On the Cayley isomorphism problem for Cayley objects of nilpotent groups of some orders

Edward Dobson

Department of Mathematics and Statistics
Mississippi State University
PO Drawer MA Mississippi State, MS 39762 U.S.A

dobson@math.msstate.edu

and

IAM
University of Primorska
6000 Koper, Slovenia

Submitted: Feb 11, 2013; Accepted: Jul 4, 2014; Published: Jul 21, 2014
Mathematics Subject Classifications: 05E18, 05C25, 20F18

Abstract

We give a necessary condition to reduce the Cayley isomorphism problem for Cayley objects of a nilpotent or abelian group G whose order satisfies certain arithmetic properties to the Cayley isomorphism problem of Cayley objects of the Sylow subgroups of G in the case of nilpotent groups, and in the case of abelian groups to certain natural subgroups. As an application of this result, we show that $\mathbb{Z}_q \times \mathbb{Z}_p^2 \times \mathbb{Z}_m$ is a CI-group with respect to digraphs, where q and p are primes with $p^2 < q$ and m is a square-free integer satisfying certain arithmetic conditions (but there are no other restrictions on q and p).

Keywords: Cayley object; Cayley graph; isomorphism; CI-group

1 Introduction

In 1967 Ádám [1] conjectured that any two circulant graphs of order n are isomorphic if and only if they are isomorphic by a group automorphism of $\mathbb{Z}_n$. While Ádám's conjecture was quickly shown to be false [4], the conjecture nonetheless generated much interest in the following question: Are two Cayley graphs of a group G isomorphic if and only if they are isomorphic by a group automorphism of G? If so, we say that G is a **CI-group with respect to graphs**. This problem naturally generalizes to any class of

combinatorial objects (see [11] for several equivalent formulations of the precise definition of a combinatorial object). Namely, is it true that two Cayley objects of a group G in some class $\mathcal{K}$ of combinatorial objects are isomorphic if and only if they are isomorphic by a group automorphism of G? If so, we say that **G is a CI-group with respect to $\mathcal{K}$**. If G is a CI-group with respect to *every* class of combinatorial objects, we say that G is a **CI-group**. In 1987, Pálfy [13] proved the following remarkable result:

Theorem 1. *A group G is a CI-group if and only if* $\gcd(n, \varphi(n)) = 1$ *or* $n = 4$*, where φ is Euler's phi function.*

While Pálfy's result is quite powerful, it does not tell us anything in general about isomorphisms between Cayley objects of a group G if G is not a CI-group, other than there exists isomorphic Cayley objects of G which are not isomorphic by a group automorphism of G. For such groups, we are then left with the question of if two Cayley objects of G are isomorphic, then what are the possible isomorphisms between them? This is sometimes known as the Cayley isomorphism problem. Usually, one would like the solution to this question to be a (hopefully) short list L of possible isomorphisms. That is, two Cayley objects of G are isomorphic if and only if they are isomorphic by a function in the list L. In 1999, Muzychuk [11] showed that if G is a cyclic group of order n and for any distinct primes p and q dividing n we have that q does not divide $p - 1$, then any two Cayley objects of G are isomorphic by an automorphism that can be found in a natural way from isomorphisms of Cayley objects of prime-power orders that divide n. Thus Muzychuk reduced the Cayley isomorphism problem for Cayley objects of cyclic groups of some orders to the Cayley isomorphism problem for Cayley objects of cyclic groups of prime-power orders. In 2003, the author [3], found a sufficient condition to extend Muzychuk's result to all abelian groups (with the same order conditions), and showed this sufficient condition was satisfied by some abelian groups. In this paper, we extend the author's earlier result to nilpotent groups, as well as to abelian groups with more general order conditions (Theorem 14). Finally, as an application we will extend the list of CI-groups with respect to digraphs by showing that $\mathbb{Z}_q \times \mathbb{Z}_p^2 \times \mathbb{Z}_m$ is a CI-group with respect to digraphs, where p and q are distinct primes with $p^2 < q$ and m satisfies certain arithmetic conditions (Theorem 31).

Throughout this paper, G is a finite group. For group theoretic terms not defined in this paper, see [2]. We begin with some definitions.

Definition 2. Let G be a transitive group acting on Ω. Let X be the set of all complete block systems of G. Define a partial order on X by $\mathcal{B} \preceq \mathcal{C}$ if and only if every block of $\mathcal{C}$ is a union of blocks of $\mathcal{B}$. We define $\mathcal{B}|_C$ to be the complete block system of $\mathrm{Stab}_G(C) = \{g \in G : g(C) = C\}$, the **set-wise stabilizer of $C \in \mathcal{C}$**, consisting of all those blocks of $\mathcal{B}$ that are contained in C, $C \in \mathcal{C}$, and remark that $\mathcal{B}|_C$ is a complete block system of $\mathrm{Stab}_G(C)$ in its action on C. By $\mathrm{fix}_G(\mathcal{B})$ we mean the subgroup of G which fixes each block of $\mathcal{B}$ set-wise. That is, $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for all } B \in \mathcal{B}\}$. We denote by $\mathrm{Stab}_G(x)$ the stabilizer of $x \in X$. That is, $\mathrm{Stab}_G(x) = \{g \in G : g(x) = x\}$. Finally, $g \in G$ induces a natural permutation $g/\mathcal{B}$ in $S_{\mathcal{B}}$, and we set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$.

Definition 3. Let $n = \Pi_{i=1}^{r} p_i^{a_i}$ be the prime factorization of n and define $\Omega : \mathbb{N} \mapsto \mathbb{N}$ by $\Omega(n) = \Sigma_{i=1}^{r} a_i$. Setting $m = \Omega(n)$, we say a transitive group G of degree n is ***m*-step imprimitive** if there exists a sequence of complete block system $\mathcal{B}_0 \prec \mathcal{B}_1 \prec \ldots \prec \mathcal{B}_m$. Note that $\mathcal{B}_0$ consists of singletons, while $\mathcal{B}_m$ consists of the entire set on which G acts. A complete block system $\mathcal{B}$ will be said to be **normal** if $\mathcal{B}$ is formed by the orbits of a normal subgroup. We will say that G is **normally *m*-step imprimitive** if each $\mathcal{B}_i$, $0 \leqslant i \leqslant m$, is formed by the orbits of a normal subgroup of G.

2 The main tool

In this section, we will give a sufficient condition that will imply that the Cayley isomorphism problem for nilpotent groups of certain orders can be reduced to the Cayley isomorphism problem for groups of prime-power order (Theorem 14 and Corollary 15), and for abelian groups with more general arithmetic conditions (Theorem 14). That these results have implications for the Cayley isomorphism problem is established in Theorem 26. The following result is straightforward, and so its proof is omitted.

Lemma 4. *Let $G_1, G_2 \leqslant S_n$ be transitive such that both G_1 and G_2 admit $\mathcal{B}$ as a complete block system. Then $\langle G_1, G_2 \rangle$ admits $\mathcal{B}$ as a complete block system.*

The following result is trivial after observing that the hypothesis implies that $\mathrm{fix}_G(\mathcal{B}) = \mathrm{Stab}_G(B)$.

Lemma 5. *Let $G \leqslant S_n$ be m-step imprimitive with sequence $\mathcal{B}_0, \ldots, \mathcal{B}_m$. If $G/\mathcal{B}_{m-1}$ is cyclic of prime order p, then $\mathrm{fix}_G(\mathcal{B}_{m-1})|_B$ is $(m-1)$-step imprimitive for every $B \in \mathcal{B}_{m-1}$, with $(m-1)$-step imprimitivity sequence $\mathcal{B}_0|_B, \ldots, \mathcal{B}_{m-1}|_B$.*

We will use the following basic (and known) result implicitly throughout the paper.

Lemma 6. *Let $G \leqslant S_n$ be transitive with $H \leqslant G$ a transitive abelian subgroup. Then every complete block system of G is normal and is formed by the orbits of a normal subgroup of H.*

Proof. Let $\mathcal{B}$ be a complete block system of G consisting of m blocks of size k. As a transitive abelian group is regular [14, Proposition 1.4.4], we have that $H/\mathcal{B}$ is regular of degree m, so that $\mathrm{fix}_H(\mathcal{B}) \neq 1$ and has order k. As $\mathrm{Stab}_H(B) = \mathrm{fix}_H(\mathcal{B})$ for every $B \in \mathcal{B}$ and $\mathrm{Stab}_H(B)|_B$ is transitive [2, Exercise 1.5.6], we have that $\mathrm{fix}_H(\mathcal{B})|_B$ is transitive for every $B \in \mathcal{B}$. As the blocks of $\mathcal{B}$ have size k, we conclude that the orbits of $\mathrm{fix}_H(\mathcal{B}) \leqslant \mathrm{fix}_G(\mathcal{B})$ form $\mathcal{B}$. □

Definition 7. Let G be a permutation group acting on X and H a permutation group acting on Y. Define the **wreath product of *G* and *H***, denoted $G \wr H$, to be the group of all permutations of $G \times H$ of the form $(x, y) \to (g(x), h_x(y))$.

Lemma 8. *Let n be a positive integer and G_1, G_2 be transitive abelian groups of degree n such that $\langle G_1, G_2\rangle$ is m-step imprimitive. Let $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ be the prime-power decomposition of n. Then there exists $\delta \in \langle G_1, G_2\rangle$ and a sequence of primes $q_1, \ldots, q_m$ such that $n = q_1 \cdots q_m$ and $\langle G_1, \delta^{-1}G_2\delta\rangle$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_m)))$. Furthermore, if $\langle G_1, G_2\rangle$ is solvable, then we may take $\delta = 1$.*

Proof. We proceed by induction on m. If $m = 1$, then n is prime, and both G_1 and G_2 are Sylow n-subgroups of S_n. Hence there exists $\delta \in \langle G_1, G_2\rangle$ such that $\delta^{-1}G_2\delta = G_1$, and the result is trivial as $\langle G_1, \delta^{-1}G_2\delta\rangle$ is cyclic of order n. Now assume that the result is true for all $m - 1 \geqslant 1$, and let G_1, G_2 be transitive abelian groups of degree n, where $\Omega(n) = m$, such that $\langle G_1, G_2\rangle$ is m-step imprimitive.

As $\langle G_1, G_2\rangle$ is m-step imprimitive, $\langle G_1, G_2\rangle$ admits a normal complete block system $\mathcal{B}$ consisting of n/q_m blocks of size q_m for some prime $q_m|n$, and both $G_1/\mathcal{B}$ and $G_2/\mathcal{B}$ are transitive abelian groups of degree n/q_m and $\Omega(n/q_m) = m - 1$. Furthermore, as $\langle G_1, G_2\rangle$ is m-step imprimitive, $\langle G_1, G_2\rangle/\mathcal{B}$ is $(m-1)$-step imprimitive by [3, Lemma 8], so by the induction hypothesis, there exists $\delta_1 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_1^{-1}G_2\delta\rangle/\mathcal{B}$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_{m-1})))$ for some sequence of primes $q_1, \ldots, q_{m-1}$ such that $n/q_m = q_1 \cdots q_{m-1}$, and if $\langle G_1, G_2\rangle$ is solvable, we may take $\delta_1 = 1$. Furthermore, $\mathrm{fix}_{G_1}(\mathcal{B})$ is semiregular of order q_m, and $\mathrm{fix}_{\delta_1^{-1}G_2\delta_1}(\mathcal{B})$ is also semiregular of order q_m. Hence there exists $\delta_2 \in \mathrm{fix}_{\langle G_1, \delta_1^{-1}G_2\delta_1\rangle}(\mathcal{B})$ such that $\delta_2^{-1}\mathrm{fix}_{\delta_1^{-1}G_2\delta_1}(\mathcal{B})\delta_2$ is contained in the same Sylow q_m-subgroup of $\mathrm{fix}_{\langle G_1, \delta_1^{-1}G_2\delta_1\rangle}(\mathcal{B})$ as $\mathrm{fix}_{G_1}(\mathcal{B})$. If $\langle G_1, G_2\rangle$ is solvable, then $\mathrm{fix}_{\langle G_1, G_2\rangle}(\mathcal{B})$ is solvable, so $\mathrm{fix}_{\langle G_1, G_2\rangle}(\mathcal{B})|_B$ is solvable, and by [2, Exercise 3.5.1], $\mathrm{fix}_{\langle G_1, G_2\rangle}(\mathcal{B})|_B$ has a unique Sylow q_m-subgroup, so we may take $\delta_2 = 1$. Let $\delta = \delta_1\delta_2$. As a Sylow q_m-subgroup of $\mathrm{fix}_{\langle G, \delta^{-1}G\delta\rangle}(\mathcal{B})$ is contained in $1_{S_{n/q_m}} \wr \mathbb{Z}_{q_m}$ we have that both G_1 and $\delta^{-1}G_2\delta$ normalize $1_{S_{n/q_m}} \wr \mathbb{Z}_{q_m}$. This then implies that $\mathrm{Stab}_{\langle G_1, \delta^{-1}G_2\delta\rangle}(B)|_B$ has a normal Sylow q_m-subgroup, so that $\mathrm{Stab}_{\langle G_1, \delta^{-1}G_2\delta\rangle}(B)|_B$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_m)$ for every $B \in \mathcal{B}$. It then follows by the Embedding Theorem [9, Theorem 2.6], that $\langle G_1, \delta^{-1}G_2\delta\rangle$ is permutation isomorphic to a subgroup of $\mathrm{AGL}(1, q_1) \wr (\mathrm{AGL}(1, q_2) \wr (\cdots \wr \mathrm{AGL}(1, q_m)))$, and the result follows by induction. □

Definition 9. Let π be a set of primes. A **π-group** G is a group such that every prime divisor of $|G|$ is contained in π. A subgroup H of G is an **S_π-subgroup of G** if no prime in π divides $|G|/|H|$. By π', we denote the set of primes dividing $|G|$ that are not contained in π.

We shall have need a consequence of the preceding result.

Lemma 10. *Let n be a positive integer and π be the set of distinct prime numbers dividing n. If G_1, G_2 are transitive abelian groups of degree n such that $\langle G_1, G_2\rangle$ is m-step imprimitive then there exists $\delta \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta^{-1}G_2\delta\rangle$ is a solvable π-group.*

Proof. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the prime-power decomposition of n. By Lemma 8, there exists $\delta_1 \in \langle G_1, G_2\rangle$ and a sequence $q_1, \ldots, q_m$ of primes such that $n = q_1 \cdots q_m$ and

$\langle G_1, \delta_1^{-1}G_2\delta_1\rangle \leqslant \mathrm{AGL}(1,q_1) \wr (\mathrm{AGL}(1,q_2) \wr (\cdots \wr \mathrm{AGL}(1,q_m)))$. As $\mathrm{AGL}(1,q_i)$ is solvable for every $1 \leqslant i \leqslant m$, $\langle G_1, \delta_1^{-1}G_2\delta_1\rangle$ is solvable. By Hall's Theorem [5, Theorem 6.4.1], we have that G_1 is contained in an S_π-subgroup H_1 of $\langle G_1, \delta_1^{-1}G_2\delta_1\rangle$ and that G_2 is contained in an S_π-subgroup H_2 of $\langle G_1, \delta_1^{-1}G_2\delta_1\rangle$. Also by Hall's Theorem, there exists $\delta_2 \in \langle G_1, \delta_1^{-1}G_2\delta_1\rangle$ such that $\delta_2^{-1}H_2\delta = H_1$. Let $\delta = \delta_1\delta_2$. Then $\langle G_1, \delta^{-1}G_2\delta\rangle \leqslant H_1$, and H_1 is a solvable π-group. □

Let $\mathcal{L} = \mathcal{L}_G$ be the set of all normal complete block systems of a transitive group G. Then $\preceq$ is a canonical partial order on $\mathcal{L}$. Define operations $\cup$ and $\cap$ on $\mathcal{L}$ by $\mathcal{B} \cup \mathcal{C}$ is the normal complete block system of G formed by the orbits of $\langle \mathrm{fix}_G(\mathcal{B}), \mathrm{fix}_G(\mathcal{C})\rangle = \mathrm{fix}_G(\mathcal{B}) \cdot \mathrm{fix}_G(\mathcal{C})$ (as both of these groups are normal), and $\mathcal{B} \cap \mathcal{C}$ is the normal complete block system of G formed by the orbits of $\mathrm{fix}_G(\mathcal{B}) \cap \mathrm{fix}_G(\mathcal{C})$. Notice that both of these operation do in fact give normal complete block systems as $\langle \mathrm{fix}_G(\mathcal{B}), \mathrm{fix}_G(\mathcal{C})\rangle \triangleleft G$ and $\mathrm{fix}_G(\mathcal{G}) \cap \mathrm{fix}_G(\mathcal{C}) \triangleleft G$. Thus $\mathcal{L}_G$ is a lattice. See [6] for terms regarding lattices not defined here. We also have that

Lemma 11. *If G contains a transitive abelian group H, then $\mathcal{L}_G$ is a modular lattice.*

Proof. We must show that if $\mathcal{B} \preceq \mathcal{A}$, then $\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C}) = \mathcal{B} \cup (\mathcal{A} \cap \mathcal{C})$. By Lemma 6, there exists $A, B, C \leqslant H$ such that $\mathcal{A}$ is formed by the orbits of A, $\mathcal{B}$ is formed by the orbits of B, and $\mathcal{C}$ is formed by the orbits of C. As $\mathcal{B} \preceq \mathcal{A}$, we have that $B \leqslant A$. By [6, Theorem 8.4.1], we have that $A \cap (B \cdot C) = B \cdot (A \cap C)$. Then the orbits of $A \cap (B \cdot C)$ are the same as the orbits of $B \cdot (A \cap C)$. □

We remark that the previous result is contained in [12, Theorem 2.10]

In the following three results, we will have in the hypothesis that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$. Notice that this implies that $\gcd(n_i, n_j) = 1$, and that if $p_i | n_i$ is prime, then p_i does not divide $p_j - 1$ for any prime $p_j | n_j$.

Lemma 12. *Let $n_1, \ldots, n_r$ be positive integers such that if $i \neq j$, then $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$, π_i the set of primes dividing n_i, and H_i be a transitive, solvable, π_i-group of degree n_i, $1 \leqslant i \leqslant r$. Let G be a transitive m-step imprimitive subgroup of $\Pi_{i=1}^r H_i$ acting coordinate-wise, where $\Omega(n_1 \cdots n_r) = m$. Then there exists transitive subgroups $L_i \leqslant H_i$ such that $G = \Pi_{i=1}^r L_i$.*

Proof. It is not difficult to see that $\Pi_{i=1}^r H_i$ admits complete block systems $\mathcal{C}_i$ consisting of n/n_i blocks of size n_i, $1 \leqslant i \leqslant r$, formed by the orbits of H_i. As each H_i is solvable, we have that G is solvable, and so contains an S_{π_i}-subgroup L_i for every $1 \leqslant i \leqslant r$. As $\Pi_{i=1}^r H_i/\mathcal{C}_i$ is a π_i'-group, $G/\mathcal{C}_i$ is also a π_i'-group, and so $\mathrm{fix}_G(\mathcal{C}_i) = L_i$. Then $L_i \cap L_j = 1$ for every $i \neq j$, $L_i \triangleleft G$, and $\langle L_i : 1 \leqslant i \leqslant r\rangle = G$. The result now follows. □

We now need only one more tool to prove the main result (Theorem 14) of this section. Before proceeding to this last tool, it will be useful to develop some terminology which will simplify the statement. First, the proof of Theorem 14 will proceed by induction on $m = \Omega(n)$. So when proving Theorem 14, we will be assuming that the conclusion of Theorem 14 holds for all integers n/p, where p divides n is prime. In particular, with

$m, n_1, \ldots, n_r$ and n satisfying the hypothesis of Theorem 14 and G_1, G_2 transitive abelian or nilpotent groups of degree n, then whenever K_1, K_2 are transitive nilpotent or abelian groups of degree n/p - and to simplify our notation, there is no harm in assuming that $p|n_1$ - such that $\langle K_1, K_2\rangle$ are $(m-1)$-step imprimitive, then there exists $\delta \in \langle K_1, K_2\rangle$ such that $\langle K_1, \delta^{-1}K_2\delta\rangle \leqslant \Pi_{i=1}^r \bar{H}_i$, where $\bar{H}_i$ is a solvable $\bar{\pi}_i$ group of degree $\bar{n}_i$. Here $\bar{n}_i = n_i$ if $i \neq 1$ while $\bar{n}_1 = n_1/p$, and $\bar{\pi}_i$ is the set of prime divisors of $\bar{n}_i$. In this situation, we will say that n **satisfies the main induction hypothesis**.

Lemma 13. *Let $n_1, \ldots, n_r$ be positive integers such that if $i \neq j$, then $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$. Let $n = n_1 \cdots n_r$ with $\Omega(n) = m$, $p|n$ (and without loss of generality, $p|n_1$), and $\bar{\pi} = \cup_{j\in I}\bar{\pi}_j$ for some $I \subseteq [r]$. If*

1. *n satisfies the main induction hypothesis,*
2. *$\langle G_1, G_2\rangle$ is m-step imprimitive,*
3. *$\langle G_1, G_2\rangle$ admits a complete block system $\mathcal{B}$ of p blocks of size n/p, and*
4. *$\langle G_1, G_2\rangle/\mathcal{B}$ is a p-group,*

then there exists $\delta \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta^{-1}G_2\delta\rangle$ admits a complete block system formed by the orbits of the unique $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$, $i = 1, 2$.

Proof. Let $B \in \mathcal{B}$ and $K_i = \mathrm{fix}_{G_i}(\mathcal{B})|_B$, $i = 1, 2$. As $\langle G_1, G_2\rangle/\mathcal{B}$ has prime order p, we must have that $\mathrm{Stab}_{\langle G_1,G_2\rangle}(B) = \mathrm{fix}_{\langle G_1,G_2\rangle}(\mathcal{B})$. Note that K_i is transitive on B, and if G_i is nilpotent or abelian, then K_i is nilpotent or abelian, $i = 1, 2$. Clearly $\mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B}) \leqslant \mathrm{fix}_{\langle G_1,G_2\rangle}(\mathcal{B})$. By Lemma 5, $\mathrm{fix}_{\langle G_1,G_2\rangle}(\mathcal{B})|_B$ is $(m-1)$-step imprimitive, so that $\langle K_1, K_2\rangle$ is $(m-1)$-step imprimitive.

By hypothesis, there exists $\delta_1 \in \langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle$ such that

$$\langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\rangle|_B \leqslant \Pi_{j=1}^r \bar{H}_{B,j},$$

where each $\bar{H}_{B,j}$ is a transitive solvable $\bar{\pi}_j$-group of degree $\bar{n}_j$. Similarly, if $B \neq B' \in \mathcal{B}$, then there exists $\delta_2 \in \langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\rangle$ such that

$$\langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_2^{-1}\delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\delta_2\rangle|_{B'} \leqslant \Pi_{j=1}^r \bar{H}_{B',j},$$

where each $\bar{H}_{B',j}$ is a transitive solvable $\bar{\pi}_j$-group of degree $\bar{n}_j$. Furthermore, we have that $\delta_2|_B \in \langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\rangle|_B$. This then implies that

$$\langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_2^{-1}\delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\delta_2\rangle|_B \leqslant \langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\rangle|_B.$$

Hence $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta_2^{-1}\delta_1^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta_1\delta_2\rangle|_B \leqslant \Pi_{j=1}^r \bar{H}_{B,j}$. Continuing inductively, we have that there exists $\delta \in \langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle$ such that $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \delta^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta\rangle|_B \leqslant \Pi_{j=1}^r \bar{H}_{B,j}$ for every $B \in \mathcal{B}$, where each $\bar{H}_{B,j}$ is a transitive solvable $\bar{\pi}_j$-group of degree $\bar{n}_j$. Note that $\delta^{-1}\mathrm{fix}_{G_2}(\mathcal{B})\delta = \mathrm{fix}_{\delta^{-1}G_2\delta}(\mathcal{B})$ as $\delta/\mathcal{B} = 1$. For ease of notation, we will replace $\delta^{-1}G_2\delta$ by G_2 and thus assume without loss of generality that $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle|_B \leqslant$

$\Pi_{j=1}^r H_{B,j}$ for each $B \in \mathcal{B}$. By Lemma 12, we may assume without loss of generality that $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle|_B = \Pi_{j=1}^r \bar{H}_{B,j}$ for each $B \in \mathcal{B}$.

As $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle|_B = \Pi_{j=1}^r H_{B,j}$ for each $B \in \mathcal{B}$, $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle|_B$ has a normal subgroup L_B with orbits of size $\Pi_{j\in I}\bar{n}_j$, and so $\langle \mathrm{fix}_{G_1}(\mathcal{B}), \mathrm{fix}_{G_2}(\mathcal{B})\rangle|_B$ admits a complete block system $\mathcal{C}_B$ formed by the orbits of L_B, $B \in \mathcal{B}$. Also note that the $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})|_B$ must be contained in L_B, as otherwise $(\mathrm{fix}_{G_i}(\mathcal{B})|_B)/\mathcal{C}_B$ contains a nontrivial normal subgroup with orbits of size dividing $\Pi_{j\in I}\bar{n}_j$, $i = 1, 2$. However, $(\mathrm{fix}_{G_i}(\mathcal{B})|_B)/\mathcal{C}_B$ is a solvable $\bar{\pi}'$-subgroup and $\gcd(\Pi_{j\in I}\bar{n}_j, \Pi_{j\notin I, j\in[r]}\bar{n}_j) = 1$, $i = 1, 2$, a contradiction. Then $\mathrm{fix}_{G_i}(\mathcal{B})|_B$, $i = 1, 2$, admit complete block systems $\mathcal{D}_B$ formed by the orbits of their unique $S_{\bar{\pi}}$-subgroups, respectively, and these complete block systems must be precisely $\mathcal{C}_B$, for $B \in \mathcal{B}$.

Let $\mathcal{C} = \cup_{B\in\mathcal{B}}\mathcal{C}_B$. Clearly a normal $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$ has relatively prime order and index in $\mathrm{fix}_{G_k}(\mathcal{B})$, $i = 1, 2$. Hence by [6, Theorem 1.1.13], an $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$ is characteristic in $\mathrm{fix}_{G_i}(\mathcal{B})$, $i = 1, 2$. Whence an $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$ is normal in G_i, $i = 1, 2$. Thus G_i admits complete block systems formed by the orbits of the $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$, $i = 1, 2$. As each $\mathcal{C}_B$ is formed by the orbits of the $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$ restricted to the block $B \in \mathcal{B}$, the orbits of the $S_{\bar{\pi}}$-subgroup of $\mathrm{fix}_{G_i}(\mathcal{B})$ form the complete block system $\mathcal{C}$, $i = 1, 2$. Hence $\mathcal{C}$ is a block system of G_i, $i = 1, 2$, and so by Lemma 4, $\mathcal{C}$ is a complete block system of $\langle G_1, G_2\rangle$. □

We now prove the main result of this section.

Theorem 14. *Let $n_1, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ if $i \neq j$, and π_i be the set of distinct prime numbers dividing n_i. Let $n = n_1 \cdots n_r$ and $m = \Omega(n)$. If either*

1. *each n_i is a prime-power, and G_1, G_2 are transitive nilpotent groups of degree n such that $\langle G_1, G_2\rangle$ is m-step imprimitive, or*

2. *G_1, G_2 are transitive abelian groups of degree n such that $\langle G_1, G_2\rangle$ is m-step imprimitive,*

then there exists $\delta \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta^{-1}G_2\delta\rangle = \Pi_{i=1}^r H_i$, where each H_i is a transitive solvable π_i-group of degree n_i.

Proof. Throughout the proof, if case (1) holds, we let p_i be prime such that $n_i = p_i^{a_i}$, $a_i \geqslant 1$. First suppose that case (1) holds and $r = 1$. Then $G_1 \leqslant \Pi_1$, $G_2 \leqslant \Pi_2$, where Π_1, Π_2 are Sylow p_1-subgroups of $\langle G_1, G_2\rangle$. By a Sylow Theorem, there exists $\delta \in \langle G_1, G_2\rangle$ such that $\delta^{-1}G_2\delta \leqslant \Pi_1$. Then $\langle G_1, \delta^{-1}G_2\delta\rangle$ is a p_1-group and so nilpotent.

In both cases, we proceed by induction on m. Suppose that $m = 1$. Then the only case that occurs is case (1) and $r = 1$. The result then follows by arguments above. Assume that the result is true for all G_1 and G_2 that satisfy the hypothesis with $\Omega(n) = m-1 \geqslant 1$, and let $G_1, G_2 \leqslant S_n$ satisfy the hypothesis where $\Omega(n) = m$. In case (1), by arguments above, we may assume that $r \geqslant 2$. In case (2), if $r = 1$ then the result follows from Lemma 10, so in any case we may assume without loss of generality that $r \geqslant 2$. Let $\mathcal{B}_1$

be a complete block system of $\langle G_1, G_2\rangle$ consisting of p_i blocks of size n/p_i, where $p_i|m_i$. Then $\mathcal{B}_1$ is a complete block system of both G_1 and G_2. As both G_1 and G_2 are nilpotent, $G_1/\mathcal{B}_1$ and $G_2/\mathcal{B}_1$ are nilpotent. We conclude that both $G_1/\mathcal{B}_1$ and $G_2/\mathcal{B}_1$ are p_i-groups. Hence there exists $\delta_1 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta^{-1}G_1\delta\rangle/\mathcal{B}_1$ has order p_i. We thus assume without loss of generality that $\langle G_1, G_2\rangle/\mathcal{B}_1$ has order p_i.

Let $\pi = \cup_{j\in J}\pi_j$ where $J = [r] - \{i\}$. As $|G_1/\mathcal{B}_1| = |G_2/\mathcal{B}_1| = p_i$, the S_π-subgroups of G_1 and G_2 are contained in $\mathrm{fix}_{\langle G_1,G_2\rangle}(\mathcal{B}_1)$. By Lemma 13 and the induction hypothesis, there exists $\delta_2 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_2^{-1}G_2\delta_2\rangle$ admits a complete block system $\mathcal{C}$ of n_i blocks of size n/n_i formed by the S_π-subgroups of G_1 and G_2. We thus assume without loss of generality that $\langle G_1, G_2\rangle$ admits $\mathcal{C}$ as a complete block system. Similarly, by Lemma 13 and the induction hypothesis, there exists $\delta_3 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_3^{-1}G_2\delta_3\rangle$ admits a complete block system $\mathcal{D}$ formed by the orbits of an S_{π_i}-subgroup of $\mathrm{fix}_{G_k}(\mathcal{B}_1)$, $k = 1, 2$, (we remark that if n_i is prime, then $\mathcal{D}$ is trivial). We thus also assume without loss of generality that $\langle G_1, G_2\rangle$ admits $\mathcal{D}$ as well.

If $n_i \neq p_i$, then $\langle G_1, G_2\rangle/\mathcal{D}$ is $(m - (a_i - 1))$-step imprimitive, where $\Omega(n_i) = a_i$, and $G_k/\mathcal{D}$ is nilpotent, $k = 1, 2$. Hence by the induction hypothesis there exists $\delta_4 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_4^{-1}G_2\delta_4\rangle/\mathcal{D} \leqslant P_i \times \Pi_{j=1,j\neq i}^r H_j'$, where $H_j' \leqslant S_{n_j}$ is a transitive solvable π_j-group, and P_i is a p_i-group of degree p_i. Then $\langle G_1, \delta_4^{-1}G_2\delta_4\rangle/\mathcal{D}$ admits a complete block system $\mathcal{E}'$ of $n/(n_i/p_i)$ blocks of size p_i, so that $\langle G_1, \delta_4^{-1}G_2\delta_4\rangle$ admits a complete block system $\mathcal{E}$ of n/n_i blocks of size n_i.

If $n_i = p_i$, then as $\langle G_1, G_2\rangle$ is m-step imprimitive, $\langle G_1, G_2\rangle$ admits a complete block system $\mathcal{B}_2$ such that $\mathcal{B}_2 \preceq \mathcal{B}_1$ and $\mathcal{B}_2$ consists of p_ip_j blocks of size $n/(p_ip_j)$ for some $p_j|n_j$ with $j \neq i$. Then $G_1/\mathcal{B}_2$ and $G_2/\mathcal{B}_2$ are nilpotent and transitive. We conclude that $G_1/\mathcal{B}_2$ and $G_2/\mathcal{B}_2$ are cyclic. By Theorem 1, there exists $\delta_3 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_3^{-1}G_2\delta_3\rangle/\mathcal{B}_2$ is cyclic. We thus assume without loss of generality that $\langle G_1, G_2\rangle/\mathcal{B}_2$ is cyclic. Thus $\langle G_1, G_2\rangle/\mathcal{B}_2$ admits a complete block system of p_j blocks of size p_i, so that $\langle G_1, G_2\rangle$ admits a complete block system $\mathcal{B}_1'$ of p_j blocks of size n/p_j, and by Lemma 5 $\mathrm{fix}_{\langle G_1,G_2\rangle}(\mathcal{B}_1')|_{B'}$ is $(m-1)$-step imprimitive for every $B' \in \mathcal{B}_1'$. Hence by Lemma 13, there exists $\delta_4 \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta_4^{-1}G_2\delta_4\rangle$ admits a complete block system $\mathcal{E}$ of n/n_i blocks of size n_i formed by the orbits of an S_{π_i}-subgroup of $\mathrm{fix}_{G_k}(\mathcal{B}_1')$, $k = 1, 2$. Hence regardless of the value of n_i, we may assume without loss of generality that $\langle G_1, G_2\rangle$ admits $\mathcal{C}$ and $\mathcal{E}$ as complete block systems. As $\langle G_1, G_2\rangle$ admits a complete block system $\mathcal{C}$ of n_i blocks of size n/n_i, $\langle G_1, G_2\rangle \leqslant S_{n_i} \wr S_{n/n_i}$. As $\langle G_1, G_2\rangle$ also admits $\mathcal{E}$ as a complete block system and $\gcd(n_i, n/n_i) = 1$, we have that $\langle G_1, G_2\rangle \leqslant S_{n/n_i} \wr S_{n_i}$. We conclude that $\langle G_1, G_2\rangle \leqslant (S_{n_i} \wr S_{n/n_i}) \cap (S_{n/n_i} \wr S_{n_i}) = S_{n_i} \times S_{n/n_i}$. We now consider (1) and (2) separately.

(1) By the induction hypothesis, we may, after a suitable conjugation, assume that $\langle G_1, G_2\rangle/\mathcal{D} \leqslant \Pi_{j\in[r]-\{i\}}S_{m_j}$, so that $\langle G_1, G_2\rangle \leqslant \Pi_{j=1}^r S_{m_j}$. The result then follows by inductively applying a Sylow Theorem and then Lemma 12.

(2) By Lemma 6 every complete block system is a normal complete block system. As $\mathcal{L}_{\langle G_1,G_2\rangle}$ is a modular lattice by Lemma 11, it follows by the Jordan-Dedekind Chain Condition [6, pg. 119] that all finite chains between two elements have the same length. As $\langle G_1, G_2\rangle$ admits $\mathcal{E}$ as a complete block system, any maximal chain between the complete

block systems consisting of singletons and the complete block system consisting of one block that contain $\mathcal{E}$ must have length m as $\langle G_1, G_2\rangle$ is normally m-step imprimitive. We conclude that $\langle G_1, G_2\rangle/\mathcal{E}$ is $(m-a_i)$-step imprimitive, so by the induction hypothesis we may assume after a suitable conjugation that $\langle G_1, G_2\rangle/\mathcal{E} \leqslant \Pi_{j=1, j\neq i}^{r} H_j$, where $H_j \leqslant S_{n_j}$ is a transitive solvable π_j-group. Similarly, we may assume that $\langle G_1, G_2\rangle/\mathcal{C} \leqslant H_i$, where H_i is a transitive solvable π_i-group. As $C \cap E$ is a singleton, for every $C \in \mathcal{C}$, $E \in \mathcal{E}$, we have that $\langle G_1, G_2\rangle \leqslant \Pi_{j=1}^{r} H_j$. By Lemma 12, we may assume that $\langle G_1, G_2\rangle = \Pi_{j=1}^{r} H_j$ as required. The result then follows by induction. □

It may be worthwhile restating Theorem 14 (1) in the following form:

Corollary 15. *Let $n = p_1^{a_1} \cdots p_r^{a_r}$, the prime-power decomposition of n, be such that $p_i \not| (p_j - 1)$, $1 \leqslant i, j \leqslant r$. Let $\Omega(n) = m$. If G_1, G_2 are transitive nilpotent groups of degree n such that $\langle G_1, G_2\rangle$ is m-step imprimitive, then there exists $\delta \in \langle G_1, G_2\rangle$ such that $\langle G_1, \delta^{-1} G_2 \delta\rangle$ is nilpotent.*

3 Solving Sets

In this section, we further develop the terminology regarding solving sets as well as the characterizations of when a particular set is a solving set that will be needed for our main results.

Definition 16. Let G be a group and define $g_L : G \to G$ by $g_L(x) = gx$. Let $G_L = \{g_L : g \in G\}$. Then G_L is the **left-regular representation of G**. We define a **Cayley object of G** to be a combinatorial object X (e.g. digraph, graph, design, code) such that $G_L \leqslant \mathrm{Aut}(X)$, where $\mathrm{Aut}(X)$ is the **automorphism group of X** (note that this implies that the vertex set of X is in fact G). If X is a Cayley object of G in some class $\mathcal{K}$ of combinatorial objects with the property that whenever Y is another Cayley object of G in $\mathcal{K}$, then X and Y are isomorphic if and only if they are isomorphic by a group automorphism of G, then we say that X is a **CI-object of G in $\mathcal{K}$**. If every Cayley object of G in $\mathcal{K}$ is a CI-object of G in $\mathcal{K}$, then we say that G is a **CI-group with respect to $\mathcal{K}$**. If G is a CI-group with respect to every class of combinatorial objects, then G is a **CI-group**.

Definition 17. Let G be a finite group. We say that $S \subseteq S_G$ is a **solving set for a Cayley object X** in a class of Cayley objects $\mathcal{K}$ if for every $X' \in \mathcal{K}$ such that $X \cong X'$, there exists $s \in S$ such that $s(X) = X'$, $s(1_G) = 1_G$ for every $s \in S$, and $\mathrm{Aut}(G) \leqslant S$. We say that $S \subseteq S_G$ is a **solving set for a class $\mathcal{K}$ of Cayley objects of G** if whenever $X, X' \in \mathcal{K}$ are Cayley objects of G and $X \cong X'$, then $s(X) = X'$ for some $s \in S$, and $s(1_G) = 1_G$ for every $s \in S$, and $\mathrm{Aut}(G) \leqslant S$. Finally, a set S is a **solving set for G** if whenever X, X' are isomorphic Cayley objects of G in any class $\mathcal{K}$ of combinatorial objects, then $s(X) = X'$ for some $s \in S$, $s(1_G) = 1_G$ for all $s \in S$, and $\mathrm{Aut}(G) \leqslant S$.

Remark 18. Note that the definition of a solving set given above differs from those in [11] and [3], as here, to simplify both the statements of results and their proofs, we insist that

every element of the solving set fixes 1_G. It is easy to see that $\alpha^{-1}G_L\alpha = G_L$ for every $\alpha \in \mathrm{Aut}(G)$, so the image of a Cayley object of G under a group automorphism of G is a Cayley object of G. That is, in order to test for isomorphism, automorphisms of G must be considered. However, it is not always the case that *every* automorphism of G needs to be considered when testing for isomorphism. For example, Cayley graphs of cyclic groups of order n each have an automorphism $x \to -x$ that is also a group automorphism of $\mathbb{Z}_n$, and so the image of a Cayley graph under this automorphism of $\mathbb{Z}_n$ is itself. So, while our definition of a solving set is convenient for this paper, it does not always capture the idea behind a solving set (i.e. that it should be as small as possible) exactly, but will only necessarily include extra automorphism of G (which could then be excluded). Also note that in [11] and [3], solving sets were only defined for abelian groups.

Let X be a Cayley object of G in $\mathcal{K}$. We define a **CI-extension of G with respect to X**, denoted by $\mathrm{CI}(G, X)$, to be a set of permutations in S_G that each fix 1_G and whenever $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$, then there exists $v \in \mathrm{Aut}(X)$ such that $v^{-1}\delta^{-1}G_L\delta v = t^{-1}G_L t$ for some $t \in \mathrm{CI}(G, X)$.

Lemma 19. *Let G be a finite group, and X a Cayley object of G in some class $\mathcal{K}$ of combinatorial objects. Then $\mathrm{CI}(G, X)$ exists.*

Proof. To show existence, we only need show that there is a set of permutations T in S_G such that whenever $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$ and $v \in \mathrm{Aut}(X)$, then $v^{-1}\delta^{-1}G_L\delta v = t^{-1}G_L t$ for some $t \in T$ and $t(1_G) = 1_G$. This follows almost immediately. As δv is a permutation, there exists $g \in G$ such that $\delta v(1_G) = g$. Let $t_{\delta v} = g_L^{-1}\delta v$. Then $t_{\delta v}(1_G) = g_L^{-1}\delta v(1_G) = g_L^{-1}(g) = g^{-1}g = 1_G$. Furthermore, $t_{\delta v}^{-1}G_L t_{\delta v} = v^{-1}\delta^{-1}g_L G_L g_L^{-1}\delta v = v^{-1}\delta^{-1}G_L\delta v$, and existence is established with $T = \{t_{\delta v} : \delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X), v \in \mathrm{Aut}(X)\}$. □

Note for X a Cayley object of G in $\mathcal{K}$, $\mathrm{CI}(G, X)$ is not unique as if T is CI-extension of X with respect to G, then for $\alpha \in \mathrm{Aut}(G)$, $\{\alpha t : t \in T\}$ is also a CI-extension of X with respect to G. The following result shows the importance of $\mathrm{CI}(G, X)$, as if $\mathrm{CI}(G, X)$ is known, then the isomorphism problem is solved.

Lemma 20. *Let G be a finite group, and X a Cayley object of G in some class $\mathcal{K}$ of combinatorial objects. Then the following are equivalent:*

1. *$S = \{\alpha t : \alpha \in \mathrm{Aut}(G), t \in T\}$ is a solving set for X,*
2. *T is a $\mathrm{CI}(G, X)$.*

Proof. 1) implies 2). Let $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$. Then $\delta(X)$ is a Cayley object of G in $\mathcal{K}$ as $\mathrm{Aut}(\delta(X)) = \delta\mathrm{Aut}(X)\delta^{-1} \geqslant G_L$. As S is a solving set for X, $\delta(X) = s(X)$ for some $s \in S$, and $s = \alpha t$ for some $\alpha \in \mathrm{Aut}(G)$ and $t \in T$. Thus $v = \delta^{-1}s \in \mathrm{Aut}(X)$. Then

$$\begin{aligned} v^{-1}\delta^{-1}G_L\delta v &= s^{-1}\delta\delta^{-1}G_L\delta\delta^{-1}s \\ &= s^{-1}G_L s = t^{-1}\alpha^{-1}G_L\alpha t \\ &= t^{-1}G_L t \end{aligned}$$

and T is a $\mathrm{CI}(X, G)$.

2) implies 1). Let X and X' be isomorphic Cayley objects of G in $\mathcal{K}$. Then there exists $\delta \in S_G$ such that $\delta(X) = X'$. As $G_L \leqslant \mathrm{Aut}(X')$, $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$. As T is a $\mathrm{CI}(X, G)$, there exists $t \in T$ and $v \in \mathrm{Aut}(X)$ such that $v^{-1}\delta^{-1}G_L\delta v = t^{-1}G_L t$. Hence $tv^{-1}\delta^{-1}G_L\delta vt^{-1} = G_L$. As G_L is transitive, there exists $h \in G$ such that $h_L\delta vt^{-1}(1_G) = 1_G$. Clearly then $tv^{-1}\delta^{-1}h_L^{-1}G_Lh_L\delta vt^{-1} = G_L$ so that $h_L\delta vt^{-1}$ normalizes G_L and fixes 1_G. By [2, Corollary 4.2B], we have that $h_L\delta vt^{-1} = \alpha \in \mathrm{Aut}(G)$. Then $\alpha tv^{-1}\delta^{-1}h_L^{-1} = (1_G)_L$ and $\alpha t = h_L\delta v$. Then $\alpha t(X) = h_L\delta v(X) = h_L\delta(X) = h_L(X') = X'$. □

The following result shows that if a solving set for X has been found, then some $\mathrm{CI}(G, X)$ has also been found.

Lemma 21. *Let G be a group, X a Cayley object of G, and S a solving set for X. Define an equivalence relation $\equiv$ on S by $s_1 \equiv s_2$ if and only if $s_1 = \alpha s_2$ for some $\alpha \in \mathrm{Aut}(G)$. Let T be a set consisting of one representative from each equivalence class of $\equiv$. Then T is a $\mathrm{CI}(G, X)$.*

Proof. It is straightforward to show that $\equiv$ is indeed an equivalence relation. Choose a T as is given in the statement. Let X' be a Cayley object of G isomorphic to X with $\delta : X \to X'$ an isomorphism. Then $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$. Also, as S is a solving set for X, there exists $s \in S$ such that $s(X) = X'$ so that $v = \delta^{-1}s \in \mathrm{Aut}(X)$. Let $t \in T$ such that $t \equiv s$ so that $\alpha t = s$ for some $\alpha \in \mathrm{Aut}(G)$. Then $v^{-1}\delta^{-1}G_L\delta v = t^{-1}\alpha^{-1}G_L\alpha t = t^{-1}G_L t$. □

Let $\mathcal{K}$ be a class of combinatorial objects, and G a group. We define a **CI-extension of G with respect to $\mathcal{K}$**, denoted by $\mathrm{CI}(G, \mathcal{K})$, to be a set of permutations in S_G that each fix 1_G and whenever $X \in \mathcal{K}$ is a Cayley object of G and $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$, then there exists $t \in \mathrm{CI}(G, \mathcal{K})$ and $v \in \mathrm{Aut}(X)$ such that $v^{-1}\delta^{-1}G_L\delta v = t^{-1}G_L t$. The proofs of the following results are straightforward.

Lemma 22. *Let G be a finite group, and $\mathcal{K}$ a class of combinatorial objects. Then the following are equivalent:*

1. *$S = \{\alpha t : \alpha \in \mathrm{Aut}(G), t \in T\}$ is a solving set for G in $\mathcal{K}$,*
2. *T is a $\mathrm{CI}(G, \mathcal{K})$.*

Lemma 23. *Let G be a group, $\mathcal{K}$ a class of combinatorial objects, and S a solving set for G in $\mathcal{K}$. Define an equivalence relation $\equiv$ on S by $s_1 \equiv s_2$ if and only if $s_1 = \alpha s_2$ for some $\alpha \in \mathrm{Aut}(G)$. Let T be a set consisting of one representative from each equivalence class of $\equiv$. Then T is a $\mathrm{CI}(G, \mathcal{K})$.*

Let G be a finite group. We define a **CI-extension of G**, denoted by $\mathrm{CI}(G)$, to be a set of permutations in S_G that each fix 1_G and whenever $X \in \mathcal{K}$ is a Cayley object of G in some class $\mathcal{K}$ of combinatorial objects, and $\delta \in S_G$ such that $\delta^{-1}G_L\delta \leqslant \mathrm{Aut}(X)$, then there exists $t \in \mathrm{CI}(G)$ and $v \in \langle G_L, \delta^{-1}G_L\delta\rangle$ such that $v^{-1}\delta^{-1}G_L\delta v = t^{-1}G_L t$.

Repeated application of Lemma 19 for every combinatorial object X in every class $\mathcal{K}$ of combinatorial objects shows that $\mathrm{CI}(G)$ exists. The proofs of the following results are straightforward.

Lemma 24. *Let G be a finite group. Then the following are equivalent:*

1. *$S = \{\alpha t : \alpha \in \mathrm{Aut}(G), t \in T\}$ is a solving set for G,*
2. *T is a $\mathrm{CI}(G)$.*

Lemma 25. *Let G be a group, and S a solving set for X. Define an equivalence relation $\equiv$ on S by $s_1 \equiv s_2$ if and only if $s_1 = \alpha s_2$ for some $\alpha \in \mathrm{Aut}(G)$. Let T be a set consisting of one representative from each equivalence class of $\equiv$. Then T is a $\mathrm{CI}(G)$.*

4 Applications

At the present time, the isomorphism problem has not been solved for any nilpotent group that is not abelian in any class of combinatorial objects, so there are not at this time any applications for Theorem 14 (1) (although as soon as the isomorphism problem has been solved for any nonabelian p-group in certain classes of combinatorial objects, such as color digraphs, that will change immediately). We do though have an application of Theorem 14 (2) which will not only provide new examples of CI-groups with respect to color digraphs, but also illustrate how Theorem 14 (2) generalizes the main result of [3].

The following result weakens the hypothesis (replacing normally s-step imprimitive with s-step imprimitive) of [3, Theorem 16] and generalizes this result from abelian to nilpotent groups.

Theorem 26. *Let $n_1, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ if $i \neq j$, and π_i be the set of distinct prime numbers dividing n_i. Let $n = n_1 \cdots n_r$, $\Omega(n) = m$, and G a nilpotent group of degree n. Let $G = \Pi_{i=1}^r N_i$ where each N_i is a π_i-subgroup of G, and $S(i)$ a solving set for N_i. If*

1. *each n_i is prime-power or G is abelian, and*
2. *whenever $\delta \in S_G$ there exists $\phi \in \langle G_L, \delta^{-1} G_L \delta \rangle$ such that $\langle G_L, \phi^{-1}\delta^{-1} G_L \phi\delta \rangle$ is m-step imprimitive,*

then $\Pi_{i=1}^r S(i)$ is a solving set for G.

Proof. Let $\delta \in S_G$. By the hypothesis, we have that there exists $\phi \in \langle G_L, \delta^{-1} G_L \delta \rangle$ such that $\langle G_L, \phi^{-1}\delta^{-1} G_L \delta\phi \rangle$ is m-step imprimitive. By Theorem 14, there exists $\omega \in \langle G_L, \phi^{-1}\delta^{-1} G_L \delta\phi \rangle$ such that $L = \langle G_L, \omega^{-1}\phi^{-1}\delta^{-1} G_L \delta\phi\omega \rangle = \Pi_{i=1}^r L_i$, where each L_i is a transitive π_i-group of degree n_i, $1 \leqslant i \leqslant r$. Let $\mathrm{CI}(N_i)$ be a CI-extension of N_i as given by Lemma 25. As $S(i)$ is a solving set for N_i, by Lemma 24 there exists $t_i \in \mathrm{CI}(N_i)$ and $v_i \in L_i$ such that $v_i^{-1}((\omega^{-1}\phi^{-1}\delta^{-1} G_L \delta\phi\omega)/\mathcal{C}_i)v_i = t_i^{-1}(G_L/\mathcal{C}_i)t_i$, where $\mathcal{C}_i$ is the complete block system of L formed by the orbits of $\Pi_{j=1, j\neq i}^r L_i$. Let $t = (t_1, \ldots, t_r)$

and $v = (v_1, \ldots, v_r)$. Note that t fixes 1_G. As $L = \Pi_{i=1}^r L_i$, we have that $v \in L$ and $t^{-1}G_L t = v^{-1}\omega^{-1}\phi^{-1}\delta^{-1}G_L\delta\phi\omega v$. By definition, $\Pi_{i=1}^r \mathrm{CI}(N_i)$ is a CI-extension of G, and so by Lemma 24, $S = \{\alpha t : t \in \Pi_{i=1}^r \mathrm{CI}(N_i), \alpha \in \mathrm{Aut}(G)\}$ is a solving set for G. Finally, it is not difficult to see that $\mathrm{Aut}(G) = \Pi_{i=1}^r \mathrm{Aut}(N_i)$ as G is nilpotent and if $i \neq j$ then $\gcd(n_i, n_j) = 1$, and so $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_r)$, $\alpha_i \in \mathrm{Aut}(N_i)$. Then $\alpha t = (\alpha_1 t_1, \alpha_2 t_2, \ldots, \alpha_r t_r)$, $\alpha_i \in \mathrm{Aut}(N_i)$ and $t_i \in \mathrm{CI}(N_i)$. Thus $\alpha t \in \Pi_{i=1}^r S(i)$, $S \leqslant \Pi_{i=1}^r S(i)$, and $\Pi_{i=1}^r S(i)$ is a solving set for G. □

Definition 27. Let Ω be a set. A ***k*-ary relational structure** on Ω is an ordered pair (Ω, U), where $U \subseteq \Omega^k = \Pi_{i=1}^k \Omega$. A group $G \leqslant S_\Omega$ is called ***k*-closed** if G is the intersection of the automorphism groups of some set of k-ary relational structures. The ***k*-closure of *G***, denoted $G^{(k)}$, is the intersection of all k-closed subgroups of S_Ω that contain G.

Note that a 2-closed group is the automorphism group of a color digraph. The following result of Kalužnin and Klin [7] will prove useful.

Lemma 28. *Let $G \leqslant S_X$ and $H \leqslant S_Y$. Let $G \times H$ act canonically on $X \times Y$. Then $(G \times H)^{(k)} = G^{(k)} \times H^{(k)}$ for every $k \geqslant 2$.*

If, in Theorem 26, $\mathcal{K}$ is the class of k-ary relational structures, and the groups $L/\mathcal{C}_i$ are as in the proof of Theorem 26, then by Lemma 28 we may assume that each $L/\mathcal{C}_i$ is k-closed (although there is no reason to believe that each $L/\mathcal{C}_i$ is a π_i-subgroup - but this fact is not used in the proof of Theorem 26). Proceeding as in Theorem 26 and applying Lemma 22 instead of Lemma 24, we have the following result.

Corollary 29. *Let $n_1, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ if $i \neq j$, and π_i be the set of distinct prime numbers dividing n_i. Let $n = n_1 \cdots n_r$, $\Omega(n) = m$, and G a nilpotent group of degree n. Let $G = \Pi_{i=1}^r N_i$ where each N_i is a π_i-subgroup of G, and $S(i)$ a solving set for N_i in the class of k-ary relational structures. If*

1. *each n_i is prime or G is abelian, and*
2. *whenever $\delta \in S_G$ there exists $\phi \in \langle G_L, \delta^{-1}G_L\delta\rangle$ such that $\langle G_L, \phi^{-1}\delta^{-1}G_L\phi\delta\rangle$ is m-step imprimitive,*

then $\Pi_{i=1}^r S(i)$ is a solving set for G in the class of k-ary relational structures.

We now give the promised application of Theorem 14 (2) which gives new CI-groups with respect to Cayley color digraphs of a particular group. Using the results in [3], this result could be obtained but only in the special cases where the following additional arithmetic conditions hold: p does not divide $q - 1$, and each n_i is prime. Before proceeding, we need a preliminary lemma.

Lemma 30. *Let n be a positive integer with a prime divisor $p|n$ such that $n/p < p$. If G is a regular group of order n, and $\phi \in S_n$, then there exists $\delta \in \langle G, \phi^{-1}G\phi\rangle$ such that $\langle G, \delta^{-1}\phi^{-1}G\phi\delta\rangle$ admits a normal complete block system with blocks of size p.*

Proof. First observe that as $n/p < p$, G must have a unique cyclic Sylow p-subgroup P of order p. So $P \triangleleft G$ and G admits a normal complete block system $\mathcal{B}$ consisting of blocks of size p, formed by the orbits of P. Furthermore, a Sylow p-subgroup of S_n is of the form $1_{S_{n/p}} \wr \mathbb{Z}_p$, so we see that $\langle P|_B : B \in \mathcal{B}\rangle$ is a Sylow p-subgroup of S_n. By a Sylow theorem, there exists $\delta \in \langle G, \phi^{-1}G\phi\rangle$ such that $\delta^{-1}\phi^{-1}G\phi\delta \leqslant \langle P|_B : B \in \mathcal{B}\rangle$. Let P_1 be the largest subgroup of $\langle G, \delta^{-1}\phi^{-1}G\phi\delta\rangle$ contained in $\langle P|_B : B \in \mathcal{B}\rangle$. Then G normalizes P_1 as does $\delta^{-1}\phi^{-1}G\phi\delta$. Hence the orbits of P_1, which is $\mathcal{B}$, is a complete block system of $\langle G, \delta^{-1}\phi^{-1}G\phi\delta\rangle$ and the result follows. □

Theorem 31. *Let p and q be distinct primes with $p^2 < q$, and $q_1, \ldots, q_r$ distinct primes such that $qp^2 < q_1$ and $qp^2q_1 \cdots q_i < q_{i+1}$, $1 \leqslant i \leqslant r-1$. Let $m = q_1 \cdots q_r$, $n_0 = p^2q$, and $n_1, \ldots, n_s$ divisors of m such that $n_1 \cdots n_s = m$. If $\gcd(n_i, n_j \cdot \varphi(n_j)) = 1$ then $\mathbb{Z}_q \times \mathbb{Z}_p^2 \times \mathbb{Z}_m$ is a CI-group with respect to digraphs.*

Proof. Let Γ be a Cayley color digraph of $G = \mathbb{Z}_q \times \mathbb{Z}_p^2 \times \mathbb{Z}_m$, and $\phi \in S_G$ such that $\phi^{-1}G_L\phi \leqslant \mathrm{Aut}(\Gamma)$. We first show by induction on r that $\langle G_L, \phi^{-1}G_L\phi\rangle$ is s-step imprimitive, where $s = r + 3$. If $r = 0$, then as $p^2 < q$ by Lemma 30 we may assume after an appropriate conjugation that $\langle G, \phi^{-1}G\phi\rangle$ admits a (normal) complete block system $\mathcal{B}_q$ with blocks of size q. Then $G_L/\mathcal{B}_q$ and $\phi^{-1}G_L\phi/\mathcal{B}_q$ are contained in conjugate Sylow p-subgroups of $\langle G_L, \phi^{-1}G_L\phi\rangle/\mathcal{B}_q$, and so after another appropriate conjugation we may assume that $\langle G_L, \phi^{-1}G_L\phi\rangle/\mathcal{B}_q$ is a p-group. The center of $\langle G_L, \phi^{-1}G_L\phi\rangle/\mathcal{B}_q$ contains an element of order p whose orbits give a complete block system $\mathcal{B}_p$ consisting of blocks of size p. Then $\mathcal{B}_p$ induces a complete block system $\mathcal{B}_q \prec \mathcal{B}_{pq}$ of $\langle G_L, \phi^{-1}G_L\phi\rangle$ with blocks of size pq. Hence $\langle G_L, \phi^{-1}G_L\phi\rangle$ is 3-step imprimitive. Assume that $\langle G_L, \phi^{-1}G_L\phi\rangle$ is s-step imprimitive when $r \geqslant 0$ and let G_L be such that m is a product of $r+1$ primes. Again, after an application of Lemma 30, we may assume that $\langle G_L, \phi^{-1}G_L\phi\rangle$ admits a complete block system $\mathcal{B}_{r+1}$ with blocks of size q_{r+1}. By induction we may assume that $\langle G_L, \phi^{-1}G_L\phi\rangle/\mathcal{B}_{q_{r+1}}$ is $(r+3)$-step imprimitive. It is then not difficult to see that $\langle G_L, \phi^{-1}G_L\phi\rangle$ is $(r+4)$-step imprimitive. By induction, we then have $\langle G_L, \phi^{-1}G_L\phi\rangle$ is $(r+3)$-step imprimitive as required.

Write $G_L = \Pi_{i=0}^{s} G_i$, where $G_i \leqslant G_L$ is of order n_i. As G_i is a CI-group with respect to Cayley color digraphs by [8] if $i = 0$ and by [10] otherwise, by Corollary 29, we see that if S is a solving set of G in the class of color digraphs then $S \subseteq \Pi_{i=1}^{r}\mathrm{Aut}(G_i) \leqslant \mathrm{Aut}(G)$. Hence G is a CI-group with respect to color digraphs. □

References

[1] A. Ádám. *Research problem 2-10.* J. Combin. Theory 2:393, 1967.

[2] John D. Dixon and Brian Mortimer. *Permutation groups.* Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[3] Edward Dobson. *On isomorphisms of abelian Cayley objects of certain orders.* Discrete Math. 266:203–215, 2003.

[4] Bernard Elspas and James Turner. *Graphs with circulant adjacency matrices* J. Combinatorial Theory 9:297–307, 1970.

[5] Daniel Gorenstein. *Finite groups*. Harper & Row Publishers, New York, 1968.

[6] Marshall Hall, Jr. *The theory of groups*. Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition.

[7] L. A. Kalužnin and M. H. Klin. *Some numerical invariants of permutation groups*. Latviĭsk. Mat. Ežegodnik 18:81–99, 1976.

[8] I. Kovács and M. Muzychuk. *The group $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ is a CI-group*. Comm. Algebra 37:3500-3515, 2009.

[9] J. D. P. Meldrum. *Wreath products of groups and semigroups*. Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 74, Longman, Harlow, 1995.

[10] Mikhail Muzychuk. *On Ádám's conjecture for circulant graphs* Discrete Math. 176:285–298, 1997.

[11] Mikhail Muzychuk. *On the isomorphism problem for cyclic combinatorial objects*. Discrete Math. 197/198:589–606.

[12] M. Muzychuk and F. Pakovich. *Jordan-Hölder theorem for imprimitivity systems and maximal decompositions of rational functions*. Proc. Lond. Math. Soc. 102:1–24, 2011.

[13] P. P. Pálfy. *Isomorphism problem for relational structures with a cyclic automorphism*. European J. Combin. 8:35–43, 1987.

[14] Helmut Wielandt, *Finite permutation groups*. Translated from the German by R. Bercov, Academic Press, New York, 1964.