On the Group and Color Isomorphism Problems

François Le Gall
Graduate School of Informatics
Kyoto University
Email: legall@i.kyoto-u.ac.jp

David J. Rosenbaum
The University of Tokyo
Department of Computer Science
Email: djr7c4@gmail.com

September 27, 2016

Abstract

In this paper, we prove results on the relationship between the complexity of the group and color isomorphism problems. The difficulty of color isomorphism problems is known to be closely linked to the the composition factors of the permutation group involved. Previous works are primarily concerned with applying color isomorphism to bounded degree graph isomorphism, and have therefore focused on the alternating composition factors, since those are the bottleneck in the case of graph isomorphism.

We consider the color isomorphism problem with composition factors restricted to those other than the alternating group, show that group isomorphism reduces in $n^{O(\log \log n)}$ time to this problem, and, conversely, that a special case of this color isomorphism problem reduces to a slight generalization of group isomorphism. We then sharpen our results by identifying the projective special linear group as the main obstacle to faster algorithms for group isomorphism and prove that the aforementioned reduction from group isomorphism to color isomorphism in fact produces only cyclic and projective special linear factors. Our results demonstrate that, just as the alternating group was a barrier to faster algorithms for graph isomorphism for three decades, the projective special linear group is an obstacle to faster algorithms for group isomorphism.
1 Introduction

The complexity of isomorphism testing problems is worthy of study both because they are fundamental computational questions and also because many of them are not known to be in \( P \), but nevertheless appear to be easier than the \( \text{NP} \)-complete problems. The most heavily studied of these is the graph isomorphism problem. It is strongly suspected that graph isomorphism is not \( \text{NP} \)-complete both because this would imply the collapse of the polynomial hierarchy \([4, 10, 15, 14]\) and also because there are subexponential time algorithms \([24, 8, 7, 2]\) for testing isomorphism of general graphs, which is much better than the \( 2^{O(n^2)} \) time complexity that we would expect based on the exponential-time hypothesis \([19]\).

For more than three decades, the \( 2^{O(\sqrt{n \log n})} \) time bound from \([24, 8, 7]\) was the best known for testing isomorphism of general graphs in the worst case. This result is based on (a) reducing testing isomorphism of a pair of arbitrary graphs to testing isomorphism of many pairs of graphs of degree \( \sqrt{n/\log n} \) using Zemlyachenko’s lemma (cf. \([3]\)), and (b) reducing \([24, 8, 7]\) testing isomorphism of graphs of degree at most \( d \) to another problem known as the color automorphism problem \([24, 8, 7]\).

In this problem, we are given a set \( X \) of size \( n \) and a coset \( \sigma \Gamma \) where \( \Gamma \) is a subgroup of the symmetric group on \( X \) and \( \sigma \) is a permutation of \( X \). We are also given a function \( f : X \rightarrow [n] \) that specifies the color of each element of \( X \). The problem is to compute all \( \pi \in \sigma \Gamma \) such that \( f(\pi x) = f(x) \) for all \( x \in X \). It is important to note that the set of all such \( \pi \) forms a subcoset of \( \sigma \Gamma \) \([24]\), so the solution can be represented compactly as a coset representative along with the generators of a subgroup of \( \Gamma \). In this paper, we consider a slight generalization of the color automorphism problem in which there are two functions \( f_1 \) and \( f_2 \).

Definition 1.1. In the color isomorphism problem, we are given a set \( X \) of size \( n \) and a coset \( \sigma \Gamma \) containing permutations of \( X \) and two functions \( f_1 : X \rightarrow [n] \) and \( f_2 : X \rightarrow [n] \). The goal is to find all \( \pi \in \sigma \Gamma \) such that \( f_2(\pi x) = f_1(x) \) for all \( x \in X \).

Note that we can recover the color automorphism problem by stipulating that \( f_1 = f_2 \).

The complexity of the color isomorphism problem is strongly dependent on the non-Abelian composition factors (which we define later) of the group \( \Gamma \): if every non-Abelian composition factor of \( \Gamma \) is isomorphic to a subgroup of the symmetric group on \( d \) elements, then any color isomorphism problem on a subcoset \( \sigma \Gamma \) can be solved in \( n^{O(d/\log d)} \) time \([8, 7]\). The barrier to improving the \( n^{O(d/\log d)} \) time bound, and hence also the \( 2^{O(\sqrt{n \log n})} \) time bound for graph isomorphism, depends only on the composition factors that are isomorphic to alternating groups \([7]\). All other composition factors can be handled simply by brute force in \( n^{O(\log n)} \) time by a result of Pyber \([28]\).

In a recent paper \([2]\), Babai overcame the obstacle of the alternating composition factors with an algorithm that solves the graph and color isomorphism problems in \( 2^{O(\log^{2+O(1)} n)} \) time. This is almost an exponential speedup. However, the statement of this result does not allow us to obtain speedups for other types of composition factors since — as mentioned above — they can be dealt with exhaustively in \( n^{O(\log n)} \) time.

In this work, we study the complexity of color isomorphism problems involving composition factors other than the alternating group. We accomplish this by comparing this class of color isomorphism problems to the group isomorphism problem — a fundamental problem in computational group theory that has been well studied and has seen a surge of activity in the last few

\(^1\)In these previous papers, color automorphism and string canonization were the problems that were considered. However, the techniques in these papers can easily be adapted to solve color isomorphism within the same bounds.
years \[23, 33, 35, 1, 20, 21, 29, 5, 13, 9, 6, 22, 16, 27, 17\]. As we will show, group isomorphism depends only on the cyclic and projective special linear composition factors, so we focus our attention on color isomorphism problems with cyclic and projective special linear composition factors. Our first result shows that, just as the alternating group was a barrier to placing graph isomorphism in quasi-polynomial time for more than thirty years, the projective special linear group is a barrier to faster algorithms for group isomorphism. Before we can present our reduction, we need to introduce some notation. Let \( CI \) denote the class of all color isomorphism problems and let \( CI^* \) be all color isomorphism problems with cyclic and projective special linear composition factors. We denote the group isomorphism problem by \( GrI \).

**Theorem 1.2.** \( GrI \) is Turing reducible to \( CI^* \) in \( n^{O(\log \log n)} \) time.

It is important to note that this result is trivial when \( CI^* \) is replaced with \( CI \). The main difficulty here is to restrict the non-Abelian composition factors to the projective special linear group.

Our proof is based a holomorph trick suggested by Babai (personal communication), a new notation for dealing with iterated wreath products, structural results on automorphisms of finite\(^2\) Abelian groups (which we prove using \(18\)) and the algorithm of \(5\). The holomorph trick can also be replaced by the framework introduced by Luks’ in his recent paper \(25\) that shows how to test isomorphism of composition series in polynomial time. We discuss the relationship between our work and Babai’s holomorph trick in more detail in Subsection 2.2.

Our next result is the simple (but to our knowledge previously unknown) observation\(^3\) that the color isomorphism problem is equivalent to a slight generalization of graph isomorphism. The main reasons for mentioning this result are to make the relationship between general graph isomorphism and color isomorphism explicit and also to motivate one of our later results in this paper. Let \( GI^* \) be the problem of computing all isomorphisms between two graphs \(X\) and \(Y\) that are contained in a specified subcoset \(\sigma \Gamma\) that maps the vertices of \(X\) to the vertices of \(Y\).

**Theorem 1.3.** \( CI \) and \( GI^* \) are equivalent under polynomial-time many-one reductions.

Next, we explore the question of how much more difficult \( CI^* \) is compared to \( GrI \). To do this, we introduce a slight generalization of group isomorphism and show that a special case of \( CI^* \) can be reduced to it. To this end, we define \( GrI^* \) to be the problem of computing all isomorphisms from a group \(G\) to a group \(H\) that are contained within a coset \(\sigma \Gamma\) that maps the elements of \( \Gamma \) to \(H\) analogously to \(GI^*\) for graphs. It seems unlikely that \(GrI^*\) is much harder than \(GrI\); currently, the fastest worst-case algorithms for both problems run in \(n^{O(\log n)}\) time. Before we can define the special case \(Bl\) of \(CI^*\) that we will reduce to \(GrI^*\), we need to introduce some additional terminology.

**Definition 1.4.** Let \(f: B \times B \rightarrow A\) be a bilinear map defined on Abelian groups (regarded as \(\mathbb{Z}\)-modules). Then an isometry is a map \(\alpha \in \text{Aut}(B)\) such that \(f(x, y) = f(\beta x, \beta y)\) for all \(x, y \in B\).

It is easy to see that the isometries of a bilinear map form a group. Now we can define the problem \(Bl\).

**Definition 1.5.** Let \(A\) and \(B\) be Abelian groups and let \(f: B \times B \rightarrow A\) be a bilinear map given as a table of the values \(f(x, y)\) for all \(x, y \in B\). Then \(Bl\) is the problem of computing the isometry group of \(f\).

\(^2\)All of the groups that we deal with in this paper are finite and we shall omit the adjective finite from now on.

\(^3\)The proof of this result is straightforward. However, for the sake of completeness, we give a proof in Appendix A.
This redundancy in the representation of \( f \) is similar in spirit to the Cayley table representation used in group isomorphism. Another reason to use this redundant representation is that it means that \( Bl \) corresponds to a color isomorphism problem involving an action of \( \text{Aut}(B) \) on the Abelian group \( B \times B \times A \). Since the composition factors of \( \text{Aut}(B) \) are either cyclic or projective special linear, this implies that \( Bl \) is a special case of \( Cl^* \).

Versions of this problem in which the bilinear map is specified compactly as a matrix and \( A \) and \( B \) are vector spaces have been studied. Brooksbank and Wilson showed [11] that for bilinear maps that are Hermitian, one can compute the isometry group in polynomial time. Hermitian matrices generalize the symmetric and skew-symmetric matrices, but there are many matrices that are not hermitian.

Our next result shows that \( Bl \) is polynomial-time many-one reducible to \( Grl^* \).

**Theorem 1.6.** \( Bl \) is polynomial-time many-one reducible to \( Grl^* \).

Previously, Grochow and Qiao studied [16, 17] a generalization of the reverse direction of this reduction and used it to prove several interesting results. Our result complements theirs, and, to our knowledge, is the first reduction to (a slight generalization of) group isomorphism.

Our proof is based on using cohomology to construct a group \( G_f \) from the bilinear map \( f \) that contains \( A \) as a normal subgroup. We then compute a certain subgroup of the automorphism group of \( G_f \) by solving a problem in \( Grl^* \). We show that every automorphism \( \phi \) in this subgroup defines a map \( \varphi_\phi : G_f/A \to A \) and prove that \( \phi \) gives rise to an isometry of \( f \) precisely when \( \varphi_\phi \) is a homomorphism. By further restricting the subcoset in the instance of \( Grl^* \) above, we can ensure that every element of the resulting subgroup of automorphisms gives rise to a homomorphism and that every isometry can be obtained from an automorphism in this subgroup.

Additionally, \( Bl \) is likely to be equivalent to \( Grl \). The reason is as follows. The hard case of \( Grl \) is conjectured to be testing isomorphism of nilpotent groups of class 2 (\( NGrl \)). Theorem 1.6 in fact reduces to \( NGrl^* \), where \( NGrl^* \) is defined analogously to \( Grl^* \). Moreover, one can show that \( NGrl \) reduces to the problem of computing all \( \alpha \in \text{Aut}(A) \), \( \beta \in \text{Aut}(B) \) and \( b \in B \) such that \( f(x,y) = \alpha f(\beta x, \beta y) + b \) for all \( x,y \in B \) where \( A, B \) are abelian groups, \( B \) is a known subgroup of the group of bilinear maps from \( B \times B \) to \( A \) and \( f : B \times B \to A \) is bilinear. One can then recover \( Bl \) as a special case by setting \( \alpha = 1 \) and \( b = 0 \). This only removes cyclic composition factors from the resulting corresponding color isomorphism problem.

## 2 Background

In this section, we introduce some of the basic group theoretic concepts used later in the paper. We also discuss related results on testing isomorphism of composition series.

### 2.1 Group theory background

A subnormal series of a group \( G \) is a chain of subgroups \( G_1 = 1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_k = G \) where each subgroup is normal in the next and 1 denotes the trivial subgroup. The factor groups of this series are the groups \( G_{i+1}/G_i \). For a group \( G \), let \( [G,G] \) be the subgroup of \( G \) generated by the commutators \( [g_1,g_2] = g_1g_2g_1^{-1}g_2^{-1} \) where \( g_1, g_2 \in G \). One series that will be of interest is the derived series \( G^{(k)} \triangleleft \cdots \triangleleft G^{(0)} = G \). Here, \( G^{(0)} = G \) and each \( G^{(i+1)} = [G^{(i)}, G^{(i)}] \) and \( k \) is the smallest natural number such that \( G^{(k+1)} = G^{(k)} \). It need not be the case that \( G^{(k)} = 1 \). If this holds, then \( G \) is a solvable group.
If a subnormal series is maximal so that no more intermediate subgroup can be inserted that are distinct from the subgroups already in the series, then it is called a composition series. The factor groups of a composition series are called composition factors and are simple groups. That is, each of their normal subgroups is either the whole group or is trivial. One can equivalently define a composition series as a subnormal series in which all the factor groups are simple. In a solvable group, all of the composition factors are cyclic so that there are no non-Abelian composition factors.

Much of the motivation for this work is based on a simple group called the projective special linear group. To obtain this group, one starts with the general linear group $GL_d(\mathbb{F})$ of all invertible matrices over the field $\mathbb{F}$. By restricting to the subgroup of matrices with determinant 1, we obtain the special linear group $SL_d(\mathbb{F})$. The projective linear group is then defined to be the quotient of $SL_d(\mathbb{F})$ mod the subgroup consisting of multiples of the identity matrix by roots of unity. Dealing with the projective linear group is about as difficult as dealing with the general linear group since its non-Abelian composition factors consist of a single copy of the projective special linear group.

The holomorph $\text{Hol}(G)$ of a group $G$ is a semidirect product of $G$ with its automorphism group. An element $(g, \phi) \in \text{Hol}(G)$ acts on each element $x \in G$ by $(g, \phi)(x) = g \cdot \phi(x)$. The product of two elements $(g_1, \phi_1), (g_2, \phi_2) \in \text{Hol}(G)$ is $(g_1, \phi_1) \cdot (g_2, \phi_2) = (g_1 \phi_1(g_2), \phi_1 \phi_2)$. The wreath product $G \wr H$ of two permutation groups $G$ and $H$ that act on the sets $Y$ and $X$ is a semidirect product of the groups $G^H$ and $H$. Here, $G^H$ means a direct product of $|H|$ copies of $G$; each copy of $G$ is indexed by a different element of $H$. Each element of the wreath product $G \wr H$ corresponds to a pair $(g, h)$ where $g \in G^H$ is a vector indexed by the elements of $H$. Then $(g, h)$ acts on an element $x, y \in X \times Y$ by $(g, h)(x, y) = (g_{hy}x, hy)$. Intuitively, a wreath product corresponds to a group of automorphisms of a full rooted tree of depth 2. The children of the root correspond to the elements of $Y$ while their children correspond to elements of $X \times Y$. The element $h$ indicates how the children of the root should be permuted and the vector $g$ of elements of $G$ indexed by $H$ indicates how the children of each child of the root should be permuted after the children of the root are permuted. In particular, if $T$ is a rooted tree of depth 2 where all nodes at depth 1 have degree $d_1$ and all nodes at depth $d_2$, then $\text{Aut}(T) = S_{d_2} \wr S_{d_1}$.

In this section, we shall be concerned with iterated wreath products of the form $G_1 \wr \cdots \wr G_k$ of groups $G_i$ which each acts on a set $X_i$. The iterated wreath product $G_1 \wr \cdots \wr G_k$ acts on $X_1 \times \cdots \times X_k$ by recursively applying the definition of a wreath product. If one imagines a rooted tree where the first level consists of the elements of $X_k$ and the $i^{th}$ level consists of the elements of $X_{k-i+1} \times \cdots \times X_k$, then $G_1 \wr \cdots \wr G_k$ is a group of automorphisms of this rooted tree. The group $G_k$ determines how the children of the root are permuted and there is a copy of each $G_{k-i+1}$ for all $(x_{k-i+1}, \ldots, x_k) \in X_{k-i+1} \times \cdots \times X_1$ that determines how its children are permuted. If one considers the full rooted tree of depth $k$ where every node in the $i^{th}$ level has degree $d_i$, then its automorphism group is the iterated wreath product $S_{d_k} \wr \cdots \wr S_{d_1}$. This notation quickly becomes cumbersome to deal with as the number of groups $k$ increases. We address this problem by introducing a new notation for wreath products that is much more convenient for our purposes in Section 3.3.

### 2.2 Previous work on composition series isomorphism

Our techniques rely on recent ideas by Luks [25] and Babai (personal communication) on composition series isomorphism. We say that two series $S$ and $S'$ for groups $G$ and $H$ are isomorphic if there is an isomorphism from $G$ to $H$ that maps each subgroup in $S$ to the corresponding subgroup in
Babai showed (personal communication) that if $\phi$ is an isomorphism between subnormal series $S$ and $S'$ for groups $G$ and $H$, then $\phi \in \text{Hol}(F_0) \wr \cdots \wr \text{Hol}(F_k)$ where $F_0, \ldots, F_k$ are the factors of the isomorphic subnormal series $S$ and $S'$. If $G$ and $H$ are solvable, then so is each $\text{Hol}(F_i)$; this implies that testing isomorphism of composition series of solvable groups is in polynomial time \cite{26, 8}, this implies that testing isomorphism of composition series of solvable groups is in polynomial time since $\text{Hol}(F_0) \wr \cdots \wr \text{Hol}(F_k)$ does not have any non-Abelian composition for solvable groups.

The solvable radical $\text{Rad}(G)$ of a group $G$ is its unique maximal solvable normal subgroup. Babai (personal communication) further proved that one can decide isomorphism of subnormal series of arbitrary groups in $n^{O(\log \log n)}$ time by using the algorithm of \cite{3} assuming that they have the form $1 \triangleleft G_1 \triangleleft \cdots \triangleleft G_k \triangleleft \text{Rad}(G) \triangleleft G_{k+1} \triangleleft \cdots \triangleleft G_m = G$. Using different but related ideas, Luks' went further and showed \cite{25} that testing isomorphism of arbitrary composition series can be done in polynomial time. In an upcoming paper (cf. \cite{25}), Luks' plans to build this into the stronger result that canonical forms of composition series can be computed in polynomial time. Let $p$ be the smallest prime divisor of the group. Since every group has at most $n^{(1/2) \log_p n + O(1)}$ composition series, this method can be combined with the bidirectional collision detection methods introduced by the second author \cite{31} (which provide a deterministic square-root speedup) to solve group isomorphism in $n^{(1/4) \log_p n + G(1)}$ time.

In this work, we apply Babai's holomorph trick and his idea to a different series that we call the radical derived series \cite{5} (which we shall define shortly). Unlike the classes of composition series and subnormal series, this series has the property that there is only one way to construct it for a given group. Consequently, if $S$ and $S'$ denote the radical derived series for the groups $G$ and $H$, then $G$ and $H$ are isomorphic if and only if $S$ and $S'$ are isomorphic. The advantage of this approach is that it allows us to avoid the $n^{(1/4) \log_p n}$ factor in the runtime above. The difficulty of the group isomorphism problem is instead handled by allowing projective special linear composition factors in the resulting color isomorphism problem. The radical derived series is defined as follows.

**Definition 2.1.** Let $G$ be a group. Then the radical derived series of $G$ is

$$
\text{Rad}(G)^{(m)} = 1 \triangleleft \text{Rad}(G)^{(m-1)} \triangleleft \cdots \triangleleft \text{Rad}(G)^{(0)} = \text{Rad}(G) \triangleleft G
$$

Here, $\text{Rad}(G)^{(i)}$ denotes the $i$th subgroup in the derived series of $\text{Rad}(G)$ starting with $\text{Rad}(G)$.

Because the iterated wreath products that arise in this reduction are quite complicated and difficult to handle, we also introduce a new notation for describing elements of iterated wreath products which makes our proofs much easier. It is our hope that our notation will prove useful in future work in this area. Our proof also requires us to prove a result on the composition factors of the automorphism groups of Abelian groups. We accomplish this by using the framework for dealing with automorphisms of Abelian groups given in \cite{18}.

### 3 Reducing group isomorphism to color isomorphism

In this section, we prove that group isomorphism reduces to the color isomorphism problem with cyclic and projective special linear composition factors.
The first step is to identify the elements of $G$ and $H$. Clearly, this does not solve the isomorphism problem since the resulting groups can have different multiplication rules and the identification does not necessarily yield an isomorphism. We accomplish this using the following definitions.

**Definition 3.1.** Let $G$ be a group, let $G_m = 1 < \cdots < G_0 = G$ be its radical derived series and let $F_i = G_{m-i}/G_{m-i+1}$ and choose an arbitrary lift $\ell_i : F_i \to G_i$ for each $1 \leq i \leq m$. Then for each $g \in G$, there exists a unique $(x_1, \ldots, x_m) \in F_1 \times_c \cdots \times_c F_m$ such that $g = \ell_m(x_0) \cdots \ell_1(x_{m-1})$. Let $\ell : F_1 \times_c \cdots \times_c F_m \to G$ denote this bijection. Then we define $\hat{G}$ to be the group on the set $F_1 \times_c \cdots \times_c F_m$ whose multiplication rule is induced by $G$ under the bijection $\ell$.

Here, we distinguish between Cartesian products (denoted by $\times$) which operate on sets and direct products (denoted by $\times_c$) which operate on groups. Therefore, $F_1 \times_c \cdots \times_c F_m$ is the subset of $G$ that corresponds to $(\hat{G})^{(i)}$. We use $\times_c$ instead of $\times$ in order to avoid suggesting that $F_1 \times_c \cdots \times_c F_m$ is a direct product of the groups $F_1, \ldots, F_m$. This would be very misleading since $(\hat{G})^{(i)}$ can be non-Abelian.

Our next step is to identify the factor groups in the radical derived series for the groups $G$ and $H$. Let us say that the canonical representation of an Abelian group $A$ is the unique group of the form $C(A) = \times^k_{i=1} \mathbb{Z}^{\epsilon_i}_{p_i}$ that is isomorphic to $A$ where $p_1 < \cdots < p_k$ are primes and each $\epsilon_i$ is a natural number. This takes care of the Abelian factors in the radical derived series. However, we also need a way to identify the factor groups $G/\text{Rad}(G)$ and $H/\text{Rad}(H)$. These are non-Abelian groups that do not have any normal Abelian subgroups. We identify them by using the algorithm of [5] which can enumerate all the isomorphisms between two groups of order $n$ that do not have any normal Abelian subgroups in $n^{O(\log \log n)}$ time. To do this, we first define $C(G/\text{Rad}(G)) = G/\text{Rad}(G)$; we then define $C(H/\text{Rad}(H)) = G/\text{Rad}(G)$. The later identification is performed in $n^{O(\log \log n)}$ time using [5]. Note that our definition of $C$ on non-Abelian groups depends on whether we are given $G$ or $H$ and is thus specific to our problem instance.

**Definition 3.2.** Let $G$ be a group, let $G_m = 1 < \cdots < G_0 = G$ be its radical derived series and let $F_i = G_{m-i}/G_{m-i+1}$. For each $F_i$, let $\bar{F}_i = C(F_i)$ and choose an arbitrary isomorphism $\varphi_i : F_i \to \bar{F}_i$. This defines a bijection $\varphi : F_1 \times_c \cdots \times_c F_m \to \bar{F}_1 \times_c \cdots \times_c F_m$. We let $\hat{G}$ be the group on the set $F_1 \times_c \cdots \times_c F_m$ whose multiplication rule is induced by the group $\hat{G}$ under the bijection $\varphi : \hat{G} \to \hat{G}$.

Note that $\varphi \circ \ell^{-1} : G \to \hat{G}$ is an isomorphism from $G$ to $\hat{G}$. A key fact that we shall need about $\hat{G}$ is that its derived subgroups correspond to iteratively removing factors from the product $C(F_1) \times_c \cdots \times_c C(F_m)$ as we move down the series. This is stated in the following proposition. The proof follows easily from the definitions.

**Proposition 3.3.** Let $G$ be a group, let $G_m = 1 < \cdots < G_0 = G$ be its radical derived series and let $F_i = G_{m-i}/G_{m-i+1}$. Then $(\hat{G})^{(i)} = C(F_1) \times_c \cdots \times_c C(F_{m-i})$.

The next lemma allows us to treat isomorphisms between groups as members of a wreath product.

**Lemma 3.4.** Let $G$ and $H$ be groups and suppose that $\phi : \hat{G} \to \hat{H}$ is an isomorphism. Let $G_m = 1 < \cdots < G_0 = G$ and $H_m = 1 < \cdots < H_0 = H$ be the radical derived series for $G$ and $H$ and let $\bar{F}_i = C(G_{m-i}/G_{m-i+1}) = C(H_{m-i}/H_{m-i+1})$. Then $\phi \in \text{Hol}(\bar{F}_1) \cdots \text{Hol}(\bar{F}_m)$.

Before we can present the proof, we need a better way of dealing with iterated wreath products since using the standard wreath product definition recursively quickly becomes very cumbersome.
Without better notation, our proof would be extremely tedious. We accomplish this by defining a wreath product as a indexes set of elements that satisfies certain conditions.

**Definition 3.5.** Consider the iterated wreath product $G_1 \wr \cdots \wr G_k$ of groups $G_i$ which each acts on a set $X_i$. Let $\pi_{x_{i+1}, \ldots, x_k} \in G_i$ for each $x_{i+1}, \ldots, x_k \in X_{i+1} \times \cdots \times X_k$ and each $1 \leq i \leq k$. Then this set of elements defines the permutation $\pi(x_1, \ldots, x_k) = (\pi_{x_2, \ldots, x_k}(x_1), \ldots, \pi_{x_k}(x_{k-1}), \pi_k(x_k))$.

Note that in the above definition, $\pi() \in G_k$ denotes the case where $i = k + 1$ so that the list of subscripts is empty. It is easy to show that the functions are permutations and are precisely the elements of the iterated wreath product $G_1 \wr \cdots \wr G_k$.

**Lemma 3.6.** Consider the iterated wreath product $G_1 \wr \cdots \wr G_k$ of groups $G_i$ which each acts on a set $X_i$. Then every $\pi$ defined by Definition 3.5 is a permutation contained in $G_1 \wr \cdots \wr G_k$. Moreover, every element of $G_1 \wr \cdots \wr G_k$ can be expressed in the form of Definition 3.5.

Now, we are ready to prove Lemma 3.4. Because our proof deals with many subsequences of vectors, we introduce a shorthand. If $a \in A_1 \times \cdots \times A_k$, then $a_{i,j}$ denotes the subsequence $(a_i, \ldots, a_j)$.

**Proof.** For each $1 \leq i \leq m$, let $\phi_i = \phi|_{F_i} : \tilde{F}_i \to \tilde{F}_i$ be the automorphism of $\tilde{F}_i$ induced by $\phi$. Define

$$\tilde{\phi}_{x_{i+1}, m} = (f_i(x_{i+1}, m), \phi_i) \in \text{Hol}(\tilde{F}_i)$$

for each $x \in F_1 \times_c \cdots \times_c F_m$ and $1 \leq i \leq m$ where the $f_i : F_{i+1} \times_c \cdots \times_c F_m \to F_i$ are functions that are to be determined in the course of the proof. Whatever we later choose these functions to be, note that by Definition 3.5 and Lemma 3.6 it defines a permutation $\dot{\phi} \in \text{Hol}(\tilde{F}_1) \cdots \text{Hol}(\tilde{F}_m)$. Our aim is to choose them so that $\phi = \dot{\phi}$.

We accomplish this by induction on $i$. Our goal is to show that

$$\phi(1^i, x_{i+1}, m) = \tilde{\phi}(1^i, x_{i+1}, m)$$

for all $0 \leq i \leq m$ where $1^i$ is a shorthand for $1, \ldots, 1$.

We start with the basis case $i = m$. This corresponds to the claim that

$$\phi(1^m) = \tilde{\phi}(1^m)$$

which is equivalent to asserting that

$$1^m = (f_1(1^{m-1}), \ldots, f_{m-1}(1), f_m)$$

Since we can choose the $f_i$ functions as desired, we simply define $(f_1(1^{m-1}), \ldots, f_{m-1}(1), f_m) = 1^m$.

This proves the basis case, so now proceed to the inductive case.

Assume that (1) holds for some $1 \leq i \leq m$; we will show that it holds for $i - 1$ as well. By Proposition 3.3 $(1^{i-1}, x_i, 1^{m-i}) \in (\tilde{G})^{(m-i)}$ so

$$\phi(1^{i-1}, x_i, m) = \phi(1^{i-1}, x_i, 1^{m-i})\phi(1^i, x_{i+1}, m)$$

Now, again because $\phi(1^{i-1}, x_i, 1^{m-i}) \in (\tilde{G})^{(m-i)}$, we have $\phi(1^{i-1}, x_i, 1^{m-i}) = (a_{i-1}(x_i), \phi_i(x_i), 1^{m-i})$ for some $a_{i-1}(x_i) \in \tilde{F}_{i-1} \times_c \cdots \times_c \tilde{F}_{i-1}$. Thus, by the inductive hypothesis

$$\phi(1^{i-1}, x_i, m) = (a_{i-1}(x_i), \phi_i(x_i), 1^{m-i}) \cdot \tilde{\phi}(1^i, x_{i+1}, m)$$

(2)
By Definition 3.5 and noting that $f_m = 1$ from the basis case, we see that $\tilde{\phi}(1^i, x_{i+1,m})$ is equal to
\[(f_1(1^{i-1}, x_{i+1,m}), \ldots, f_i(x_{i+1,m}), f_{i+1}(x_{i+2,m})\phi_i(x_{i+1}), \ldots, f_{m-1}(x_m)\phi_i(x_{m-1}), \phi_m(x_m))\]
By applying Proposition 3.3, we see that this is equal to
\[(f_1(1^{i-1}, x_{i+1,m}), \ldots, f_i(x_{i+1,m}), 1^{m-i}) \cdot (1^i, f_{i+1}(x_{i+2,m})\phi_i(x_{i+1}), \ldots, f_{m-1}(x_m)\phi_i(x_{m-1}), \phi_m(x_m)) \]
By replacing $\tilde{\phi}(1^i, x_{i+1,m})$ in (2) with (3), we see that
\[\phi(1^{i-1}, x_{i,m}) = (a_{i-1}(x_i), \phi_i(x_i), 1^{m-i}) \]
\[\cdot (f_1(1^{i-1}, x_{i+1,m}), \ldots, f_i(x_{i+1,m}), 1^{m-i}) \]
\[\cdot (1^i, f_{i+1}(x_{i+2,m})\phi_i(x_{i+1}), \ldots, f_{m-1}(x_m)\phi_i(x_{m-1}), \phi_m(x_m))\]
Now $\tilde{F}_i$ is Abelian for $i < m$ and $f_i = 1$ for $i = m$. Thus, $\phi_i(x_i)f_i(x_{i+1,m}) = f_i(x_{i+1,m})\phi_i(x_i)$, so
\[\phi(1^{i-1}, x_{i,m}) = (b_{i-1}(B), f_i(x_{i+1,m})\phi_i(x_i), 1^{m-i}) \]
\[\cdot (1^i, f_{i+1}(x_{i+2,m})\phi_i(x_{i+1}), \ldots, f_{m-1}(x_m)\phi_i(x_{m-1}), \phi_m(x_m))\]
\[\cdot (1^i, f_{i+1}(x_{i+2,m})\phi_i(x_{i+1}), \ldots, f_{m-1}(x_m)\phi_i(x_{m-1}), \phi_m(x_m))\]
where $B = (x_i, f_1(1^{i-1}, x_{i+1,m}), \ldots, f_i(x_{i+1,m}))$ indicates the values on which $b_{i-1}(B)$ depends. If $i = 1$, then $b_{i-1}(B) = b_0(B) = ()$ and we have $\phi(1^{i-1}, x_{i,m}) = \tilde{\phi}(1^{i-1}, x_{i,m})$ as desired. Also, if $x_i = 1$, then $\phi(1^{i-1}, x_{i,m}) = \tilde{\phi}(1^{i-1}, x_{i,m})$ by the inductive hypothesis. Therefore, we may assume that $i \geq 2$ and $x_i \neq 1$. Then by Definition 3.5 we have
\[\tilde{\phi}(1^{i-1}, x_{i,m}) = (f_1(1^{i-2}, x_{i,m}), \ldots, f_{i-1}(x_{i,m}), f_i(x_{i+1,m})\phi_i(x_i), \ldots, f_{m-1}(x_m)\phi_m(x_{m-1}), \phi_m(x_m))\]
So to show that $\phi(1^{i-1}, x_{i,m}) = \tilde{\phi}(1^{i-1}, x_{i,m})$, we need to choose $(f_1(1^{i-2}, x_{i,m}), \ldots, f_{i-1}(x_{i,m})) = b_{i-1}(B)$.

Now, we just need to argue that all the assignments that we make at each step are independent. Let us say that the weight of a vector $y$ is $d - k$ where $d$ is the length of $y$ and $k$ is the smallest index such that $y_k \neq 1$. Then, the $i^{th}$ step of the induction assigns values to the functions $f_j$ with $j < i$ on arguments of weight exactly $m - i + 1$. It follows that the assignments made at each step are independent which proves that (1) holds for $i - 1$. By induction, we conclude that the functions $f_i$ can be chosen so that $\phi = \tilde{\phi}$.

Before we can prove Theorem 1.2, we need a lemma about the structure of automorphisms of Abelian groups.

**Lemma 3.7.** Let $A$ be an Abelian group. Then every composition factor of Aut($A$) is either cyclic or projective special linear.

To prove this lemma, we need to introduce a few definitions and results on the theory of automorphisms of Abelian groups. These were first studied by Ranum [30]; however, we follow the more modern treatment by Hillar and Rhea [18] since it is more convenient. Since the group of automorphisms of a direct product of groups of relatively prime order is the direct product of the automorphisms of each group, it suffices to consider Abelian $p$-groups. First, we characterize the endomorphisms of Abelian $p$-groups.

---

6There is no need to include $\phi_i(x_i)$ in addition to $x_i$ since $\phi$ is fixed and therefore so is $\phi_i$. 8
Definition 3.8 (30, cf. [18]). Let $A = \times_{i=1}^{d} \mathbb{Z}_{p}^{e_{i}}$ be a Abelian $p$-group where $e_{1} < \cdots < e_{d}$. Define

$$R(A) = \left\{ (m_{ij}) \in \mathbb{Z}_{p}^{d \times d} \mid p^{e_{i} - e_{j}} \text{ divides } a_{ij} \text{ for all } 1 \leq j \leq i \leq d \right\}$$

One can show that $R(A)$ is a ring (30) (cf. [18]). The endomorphisms $\text{End}(A)$ of $A$ then arise via a homomorphism defined on $R(A)$.

Theorem 3.9 (18). Let $A = \times_{i=1}^{d} \mathbb{Z}_{p}^{e_{i}}$ be a Abelian $p$-group where $e_{1} < \cdots < e_{d}$ and define $\psi : R(A) \to \text{End}(A)$ by

$$\psi(M)(\pi(a)) = \pi(Ma)$$

where $\pi : \mathbb{Z}^{d} \to A$ is the projection that maps each $a \in \mathbb{Z}^{d}$ to $(a_{1} + \mathbb{Z}_{p}^{e_{1}}, \ldots, a_{d} + \mathbb{Z}_{p}^{e_{d}})$. Then $\psi$ is a surjective homomorphism.

We also need another result that relates the endomorphisms to automorphisms.

Theorem 3.10 (30, cf. [18]). Let $A = \times_{i=1}^{d} \mathbb{Z}_{p}^{e_{i}}$ be an Abelian $p$-group where $e_{1} < \cdots < e_{d}$. Then $\psi(M)$ is an automorphism if and only if $\psi(M) \mod p \in \text{GL}_{d}(p)$ (where the modulo division is performed entrywise).

Now, we are ready to prove Lemma 3.7.

Proof of Lemma 3.7. Since the automorphism group of $A$ is the direct product of the automorphism groups of its Sylow subgroups, it suffices to prove this for the case where $A$ is a $p$-group. Let $A = \times_{i=1}^{d} \mathbb{Z}_{p}^{e_{i}}$ be a Abelian $p$-group where $e_{1} < \cdots < e_{d}$ and let us define $\rho : \text{End}(A) \to \mathbb{Z}_{p}^{d \times d}$ by $\rho(\psi(M)) = \psi(M) \mod p$ for each $\psi(M) \in \text{End}(A)$. Observe that $\rho$ is a ring homomorphism.

By Definition 3.8 and Theorem 3.9, the image of $\rho$ is

$$\text{Im } \rho = \left\{ (m_{ij}) \in \mathbb{Z}_{p}^{d \times d} \mid m_{ij} = 0 \text{ if } 1 \leq j \leq i \leq d \text{ and } e_{i} \neq e_{j} \right\}$$

In other words, the image of $\rho$ consists of block-upper triangular matrices in $\mathbb{Z}_{p}^{d \times d}$ where the blocks consist of those $(i, j)$ such that $e_{i} = e_{j}$. Let $B_{k}$ denote the set of indexes $(i, j)$ in the $k^{th}$ block on the main diagonal of these matrices where $1 \leq k \leq \ell$. Since the determinant of a block-upper triangular matrix is equal to the product of the determinants of the blocks, we see that $\rho[\text{Aut}(A)]$ consists of those matrices in $\text{Im } \rho$ where the blocks on the diagonal are invertible. Thus,

$$\rho[\text{Aut}(A)] = \left\{ (m_{ij}) \in \text{Im } \rho \mid \det [(m_{ij})_{B_{k}}] \neq 0 \text{ for each } k \right\}$$

where $(m_{ij})_{B_{k}}$ denotes the submatrix of $(m_{ij})$ on the block $B_{k}$.

We now shift our attention to $\sigma = \rho |_{\text{Aut}(A)} : \text{Aut}(A) \to \rho[\text{Aut}(A)]$ which we interpret as a surjective homomorphism between multiplicative groups. Since $\text{Aut}(A) / \ker \sigma \cong \text{Im } \sigma$, to find the composition factors of $\text{Aut}(A)$, it suffices to show that the composition factors of the kernel and image of $\rho$ are either cyclic or projective special linear. Now, $\text{Im } \sigma = \rho[\text{Aut}(A)]$.

To find its composition factors, we define another homomorphism $\theta : \text{Im } \sigma \to \text{GL}_{d}(p)$ where $d_{k}$ is the dimension of the $k^{th}$ block $B_{k}$. Then we define $\theta(M) = \text{diag}(M_{1}, \ldots, M_{\ell})$ where $M_{k} = (m_{ij})_{B_{k}}$ is the submatrix on the block $B_{k}$ in $M$. Now, $\text{Im } \theta = \text{GL}_{d_{1}}(p) \times \cdots \times \text{GL}_{d_{\ell}}(p)$ and the composition factors of general linear groups are cyclic and projective special linear. The kernel of $\theta$ is a $p$-group and therefore has cyclic composition factors. It follows that $\text{Im } \sigma$ has only cyclic and projective special linear composition factors.
All the remains is to determine the composition factors of \( \ker \sigma \). However, \( \ker \sigma \) is also a \( p \)-group, so its composition factors are all cyclic. It follows that the composition factors of \( \text{Aut}(\tilde{G}) \) are cyclic and projective special linear.

\[ \text{Theorem 1.2.} \quad \text{Gr1 is Turing reducible to Cl* in } n^{O(\log \log n)} \text{ time.} \]

\[ \text{Proof.} \quad \text{Let } G_m = 1 \triangleleft \cdots \triangleleft G_0 = G \text{ and } H_m = 1 \triangleleft \cdots \triangleleft H_0 = H \text{ be the radical derived series for two groups } G \text{ and } H \text{ and let } \tilde{F}_i = C(G_m/iG_{m-i}) = C(H_m/iH_{m-i}). \text{ We will first compute the isomorphisms } \text{Iso}(\tilde{G}, \tilde{H}) \text{ from } \tilde{G} \text{ to } \tilde{H} \text{ and then use this to find the isomorphisms } \text{Iso}(G,H) \text{ from } G \text{ to } H. \text{ If } G \text{ and } H \text{ are isomorphic, then Lemma 3.4 tells us that } \text{Iso}(\tilde{G}, \tilde{H}) \subseteq \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_m). \text{ Now, by the definition of the holomorph and Lemma 3.7, the composition factors of } \text{Hol}(\tilde{F}_i) \text{ are either cyclic or projective special linear for } 1 \leq i < m. \text{ Therefore, the composition factors of the normal subgroup } \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \text{ are all either cyclic or projective special linear. (As before, } \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \text{ denotes a direct product of copies of } \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \text{ indexed by } \tilde{F}_m). \text{ Since } \tilde{F}_m \text{ can be non-Abelian, } \text{Hol}(\tilde{F}_m) \text{ can have other composition factors which we must somehow eliminate if we are to place Gr1 in Cl*}. \]

\[ \text{We accomplish this using the results of [5], which show that a group of order } n \text{ that does not have any Abelian normal subgroups has at most } n^{O(\log \log n)} \text{ automorphisms and that all of them can be enumerated within the same bound. This implies that } |\text{Aut}(\tilde{F}_m)| \leq |\tilde{F}_m|^{O(\log \log |\tilde{F}_m|)} \leq n^{O(\log \log n)} \text{ where } n = |G| = |H| \text{ and that we can enumerate Aut}(\tilde{F}_m) \text{ within the same bound. Consequently, we can also enumerate Hol}(\tilde{F}_m) \text{ in } n^{O(\log \log n)} \text{ time.} \]

\[ \text{Therefore, we can transform our instance of Gr1 into } n^{O(\log \log n)} \text{ instances of Cl* as follows. For each } (f_m, \phi_m) \in \text{Hol}(\tilde{F}_m), \text{ we consider the coset } \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \cdot (f_m, \phi_m). \text{ Note that} \]

\[ \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_m) = \bigcup_{(f_m, \phi_m) \in \text{Hol}(\tilde{F}_m)} \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \cdot (f_m, \phi_m) \]

\[ \text{so it suffices to find the isomorphisms from } \tilde{G} \text{ to } \tilde{H} \text{ that are contained in each such coset and accumulate the results. For each } \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \cdot (f_m, \phi_m), \text{ we define a color isomorphism problem where we extend } \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \cdot (f_m, \phi_m) \text{ to act on the set} \]

\[ X = \left( \tilde{F}_1 \times_c \cdots \times_c \tilde{F}_m \right)^3. \]

\[ \text{Recalling that } \tilde{F}_1 \times_c \cdots \times_c \tilde{F}_m \text{ is the underlying set of both } \tilde{G} \text{ and } \tilde{H}, \text{ we solve the instance of Cl* that arises when we let } f_1 : X \to [n^3] \text{ and } f_2 : X \to [n^3] \text{ be the indicator functions on the subsets } \{(x, y, xy) \mid x, y \in \tilde{G}\} \text{ and } \{(x, y, xy) \mid x, y \in \tilde{H}\} \text{ of } X. \text{ This yields all isomorphisms from } \tilde{G} \text{ to } \tilde{H} \text{ that are contained in the coset } \left( \text{Hol}(\tilde{F}_1) \cdot \cdots \cdot \text{Hol}(\tilde{F}_{m-1}) \right)^{\tilde{F}_m} \cdot (f_m, \phi_m). \]

\[ \text{By taking the union of all of the isomorphisms found, we obtain Iso}(\tilde{G}, \tilde{H}) \text{ in } n^{O(\log \log n)} \text{ time.} \]

\[ \text{All that remains is to show how to compute } \text{Iso}(G,H) \text{ from } \text{Iso}(\tilde{G}, \tilde{H}). \text{ Since it was computed from } n^{O(\log \log n)} \text{ cosets, the description of } \text{Iso}(\tilde{G}, \tilde{H}) \text{ may use up to } n^{O(\log \log n)} \text{ generators. For convenience, we reduce this to } O(\log^2 n) \text{ generators in polynomial time using standard permutation group algorithms (cf. [34]). Using Definitions 3.1 and 3.2, we can define isomorphisms } \alpha : G \to \tilde{G} \text{ and } \beta : H \to \tilde{H}. \text{ Then } \text{Iso}(G,H) = \beta^{-1}\text{Iso}(\tilde{G}, \tilde{H})\alpha. \]

\[ \square \]
4 Reducing color isomorphism to a generalization of group isomorphism

In this section, we show that the problem of computing the isometry group of a bilinear map can be reduced to a generalization of group isomorphism in polynomial time. The first step is to construct a group whose structure depends on the bilinear map.

**Definition 4.1.** Let \( f : B \to A \times A \) be a bilinear map. Then we define \( G_f \) to be the group on the set \( B \times A \) with the operation \((b_1, a_1) \cdot (b_2, a_2) = (b_1b_2, a_1a_2f(b_1, b_2))\).

The fact that \( G_f \) is a group follows easily from the assumption that \( f \) is bilinear. Readers familiar with group cohomology theory will note that this is also a consequence of a construction from group cohomology involving factor sets (cf. [32]). Moreover, since \( A \leq Z(G) \), \( G_f/Z(G_f) \) is isomorphic to a subgroup of the Abelian group \( B \), so it follows that \( G_f \) is nilpotent of class at most 2.

**Proposition 4.2.** \( G_f \) is a nilpotent group of class at most 2.

Let \( b \in B \). It is convenient to define \( \ell(b) = (b, 0) \). We can then write \( \ell(b)a \) for \((b, a)\).

Our next step is to show that every isometry of \( f \) gives rise to an automorphism of \( G_f \).

**Lemma 4.3.** Let \( \beta : B \to B \) be an isometry of a bilinear map \( f : B \times B \to A \). Then the map \( \phi : G_f \to G_f \) defined by \( \phi(\ell(b)a) = \ell(\beta b)a \) is an automorphism of \( G_f \).

**Proof.** Let \( \ell(b_1)a_1, \ell(b_2)a_2 \in G_f \). Then
\[
\phi((\ell(b_1)a_1)(\ell(b_2)a_2)) = \phi(\ell(b_1b_2)f(b_1, b_2)a_1a_2) \\
= \ell(\beta(b_1)b_2))f(b_1, b_2)a_1a_2 \\
= \ell(\beta(b_1))\ell(\beta(b_2))f(\beta b_1, \beta b_2)^{-1}f(b_1, b_2)a_1a_2 \\
= \ell(\beta(b_1))a_1\ell(\beta(b_2))a_2 \\
= \phi(\ell(b_1)a_1)\phi(\ell(b_2)a_2)
\]
which completes the proof. \( \square \)

We also need to show that certain types of automorphisms of \( G_f \) yield isometries of \( f \). Our first step towards this goal is to prove the following characterization of which automorphisms of \( G_f \) that fix \( A \) induce isometries. For convenience, we identify \( B \) with \( G_f/A \) via \( b \mapsto \ell(b)A \). An automorphism \( \phi \) of \( G_f \) can then induces an automorphism \( \beta = \phi|_B \) of \( B \) by taking images of the cosets \( \ell(b)A \).

**Lemma 4.4.** Let \( f : B \times B \to A \) be a bilinear map and let \( \phi \in \text{Aut}(G_f) \) such that \( \phi|A = A \). Let \( \beta = \phi|_B : B \to B \) and define \( \ell_\phi = \phi \ell \beta^{-1} : B \to G_f \) and \( \varphi_\phi : B \to A \) by \( \varphi_\phi(b) = \ell(\beta(b))^{-1} \). Then \( \varphi_\phi \in \text{Hom}(B, A) \) if and only if \( f(b_1, b_2) = f(\beta^{-1}b_1, \beta^{-1}b_2) \) for all \( b_1, b_2 \in B \).
Proof. Let $b_1, b_2 \in B$. Then
\[
\varphi_\beta(b_1 b_2) = \ell(b_1 b_2) \left[ \phi \ell(\beta^{-1}(b_1 b_2)) \right]^{-1}
= \ell(b_1) \ell(b_2) f(b_1, b_2)^{-1} \left[ \phi \left[ \ell(\beta^{-1} b_1) \ell(\beta^{-1} b_2) f(\beta^{-1} b_1, \beta^{-1} b_2)^{-1} \right] \right]^{-1}
= \ell(b_1) \ell(b_2) \ell_\phi(b_1)^{-1} \ell_\phi(b_2)^{-1} f(b_1, b_2)^{-1} f(\beta^{-1} b_1, \beta^{-1} b_2)
= \ell(b_1) \ell_\phi(b_1)^{-1} \varphi_\beta(b_2) f(b_1, b_2)^{-1} f(\beta^{-1} b_1, \beta^{-1} b_2)
= \varphi_\beta(b_1) \varphi_\beta(b_2) f(b_1, b_2)^{-1} f(\beta^{-1} b_1, \beta^{-1} b_2)
\]

Now, $\varphi_\beta$ is a homomorphism if and only if $\varphi_\beta(b_1 b_2) = \varphi_\beta(b_1) \varphi_\beta(b_2)$ for all $b_1, b_2 \in B$. By the above calculation, this holds if and only if $f(b_1, b_2)^{-1} f(\beta^{-1} b_1, \beta^{-1} b_2) = 1$ for all $b_1, b_2 \in B$. \qed

Next, we show that every automorphism of $G_f$ that fixes the sets $A$ and $\ell[B]$ induces an isometry of $f$.

**Lemma 4.5.** Let $f : B \times B \to A$ be a bilinear map and let $\phi \in \text{Aut}(G_f)$ such that $\phi[A] = A$ and $\phi[\ell[B]] = \ell[B]$. Then $\beta = \phi|_B : B \to B$ is an isometry of $f$.

Proof. Let $b \in B$. Then $\phi(\ell(b)) \in \phi(\ell(b)A) = \ell(\beta b)A$. Since this holds for all $b \in B$, we have $\phi(\ell^{-1} b) \in \ell(b)A$. Since $\phi(\ell[B]) = \ell[B]$, we see that in fact, $\phi(\ell^{-1} b) = \ell(b)$. Hence, $\varphi_\beta = 1$, which is a homomorphism. Lemma 4.4 then implies that $\beta$ is an isometry of $f$. \qed

We are now ready to reduce $\text{Bl}$ to $\text{Grl}^*$.

**Theorem 1.6.** $\text{Bl}$ is polynomial-time many-one reducible to $\text{Grl}^*$.

Proof. Let $f : B \times B \to A$ be an instance of $\text{Bl}$ and construct the group $G_f$. The order of this group is $|A||B|$, which is polynomial in the size of our instance of $\text{Bl}$ by Definition 1.5. We wish to compute the subgroup $\text{Aut}(G_f)_{A,\ell[B]}$ of $\text{Aut}(G_f)$ that maps $A$ to $A$ and $\ell[B]$ to $\ell[B]$. This is a subgroup of $\text{Sym}(B) \times \text{Sym}(A)$ that acts on $G_f$ by $(\pi, \sigma)(\ell(b)a) = \ell(\pi b)\sigma a$. Therefore, we can compute $\text{Aut}(G_f)_{A,\ell[B]}$ of $\text{Aut}(G_f)$ by solving a $\text{Grl}^*$ problem for the group $\text{Sym}(B) \times \text{Sym}(A)$.

By Lemma 4.5 for each $\phi \in \text{Aut}(G_f)_{A,\ell[B]}$, $\beta = \phi|_B$ is an isometry of $f$. Moreover, by Lemma 4.3 for every isometry $\beta : B \to B$ of $f$, there is an automorphism $\phi \in \text{Aut}(G_f)_{A,\ell[B]}$ such that $\beta = \phi|_B$. It follows that we can compute the isometry group of $f$ from $\text{Aut}(G_f)_{A,\ell[B]}$ in polynomial time. Therefore, $\text{Bl}$ is many-one reducible to $\text{Grl}^*$ in polynomial time. \qed

**Acknowledgements**

We thank Laci Babai for discussing his Holomorph idea with us. FLG is supported by the Grant-in-Aid for Young Scientists (A) No. 16H05853 and the Grant-in-Aid for Scientific Research (A) No. 16H01705 of the Japan Society for the Promotion of Science, and the Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the Ministry of Education, Culture, Sports, Science and Technology in Japan. DJR was funded by a Japan Society for the Promotion of Science Postdoctoral Fellowship No. PE15020.
A Equivalence of CI and GI∗

We now give the proof of Theorem 1.3.

**Theorem 1.3.** CI and GI∗ are equivalent under polynomial-time many-one reductions.

**Proof.** We start with the reduction from GI∗ to CI. Let X and Y be graphs and suppose that we wish to find an isomorphism from X to Y in a subcoset σΓ the maps the vertices of X to those of Y. The reduction is immediate once we extend each σπ ∈ σΓ to map X × X to Y × Y and define colors according to the graphs X and Y.

The reduction from CI to GI∗ is slightly more complicated. Let σΓ be a subcoset of permutations acting on a set X and let \( f_1 : X \to [n] \) and \( f_2 : X \to [n] \) be as in Definition 1.1. We define graphs \( X_i \) for \( i \in \{1, 2\} \) as follows. The vertices of \( X_i \) consist of the vertices of X as well as certain gadgets that encode the colors. For each distinct \( f_i(x) \in f_i[X] \), we add a vertex labelled \( f_i(x) \) and create a copy \( K_{f_i(x)} \) of the complete graph on \( f_i(x) + 2 \) colors. We add an edge from the vertex \( f_i(x) \) to every vertex in \( K_{f_i(x)} \). Finally, we connect every vertex \( x' \neq x \in X \) such that \( f_i(x') = f_i(x) \) to the vertex \( f_i(x) \). Since complete subgraphs of size 3 or larger appear only as the gadgets \( K_{f_i(x)} \cup \{x_i(x)\} \), it is easy to see that the graph isomorphisms from \( X_1 \) to \( X_2 \) correspond precisely to the color isomorphisms of the set X. This completes the reduction. \( \square \)

---

\(^7\)For the purposes of the color isomorphism problem, we regard each \( σπ \) as a permutation of \( X \oplus Y \).
References

[1] V. Arvind and J. Toran. Solvable group isomorphism is (almost) in \( \mathbf{NP} \cap \mathbf{coNP} \). In 19th Annual IEEE Conference on Computational Complexity, pages 91–103, 2003.

[2] L. Babai. Graph isomorphism in quasipolynomial time [extended abstract]. In Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, pages 684–697, 2016, 1512.03547.

[3] L. Babai. Moderately exponential bound for graph isomorphism. In Proceedings of the 1981 International FCT-Conference on Fundamentals of Computation Theory, pages 34–50, 1981.

[4] L. Babai. Trading group theory for randomness. In Proceedings of the Seventeenth Annual ACM Symposium on the Theory of Computing, pages 421–429, 1985.

[5] L. Babai, P. Codenotti, J. A. Grochow, and Y. Qiao. Code equivalence and group isomorphism. In Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms, pages 1395–1408, 2011.

[6] L. Babai, P. Codenotti, and Y. Qiao. Polynomial-time isomorphism test for groups with no abelian normal subgroups (extended abstract). In 39th International Colloquium on Automata, Languages and Programming, pages 51–62, 2012.

[7] L. Babai, W. M. Kantor, and E. M. Luks. Computational complexity and the classification of finite simple groups. In Proceedings of the 24th Annual Symposium on Foundations of Computer Science, pages 162–171, 1983.

[8] L. Babai and E. M. Luks. Canonical labeling of graphs. In Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing, pages 171–183, 1983.

[9] L. Babai and Y. Qiao. Polynomial-time isomorphism test for groups with abelian Sylow towers. In 29th International Symposium on Theoretical Aspects of Computer Science, pages 453–464, 2012.

[10] R. B. Boppana, J. Håstad, and S. Zachos. Does \( \mathbf{coNP} \) have short interactive proofs? Information Processing Letters, 25(2):127–132, 1987.

[11] P. Brooksbank and J. Wilson. Computing isometry groups of hermitian maps. Transactions of the American Mathematical Society, 364(4):1975–1996, 2012.

[12] J. J. Cannon and D. F. Holt. Automorphism group computation and isomorphism testing in finite groups. Journal of Symbolic Computation, 35(3):241–267, 2003.

[13] P. Codenotti. Testing Isomorphism of Combinatorial and Algebraic Structures. PhD thesis, University of Chicago, 2011.

[14] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in \( \mathbf{NP} \) have zero-knowledge proof systems. Journal of the ACM, 38(3):690–728, 1991.
[15] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208, 1989.

[16] J. Grochow and Y. Qiao. Algorithms for group isomorphism via group extensions and cohomology. In *Proceedings of the 29th IEEE Conference on Computational Complexity*, pages 110–119, 2014, [1309.1776](https://arxiv.org/abs/1309.1776).

[17] J. A. Grochow and Y. Qiao. Polynomial-time isomorphism test of groups that are tame extensions. In *The 26th International Symposium on Algorithms and Computation*, pages 578–589, 2015, [1507.01917](https://arxiv.org/abs/1507.01917).

[18] C. J. Hillar and D. L. Rhea. Automorphisms of finite abelian groups. *The American Mathematical Monthly*, 114(10):917–923, 2007, [math/0605185](https://arxiv.org/abs/math/0605185).

[19] R. Impagliazzo and R. Paturi. Complexity of k-SAT. In *Proceedings of the Fourteenth Annual IEEE Conference on Computational Complexity*, pages 237–240, 1999.

[20] T. Kavitha. Linear time algorithms for Abelian group isomorphism and related problems. *Journal of Computer and System Sciences*, 73(6):986–996, 2007.

[21] F. Le Gall. Efficient isomorphism testing for a class of group extensions. In *26th International Symposium on Theoretical Aspects of Computer Science*, pages 625–636, 2009, [0812.2298](https://arxiv.org/abs/0812.2298).

[22] M. Lewis and J. Wilson. Isomorphism in expanding families of indistinguishable groups. *Groups-Complexity-Cryptology*, 4(1):73–110, 2012.

[23] R. Lipton, L. Snyder, and Y. Zalcstein. *The Complexity of Word and Isomorphism Problems for Finite Groups*. Defense Technical Information Center, 1977.

[24] E. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, 25(1):42–65, 1982.

[25] E. M. Luks. Group isomorphism with fixed subnormal chains. 2015, [1511.00151](https://arxiv.org/abs/1511.00151).

[26] P. P. Pálfy. A polynomial bound for the orders of primitive solvable groups. *Journal of Algebra*, 77(1):127–137, 1982.

[27] P. Papakonstantinou. The depth irreducibility hypothesis. *Electronic Colloquium on Computational Complexity*, 2014. TR14-124.

[28] L. Pyber. Asymptotic results for permutation groups. In *Workshop on Groups and Computation*, 1991.

[29] Y. Qiao, J. Sarma, and B. Tang. On isomorphism testing of groups with normal Hall subgroups. In *28th International Symposium on Theoretical Aspects of Computer Science*, pages 567–578, 2011.

[30] 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.
[31] D. J. Rosenbaum. Bidirectional collision detection and faster deterministic isomorphism testing. April 2013, arXiv:1304.3935. Submitted to Theoretical Computer Science.

[32] J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer, 1995.

[33] C. Savage. *An O(n^2) algorithm for Abelian group isomorphism*. Computer Studies Program, North Carolina State University, 1980.

[34] Á. Seress. *Permutation Group Algorithms*. Cambridge Tracts in Mathematics. Cambridge University Press, 2003.

[35] N. Vikas. An O(n) algorithm for Abelian p-group isomorphism and an O(n log n) algorithm for Abelian group isomorphism. *Journal of Computer and System Sciences*, 53(1):1–9, 1996.