On the Isomorphism Problem for Finite Cayley Graphs of Bounded Valency

CAI HENG LI AND CHERYL E. PRAEGER

For a subset \( S \) of a group \( G \) such that \( 1 \not\in S \) and \( S = S^{-1} := \{ s^{-1} \mid s \in S \} \), the associated Cayley graph \( \text{Cay}(G, S) \) is the graph with vertex set \( G \) such that \( \{ x, y \} \) is an edge if and only if \( xy^{-1} \in S \). Each \( \sigma \in \text{Aut}(G) \) induces an isomorphism from \( \text{Cay}(G, S) \) to the Cayley graph \( \text{Cay}(G, S^\sigma) \). For a positive integer \( m \), the group \( G \) is called an \( m \)-CI-group if, for all Cayley subsets \( S \) of size at most \( m \), whenever \( \text{Cay}(G, S) \cong \text{Cay}(G, T) \) there is an element \( \sigma \in \text{Aut}(G) \) such that \( S^\sigma = T \). It is shown that if \( G \) is an \( m \)-CI-group for some \( m \geq 4 \), then \( G = U \times V \), where \( |U|, |V| = 1 \), \( U \) is abelian, and \( V \) belongs to an explicitly determined list of groups. Moreover, Sylow subgroups of such groups satisfy some very restrictive conditions. This classification yields, as corollaries, improvements of results of Babai and Frankl. We note that our classification relies on the finite simple group classification.

1. Introduction

This paper is a contribution to the study of isomorphisms between Cayley graphs for a finite group \( G \). Automorphisms of the group \( G \) induce isomorphisms of Cayley graphs for \( G \) in a natural way, and for some groups \( G \), whenever two Cayley graphs for \( G \) are isomorphic there is an isomorphism between them which is induced by an automorphism of \( G \). If the latter property is true for all Cayley graphs of \( G \) of valency at most \( m \) (for a positive integer \( m \)), then the group \( G \) is called an \( m \)-CI-group. In this paper we give a classification of finite \( m \)-CI-groups for \( m \geq 4 \). Further, we derive, as corollaries of this classification, improvements of several results of Babai and Frankl [4, 5]. We also derive strong restrictions on the Sylow subgroups of \( m \)-CI-groups for \( m \geq 2 \).

Let \( G \) be a finite group. A subset \( S \) of \( G \) is called a Cayley subset if \( 1_G \not\in S \) and \( S = S^{-1} := \{ s^{-1} \mid s \in S \} \), and the Cayley graph of \( G \) with respect to \( S \) is the graph \( \text{Cay}(G, S) \) with vertex set \( G \) and with \( x \) and \( y \) adjacent if and only if \( xy^{-1} \in S \). Each element \( \sigma \in \text{Aut}(G) \) induces an isomorphism from \( \text{Cay}(G, S) \) to \( \text{Cay}(G, S^\sigma) \), and \( \text{Cay}(G, S) \) is called a CI-graph of \( G \) if, whenever \( \text{Cay}(G, S) \cong \text{Cay}(G, T) \), there is an element \( \sigma \in \text{Aut}(G) \) such that \( S^\sigma = T \) (CI stands for Cayley Isomorphism). Note that \( \text{Cay}(G, S) \) is a regular graph of valency \( |S| \). Thus \( G \) is an \( m \)-CI-group if all Cayley graphs for \( G \) of valency at most \( m \) are CI-graphs, and further we say that a finite group \( G \) is aCI-group if \( G \) is a \([G]\)-CI-group.

The problem of determining CI-groups has received considerable attention in the literature. Interest in the problem stems from a conjecture of Adám [1] in 1967 that all finite cyclic groups are CI-groups. This conjecture was disproved by Elspas and Turner [9] shortly afterwards, when they showed that \( \mathbb{Z}_{16} \) is not a CI-group. However, since then, a lot of work has been done to determine which cyclic groups are CI-groups (see for example [2, 18, 21]). The study of finite CI-groups in general began with a paper of Babai [3] in 1977. In 1978 Babai and Frankl [4] proved that if \( G \) is a CI-group of odd order, then either \( G \) is abelian or \( G \) has an abelian normal subgroup of index 3 and its Sylow 3-subgroup is elementary abelian, \( \mathbb{Z}_3 \) or \( \mathbb{Z}_{27} \); they also showed in [5] that if \( G \) is a finite insoluble CI-group, then \( G = L \times N \), where \( |L|, |N| = 1 \), \( L \cong L_2(5), SL_2(5), L_2(13) \) or \( SL_2(13) \), and \( N \) is a direct product of elementary abelian groups. Further results on elementary abelian CI-groups can be found in [8, 11, 13, 20].
improvement of the results of Babai and Frankl in [4, 5].

all such groups is given. As a corollary, we obtain a classification of CI-groups which is an improvement of the results of Babai and Frankl in [4, 5].

Two elements $a, b$ of a group $G$ are said to be fused if $a = b^\sigma$ for some $\sigma \in \text{Aut}(G)$, and to be inverse-fused if $a = (b^{-1})^\sigma$ for some $\sigma \in \text{Aut}(G)$. The only Cayley subsets of size 1 consist of a single involution (element of order 2), and hence $G$ is a 1-CI-group if and only if all involutions of $G$ (if any) are fused. It is clear that an $m$-CI-group is also a $k$-CI-group for each positive integer $k \leq m$, so it follows from the definition that if $G$ is a 2-CI-group then any two elements of $G$ of the same order are fused or inverse-fused (see Lemma 2.2). For convenience, we call a group with the latter property an FIF-group (FIF stands for fused or inverse-fused). In [15] we classified the finite nonabelian simple FIF-groups, and further in [16] we gave a good description of arbitrary finite FIF-groups. In the present paper we apply these results to obtain a classification of $m$-CI-groups with $m \geq 4$.

The notation and terminology used in this paper are standard (see for example [23, 25]). In particular, a direct product of cyclic groups of the same order is said to be homocyclic. For groups $G$ and $H$, $G \times H$ will denote an arbitrary semi-direct product of $G$ by $H$. Let $M$ be an abelian group all of whose Sylow subgroups are homocyclic, and let $n$ be the exponent of $M$. We define certain nonabelian extensions of such homocyclic groups $M$. Let $r, s$ be non-negative integers such that $r + s \geq 1$, and suppose that there exists an integer $l$ such that $1 < l < n$ and $l$ has order $e$ modulo $n$ (that is, $e$ is the least positive integer such that $l^e \equiv 1 \pmod{n}$ and we write $o(l \pmod{n}) = e$) and in addition $r, s, e$ are as in one of the lines of Table 1.

Then we define

$$H_e(M, 2^r3^s, l) = M \rtimes (\langle z \rangle) = M \rtimes \mathbb{Z}_{2^e3^s},$$

where $x^z = x^l$ for all $x \in M$. Note that the assumptions on $l$ imply that no nontrivial Sylow subgroup of $\langle z \rangle$ centralizes $M$. The main result of this paper is the following.

**Theorem 1.1.** Let $G$ be an $m$-CI-group for some $m \geq 4$. Then $G = U \times V$, where $(|U|, |V|) = 1$, $U$ is abelian, and either $V = 1$ or $V$ is one of the following:

(i) $Q_8 \times \mathbb{Z}_3^2 \rtimes Q_8$, $A_5$, $SL_2(5)$;

(ii) $\mathbb{Z}_{2^e} \rtimes \mathbb{Z}_{2^s}$, $Q_8 \rtimes \mathbb{Z}_{2^s}$ for some $s \geq 1$;

(iii) $H_e(M, 2^r3^s, l)$, where $M$ is abelian, $r, s$ and $e$ satisfy one of the lines of Table 1 and $o(l \pmod{n}) = e$;

(iv) $Q_8 \times H_3(M', 3^s, l')$, $H_2(M, 2^r, l) \times H_3(M', 3^s, l')$, where $2, 3, |M|$ and $|M'|$ are pairwise coprime; $M$, $M'$ are abelian, $r, s \geq 1$ and $l, l' > 1$.

<table>
<thead>
<tr>
<th>$r, s$</th>
<th>$e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r = 0, s \geq 1$</td>
<td>$3$</td>
</tr>
<tr>
<td>$r \geq 1, s = 0$</td>
<td>$2$ or $4$</td>
</tr>
<tr>
<td>$r \geq 1, s \geq 1$</td>
<td>$6$</td>
</tr>
</tbody>
</table>
Further, let \( p \) be a prime dividing \(|G|\) and let \( G_p \) be a Sylow \( p \)-subgroup of \( G \). If \( p > \left\lceil \frac{|G|}{4} \right\rceil \), then \( G_p \) is homocyclic; if \( p = \left\lceil \frac{|G|}{4} \right\rceil \), then \( G_p \) is elementary abelian, cyclic or \( Q_8 \); if \( p < \left\lceil \frac{|G|}{4} \right\rceil \), then either \( G_p \) is elementary abelian, or \( G_p \cong \mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_9 \) or \( Q_8 \).

It was proved in [14] that \( A_5 \) is not a 29-CI-group and \( SL_2(5) \) is not a 58-CI-group. It therefore follows from Theorem 1.1 and [14] that all 58-CI-groups are soluble. In particular, neither \( A_5 \) nor \( SL_2(5) \) is a CI-group. Taking \( m = |G| \), Theorem 1.1 gives a classification of CI-groups which is an improvement of the results of [4, 5]. We must point out that, since the results of [15, 16] rely on the finite simple group classification, so also do the results of this paper.

**Theorem 1.1**. Suppose that \( G \) is a CI-group. Then each Sylow subgroup of \( G \) is elementary abelian, or isomorphic to \( \mathbb{Z}_4, \mathbb{Z}_8, \mathbb{Z}_9 \) or \( Q_8 \). Moreover, \( G = U \times V \), where \(|U|, |V| = 1, U \) is abelian, and either \( V = 1 \) or \( V \) is one of the following:

1. \( Q_8, \mathbb{Z}_2^2 \times \mathbb{Z}_3, \mathbb{Z}_2^2 \times \mathbb{Z}_5, \mathbb{Z}_8 \times \mathbb{Z}_5, \mathbb{Z}_8 \times \mathbb{Z}_9, \mathbb{Z}_2^2 \times Q_8 \);
2. \( H_4(M, 2^r 3^s) \), where \( M \) is abelian, \( r \) and \( s \) satisfy one of the lines of Table 1 and \( o(l \mod m) = e \);
3. \( Q_8 \times H_3(M', 3^r), H_2(M, 2^s, l) \times H_3(M', 3^s, l') \), where \( M, M' \) are abelian, \( 1 \leq r \leq 3, 1 \leq s \leq 2 \) and \( l, l' > 1 \).

**Remark.** (i) Nowitz [20] proved that \( \mathbb{Z}_2^2 \) is not a 31-CI-group. So not all of the groups listed in Theorem 1.1 are necessarily \( m \)-CI-groups for every value of \( m \). It is difficult to determine precisely which groups listed in Theorem 1.1 are indeed \( m \)-CI-groups for a given \( m \geq 4 \). For example, for a prime \( p \), it is not known whether \( \mathbb{Z}_p^4 \) is a CI-group, see [20, Question (1)] and [8]. It would be interesting to know whether \( \mathbb{Z}_p^4 \) was an \( m \)-CI-group for ‘small’ values of \( m \).

**Problem 1.3.** Determine which of the groups listed in Theorem 1.1 are \( m \)-CI-groups for certain small values of \( m \).

In Section 2 we collect together several preliminary results which will be used later. Then in Section 3 we determine the possible structure of Sylow subgroups of \( m \)-CI-groups for \( m \geq 2 \). In Section 4 we use the results of [16] to obtain a good description of the structure of finite 2-CI-groups and investigate in more detail the structure of certain families of examples. We prove some technical lemmas in Section 5, and finally we prove Theorem 1.1 in Section 6.

## 2. Preliminary Results

We begin with some elementary observations about \( m \)-CI-groups. Let \( n \) be a positive integer. Then \( C_n \) denotes a cycle of size \( n \), \( K_{a,n} \) the complete bipartite graph of order \( 2n \), and for a graph \( \Gamma \), \( n\Gamma \) denotes a graph which consists of \( n \) vertex-disjoint copies of \( \Gamma \). The first lemma is an immediate consequence of the definitions given in Section 1.

**Lemma 2.1.** Let \( G \) be a finite group.

1. For any \( S, T \subseteq G \setminus \{1\}, \text{Cay}(G, S) \cong \text{Cay}(G, T) \) if and only if \( \text{Cay}(\langle S \rangle, S) \cong \text{Cay}(\langle T \rangle, T) \).
2. If \( G \) is an \( m \)-CI-group for some integer \( m \geq 1 \) and \( N \) is a characteristic subgroup of \( G \), then \( N \) is also an \( m \)-CI-group.

**Lemma 2.2.** If \( G \) is an \( m \)-CI-group for some \( m \geq 2 \), then any two elements of \( G \) of the same order are fused or inverse-fused under \( \text{Aut}(G) \).
PROOF. Suppose that $G$ is an $m$-CI-group for some $m \geq 2$. Since $m$-CI-groups are 1-CI-
groups, all involutions of $G$ are fused under Aut$(G)$. Let $a, b \in G$ be such that $o(a) = o(b) > 2$. Then clearly Cay$(G, \{a, a^{-1}\}) \cong \frac{|G|}{o(a)}C_{o(a)} \cong \text{Cay}(G, \{b, b^{-1}\})$. Since $G$ is a 2-CI-group, there exists $\alpha \in \text{Aut}(G)$ such that $\{a, a^{-1}\}^\alpha = \{b, b^{-1}\}$, that is, $a^\alpha = b$ or $b^\alpha$.

Next, we quote two results about FIF-groups from [16], the first quite elementary, but the second less so.

**Lemma 2.3.** Let $G$ be an FIF-group, and let $N$ be a characteristic subgroup of $G$.

(i) ([16, Lemma 2.1]) Both $N$ and $G/N$ are FIF-groups.

(ii) Suppose that $N \cong \mathbb{Z}_d^2$ for some $d \geq 1$ and some prime $p$, that

$N$ is a minimal normal subgroup of $G$ with $C_G(N) = N$, and that $G \cong \mathbb{Z}_p^d \rtimes \mathbb{Z}_k$ for

some $k > 1$. Then $\frac{1}{2}\phi(k)$ divides $d$, where $\phi(k)$ is the Euler phi-function (that is, the

number of positive integers less than $k$ and coprime to $k$).

As usual a group $G$ is said to be indecomposable if $G = A \times B$ implies that $A = 1$ or

$B = 1$. In the following, we shall say that $G$ is coprime-indecomposable if $G = A \times B$ such

that $(|A|, |B|) = 1$ implies that $A = 1$ or $B = 1$. For a group $G$ and a subgroup $H$ of $G$, we

shall denote by $H \text{ char } G$ the fact that $H$ is a characteristic subgroup of $G$.

3. Sylow Subgroups of $m$-CI-Groups

In this section we give a description of Sylow subgroups of $m$-CI-groups for $m \geq 2$. First

we consider Sylow 2-subgroups.

**Lemma 3.1.** Let $G$ be an $m$-CI-group with $m \geq 2$ and let $G_2$ be a Sylow 2-subgroup of $G$.

Then $G_2$ is elementary abelian, cyclic, or generalized quaternion. Further, if $m \geq 4$, then $G_2$

is elementary abelian, cyclic or $Q_8$: if $m \geq 6$, then $G_2$ is elementary abelian, $\mathbb{Z}_4$, $\mathbb{Z}_8$ or $Q_8$.

**Proof.** By [17, Theorem 1.3], $G_2$ is elementary abelian, cyclic, or generalized quaternion.

Assume that $m \geq 4$ and that $G_2$ is generalized quaternion, that is,

$G_2 = \langle x, y \mid x^{2^m} = 1, y^2 = x^{2^{m-1}}, y^{-1}xy = x^{-1} \rangle$.

Suppose that $n \geq 3$, and let $z = x^{2^{n-3}}$. Then $\langle z \rangle \cong \mathbb{Z}_8$ and $\langle y, z^2 \rangle \cong Q_8$. Let $S = \{z, z^{-1}, z^{-3}, z^{-3}\} (= \langle z \rangle \setminus \langle z^2 \rangle)$ and $T = \{z^2, z^{-2}, y, y^{-1}\} (= \langle y, z^2 \rangle \setminus \langle yz \rangle)$. Then $S = \mathbb{Z}_8 \setminus \mathbb{Z}_4$ and $T = Q_8 \setminus \mathbb{Z}_4$. Thus it is easy to see that Cay$(\langle S \rangle, S) \cong K_{4,4} \cong \text{Cay}(\langle T \rangle, T)$ and so

Cay$(G, S) \cong \text{Cay}(G, T)$. However, since $o(z) = 8$ and $o(z^2) = o(y) = 4$, $S$ and $T$ cannot be conjugate under Aut$(G)$, which is a contradiction. Thus $n = 2$ and $G_2 = Q_8$.

Assume that $m \geq 6$ and that $G_2$ is cyclic. Then by [13, Proposition 3.2(1)], $G_2 \cong \mathbb{Z}_2$, $\mathbb{Z}_4$ or $\mathbb{Z}_8$.

Next we consider Sylow $p$-groups for odd primes $p$. For a positive integer $k$, a group $G$ is

said to have the $k$-CI property if all Cayley graphs of $G$ of valency $k$ are CI-graphs. Thus an

$m$-CI-group has the $k$-CI property for all $k \leq m$. The following lemma draws together some

elementary results from [16] and [17].

**Lemma 3.2.** Suppose that $G$ is an $m$-CI-group for $m \geq 2$. Let $p$ be an odd prime dividing

$|G|$ and $G_p$ a Sylow $p$-subgroup of $G$. Then $G_p$ is homocyclic. Moreover,
(i) if \( p = \left[ \frac{m}{2} \right] \), then \( G_p \) is elementary abelian or cyclic;

(ii) if \( p < \left[ \frac{m}{2} \right] \), then \( G_p \) is elementary abelian or \( \mathbb{Z}_9 \).

**Proof.** By Lemma 2.2, \( G \) is an FIF-group, and so, by [16, Theorem 1.1], \( G_p \) is homocyclic. Further, by [17, Theorem 1.5], if \( p = \left[ \frac{m}{2} \right] \), then either \( G_p \) is of exponent \( p \), or \( G_p \) is cyclic, so part (i) holds; if \( p < \left[ \frac{m}{2} \right] \), then either \( G_p \) is of exponent \( p \), or \( G_p \) is both cyclic and of exponent 9, so part (ii) holds.

**4. Finite \( m \)-CI-Groups for \( m \leq 3 \)**

In this section we study \( m \)-CI-groups for \( m \leq 3 \). By the definition, a group \( G \) is a 1-CI-group if and only if all involutions of \( G \) are fused under \( \text{Aut}(G) \). So from now on we shall assume that \( m \geq 2 \). The simple \( m \)-CI-groups for \( m = 2, 3 \) are known.

**Theorem 4.1 ([16, Theorem 1.3]).** Suppose that \( G \) is a nonabelian simple group. Then

(i) \( G \) is a 2-CI-group if and only if \( G = \text{A}_5 \) or \( \text{L}_2(8) \),

(ii) \( G \) is a 3-CI-group if and only if \( G = \text{A}_5 \).

A classification of finite FIF-groups is given in [16], which, together with Lemma 3.1, provides a good description of finite 2-CI-groups.

**Theorem 4.2.** Suppose that \( G \) is a finite 2-CI-group. Then a Sylow \( p \)-subgroup \( G_p \) of \( G \) is either homocyclic, or \( p = 2 \) and \( G_2 \) is elementary abelian, cyclic or generalized quaternion. Moreover, \( G = X_1 \times \cdots \times X_l \), where \(|X_1|, |X_j| = 1 \) and \( X_j \) is coprime-indecomposable, and one of the following holds:

1. \( X_i = M \times \mathbb{Z}_n \), where \(|M|, n = 1\), and \( M \) is nilpotent;
2. \( X_i = (L \times M) \rtimes ((H \rtimes K) \times \mathbb{Z}_n) \), where \(|L|, |M|, |H|, |K| \) and \( n \) are pairwise coprime, and
   
   (i) \( L \times M \) is nilpotent, and is maximal among the normal nilpotent Hall subgroups of \( X_i \); \( (M, H) = M \times H \) and \( (L, \mathbb{Z}_n) = L \times \mathbb{Z}_n \),
   
   (ii) \( H \rtimes K \) is indecomposable and noncyclic, neither \( H \) nor \( K \) centralizes a Sylow subgroup of \( L \), and \( (L, H \rtimes K) \) satisfies one of the lines in Table 2.
3. \( X_i = \text{A}_5, \text{L}_2(8), \text{SL}_2(5), \text{SL}_2(7) \) or \( \text{SL}_2(9) \).

**Proof.** By Lemmas 3.1 and 3.2, we have the conclusions about Sylow subgroups of \( G \).

By Lemma 2.2, any two elements of \( G \) of the same order are fused or inverse-fused, so \( G \) is a group on the list of [16, Theorem 1.1]. Thus \( G = X_1 \times \cdots \times X_l \), where \(|X_1|, |X_j| = 1 \) and each \( X_j \) is coprime-indecomposable. Further, by Lemma 3.1, a Sylow 2-subgroup of a 2-CI-group is elementary abelian, cyclic or generalized quaternion. Therefore, if \( X_j \) is soluble, then we conclude from [16] that \( X_j \) is as in part (1) or (2); if \( X_i \) is insoluble, then it follows from [16] and the Atlas [6] that \( X_i \) is as in part (3).

Next we prove several properties about the semidirect products occurring in Theorem 4.2, which will be used in the ensuing sections. First we consider the groups appearing in Theorem 4.2 (1).
LEMMA 4.3. Let \( G = M \rtimes (z) \) be a 2-CL-group, where \(|M|, o(z) = 1 \) and \( M \) is nilpotent, and suppose that \( M \) has a Sylow \( p \)-subgroup \( M_p = \mathbb{Z}_p^d \) for some prime \( p \). Suppose further that \( M_p \not\cong \mathbb{Z}(G) \), and let \( g \in \langle z \rangle \setminus C_{(z)}(M_p) \). Then either

(i) \( g^2 \not\in C_{(z)}(M_p) \) and \( (a) \cap \langle a^g \rangle = 1 \) for all \( a \in M_p \), or

(ii) \( p \geq 3 \), and there exist positive integers \( e, l \) such that \( e \in \{2, 3, 4, 6\} \), \( e \) divides \( o(g) \), \( 1 < l < p^e \), \( o(l \mod p^e) = e \), and \( g^{-1}ag = a^l \) for all \( a \in M_p \); in particular, \( g^e \in C_{(z)}(M_p) \).

PROOF. Let \( K = \langle M, g \rangle \). Since \( M \) is characteristic in \( G \) and \( \langle g \rangle \) is characteristic in \( \langle z \rangle \), it follows that \( K \) is characteristic in \( G \), and so by Lemma 2.3, \( K \) is a FIF-group. Let \( e \) be the smallest positive integer such that \( g^e \in C_{(z)}(M_p) \). Then \( e \) divides \( o(g) \) and \( (e, p) = 1 \) (since \((o(g), p) = 1\)).

First assume that \( g \) normalizes no nontrivial cyclic subgroups of \( M_p \), that is, for all \( x \in M_p \setminus \{1\} \), \( x^g \not\in \langle x \rangle \). Then it follows that \( \langle x \rangle \cap \langle x^g \rangle = 1 \) for all \( x \in M_p \). If \( g^2 \not\in C_{(z)}(M_p) \) then for some \( x \in M_p \setminus \{1\} \), \( x^{g^2} = x \) and so \( x \cdot x^{g^2} = x \cdot x \cdot x^g \) and by our assumption on \( g \) we must therefore have \( x \cdot x^{g^2} = 1 \), that is \( x^{g^2} = x^{-1} \), which is a contradiction. Thus \( g^2 \not\in C_{(z)}(M_p) \), and part (i) holds.

Now assume that \( g \) normalizes at least one nontrivial cyclic subgroup of \( M_p \). Let \( p^l \) be the maximum of the orders of the cyclic subgroups of \( M_p \) which are normalized by \( g \). Take \( a \in M_p \) such that \( o(a) = p^l \) and \( a = a^l \) for some integer \( l \) with \( 1 \leq l < p^l \). Note that since \( o(a^i) = o(a), (i, p) = 1 \). Further, \( a^{p^l} = a^{p^{l-1}} = a \) and so \( l = 1 \mod p^l \). We use the following steps to complete the proof of the lemma.

1. For each \( x \in M_p \) with \( o(x) = p^l \), \( x^g = x^{i(x)} \) for some integer \( i(x) \) with \( 1 \leq i(x) < p^l \). Since \( o(x) = o(a) \) and \( K \) is an FIF-group, there exists \( \alpha \in \text{Aut}(K) \) and \( \varepsilon = \pm 1 \) such that \( a^\alpha = x^\varepsilon \). Since \( K = M \rtimes \langle g \rangle \), \( g^\alpha = cg^j \) where \( c \in M \leq C_K(M_p) \) and \( j \) is an integer coprime to \( o(g) \). Therefore,

\[ g^{-j}x^cg^j = g^{-j}c^{-1}x^cg^j = (g^\alpha)^{-1}a^\alpha g^\alpha = (g^{-1}ag)^{\alpha} = (a^l)^{\alpha} = x^{i(x)}. \]
Thus $g^{-j}xg^j = x^j$. Since $(j, o(g)) = 1$, we have $g^{-1}xg = x^{i(x)}$ for some integer $i(x)$ with $1 \leq i(x) < p'$. 

(2). For each $x \in M_p$ with $o(x) = p'$, we have $i(x) = 1$. If $M_p$ is cyclic, then clearly $i(x) = 1$. Thus assume that $M_p$ is not cyclic, so there exists $b \in M_p$ such that $o(b) = p'$ and $(b) \cap (a) = 1$. Then $o(ab) = p'$, and by step (1), $(ab)^s = (ab)^{i(ab)}$ for some integer $i(ab)$ such that $1 \leq i(ab) < p'$. So 

$$a^ib^{i(ab)} = a^s b^s = (ab)^s = (ab)^{i(ab)} = a^{i(ab)} b^{i(ab)},$$

and hence $a^{i(ab)} = b^{i(ab) - i(b)}$. Since $(a) \cap (b) = 1$, it follows that $i(b) = i(ab) = 1$. Let $x \in M_p$ be an arbitrary element of order $p'$. Then either $(x) \cap (a) = 1$ or $(x) \cap (b) = 1$. Thus by the previous argument, $i(x) = i(a)$ or $i(b)$, so $i(x) = 1$.

(3). $p' = p^s$, and $o(l \mod p^s) = e$. It follows from step (2) that, for all $y \in M_p$ with $o(y) \leq p^s$, $y^s = y^j$. Suppose that $p^s < p'$. Take an element $b \in M_p$ with $o(b) = p'^j$. Then the maximality of $t$, $b^s \notin (b)$. However, since $o(b^p) = p'$, by step (2), $(b^p)^s = b^{ps}$. Thus $(b) \cap (b^p) = (b^p)$, and so $(b, b^p) \cong \mathbb{Z}_{p^j+1} \times \mathbb{Z}_p$. Hence $b^s = b^j c$ for some integer $j$ and some $c \in M_p$ such that $o(c) = p$ and $(b) \cap (c) = 1$. Therefore, $b^{ip} = (b^j c)^p = (b^j)^p = (b^p)^s = b^{ps}$. Consequently, $jp \equiv j'p \mod p^{j+1}$, and so $j = kp^j + l$ for some integer $k$. Thus $b^s = b^{j+k} c = b^{j+k} c$. Let $c_0 = b^{j+k} c$. Then $o(c_0) = p$, $(c_0) \cap (b) = 1$, $b^s = b^{j+k} c$ and $c_0^s = c_0^l$ (since $o(c_0) = p < p^{j+1}$). By induction on $i$, we have 

$$b^{si} = b^{i+j+k} c_0^l, \quad i \geq 1.$$ 

Taking $i = e$, we have $c_0^{p^{-e-1}} = b^{j-l} c_0^l$ as $b^s = b$. Since $(c_0) \cap (b) = 1$, we have that $c_0^{p^{-e-1}} = 1$ and so $p$ divides $el^{e-1}$, contradicting the fact that $(el, p) = 1$. Therefore, $p' = p^s$, and so for all $x \in M_p$, $x^s = x^j$. From the definition of $e$ it follows that $o(l \mod p^s) = e$.

(4). $e = 2, 3, 4$ or $6$, and $p$ is odd. Assume that $q(e) \geq 3$. Then there exists $i$ such that $1 < i < e - 1$ and $(i, e) = 1$. We may write $g = g_1 g_2$ such that $(o(g_1), i) = 1$ and each prime factor of $o(g_2)$ divides $i$. Then $o(g_1) = o(g_1^i)$ and $(o(g_1), o(g_2)) = 1$. Also, since $(i, e) = 1$, we have $(o(g_2), e) = 1$. Since $g_1^i g_2 = g^r \in C_{(c)}(M_p)$, also $g_2^{o(g_2)} = g^{o(g_2)} \in C_{(c)}(M_p)$. Further, since $(o(g_2), o(g_1)) = 1$, there exists an integer $k$ such that $o(g_1^i)k \equiv 1 \mod (o(g_2))$. Therefore, $g_2 = g_2^{o(g_2)k} \in C_{(c)}(M_p)$, and so $g_2^e = g_2^{eg_2^{-e}} \in C_{(c)}(M_p)$. Now $x^e_1 = x_1^{x^e_1} = x^s = x^j = x^j$. From the definition of $e$ it follows that $o(l \mod p^s) = e$. 

$$g_1^{-e_1} x g_1^{e_1} = (g_1^{-1} x g_1)^a = (x^j)^a = y^e = g_1^{-1} y g_1,$$

that is, $g_1^{-e_1} x g_1^{e_1} = y$. Consequently, $y^{e-1} = g_1^{-e} x_1^{e-1} = y$, and hence, taking $x \in M_p$ with $o(x) = p'$ so that $o(y) = p'$, we have $i^{e-1} \equiv 1 \mod (o(y))$. Therefore, if $e = 1$, then $e$ divides $i-1$; if $e = -1$, then $e$ divides $i+1$, either of which is contrary to $1 < i < e-1$. Hence $q(e) = 2$ and so $e = 2, 3, 4$ or $6$.

Since $(a)^s = (a)$ and $a^e = a^d$ for $d \neq a, g$ induces a nontrivial automorphism of $(a)$. If $p = 2$ then $\text{Aut}(a))$ is a $2$-group. Thus $g$ is of even order, a contradiction. Therefore, $p \geq 3$. Hence part (ii) holds.
The next result characterises a special subclass of the 2-CI-groups occurring in Theorem 4.2 (1).

**Proposition 4.4.** Suppose that $G = M \rtimes \langle z \rangle$ is a 2-CI-group, where

(i) $M$ is abelian and each Sylow subgroup is homocyclic;
(ii) $(|M|, o(z)) = 1$, $z$ normalizes each cyclic subgroup of $M$ of prime-power order; and
(iii) $G$ is not nilpotent and is coprime-indecomposable.

Then $G = H_e(M, 2^3 3, 1)$, where $l$ has order $e$ modulo $\exp(M)$ and $e, r, s$ are as in Table 1.

**Proof.** Let $n$ be the exponent of $M$. First we prove that there exist integers $e \in \{2, 3, 4, 6\}$, and $l$ of order $e$ modulo $n$, such that $x^e = x^l$ for all $x \in M$. Since $M$ is nilpotent, $M = M_1 \times \cdots \times M_t$ where $M_i = Z^{p_{i_1}}_{p_{i_2}}$ is the Sylow $p_i$-subgroup of $M$ and $p_1, \ldots, p_t$ are the distinct prime divisors of $|M|$. Note that $n = \prod p_i^{j_i}$. Choose $i \leq t$. Since $G$ is coprime-indecomposable, $z$ does not centralize $M_i$. Hence, by Lemma 4.3, there exist integers $l_i$ and $e_i$ such that $e_i \in \{2, 3, 4, 6\}$, $l_i$ has order $e_i$ modulo $p_i^{j_i}$, and $x^e = x^{l_i}$ for all $x \in M_i$. By the Chinese Remainder Theorem (see [19, p. 64]), there is an integer $l$ such that $l \leq n$ and for all $i$, $l \equiv l_i \pmod{p_i^{j_i}}$. Each $x \in M$ has a unique expression as $x = x_1 \cdots x_t$ with $x_i \in M_i$ and we have, therefore, $x^e = x_1^e \cdots x_t^e = x_1^{l_1} \cdots x_t^{l_t} = x^{l_1} \cdots x^{l_t} = x^l$ for all $x \in M$. Let $e = \text{lcm}(e_1, \ldots, e_t)$, so $e \in \{2, 3, 4, 6\}$. Since $o(l_i \mod p_i^{j_i}) = e_i$ for all $i$, also $o(l \mod p_i^{j_i}) = e_i$ for all $i$, and hence $o(l \mod n) = e$. Suppose that for some prime $q$ dividing $o(z)$, a Sylow $q$-subgroup $(z_q)$ of $(z)$ centralizes $M$. Then $G = M \rtimes ((z_q)') \rtimes (z_q) = (M \rtimes (z_q')) \rtimes (z_q)$, where $(z_q')$ is the Hall $q'$-subgroup of $(z)$. This is a contradiction since $G$ is coprime-indecomposable. Hence no nontrivial Sylow subgroup of $(z)$ centralizes $M$. In particular, since $z^e$ centralizes $M$ and $e$ divides 12, we must have $o(z) = 2^3 3^s$ for some integers $r$ and $s$. Suppose that $e = 12$. Since $G$ is a 2-CI-group and $o(z) = o(z^2)$, there exists $a \in \text{Aut}(G)$ such that $z^a = z^s$ for some $s = \pm 1$. As $M$ is characteristic in $G$, there exists $u := x^a \in M$ with $o(u) = n$, and so

$$z^{-5e} u z^{5e} = (z^{-1} x z)^a = (x^l)^a = u^e = z^{-1} u z,$$

that is, $z^{-5e+1} u z^{5e-1} = u$. Thus $u^{l_{5e-1}} = z^{-5e+1} u z^{5e-1} = u$, and hence $l_{5e-1} \equiv 1 \pmod{n}$. Hence $5e - 1$ is divisible by $e = 12$, which is not possible. Thus $e = 2, 3, 4$ or 6. Note that $e$ divides $o(z)$. Thus if $r = 0$, then $e = e_1 = \cdots = e_t = 3$, and if $s = 0$, then each $e_i$ is 2 or 4, so $e$ is 2 or 4. Suppose that $r > 0$ and $s > 0$. If all the $e_i$ are 2 or 4, then a Sylow $3$-subgroup $(z_3)$ of $(z)$ is nontrivial and centralizes $M$ which is not the case. Hence, at least one of the $e_i$ is equal to 3. Similarly at least one of the $e_i$ is even, and hence $e = 6$. It now follows that $G = H_s(M, 2^2 3^3, 1)$ and $r, s, e$ are as in Table 1.

Finally, we investigate another special subclass of 2-CI-groups satisfying Theorem 4.2 (1).

**Lemma 4.5.** Suppose that $G$ is a 2-CI-group which is coprime-indecomposable and not nilpotent. Suppose further that $G$ satisfies Theorem 4.2 (1) and that $G = M \rtimes \langle z \rangle$ with $(|M|, o(z)) = 1$ and $M = Z^6_2$ or $Q_8$. Then $(z)$ is a 3-group and acts nontrivially on $M$.

**Proof.** Since $(|M|, o(z)) = 1$, $o(z)$ is odd. Also $G/\langle C_G(M)M \rangle \leq \text{Out}(M) \cong S_3$, and since $o(z)$ is odd, we have that $|G/C_G(M)M| = 3$. If there is a prime $q$ dividing $o(z)$ such that $q$ does not divide $|G/C_G(M)M|$, then a Sylow $q$-subgroup $(z_q)$ of $(z)$ centralizes $M$. Thus $G = M \rtimes ((z_q)') \rtimes (z_q) = (M \rtimes (z_q')) \rtimes (z_q)$, where $(z_q')$ is a Hall $q'$-subgroup of $(z)$, which is a contradiction since $G$ is coprime-indecomposable. Since $G$ is coprime-indecomposable and not nilpotent, we have that $|G/C_G(M)M| = 3$, and so $(z)$ is a 3-group.


5. Structure of Certain Cayley Graphs

In this section we prove several technical lemmas concerning 4-CI-groups, which will be applied to prove Theorem 1.1 in the next section. Recall that the direct product $\Gamma_1 \times \Gamma_2$ of two graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ is the graph with vertex set $V_1 \times V_2$ such that $(u_1, u_2)$ is adjacent to $(v_1, v_2)$ if and only if either $[u_1, v_1] \in E_1$ and $u_2 = v_2$, or $[u_2, v_2] \in E_2$ and $u_1 = v_1$. The first lemma analyses the groups listed in Theorem 4.2 (1). It will also be used to assist our analysis of the groups in Theorem 4.2 (2).

**Proposition 5.1.** Suppose that $G = M \rtimes (z)$ is a 4-CI-group satisfying Theorem 4.2 (1), where

(i) $M$ has a homocyclic Sylow $p$-subgroup $M_p$ for some prime $p$ dividing $|M|$;
(ii) $(|M|, o(z)) = 1$, and $(z)$ has a Sylow $q$-subgroup $G_q = \langle h \rangle$ for some prime $q$ dividing $o(z)$ such that there is a cyclic subgroup $\langle a_0 \rangle$ of $M_p$ which is not normalized by $h$;
(iii) $G$ is coprime-indecomposable.

Then $p = 2$, $q = 3$, $M_p = \mathbb{Z}_2^2$, and $h^3$ centralizes $M_p$.

**Proof.** Now $M_p = \mathbb{Z}_2^t$ for some $t \geq 1$, and we must have $d \geq 2$ since $G_q$ does not normalize $(a_0)$. Set $K := M \rtimes G_q$. Since $G_q$ is characteristic in $(z)$, it follows that $K$ is characteristic in $G$, and so $K$ is also a 4-CI-group (see Lemma 2.1). Since $G_q$ does not normalize $(a_0)$, by Lemma 4.3, $(a) \cap (a^h) = 1$ for all $a \in M_p$. Let $g$ be an element of $G_q$ with minimal order such that $(a) \cap (a^g) = 1$ for all $a \in M_p$. Then $(a) \cap (a^g) \neq 1$ for some $a \in M_p$. By Lemma 4.3, $g^a$ normalizes every cyclic subgroup of $M_p$.

Let $\text{Sub}(p')$ be the set of all cyclic subgroups of $M_p$ of order $p'$. We claim that $G_q$ acts transitively on $\text{Sub}(p')$ by conjugation. Take $(a) \in \text{Sub}(p')$ and let $b = a^g$. Then $(a) \cap (b) = 1$, and thus, for any $(x) \in \text{Sub}(p')$, either $(x) \cap (a) = 1$ or $(x) \cap (b) = 1$. Assume first that $(x) \cap (a) = 1$, and let $S = \{a, a^{-1}, b, b^{-1}\}$ and $T = \{a, a^{-1}, x, x^{-1}\}$. Then $\text{Cay}(\langle S, T \rangle) \cong \text{Cay}(\langle S \rangle)$, and so $\text{Cay}(\langle K, S \rangle) \cong \text{Cay}(\langle K, T \rangle)$ (by Lemma 2.1). Since $K$ is a 4-CI-group, there exists $\alpha \in \text{Aut}(K)$ such that $\alpha^S = T$. Hence $(\langle a \rangle, \langle b \rangle)^\alpha = (\langle a \rangle, \langle x \rangle)$ or $(\langle x \rangle, \langle a \rangle)$. Note that, since $g^{-1}ag = b$,

\[(g^a)^{-1}(a)g^a = (g^{-1}ag)^a = (b)^a.
\]

Thus in the first case $(g^a)^{-1}(a)g^a = (x)$, while in the second case $(g^a)^{-1}(x)g^a = (b)^a = (a)$.

Now $g^\alpha = c_1 g^i$ for some $c \in M$ and some integer $i$, and since $c$ centralizes $M_p$, we have either $g^{-i}(a)g^i = (x)$ or $g^{-i}(x)g^i = (a)$. Thus in either case, $(x)$ is conjugate to $(a)$ by some element of $(g)$. If $(x) \cap (b) = 1$, then similarly $(x)$ is conjugate to $(b)$ by some element of $(g)$.

Consequently, since $(a)^\alpha = (b)$, in this case also $(x)$ is conjugate to $(a)$ by some element of $(g)$.

Thus $(g)$ is transitive on $\text{Sub}(p')$ by conjugation. Since $G_q \geq (g)$, $G_q$ also acts transitively on $\text{Sub}(p')$, and since $G_q$ is abelian, $G_q$ induces a regular permutation group on $\text{Sub}(p')$ (see [25, Proposition 4.4]). Let $E$ be the kernel of this $G_q$-action. Then $|G_q : E| = |\text{Sub}(p')| = s$, say, and $E = \langle h^t \rangle$. Since $(g)$ is transitive on $\text{Sub}(p')$, it follows that $G_q = \langle g \rangle$, and since $g^\alpha$ normalizes every cyclic subgroup of $M_p$, we have $E = \langle g^\alpha \rangle = \langle h^t \rangle$ and $q = |\text{Sub}(p')|$. Therefore,

\[q = |\text{Sub}(p')| = \frac{p^{td} - p^{(t-1)d}}{\phi(p^d)} = p^{(t-1)(d-1)} \frac{p^d - 1}{p - 1}.
\]

Since $q$ is a prime and $d \geq 2$, it follows that $p^{(t-1)(d-1)} = 1$, and so $t = 1$, $M_p \cong \mathbb{Z}_2^2$ and $q = \frac{p^d - 1}{p - 1}$. In particular $q \geq 3$, and since $\frac{p^d - 1}{p - 1}$ is prime, $d$ must also be a prime. If $q = 3$, then $p^d = 2^2$ and so $h^q$ centralizes $M_p$ and the lemma holds.
Thus we may suppose that $q \geq 5$ and hence that $d$ is an odd prime. Since $g^q$ normalizes every cyclic subgroup of $M_p$, by Lemma 4.3 (ii), $(h^q)^e \in C_{G_{p}}(M_p)$ where $e \in \{2, 3, 4, 6\}$, and so also $h^q$ centralizes $M_p$. Let $C_{p'}$ be a Hall $p'$-subgroup of $C := C_{K}(M_p)$. Then $C = M_p \times C_{p'}$ and hence we have $C_p$ char $C$ char $K$. By Lemma 2.2, the 4-Cl-group $K$ is an FIF-group. Thus, by Lemma 2.3 (i), $\overline{K} := K/C_{p'}$ is an FIF-group. Since $h^q \in C_{K}(M_p)$, we have $\overline{K} = \overline{M}_p \times (\overline{h})$, where $\overline{M}_p = M_p/C_{p'}/C_{p'} \cong \mathbb{Z}_p^d$ and $(\overline{h}) = (h)C_{p'}/C_{p'} \cong (h)/(h^q) \cong \mathbb{Z}_q$. Since $\overline{K}$ is an FIF-group, it follows that all cyclic subgroups of $\overline{K}$ of order $p$ are conjugate under $\text{Aut}(\overline{K})$, and so $\overline{M}_p$ is a minimal characteristic subgroup of $\overline{K}$. Further, $h$ does not centralize $M_p$, and hence $C_{\overline{K}}(\overline{M}_p) = \overline{M}_p$. So $\overline{K}$ satisfies all the conditions of Lemma 2.3 (ii), and hence $\overline{\psi}(h)$ divides $d$. On the other hand, $\overline{\psi}(h) = q - 1 = \frac{p^d - 1}{p - 1} = \frac{p^d - p}{p - 1}$, so $\frac{p^d - p}{p - q}$ divides $d$. The only possibility for $(p, d, q)$ satisfying this divisibility condition (with $q \geq 5$ and $d$ an odd prime) is $(2, 3, 7)$. Thus $M_p \cong \mathbb{Z}_3^2$, and we may write $M_p \setminus \{1\} = \{a_0, a_1, \ldots, a_6\}$ such that $a_0^3 = a_i^{a_{i+1}}$ (reading the subscripts modulo 7). Let $S = \{a_0, a_1, a_2\}$. Then it is easy to check that $(S) = M_p$. Since $a_0, a_1, \ldots, a_6$ are distinct and $(a_0, a_1)$ contains exactly three involutions (namely, $a_0, a_1$, and $a_1 a_0$), there exists $k \in \{3, 5\}$ satisfying $a_k \notin \{a_0, a_1\}$ so that $(a_0, a_1, a_k) = M_p$. Let $T = \{a_0, a_1, a_k\}$. Then Cay$(M_p, S) \cong \mathbb{Q}_1$ and Cay$(M_p, T)$, where $Q_1$ is the cube graph of dimension 3, so Cay$(K, S) \cong \text{Cay}(K, T)$ (see Lemma 2.1). Since $K$ is a 4-Cl-group, it holds that all cyclic subgroups of $K$ are conjugate. It follows from Proposition 5.1 that each Sylow subgroup of $K$ is an FIF-group. Since $H$ is cyclic or $H = \mathbb{Q}_8$, it follows that all cyclic subgroups of $K$ are conjugate. Then we may suppose that $H \triangleleft N_K(T)$ for some $N_K(T)$ satisfying this divisibility condition (with $q \geq 5$ and $d$ an odd prime) is $(2, 3, 7)$. Thus $M_p \cong \mathbb{Z}_3^2$, and we may write $M_p \setminus \{1\} = \{a_0, a_1, \ldots, a_6\}$ such that $a_0^3 = a_i^{a_{i+1}}$ (reading the subscripts modulo 7). Let $(i, i + j, i + 2j) \equiv (0, 1, k)(\text{mod } 7)$. However, it is straightforward to check that there are no values of $i, j$ for which this holds, for $k = 3$ or $k = 5$. This completes the proof. \[\square\]

Now we consider the groups listed in Theorem 4.2 (2).

**Proposition 5.2.** Suppose that $G$ is a 4-Cl-group which is coprime-indecomposable. Suppose further that $G$ satisfies Theorem 4.2 (2). Then $G = \mathbb{Z}_3^2 \times Q_8$.

**Proof.** We use the notation of Theorem 4.2 so that $G = (L \times M) \times (H \times K \times \mathbb{Z}_3)$, every Sylow subgroup of $L \times M$ is homocyclic, $(M, H) = M \times H$, $(L, \mathbb{Z}_3) = L \times \mathbb{Z}_3$, and either $H$ is cyclic or $H = \mathbb{Q}_8$. It follows, since $(M, H) = M \times H$, that $L \times H$ is a characteristic subgroup of $G$, and so by Lemma 2.1, $L \times H$ is also a 4-Cl-group.

Suppose that $H$ is cyclic. By Theorem 4.2, $H$ is of odd order, and either $|L|$ is odd or a Sylow $2$-subgroup of $L$ is $\mathbb{Z}_3^2$. It follows from Proposition 5.1 that each Sylow subgroup of $H$ normalizes each cyclic subgroup of $L$ of prime-power order. Moreover, by Theorem 4.2, $L \times H$ is not nilpotent and is either coprime-indecomposable, or is the direct product of two non-nilpotent coprime indecomposable factors. Each coprime indecomposable factor satisfies the hypotheses of Proposition 4.4. Since $|H|$ is odd, it follows from Proposition 4.4 that $L \times H$ is coprime-indecomposable and $L \times H = H_3(L, 3^i, l)$ for some positive integers $i$ and $l$, and in particular, $H = \langle y \rangle = \mathbb{Z}_3$ and $H$ centralizes no nontrivial Sylow subgroup of $L$. It follows that $L, H \times K$ are as in line 2 of the table in Theorem 4.2. Thus $K = \langle z \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, and $L = (\mathbb{Z}_3^{a_1} \times \mathbb{Z}_3^{a_2})^2$. Let $L_p$ be a nontrivial Sylow $p$-subgroup of $L$. Then $\text{soc}(L_p) = \mathbb{Z}_p^2$ and the conjugation action induces a homomorphism $\varphi$ from $H \times K$ to $\text{Aut}(\text{soc}(L_p)) \cong \text{GL}_2(p)$. Since $\varphi(H) \neq 1$, and $H$ normalizes each cyclic subgroup of $\text{soc}(L_p)$, it follows that $\varphi(H) \cong \mathbb{Z}_3$ consists of scalar matrices, so $p = 7$. Since $\varphi(H)$ is central in $\varphi(H \times K)$ but $K$ does not centralize $H$, it follows that $y^2 \cong y^{1+3j}$ for some $j$ such that $1 \leq j < 3^i - 1$, and $j \neq 0(\text{mod } 3)$. However this means that $\varphi(z)$ is divisible by 3, which is a contradiction.

Therefore, by Theorem 4.2, $H = \mathbb{Q}_8$, $K = \mathbb{Z}_2$, $L = \mathbb{Z}_2^2$, and $F := L \times H = \mathbb{Z}_2^2 \times \mathbb{Q}_8$ is a 4-Cl-group. Let $H = \langle x, y \rangle$. Then $L \times (x^2)$ char $L \times H$, and it follows that $L \times (x^2)$ is
also a 4-CI-group. It follows from Lemma 4.3 that the involution $x^2$ normalizes every cyclic subgroup of $L$ of prime-power order. For each prime $p$ dividing $q$, let $L_p = \mathbb{Z}_p^2$. denote the Sylow $p'$-subgroup of $L$. Suppose that $x^2$ centralizes $L_p$ for some $p$. Let $L_{p'}$ be a Hall $p'$-subgroup of $L$. Then $L_{p'} / \text{char} \ L / \text{char} \ F$ and $F / L_{p'} \cong L_p \times \mathbb{Q}_8$. By Lemma 2.3, $F / L_{p'}$ is an FIF-group. Since $x^2$ centralizes $L_{p'}$, again by Lemma 2.3, $F / \langle (x^2)^{h} \rangle \cong L_p \times \mathbb{Z}_2^2$ is an FIF-group. By [16, Theorem 1.1], it follows that this group is isomorphic to $L_p \times \mathbb{Z}_2$ and hence $H$ centralizes $L_p$, which is a contradiction to Theorem 4.2(2)(i) (that is, a contradiction to the fact that $H$ centralizes no Sylow subgroup of $L$). Therefore, $x^2$ does not centralize $L_p$ for any $p$, and it follows from Lemma 4.3 that $x^2$ inverts every element of $L_p$ for all $p$ and, hence, $x^2$ inverts every element of $L$. Now let $L_p = \mathbb{Z}_p^2$ and let $a \in L_p$ of order $p'$. Since $N_F(\langle (a)^{p-1} \rangle) \cap H = 1$, at least one of $x$ and $y$ does not normalize $\langle (a)^{p-1} \rangle$, say $x$. Then $\langle (a)^{p-1} \rangle \cap H = 1$ and since $\langle (a)^{p-1} \rangle$ is the unique subgroup of $\langle a \rangle$ of order $p'$, $\langle a \rangle \cap (a) = 1$. Let $b = a^x$. Then for any $c \in L_p$ with $o(c) = p'$, either $c \cap (a) = 1$, or $c \cap (b) = 1$, say $c \cap (a) = 1$.

Set $S := \{a, a^{-1}, b, b^{-1}\}$ and $T := \{a, a^{-1}, c, c^{-1}\}$. Now Cay$(\langle S \rangle, S) \cong C_{p'} \times C_{p'} \cong$ Cay$(\langle T \rangle, T)$, and thus Cay$(F, S) \cong$ Cay$(F, T)$ (see Lemma 2.1). Since $F$ is a 4-CI-group, $S$ is conjugate to $T$ under Aut$(F)$. Consequently, there exists $a \in$ Aut$(F)$ such that $(\langle a \rangle, \langle b \rangle)^v = \langle (a), (c) \rangle$. Since $x^{-1}(a)x = (b)$, we have that $(x^v)^{-1}(a)^v x^v = (b)^v$. It follows that $a$ is conjugate to $(c)$ by $x^v$ or $(x^v)^{-1}$. Now $x^v = dx^v$ for some $d \in L$ and some $x \in H$. Since $d$ centralizes $L$, $(a)$ is conjugate to $(c)$ by $x^v$ or $(x^v)^{-1}$. It follows that $H$ acts transitively by conjugation on the set $\Omega$ of all subgroups of $L_p$ of order $p'$, and the kernel of this action contains $\langle x \rangle$ (since $x^2$ inverts each element of $L_p$). Hence $|\Omega|$ divides 4 and it follows that $p' = 3$. Thus $L = L_p = \mathbb{Z}_3^2$, and by Theorem 4.2 (2), $M = 1$, $K = 1$ and $n = 1$. Thus $G = L \times H = \mathbb{Z}_3^2 \times \mathbb{Q}_8$.

6. PROOF OF THEOREM 1.1

Let $G$ be an $m$-CI-group for some $m \geq 4$. Then $G$ is a 2-CI-group, so $G$ is one of the groups listed in Theorem 4.2. Thus $G = X_1 \times \cdots \times X_t$ such that $|X_i| = |X_j| = 1$ and each $X_i$ is coprime-indecomposable and satisfies part (1), (2) or (3) of Theorem 4.2. Since $X_i$ is homocyclic, or $X_i \cong \mathbb{Q}_8$, or $X_i$ is a Sylow subgroup of $G$, and so either $X_i$ is homocyclic, or $X_i \cong \mathbb{Q}_8$. Thus, if $X_1, \ldots, X_t$ are all nilpotent, then the theorem holds, so we may assume that this is not the case. Note that the direct product $U$ of all the nilpotent groups $X_i$ (if any) is abelian. Suppose now that $X = X_t$ is not nilpotent. We shall prove that $X$ is one of the non-nilpotent groups listed in parts (i)–(iii) of Theorem 1.1.

If $X$ satisfies Theorem 4.2 (2) then by Proposition 5.2, $X \cong \mathbb{Z}_2^2 \times \mathbb{Q}_8$, as in part (i). Suppose next that $X$ satisfies Theorem 4.2 (3), that is, $X = L_2(5), L_2(7), L_2(9), SL_2(5), SL_2(9)$. Since, by Lemma 3.1, a Sylow 2-subgroup of $X$ is elementary abelian, cyclic or $\mathbb{Q}_8$, it follows that $X$ is one of $L_2(5) \cong A_5, L_2(9) \cong SL_2(5)$. However, by Theorem 4.1, $L_2(9)$ is not a 3-CI-group. Thus $X = A_5$ or $SL_2(5)$, as in part (i).

Finally, suppose that $X$ satisfies Theorem 4.2 (1), that is, $X = M \rtimes (z)$ where $M$ is nilpotent and $|M| = n = 1$. First assume that a Sylow 2-subgroup $M_2$ of $M$ is neither $\mathbb{Z}_2$ nor $\mathbb{Q}_8$. Then every Sylow subgroup of $M$ is homocyclic and is not isomorphic to $\mathbb{Z}_2^2$. But, by Proposition 5.1, $z$ normalizes every cyclic subgroup of $M$ of prime-power order. Further, since $X$ is coprime-indecomposable, no nontrivial Sylow subgroup of $(z)$ centralizes $M$. Then by Proposition 4.4, $X = H_0(M, 2^m 3^n, I)$ where $I$ has order $e$ modulo $\exp(M)$, and $r, s, e$ are as in one of the lines of Table 1, as in part (iii).
Now assume that a Sylow 2-subgroup $M_2$ of $M$ is isomorphic to $\mathbb{Z}_2^2$ or $Q_8$. Then $n$ is odd. Let $M_2$ be the Hall $2'$-subgroup of $M$. Then $M_2$ is a characteristic abelian subgroup of $X$ and $M = M_2 \times M_2$. Note that $\text{Out}(M_2) \cong S_3$. It follows, since $n$ is odd, that $X/C_X(M_2)M_2 \leq \mathbb{Z}_3$. Suppose that there is a Sylow $p$-subgroup $M_p$ of $M$, and a Sylow $q$-subgroup $(z_q)$ of $(z)$, for some odd primes $p$ and $q$, such that $z_q$ does not centralize $M_p$. It follows from Proposition 5.1 that $z_q$ normalizes every cyclic subgroup of $M_p$ and then by Lemma 4.3 (noting that $q$ is odd) that $q = 3$, and $x^z = x^l$ for all $x \in M_p$, where $l$ has order 3 modulo the exponent of $M_p$.

Thus, if there is a prime $q > 3$ such that $q$ divides $o(z)$, then the Sylow $q$-subgroup $(z_q)$ of $(z)$ centralizes $M_2$. Hence, $z_q$ also centralizes $M_2$, and it follows that $(z_q)$ is a direct factor of $X$ contradicting the fact that $X$ is coprime-indecomposable. Hence $(z) \cong \mathbb{Z}_3$, for some $s \geq 1$. Again, since $X$ is coprime-indecomposable, $z$ does not centralize $M_2$, and if $p$ is an odd prime dividing $|M|$ then $z$ does not centralize the Sylow $p$-subgroup $M_p$. Suppose now that $M = M_2$ so that such an odd prime $p$ exists and (by the previous paragraph) $x^z = x^l$ for all $x \in M_p$, where $l$ has order 3 modulo the exponent of $M_p$. Note that $l$ has order 3 modulo $p$, so $p \equiv 1 \pmod 3$ and, in particular, $p \geq 7$.

Let $a_0, a_1$ be distinct elements of $M_2$ such that $a_0^2 = a_1$ and let $b$ be an element of $M_p$ of order $p$. Then $b^2 = b$. Set $S = \{a_0b^l, (a_0b^l)^{-1}, a_1b, (a_1b)^{-1}\}$ and $T = \{a_0b^l, (a_0b^l)^{-1}, a_1b, (a_1b)^{-1}\}$. Then $(S) = (T) = M_2 \times (b)$ and there exists an automorphism $\sigma$ of $S$ such that $(a_1b)^{\sigma} = a_0b = (a_0b^l)^{\sigma} = a_1b$. Thus $\text{Cay}((S), S) \cong \text{Cay}(T, T)$ (by Lemma 2.1). Since $X$ is a 4-Clifford group, there is an element $\rho \in \text{Aut}(X)$ such that $S^\rho = T$. Thus $(a_0b^l, a_1b) = ((a_0b)^{\rho}, (a_1b)^{\rho})$ or $(a_1b)^{\rho}$, $(a_0b)^{\rho}$, where $\rho \in \text{Aut}(X)$, and then by Lemma 4.3 (noting that $q$ is odd) that $q = 3$, and $x^z = x^l$ for all $x \in M_p$, where $l$ has order 3 modulo the exponent of $M_p$. Note that $l$ has order 3 modulo $p$, so $p \equiv 1 \pmod 3$ and, in particular, $p \geq 7$.

Let $a_0, a_1$ be distinct elements of $M_2$ such that $a_0^2 = a_1$ and let $b$ be an element of $M_p$ of order $p$. Then $b^p = b^l$, and $b^p = (b^{l^2})^p = (b^p)^{l^2} = b^{l^2}$ which implies that $p = o(b)$ divides $l^2 \pm 1$, which is a contradiction. Hence the second line holds, so $b^p = b^l$ and $b^{l^2} = (b^p)^{l^2}$. This means that $p$ divides $l^2 - 1$ whence $l^2 = 3$. Now $x^z = x^l$ for some $c \in M$ and some integer $i$, where $1 \leq i < 3^3$ and $i \equiv 1 \pmod 3$. Note that $b^p = b^l$. Thus we have

$$b^{l^2} = (b^p)^{l^2} = (z^{-1}b) = z^{-i}c^{-1}b^i = z^{-i}b^i$$

whence $l^{-i} \equiv 1 \pmod p$. Since $l^3 \equiv 1 \pmod p$ it follows that $i \equiv 1 \pmod 3$. On the other hand, since $z^{-1}a_0 = a_1$ and $z^2$ centralizes $M_2$, we have that

$$z^{-1}a_0^2z = z^{-1}a_1z = (z^{-1}a_0z)^2 = a_1^2 = a_0.$$
ACKNOWLEDGEMENTS

The first author gratefully acknowledges the support of an Overseas Postgraduate Research Scholarship of the Australian Department of Education, Employment and Training and a University Postgraduate Award from the University of Western Australia. This research forms part of an Australian Research Council small grant project.

REFERENCES