\mathrm{Rep}(G,\mathbb{F})$ denote the set of linear representations of G over $\mathbb{F}$ *up to equivalence*, and $\mathrm{Irr}(G,\mathbb{F})$ to denote the set of all irreducible representations of G over $\mathbb{F}$ *up to equivalence*. An action of $\mathrm{Aut}(G)$ on $\mathrm{Rep}(G,\mathbb{F})$ can be defined. For $\phi \in \mathrm{Aut}(G)$ and $\alpha \in \mathrm{Rep}(G,\mathbb{F})$, $\alpha^\phi(g) = \alpha(g^{\phi^{-1}})$, $\forall g \in G$. The set $\mathrm{Irr}(G,\mathbb{F})$ is a stable set under this action.

Next, we list some facts about equivalence of representations. For a representation $\alpha : G \to \mathrm{GL}(n,\mathbb{F})$, viewing $\alpha(g)$ as a matrix and taking the trace, we get the *character of* α, denoted as $\chi_\alpha : G \to \mathbb{F}$. Two representations over a field of characteristic that does not divide $|G|$ are equivalent if and only if their characters are the same. Given a completely reducible representation ϕ and an irreducible representation τ of a group G, the multiplicity of τ in ϕ is the number of occurrences of τ (up to equivalence) in the direct sum decomposition of ϕ. Comparing the multiplicities of irreducibles provides another criterion for equivalence of completely reducible representations.

2.3 Representing groups in algorithms

At different stages of the algorithm, we will be concerned with abstract groups, permutation groups, and linear groups, so we summarize their representations here. Abstract groups are given by their Cayley tables. Operations in subgroups and quotient groups are easy by referring to the tables. If a group is of some particular type (e.g., cyclic or elementary abelian), we may use their natural representations implicitly (e.g. $\mathbb{Z}_m$, $\mathbb{Z}_p^n$). For a linear group in $\mathrm{GL}(n,p)$, we assume all matrices in this group are given explicitly. A permutation group $P \leq \mathrm{Sym}(\Omega)$ is represented by a list of generators. A coset Pr in $\mathrm{Sym}(\Omega)$ is represented by a set of generators T of P and a coset representative r', denoted as $\langle T \rangle r'$. For an abstract

group G, $\mathrm{Aut}(G)$ can be viewed as a subgroup of $\mathrm{Sym}(G)$, and $\mathrm{Iso}(G, G^*)$ as a coset of $\mathrm{Aut}(G)$ in $\mathrm{Sym}(G \cup G^*)$.

We will be concerned with representing a coset of a direct product of groups. Given groups G and H, for a coset $L = Kr$ in $G \times H$, we denote by $K_G \subseteq G$ and $K_H \subseteq H$ the projections of K on the first and second coordinates, resp. For $h \in K_H$, let $K_G(h) = \{g \in G \mid (g, h) \in K\}$. It is a coset of $K_G(\mathrm{id}_H)$. We can then represent Kr as follows.

▶ Claim 1. Given $\langle T \rangle = K_H$, $\langle S \rangle = K_G$, and for every $h \in T$ some $r_h \in K_G(h)$, $\langle T \cup S \cup \{r_h \mid h \in T\}\rangle r = Kr$.

2.4 Algorithms for permutation groups and linear representations

Algorithms for permutation groups given by a list of generators have been studied and analyzed, cf., e.g. [23] and [30]. By Sims's "sifting" procedure, from any set of generators of $P \leq \mathrm{Sym}([n])$, a set of generators of size $O(n)$ can be computed. The next proposition follows from Sims's method.

▶ Proposition 1 (Point-transporter algorithm, cf. [23], Proposition 3.9). Given $\langle S \rangle = P \leq \mathrm{Sym}(\Omega)$, $|\Omega| = n$, $x, y \in \Omega$, $P_{x \to y}$ can be computed in $\mathrm{poly}(n, |S|)$.

We describe some algorithmic tasks about linear representations and their solutions. As in our setting, linear representations are given by listing all matrices, the solutions to these tasks will mostly follow from the definitions. We remark that the tasks for representations over finite fields such as the decomposition into irreducible components, and comparing if two irreducible representations are equivalent can be done much more efficiently, even when only generators are given (cf. [28] and [18, Chapter 7]). To compute a basis of $\hom(\alpha, \beta)$ (as an algebra) can be viewed as computing the kernel of a system of linear equations by writing out the linear equations by definition of $\hom(\alpha, \beta)$.

▶ Proposition 2. Given $\alpha, \beta \in \mathrm{Rep}(G, \mathbb{F}_p)$, a basis of $\hom(\alpha, \beta)$ can be computed in time $\mathrm{poly}(|G|, n)$.

▶ Proposition 3. (cf. [26, Section 2]) Given a representation $\phi : G \to \mathrm{GL}(V)$, its irreducible components can be listed in time $O(\dim(V)^2 \cdot |V| \cdot |G|)$.

We can use characters to tell the type of an irreducible representation. It follows from Proposition 3 that we can compute the multiplicities of irreducible representations.

3 About the main theorems

3.1 Reduction of Theorem 1.1 to Theorem 1.2

We explain the reduction of Theorem 1.1 to Theorem 1.2. Let G and G^* be the groups whose isomorphisms we wish to compute. Given a group G, it is not hard to show that if G possesses an abelian Sylow tower, then the Sylow tower can be computed in polynomial time. Two Sylow towers of G and H are *compatible*, if the ith factors, counting from bottom of the tower, are of the same order. Thus we first decide if G and G^* have compatible abelian Sylow towers. If they do not, it is decided that they are not isomorphic. For two compatible towers $\{\mathrm{id}\} = G_0 \lhd G_1 \lhd \cdots \lhd G_\ell = G$ and $\{\mathrm{id}\} = G_0^* \lhd G_1^* \lhd \cdots \lhd G_\ell^* = G^*$, as the base case, $G/G_{\ell-1}$ and $G^*/G^*_{\ell-1}$ are both abelian so their isomorphisms can be computed (e.g. use [10] to compute the primary decomposition, and then a set of generators of the automorphism group of an abelian p-group can be described). Given $\mathrm{Iso}(G/G_i, G^*/G_i^*)$, to compute $\mathrm{Iso}(G/G_{i-1}, G^*/G^*_{i-1})$ we can apply Theorem 1.2, as G_i/G_{i-1} is a normal Sylow

p-subgroup of G/G_{i-1} for some prime p. (Note that every two factors in the Sylow tower are of coprime orders.)

3.2 Outline of the proof of Theorem 1.2

Recall that Theorem 1.2 requires to solve the following problem. It is legitimate to consider just abelian p-groups as if the normal Hall subgroup is abelian, we can form an abelian Sylow tower of the normal Hall subgroup and apply the idea of iterating along the Sylow tower as in Section 3.1.

▶ Problem 1 (Isomorphism computing). Given a group H and $\mathrm{Aut}(H)$, let p be a prime not dividing $|H|$, and A_p an abelian p-group. Given homomorphisms $\alpha : H \to \mathrm{Aut}(A_p)$ and $\beta : H \to \mathrm{Aut}(A_p)$, compute $\mathrm{Iso}(A_p \rtimes_\alpha H, A_p \rtimes_\beta H)$, in time $\mathrm{poly}(|A_p|, |H|)$.

We introduce some further definitions. We call a homomorphism from H to $\mathrm{Aut}(D)$ a *(generalized) representation* of H on D. Usually the group D is from some specified group class. For example, when D is an elementary abelian group $\mathbb{F}_p^n$, then $\mathrm{Aut}(D) \cong \mathrm{GL}(n, p)$ and we are dealing with the representation theory over $\mathbb{F}_p$. In our more general setting, the groups D will be abelian p-groups ($p \nmid |H|$). In analogy with linear representations, two (generalized) representations $\alpha : H \to \mathrm{Aut}(D)$ and $\beta : H \to \mathrm{Aut}(D)$, α and β are called *equivalent*, if there exists $\psi \in \mathrm{Aut}(D)$, such that for every $h \in H$, $\alpha(h)^\psi = \beta(h)$. We denote this by $\alpha \sim_\psi \beta$, and $\alpha \sim \beta$ if ψ is clear from context. We also denote the set of the representations of H over D, *up to equivalence* by $\mathrm{Rep}(H, D)$. Then an action of $\mathrm{Aut}(H)$ on $\mathrm{Rep}(H, D)$ can be defined as follows: for $\phi \in \mathrm{Aut}(H)$ and $\alpha \in \mathrm{Rep}(H, D)$, $\alpha^\phi(h) = \alpha(h^{\phi^{-1}})$. For an action of a group H on the domain Ω, and two points $x, y \in \Omega$, we denote $H_{x \to y} = \{h \in H \mid x^h = y\}$. Given these definitions, in Section 4, Problem 1 breaks up to the following two problems.

▶ Problem 2 (Representation-transporting automorphisms). Given a group H and $\mathrm{Aut}(H)$, let p be a prime not dividing $|H|$, and A_p an abelian p-group. Given homomorphisms $\alpha, \beta : H \to \mathrm{Aut}(A_p)$, compute $\mathrm{Aut}(H, \alpha, \beta) := \mathrm{Aut}(H)_{\alpha \to \beta} = \{\phi \in \mathrm{Aut}(H) \mid \alpha^\phi \sim \beta\}$, in time $\mathrm{poly}(|A_p|, |H|)$.

▶ Problem 3 (Intertwining automorphisms). Given a group H and $\mathrm{Aut}(H)$, let p be a prime not dividing $|H|$, and A_p an abelian p-group. Given homomorphisms $\alpha, \beta : H \to \mathrm{Aut}(A_p)$, such that $\alpha \sim \beta$, compute $\mathrm{Aut}(A_p, \alpha \sim \beta) := \{\psi \in \mathrm{Aut}(A_p) \mid \alpha \sim_\psi \beta\}$, in time $\mathrm{poly}(|A_p|, |H|)$.

The cases when A_p is elementary abelian are of great importance. We will solve the elementary abelian case in Section 5, and reduce the abelian case to the elementary abelian case in Section 6.

4 Breaking Problem 1 to Problem 2 and Problem 3

Recall that Problem 1 requires computing the coset of isomorphisms between $A_p \rtimes_\alpha H$ and $A_p \rtimes_\beta H$, where $p \nmid |H|$. Problem 2 requires computing $\mathrm{Aut}(H, \alpha, \beta) = \{\phi \in \mathrm{Aut}(H) \mid \alpha^\phi \sim \beta\}$, and Problem 3 requires computing $\mathrm{Aut}(A_p, \alpha \sim \beta) = \{\psi \in \mathrm{Aut}(A_p) \mid \alpha \sim_\psi \beta\}$. In this section we consider the more general situation when the normal subgroup is a Hall subgroup, not necessarily abelian.

4.1 Reducing to isomorphisms preserving a decomposition

Given a group $G = N \rtimes_\alpha H$, N a normal Hall subgroup, denote automorphisms in $\mathrm{Aut}(G)$ that send H to H by $\mathrm{Aut}^*(G)$. We will show that the structure of $\mathrm{Aut}(G)$ is essentially

determined by $\mathrm{Aut}^*(G)$. First note that a normal Hall subgroup is characteristic. Then by Schur-Zassenhaus theorem, any $\phi \in \mathrm{Aut}(G)$ sends N to N and H to a conjugate of H. For $g \in G$, writing $g = nh$ where $n \in N$ and $h \in H$, it is clear that $H^g = H^{n'}$, for $n' = n^h$. Thus all conjugates of H are $\{H^n \mid n \in N\}$. For $n \in N$, let $\mathrm{Aut}(G, n) = \{\phi \in \mathrm{Aut}(G) \mid \phi(H) = H^n\}$, then we have $\mathrm{Aut}(G) = \cup_{n \in N} \mathrm{Aut}(G, n)$.

▶ Claim 2. $\phi \in \mathrm{Aut}^*(G)$ if and only if $\phi \circ \iota_n \in \mathrm{Aut}(G, n)$.

As for Problem 1, Claim 2 then tells us that it is enough to focus on the isomorphisms that send H to H, as others can be recovered by composing with an inner automorphism.

4.2 The structure of isomorphisms preserving a decomposition

The content of this subsection is adapted from [32] by Taunt (cf. Theorem 3.3 in [32]). In the following, suppose we are given $G = N \rtimes_\alpha H$ and $G^* = N \rtimes_\beta H$, N is normal Hall in G and G^*. The set of isomorphisms between G and G^* preserving the decomposition, denoted by $\mathrm{Iso}^*(G, G^*)$, is $\{\phi \in \mathrm{Iso}(G, G^*) \mid \phi(N) = N, \phi(H) = H\}$. We will develop the characterization of isomorphisms in $\mathrm{Iso}^*(G, G^*)$ by examining their restrictions to the normal subgroups and to the complements.

▶ **Definition 4.1.** (ν, η) for $\nu \in \mathrm{Aut}(N)$, $\eta \in \mathrm{Aut}(H)$ is a *compatible pair* w.r.t. α and β, if for all $h \in H$, $\alpha(h) = \nu^{-1} \circ \beta(\eta(h)) \circ \nu$.

Let the set of all compatible pairs w.r.t. G and G^* be $\mathrm{Com}(G, G^*) \subseteq \mathrm{Aut}(N) \times \mathrm{Aut}(H)$. We write $\mathrm{Com}(G)$ for $\mathrm{Com}(G, G)$. It can be verified that $\mathrm{Com}(G) \leq \mathrm{Aut}(N) \times \mathrm{Aut}(H)$, and $\mathrm{Com}(G, G^*)$ is a coset of $\mathrm{Com}(G)$. We then show that $\mathrm{Com}(G, G^*)$ captures $\mathrm{Iso}^*(G, G^*)$.

▶ **Theorem 4.2.** *For $G = N \rtimes_\alpha H$, $G^* = N \rtimes_\beta H$, there is a bijection between* $\mathrm{Iso}^*(G, G^*)$ *and* $\mathrm{Com}(G, G^*)$. *In particular,* $\mathrm{Aut}^*(G) \cong \mathrm{Com}(G)$.

4.3 Reducing Problem 1 to Problem 2 and Problem 3

We now can see how Problem 1 breaks into Problem 2 and Problem 3. Suppose we are given $G = N \rtimes_\alpha H$ and $G^* = N \rtimes_\beta H$. By discussion in Section 4.1 we know it is enough to consider isomorphisms sending H to H, that is $\mathrm{Iso}^*(G, G^*)$. Then by Theorem 4.2 we need to compute $\mathrm{Com}(G, G^*)$, which is a coset in $\mathrm{Aut}(N) \times \mathrm{Aut}(H)$. We first consider the projection of $\mathrm{Com}(G, G^*)$ on $\mathrm{Aut}(H)$. Then $\eta \in \mathrm{Aut}(H)$ is in the projection if and only if there exists $\nu \in \mathrm{Aut}(N)$ such that (ν, η) is a compatible pair, which by Definition 4.1 just induces equivalence of representations α^η, $\beta \in \mathrm{Rep}(H, N)$. Thus we get Problem 2. Suppose we are given $\langle T \rangle = \mathrm{Aut}(H, \alpha, \beta)$, to compute a set of generators for $\mathrm{Com}(G, G^*)$ Claim 1 shows that we need to compute for every $\eta \in T$ a set of generators for $\{\nu \in \mathrm{Aut}(N) \mid (\nu, \eta)$ is a compatible pair$\}$, which is essentially Problem 3.

5 When the normal subgroup is elementary abelian

5.1 Solving Problem 2 when the normal subgroup is elementary abelian

5.1.1 Parameterized setwise stabilizer problem

We first introduce the algorithmic tool that will be used. Given a permutation group $P \leq \mathrm{Sym}(\Omega)$ and $\Delta \subseteq \Omega$, Setwise stabilizer problem asks to compute $P_{\{\Delta\}} := P_{\Delta \to \Delta}$. It is one of Luks's equivalence class above Graph Isomorphism [23], and in [7], it is shown to be in NP$\cap$coAM, thus not expected to be NP-complete unless the polynomial hierarchy collapses.

Inspired by Luks's dynamic programming procedure for hypergraph isomorphism [24], our algorithms takes into account the size of the set Δ. In fact we will solve the parameterized set-transporter problem.

▶ Proposition 4 (Parameterized set-transporter problem). For $P \leq \mathrm{Sym}(\Omega)$, $A, B \subseteq \Omega$, $|\Omega| = n$ and $|A| = |B| = k$, there is an algorithm in time $2^k \cdot \mathrm{poly}(n)$ that computes $P_{A\to B}$.

Proof. Put an order to elements in A as $\{x_1, \ldots, x_k\}$, and let $A_i = \{x_1, \ldots, x_i\}$, for $i \in [k]$. We will build a dynamic programming table indexed by (A_i, C) for $C \subseteq B$ of size i to store $P_{A_i\to C}$. To start, for every $b \in B$, $P_{x_1\to b}$ can be computed by the point-transporter algorithm in Proposition 1. Now assume that for every $C' \subseteq B$ of the same size $\ell - 1$, we have computed $P_{A_{\ell-1}\to C'}$. For A_ℓ, $C \subseteq B$ of size ℓ, we can compute $P_{A_\ell\to C}$ by the equation $P_{A_\ell\to C} = \bigcup_{b\in C}(P_{A_{\ell-1}\to C\setminus\{b\}})_{x_\ell\to b}$, where $P_{A_{\ell-1}\to C\setminus\{b\}}$ can be read from the table, and $(P_{A_{\ell-1}\to C\setminus\{b\}})_{x_\ell\to b}$ can be computed by Proposition 1. After taking union over $b \in C$, apply Sims's method to get a small set of generators. To analyze the running time, the number of table entries is bounded by 2^k. For each entry we apply point transporter algorithm and sifting procedure for at most k times, which runs in time $\mathrm{poly}(n)$. ◀

Another classical problem in permutation group algorithms is the string P-isomorphism problem, where P is a permutation group acting on the indices of the strings. This problem is the starting point of Luks's polynomial time algorithm to test isomorphism of graphs of bounded degree [22]. For a permutation group $P \leq \mathrm{Sym}(\Omega)$ and a function $f : \Omega \to [\ell]$, the action of $\pi \in P$ on f, denoted as f^π, is defined by $f^\pi(x) = f(x^{\pi^{-1}})$. $[\ell]$ can be considered as a set of colors to be assigned to points in the permutation domain. Now given two functions $f_1, f_2 : \Omega \to [\ell]$, the problem asks to compute the coset $\mathrm{Iso}_P(f_1, f_2) := \{\pi \in P \mid f_1^\pi = f_2\}$. We consider the parameterized version of this problem, where the sum of sizes of *all but one* colors is bounded.

▶ **Corollary 5.1** (Parameterized string P-isomorphism problem). *For a permutation group $P \leq \mathrm{Sym}(\Omega)$, $|\Omega| = n$, and two functions $f_1, f_2 : \Omega \to [\ell]$, such that for $j \in [2]$, $\sum_{i\in[\ell-1]} |f_j^{-1}(i)| \leq k$. Then $\mathrm{Iso}_P(f_1, f_2)$ can be computed in time $2^k \cdot \mathrm{poly}(n)$.*

5.1.2 Reducing Problem 2 to parameterized string P-isomorphism problem

Recall that Problem 2, when the normal subgroup is elementary abelian, requires to compute for two linear representations $\alpha, \beta : H \to \mathrm{GL}(n, p)$, $\mathrm{Aut}(H, \alpha, \beta) = \{\phi \in H \mid \alpha^\phi \sim \beta\}$. Let Ω be the set of all irreducible representations of H. α induces $\alpha' : \Omega \to \{0, 1, \ldots, n\}$ by assigning an irreducible representation $\omega \in \Omega$ to its multiplicity in α. As the total number of irreducibles in α is bounded by the dimension of the representation, $\sum_{i\in[n]} |\alpha'^{-1}(i)| \leq |\Omega| \leq n$. Similarly we have $\beta' : \Omega \to \{0, 1, \ldots, n\}$.

▶ **Lemma 5.2.** $\mathrm{Aut}(H, \alpha, \beta) = \mathrm{Iso}_{\mathrm{Aut}(H)}(\alpha', \beta')$.

Lemma 5.2 shows the reduction from Problem 2 in elementary abelian case to string P-isomorphism problem to be executed. It can be achieved in time polynomial in $\mathrm{poly}(p^n, |H|)$ in conjunction with the algorithms for linear representations presented in Section 2.4. We leave the details to the full version.

▶ **Theorem 5.3.** *For a group H, suppose $\mathrm{Aut}(H)$ is given by generators, and representations $\alpha, \beta : H \to \mathrm{GL}(n, p)$ are given by listing the matrices. Then $\mathrm{Aut}(H, \alpha, \beta) = \{\phi \in \mathrm{Aut}(H) \mid \alpha^\phi \sim \beta\}$ can be computed in time $2^n \cdot \mathrm{poly}(|H|)$.*

5.2 Solving Problem 3 when the normal subgroup is elementary abelian

In Problem 3, when the normal subgroup is elementary abelian, we are given $\alpha, \beta : H \to \mathrm{GL}(n,p)$ such that $\alpha \sim \beta$, and we need to compute those $\psi \in \mathrm{GL}(n,p)$ inducing equivalence between α and β, that is $\mathrm{Iso}(\alpha,\beta)$. We will use $\mathrm{End}(\alpha)$ and $\mathrm{Aut}(\alpha)$ to denote $\hom(\alpha,\alpha)$ and $\mathrm{Iso}(\alpha,\alpha)$. If α and β are irreducible representations over $\mathbb{F}_p$, as discussed in Section 2.2, Schur's lemma states that the $\hom(\alpha,\beta)$ is an extension field of $\mathbb{F}_p$, and $\mathrm{Iso}(\alpha,\beta)$ is the multiplicative group of $\hom(\alpha,\beta)$. Suppose then $\hom(\alpha,\beta)$ is isomorphic to $\mathbb{F}_q$, where $q = p^m$. Since $\mathbb{F}_p^n$ is a $\mathbb{F}_q$-module, $m \mid n$. By Proposition 2, $\hom(\alpha,\beta)$ can be computed and listed in time $\mathrm{poly}(|H|, p^n)$.[1] Given α and β, we first use Proposition 3 to get irreducible components. Then group them by isomorphic types, using the character to distinguish them. As α and β are equivalent, we can assume that α and β are decomposed, and irreducible components grouped as $\mathrm{P} = \mathrm{P}_1 \oplus \mathrm{P}_2 \oplus \cdots \oplus \mathrm{P}_r$, where P_i is the direct sum of k_i copies of ρ_i, and ρ_i is irreducible. By the discussion above, we can list $\mathrm{Aut}(\rho_i) = \mathbb{F}_{q_i}^{\times}$, $q_i = p^{m_i}$. Then we need to use Wedderburn's theory on the structure of semisimple algebras.[2]

▶ **Lemma 5.4** (Lemma 12 and Lemma 13 in [1]). *$\mathrm{End}(\mathrm{P}) \cong \mathrm{End}(\mathrm{P}_1) \oplus \cdots \oplus \mathrm{End}(\mathrm{P}_r)$, and $\mathrm{End}(\mathrm{P}_i) \cong M_{k_i}(\mathbb{F}_{q_i})$, where: $q_i = p^{m_i}$ for some m_i; k_i is the number of copies of ρ_i in P_i.*

Given this lemma, note that automorphisms of P are the invertible elements in $\mathrm{End}(\mathrm{P})$.

▶ Proposition 5. $\mathrm{Aut}(\mathrm{P}) \cong \mathrm{Aut}(\mathrm{P}_1) \oplus \cdots \oplus \mathrm{Aut}(\mathrm{P}_r)$, and $\mathrm{Aut}(\mathrm{P}_i) \cong \mathrm{GL}(n_i, q_i)$, where $q_i = p^{m_i}$ for some m_i, and k_i is the number of copies of ρ_i in P_i.

Finally we recall that a set of generators of $\mathrm{GL}(n_i, q_i)$ can be described easily. We also need to store the change-of-basis matrix when we decompose representations.

6 When the normal subgroup is an abelian p-group

In this section we show that for Problem 2 and Problem 3, the abelian normal Hall subgroup can be reduced to the elementary abelian case. We exhibit the main lemma and indicate the reduction to be executed, while proofs can be found in the full version.

We describe some concepts that are generally useful for the study of p-group, following [14]. For a group G, the *Frattini subgroup* $\Phi(G)$ is the intersection of maximal subgroups, and $G/\Phi(G)$ is called the Frattini factor group of G. For a prime p, the *p-core* $O_p(G)$ is the unique largest normal p-subgroup of G. For a p-group P, it is well-known that its Frattini factor group $P/\Phi(P)$ is elementary abelian. An abelian p-group is *homocyclic*, if its primary decomposition consists of factors of the same order. We will use a slightly improved main technical lemma in [16], the proof of which is put into appendix. (The original lemma deals with the case when B is homocyclic.)

▶ **Lemma 6.1** ([16]). *Let $B = B_1 \times B_2 \times \cdots \times B_k$ be an abelian p-group, where B_i's are the homocyclic components of B of exponent p^{r_i} and order $p^{r_i n_i}$. Denote $A := \mathrm{Aut}(B)$, and $O := O_p(A)$.*

1. *$\mathrm{Aut}(B_i/\Phi(B_i)) \cong \mathrm{GL}(n_i, p)$, $A/O \cong \prod_{i\in[k]} \mathrm{Aut}(B_i/\Phi(B_i))$;*
2. *Let X be a p'-subgroup of A/O. For $i = 1, 2$, $g_i : X \to \mathrm{Aut}(B)$ is a monomorphism such that x and $g_i(x)$ induce the same element of A/O for all $x \in X$. Then there exists $t \in O$ such that $g_2(x) = t^{-1} g_1(x) t$ for all $x \in X$.*

[1] As a field $\mathbb{F}$ is a simple algebra over its prime field, any $\mathbb{F}$-module is a direct sum of some copies of $\mathbb{F}$.
[2] An algebra A is semisimple if any A-module is a direct sum of simple modules. The group algebra of G, $\mathbb{F}G$ is semisimple if $\mathrm{char}(\mathbb{F}) \nmid |G|$. cf. Chapter 5 in [1].

Let the notations as in Lemma 6.1, and $\Lambda_p : A \to A/O$ be the canonical epimorphism. As $A/O \cong \prod_i \mathrm{GL}(n_i, p)$, for $\alpha : H \to A$, $\Lambda_p \circ \alpha$ maps H to $\prod_i \mathrm{GL}(n_i, p)$. Recall that $\mathrm{Aut}(H, \alpha, \beta) = \{\phi \in \mathrm{Aut}(H) \mid \alpha^\phi \sim \beta\}$. The following corollary is an immediate consequence of Lemma 6.1.

▶ **Corollary 6.2.** $\mathrm{Aut}(H, \alpha, \beta) = \mathrm{Aut}(H, \Lambda_p \circ \alpha, \Lambda_p \circ \beta)$.

The above corollary indicates that we need to compute Λ_p as the reduction. From the algorithmic point of view we need to be able to manipulate explicitly the automorphism group of an abelian group. To achieve that Ranum's work on automorphisms of abelian groups ([27], cf. also [17] and [13]) will be crucial. This reduction is first proposed by Le Gall in [13], and he proved for for the case when the complement is cyclic. Here we just proved that the same reduction in [13] can be applied to arbitrary complements. We note that the authors in [26] overlooked the fact that Le Gall's result was proved only for cyclic complements, and used for the situation when the complement is elementary abelian. Finally, Ranum's work also enables the reduction from Problem 3 to A_p being elementary abelian, which can be viewed as solving a system of linear Diophantine equations (cf. [12]) and then a set of generators can be recovered.

Acknowledgement

Youming would like to thank J.L. Alperin and J.B. Wilson for several helpful discussions. Part of the work was done when Youming was visiting the University of Chicago and (then) Microsoft Research India, and he would also like to thank Laci Babai, Neeraj Kayal and Satya Lokam for their warm host. László Babai's work is supported in part by NSF Grant CCF-1017781. Youming Qiao's work is supported in part by the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00301, the National Natural Science Foundation of China Grant 61033001, 61061130540, 61073174.

References

1 J.L. Alperin and R.B. Bell. *Groups and representations*. Graduate texts in mathematics. Springer, 1995.

2 Vikraman Arvind, Bireswar Das, Johannes Köbler, and Seinosuke Toda. Colored hypergraph isomorphism is fixed parameter tractable. In *FSTTCS*, pages 327–337, 2010.

3 László Babai. Monte-Carlo algorithms in graph isomorphism testing. Technical Report 79-10, Univ. de Montréal, Dép. de mathématiques et de statistique, 1979.

4 László Babai. Equivalence of linear codes. Manuscript, 2010. See [5].

5 László Babai, Paolo Codenotti, Joshua A. Grochow, and Youming Qiao. Code equivalence and group isomorphism. In *SODA*, pages 1395–1408, 2011.

6 László Babai, Paolo Codenotti, and Youming Qiao. Polynomial-time isomorphism test for groups without abelian normal subgroups. Manuscript, 2011.

7 László Babai and Shlomo Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity class. *J. Comput. Syst. Sci.*, 36:254–276, April 1988.

8 Hans Ulrich Besche, Bettina Eick, and E.A. O'Brien. A millennium project: Constructing small groups. *Intern. J. Alg. and Comput*, 12:2002.

9 S.R. Blackburn, P.M. Neumann, and G. Venkataraman. *Enumeration of finite groups*. Cambridge tracts in mathematics. Cambridge University Press, 2007.

10 J. Buchmann and A. Schmidt. Computing the structure of a finite abelian group. *Mathematics of Computation*, 74(252):2017–2026, 2005.

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

12 Tsu-wu J. Chou and George E. Collins. Algorithms for the solution of systems of linear Diophantine equations. *Siam Journal on Computing*, 11:687–708, 1982.

13 François Le Gall. Efficient isomorphism testing for a class of group extensions. In *STACS*, pages 625–636, 2009.

14 D. Gorenstein. *Finite groups*. AMS Chelsea Publishing Series. American Mathematical Society, 2007.

15 M. E. Harris. On p'-automorphisms of abelian p-groups. *Rocky Mountain J. Math.*, 7:751–752, 1977.

16 M. E. Harris. On p'-automorphisms of abelian p-groups, ii. *Periodica Mathematica Hungarica*, 11:321–323, 1980. 10.1007/BF02107573.

17 Christopher Hillar and Darren Rhea. Automorphisms of finite abelian groups. *Amer. Math. Monthly*, 114(10):917–923, 2007.

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

19 B. Huppert. *Endliche Gruppen*. Number v. 1 in Endliche Gruppen. Springer, 1967.

20 Noboru Itô. Note on A-groups. *Nagoya Mathematical Journal*, 4:79–81, 1952.

21 T. Kavitha. Linear time algorithms for abelian group isomorphism and related problems. *J. Comput. Syst. Sci.*, 73(6):986–996, 2007.

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

23 Eugene M. Luks. Permutation groups and polynomial-time computation. In *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, 1993.

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

25 Gary L. Miller. On the $n \log n$ isomorphism technique (a preliminary report). In *STOC '78: Proceedings of the 10th Annual ACM Symposium on Theory of Computing*, pages 51–58, New York, NY, USA, 1978. ACM.

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

27 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.

28 Lajos Rónyai. Computing the structure of finite algebras. *J. Symb. Comput.*, 9(3):355–373, 1990.

29 C. Savage. An $O(n^2)$ algorithm for abelian group isomorphism. Technical report, North Carolina State University, 1980.

30 A. Seress. *Permutation group algorithms*, volume 152 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2003.

31 D. R. Taunt. On A-groups. *Mathematical Proceedings of the Cambridge Philosophical Society*, 45:24–42, 1949.

32 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.

33 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.

34 James B. Wilson. Decomposing p-groups via jordan algebras. *J. Algebra*, 322:2642–2679, 2009.

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