FURTHER RESTRICTIONS ON THE STRUCTURE OF FINITE CI-GROUPS

CAI HENG LI, ZAI PING LU, AND P. P. PÁLFY

Abstract. A group G is called a *CI-group* if, for any subsets $S, T \subset G$, whenever two Cayley graphs $\mathsf{Cay}(G, S)$ and $\mathsf{Cay}(G, T)$ are isomorphic, there exists an element $\sigma \in \mathsf{Aut}(G)$ such that $S^\sigma = T$. The problem of seeking finite CI-groups is a long-standing open problem in the area of Cayley graphs. This paper contributes towards a complete classification of finite CI-groups. First it is shown that the Frobenius groups of order $4p$ and $6p$, and the metacyclic groups of order $9p$ of which the centre has order 3 are not CI-groups, where p is an odd prime. Then a shorter explicit list is given of candidates for finite CI-groups. Finally, some new families of finite CI-groups are found, that is, the metacyclic groups of order $4p$ (with centre of order 2) and of order $8p$ (with centre of order 4) are CI-groups, and a proof is given for the Frobenius group of order $3p$ to be a CI-group, where p is a prime.

1. Introduction

Let G be a finite group. For a subset $S \subseteq G \setminus \{1\}$ with $S = S^{-1} := \{s^{-1} \mid s \in S\}$, the *Cayley graph* of G with respect to S is the graph $\mathsf{Cay}(G, S)$ with vertex set G such that x, y are adjacent if and only if $yx^{-1} \in S$. Clearly, each automorphism σ of G induces a graph isomorphism from $\mathsf{Cay}(G, S)$ to $\mathsf{Cay}(G, S^\sigma)$. A Cayley graph $\mathsf{Cay}(G, S)$ is called a *CI-graph* of G if, whenever $\mathsf{Cay}(G, S) \cong \mathsf{Cay}(G, T)$, there is an element $\sigma \in \mathsf{Aut}(G)$ such that $S^\sigma = T$ (CI stands for *Cayley Isomorphism*). A finite group G is called a *CI-group* if all Cayley graphs of G are CI-graphs. This paper contributes towards the complete classification of finite CI-groups.

The problem of seeking CI-groups has received considerable attention over the past thirty years, beginning with a conjecture of Ádám [1] that all finite cyclic groups were CI-groups; refer to surveys in [2, 17, 27, 28]. Ádám's conjecture was disproved by Elspas and Turner [12]. Since then, many people have worked on classifying cyclic CI-groups (see Djokovic [9], Babai [4], Alspach and Parsons [3], Pálfy [26] and Godsil [13]), and finally, a complete classification of cyclic CI-groups was obtained by Muzychuk [22, 23], that is, a cyclic group of order n is a CI-group if and only if $n = 8, 9, 18, k, 2k$ or $4k$ where k is odd and square-free. Babai [4] in 1977 initiated the study of general CI-groups. Then Babai and Frankl [5] 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 either elementary abelian or cyclic of order 9 or 27. They [6] also showed that if G is an insoluble CI-group,

Date: February 14, 2006.

The first author was supported by an Australian Research Council Discovery Grant and a QEII Fellowship. The second author was partially supported by the NNSF and TYYF of China. The third author was supported by the Hungarian Science Foundation (OTKA), grant no. T38059.

The authors are very grateful to the referees for their constructive comments.

then $G = U \times V$ with $(|U|, |V|) = 1$, where U is a direct product of elementary abelian groups, and $V = \mathrm{A}_5$, $\mathrm{SL}(2, 5)$, $\mathrm{PSL}(2, 13)$ or $\mathrm{SL}(2, 13)$. Recently the first author [16] proved that all finite CI-groups are soluble. Moreover, Praeger and the first author obtained a description of arbitrary finite CI-groups by the work of a series of papers [19, 20, 21].

The description for finite CI-groups given by [19, 20, 21] was obtained as a consequence of a description of the so-called finite m-CI-groups (groups, all of whose Cayley graphs of valency at most m are CI-graphs) for small values of m. The argument of [19, 20, 21] is dependent on the classification of finite simple groups. One of the purposes of this paper is to give an improvement of the description of finite CI-groups obtained in [21], and moreover the argument used in the paper is independent of the classification of finite simple groups. The first result of this paper shows that some groups in the list of CI-group candidates given in [21] are not CI-groups.

Theorem 1.1. *Let p be an odd prime, and let G be a group such that either G is a Frobenius group of order $4p$ or $6p$, or G is a metacyclic group of order $9p$ of which the centre is of order 3. Then G is not a CI-group.*

To state our description for finite CI-groups, we need some notation. For groups G and H, denote by $G \rtimes H$ a semidirect product of G by H, and denote by $\mathsf{exp}(G)$ the largest integer which is the order of an element of G. In our list of candidates for CI-groups, most members contain a direct factor defined as follows. Let M be an abelian group of odd order for which all Sylow subgroups are elementary abelian, and let $n \in \{2, 3, 4, 8\}$ be such that $(|M|, n) = 1$. Let

$$\mathsf{E}(M, n) = M \rtimes \langle z \rangle$$

such that $o(z) = n$, and if $o(z)$ is even then z inverts all elements of M, that is, $x^z = x^{-1}$ for all $x \in M$; while if $o(z) = 3$ then $x^z = x^l$ for all $x \in M$, where l is an integer satisfying $l^3 \equiv 1 \pmod{\mathsf{exp}(M)}$ and $(l(l-1), \mathsf{exp}(M)) = 1$. Let $\mathcal{CI}$ denote the class of finite groups G defined by one of the following two items:

(1) $G = U \times V$ with $(|U|, |V|) = 1$, where all Sylow subgroups of G are elementary abelian, or isomorphic to $\mathbb{Z}_4$ or Q_8; moreover, U is abelian, and $V = 1, \mathrm{Q}_8, \mathrm{A}_4, \mathrm{Q}_8 \times \mathsf{E}(M, 3), \mathsf{E}(M, n)$ where $n \in \{2, 3, 4\}$, or $\mathsf{E}(M, n) \times \mathsf{E}(M', 3)$ where $n = 2$ or 4, and $|M|, |M'|$ and 6 are pairwise coprime.

(2) G is one of the groups: $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{18}$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_2\ (= \mathrm{D}_{18})$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$ with centre of order 2, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ with centre of order 3, $\mathsf{E}(M, 8)$, or $\mathbb{Z}_2^d \times \mathbb{Z}_9$.

Then the following theorem shows that all finite CI-groups are in $\mathcal{CI}$.

Theorem 1.2. *Let G be a finite CI-group.*

(a) *If G does not contain elements of order 8 or 9, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise coprime, and*
   (i) *H_1 is an abelian group, and each Sylow subgroup of H_1 is elementary abelian or $\mathbb{Z}_4$;*
   (ii) *H_2 is one of the groups $\mathsf{E}(M, 2)$, $\mathsf{E}(M, 4)$, Q_8, or 1;*
   (iii) *H_3 is one of the groups $\mathsf{E}(M, 3)$, A_4, or 1.*

(b) *If G contains elements of order 8, then $G \cong \mathsf{E}(M, 8)$ or $\mathbb{Z}_8$.*

(c) *If G contains elements of order 9, then G is one of the groups $\mathbb{Z}_9 \rtimes \mathbb{Z}_2$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$, or $\mathbb{Z}_9 \times \mathbb{Z}_2^n$ with $n \leq 5$.*

However, the problem of determining whether or not a member of $\mathcal{CI}$ is really a CI-group is difficult. Nowitz [25] proved that the elementary abelian group $\mathbb{Z}_2^6$ is not a CI-group, and recently Muzychuk [24] proved that the elementary abelian group $\mathbb{Z}_p^n$ with $n \geq 2p-1+\binom{2p-1}{p}$ is not a CI-group. Actually, finite CI-groups are very rare, and the previously known examples are the following, where p is a prime:

$\mathbb{Z}_n$, where either $n \in \{8,9,18\}$, or n divides $4k$ and k is odd square-free (Muzychuk [22, 23]);
$\mathbb{Z}_p^2$ (Godsil [13]); $\mathbb{Z}_p^3$ (Dobson [10]);
$\mathbb{Z}_p^4$ (Conder and Li [7] for $p=2$, Hirasaka and Muzychuk [14] for $p>2$);
D_{2p} (Babai [4]); F_{3p}, the Frobenius group of order $3p$, (see [6]);
$\mathbb{Z}_2^2 \times \mathbb{Z}_3$, $\mathbb{Z}_2^5$ (Conder and Li [7]); Q_8; $\mathbb{Z}_3 \rtimes \mathbb{Z}_8$ (see [29]);
A_4 (see [17]); $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_2$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ (Conder and Li [7]).

Here we find some new families of CI-groups:

Theorem 1.3. *For any odd prime p, the group*

$$G = \langle a, z \mid a^p = 1, z^r = 1, z^{-1}az = a^{-1} \rangle, \quad \text{where } r = 4 \text{ or } 8,$$

of order $4p$ *or* $8p$ *is a CI-group.*

In [6] the authors refer to a paper of Babai "in preparation" that would contain—among others—the proof of the following result (Theorem 1.4). Since this paper has never appeared, we find it appropriate to include a proof here. We also noticed that Dobson [11] gave some results regarding the isomorphism problem of metacirculants of order pq with p, q distinct primes.

Theorem 1.4. *For a prime* $p \equiv 1 \pmod 3$*, the Frobenius group of order* $3p$ *is a CI-group.*

Muzychuck's result [23] and Theorems 1.3 and 1.4 motivate the following conjecture, regarding a more general critical case for classifying CI-groups.

Conjecture 1.5. Let G be a meta-cyclic group which is a member of $\mathcal{CI}$. Then G is a CI-group.

After collecting some preliminary results in Section 2, Theorem 1.1 and Theorem 1.2 will be proved in Section 3 and Section 4, respectively. Theorems 1.3 and 1.4 will then be proved in Section 5 and Section 6, respectively.

2. Preliminary results

In this section, we collect some notation and results which will be used later.

Let G be a group. We use $\mathbf{Z}(G)$, $\Phi(G)$ and $\mathsf{F}(G)$ to denote the centre, the Frattini subgroup and the Fitting subgroup of G, respectively. For $H \leq G$, that is, H is a subgroup of G, by $H \lhd G$ and $H \,\mathsf{char}\, G$ we mean H is a normal subgroup, a characteristic subgroup, respectively, of G. Further, $\mathbf{N}_G(H)$ and $\mathbf{C}_G(H)$ denote the normaliser and the centraliser of H in G, respectively. For a prime divisor p of $|G|$, by G_p, $G_{p'}$ and $\mathbf{O}_p(G)$ we mean a Sylow p-subgroup, a Hall p'-subgroup and the maximal normal p-subgroup of G, respectively.

Let G be a permutation group on Ω. For a subset $\Delta \subseteq \Omega$ and $\alpha \in \Omega$, we use G_Δ and G_α to denote the setwise stabiliser of Δ in G and the stabiliser of α

in G, respectively. For a G-invariant partition $\mathcal{B}$ of Ω, we use $G^{\mathcal{B}}$ to denote the permutation group on $\mathcal{B}$ induced by the action of G on $\mathcal{B}$.

For a group G, let $\hat{G}$ denote the regular subgroup of the symmetric group $\mathrm{Sym}(G)$ induced by the elements of G acting by right multiplication. Let $\Gamma = \mathsf{Cay}(G, S)$ be a Cayley graph of the group G. It easily follows from the definition that $\hat{G}$ is a regular subgroup of $\mathsf{Aut}\Gamma$. And, for $X \leq \mathsf{Aut}\Gamma$, we always use $X_{\mathbf{1}}$ to denote the stabiliser of the vertex $\mathbf{1}$ (corresponding to the identity of G) in X.

For a positive integer n and a graph Γ, denote by $n\Gamma$ a graph which is a disjoint union of n isomorphic copies of Γ. For graphs Γ and Σ, the *wreath product* $\Gamma[\Sigma]$ of Γ and Σ is a graph that has vertex set $V\Gamma \times V\Sigma$ such that $\{(a_1, a_2), (b_1, b_2)\}$ is an edge if and only if either $\{a_1, b_1\} \in E\Gamma$ or $a_1 = b_1$ and $\{a_2, b_2\} \in E\Sigma$. A graph Γ is said to be X*-vertex-transitive* or X*-edge-transitive*, where $X \leq \mathsf{Aut}\Gamma$, if X is transitive on the vertex set or the edge set, respectively, of Γ.

The following simple property about CI-groups will be often used later.

Lemma 2.1. *If G is a CI-group, then all cyclic subgroups of the same order are conjugate under* $\mathsf{Aut}(G)$.

The next simple lemmas about CI-groups will be used in the proof of Theorem 1.2.

Lemma 2.2. ([5, Lemmas 3.2 and 3.5]) *Let G be a CI-group. Then every subgroup of G is a CI-group, and if N is a characteristic subgroup of G then G/N is a CI-group.*

Lemma 2.3. (see [5, Lemma 5.1] and [23]) *Let G be a CI-group. Then*

(1) *for any $a \in G$, $o(a) = 8, 9, 18, k, 2k,$ or $4k$, where k is odd and square-free;*
(2) *any Sylow subgroup of G is elementary abelian, $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, or Q_8.*

To prove Theorems 1.3 and 1.4, we need a criterion of Babai for a Cayley graph to be a CI-graph. Recall that $\hat{G}$ is the regular subgroup of $\mathrm{Sym}(G)$ induced by right multiplications of elements of G.

Theorem 2.4. (Babai [4]) *Let Γ be a Cayley graph of a finite group G. Then Γ is a CI-graph if and only if, for any $\tau \in \mathrm{Sym}(G)$ with $\hat{G}^{\tau} \leq \mathsf{Aut}\,\Gamma$, there exists $\alpha \in \mathsf{Aut}\,\Gamma$ such that $\hat{G}^{\alpha} = \hat{G}^{\tau}$.*

The next lemma will be used to decide whether two given Cayley graphs are isomorphic.

Lemma 2.5. *Let G be a finite group, and let $S, T \subseteq G \setminus \{1\}$ be such that $S^{-1} = S$ and $T^{-1} = T$. Then a permutation $\phi \in \mathrm{Sym}(G)$ is an isomorphism from* $\mathsf{Cay}(G, S)$ *to* $\mathsf{Cay}(G, T)$ *if and only if $(Sg)^{\phi} = Tg^{\phi}$ for all elements $g \in G$.*

Proof. Set $\Gamma = \mathsf{Cay}(G, S)$ and $\Sigma = \mathsf{Cay}(G, T)$. If ϕ is an isomorphism from Γ to Σ, then for each $g \in G$, we have $(Sg)^{\phi} = (\Gamma(g))^{\phi} = \Sigma(g^{\phi}) = Tg^{\phi}$, where $\Gamma(g)$ and $\Sigma(g^{\phi})$ are the sets of neighbors of g and g^{ϕ} in Γ and Σ, respectively.

On the other hand, let $\phi \in \mathrm{Sym}(G)$ be such that $(Sg)^{\phi} = Tg^{\phi}$ for all $g \in G$. Then for any $x, y \in G$, we have

$$\begin{aligned} \{x, y\} \in E\Gamma \quad &\Longleftrightarrow x \in Sy \\ &\Longleftrightarrow x^{\phi} \in (Sy)^{\phi} = Ty^{\phi} \\ &\Longleftrightarrow \{x^{\phi}, y^{\phi}\} \in E\Sigma. \end{aligned}$$

Thus ϕ is an isomorphism from Γ to Σ. $\square$

Finally, we have a simple property about automorphisms of a metacyclic group.

Lemma 2.6. *Let $G = \langle a\rangle \rtimes \langle z\rangle$ such that $\mathbf{Z}(G) < \langle z\rangle$. Then for each automorphism $\sigma \in \mathsf{Aut}(G)$, we have $z^\sigma = a^i z^{1+r}$, for some integers i and r, where $z^r \in \mathbf{Z}(G)$.*

Proof. Let $\sigma \in \mathsf{Aut}(G)$. Then $a^\sigma = a^m$ and $z^\sigma = a^i z^j$ for some integers m, i, j. Now $z^{-1}az = a^l$ for some integer l. Then

$$\begin{array}{rcl} z^{-j}a^m z^j & = & (a^i z^j)^{-1} a^m (a^i z^j) = (z^{-1})^\sigma a^\sigma z^\sigma = (z^{-1}az)^\sigma \\ & = & (a^l)^\sigma = a^{lm} = (z^{-1}az)^m = z^{-1}a^m z. \end{array}$$

Thus z^{j-1} centralises a^m, and so $z^{j-1} \in \mathbf{Z}(G)$, that is, $z^\sigma = a^i z^{1+(j-1)}$. $\square$

3. Proof of Theorem 1.1

The proof of Theorem 1.1 will be given in this section, consisting of three lemmas. Throughout this section, p is an odd prime. For a positive integer n and two sets I, J of integers, by $I \equiv J \,(\mathsf{mod}\ n)$ we mean that each element of I is congruent to an element of J, and vice versa.

Lemma 3.1. *Let G be a Frobenius group of order $4p$. Then G has Cayley graphs of valency 6 which are not CI-graphs. In particular, G is not a CI-group.*

Proof. Write

$$G = \langle a, z \mid a^p = 1, z^4 = 1, zaz^{-1} = a^l\rangle,$$

where l is of order 4 modulo p, that is, $l^2 \equiv -1 \ (\mathsf{mod}\ p)$. Let

$$\begin{array}{rl} S & = \{az, a^{-1}z, az^2, a^{-1}z^2, a^l z^3, a^{-l}z^3\}, \\ T & = \{a^l z, a^{-l}z, az^2, a^{-1}z^2, az^3, a^{-1}z^3\}. \end{array}$$

As $(az)^{-1} = a^l z^3$, $(a^{-1}z)^{-1} = a^{-l}z^3$, $(a^l z)^{-1} = a^{-1}z^3$, $(a^{-l}z)^{-1} = az^3$, and $(a^{\pm1}z^2)^2 = 1$, we see that $S^{-1} = S$, $T^{-1} = T$, and $|S| = |T| = 6$. We claim that the Cayley graphs $\Gamma := \mathsf{Cay}(G, S)$ and $\Sigma := \mathsf{Cay}(G, T)$ are isomorphic.

Let ϕ be a permutation of G defined as follows:

$$\phi: \quad a^i z^j \longmapsto a^{(-1)^j i} z^{-j}.$$

For any element $g = a^i z^j \in G$, straightforward calculation shows that

$$\begin{array}{rl} (Sg)^\phi & = \{a^{(-1)^{j+1}(il+\varepsilon)}z^{3-j},\ a^{(-1)^{j+1}(i+\varepsilon)}z^{2-j},\ a^{(-1)^j(i+\varepsilon)l}z^{1-j} \mid \varepsilon = 1,\, -1\}, \\ Tg^\phi & = \{a^{(-1)^{j+1}il+\varepsilon}z^{3-j},\ a^{(-1)^{j+1}i+\varepsilon}z^{2-j},\ a^{((-1)^j i+\varepsilon)l}z^{1-j} \mid \varepsilon = 1,\, -1\}. \end{array}$$

It is easily shown that for any integers r, s and m, $\{(-1)^m(r+s), (-1)^m(r-s)\} \equiv \{(-1)^m r + s, (-1)^m r - s\}$ $(\mathsf{mod}\ p)$. It follows that $(Sg)^\phi = Tg^\phi$. By Lemma 2.5, ϕ is an isomorphism from Γ to Σ.

Suppose that $S^\alpha = T$ for some $\alpha \in \mathsf{Aut}(G)$. Then $(a^{\pm1}z)^\alpha = a^{\pm l}z$, $(a^{\pm1}z^2)^\alpha = a^{\pm1}z^2$, and $(a^{\pm l}z^3)^\alpha = a^{\pm1}z^3$. It follows that $(a^{\pm1}z^2)^\alpha = a^{\pm l}z^2$, which is a contradiction. Thus Γ is not a CI-graph, and G is not a CI-group. $\square$

We can proceed similarly for the Frobenius groups of order $6p$.

Lemma 3.2. *Let G be a Frobenius group of order $6p$. Then G has Cayley graphs of valency 9 which are not CI-graphs. In particular, G is not a CI-group.*

Proof. Now p is a prime such that $p \equiv 1 \pmod 6$, and the group G has the following presentation:

$$G = \langle a, z \mid a^p = 1, z^6 = 1, zaz^{-1} = a^l \rangle, \text{ where } l \text{ is of order 6 modulo } p.$$

In particular, $l^3 \equiv -1 \pmod p$, $l^4 \equiv -l \pmod p$, and $l^5 \equiv -l^2 \pmod p$.

We take two subsets S and T of $G \setminus \{1\}$ as follows:

$$S = \{az^2, a^{l^2}z^2, a^{l^4}z^2, az^3, a^{l^2}z^3, a^{l^4}z^3, a^l z^4, a^{l^3}z^4, a^{l^5}z^4\},$$
$$T = \{a^l z^2, a^{l^3}z^2, a^{l^5}z^2, az^3, a^{l^2}z^3, a^{l^4}z^3, az^4, a^{l^2}z^4, a^{l^4}z^4\}.$$

Then $S^{-1} = S$, $T^{-1} = T$ and $|S| = |T| = 9$. Set $\Gamma = \mathsf{Cay}(G, S)$ and $\Sigma = \mathsf{Cay}(G, T)$.

Let ϕ be a permutation of G defined by

$$\phi : \ a^i z^j \longmapsto a^{l^{4j}i} z^{-j} = a^{(-1)^j l^j i} z^{-j}, \ \text{ where } 0 \le i \le p-1 \text{ and } 0 \le j \le 5.$$

For each element $g = a^i z^j \in G$, straightforward calculation shows that the two subsets $(Sg)^\phi$ and Tg^ϕ satisfy:

$$(Sg)^\phi = \left\{ \begin{array}{lll} a^{l^{4j}(l^2-li)}z^{4-j}, & a^{l^{4j}(-l-li)}z^{4-j}, & a^{l^{4j}(1-li)}z^{4-j}, \\ a^{l^{4j}(1-i)}z^{3-j}, & a^{l^{4j}(l^2-i)}z^{3-j}, & a^{l^{4j}(-l-i)}z^{3-j}, \\ a^{l^{4j}(-l^2+l^2i)}z^{2-j}, & a^{l^{4j}(l+l^2i)}z^{2-j}, & a^{l^{4j}(-1+l^2i)}z^{2-j} \end{array} \right\},$$
$$Tg^\phi = \left\{ \begin{array}{lll} a^{l^2-l^{4j}li}z^{4-j}, & a^{-l-l^{4j}li}z^{4-j}, & a^{1-l^{4j}li}z^{4-j}, \\ a^{1-l^{4j}i}z^{3-j}, & a^{l^2-l^{4j}i}z^{3-j}, & a^{-l-l^{4j}i}z^{3-j}, \\ a^{-l^2+l^{4j}l^2i}z^{2-j}, & a^{l+l^{4j}l^2i}z^{2-j}, & a^{-1+l^{4j}l^2i}z^{2-j} \end{array} \right\}.$$

Noting that $l^6 \equiv 1 \pmod p$, we have that $\{l^{4j}, -ll^{4j}, l^2l^{4j}\} \equiv \{1, -l, l^2\} \pmod p$. This implies that $(Sg)^\phi = Tg^\phi$. Thus by Lemma 2.5, the permutation ϕ is an isomorphism from Γ to Σ.

Suppose that there exists $\alpha \in \mathsf{Aut}(G)$ such that $S^\alpha = T$. Then by Lemma 2.6, we have $a^\alpha = a^i$, and $z^\alpha = a^j z$, where $0 \le i, j \le p-1$. Thus for $k \in \{0, 1, 2\}$, we have $(a^{l^{2k}}z^2)^\alpha = a^{il^{2k}+j+jl}z^2 \in T$, and so $il^{2k} + j + jl \equiv l, l^3$ or $l^5 \pmod p$. It then follows that $3j(l+1) \equiv 0 \pmod p$. Hence $j \equiv 0 \pmod p$ and so $i \equiv -l^{2t} \equiv l^{3+2t} \pmod p$ for some $t \in \{0, 1, 2\}$. But then $(az^3)^\alpha = a^{-l^{2t}}z^3 = a^{l^{3+2t}}z^3 \notin T$, which is a contradiction since $az^3 \in S$ and $S^\alpha = T$. Thus Γ is not a CI-graph, and G is not a CI-group. $\square$

The final lemma treats metacyclic groups of order $9p$ with centre of order 3.

Lemma 3.3. *Let G be a metacyclic group of order $9p$ such that the centre of G has order 3. Then G has Cayley graphs of valency 20 which are not CI-graphs. In particular, G is not a CI-group.*

Proof. We write $G = \langle a, z \mid a^p = z^9 = 1, zaz^{-1} = a^l \rangle$, where $l \not\equiv 1 \pmod p$ and $l^3 \equiv 1 \pmod p$. By the Sylow Theorem, noting that 3 divides $p-1$, we know that $p \ge 7$. Take two subsets of G as follows:

$$S = \{(a^m z^k)^{\pm 1} \mid m \in \{0, 1, 3\}, k \in \{1, 4, 7\}\} \cup \{az^3, a^{-1}z^6\},$$
$$T = \{(a^m z^k)^{\pm 1} \mid m \in \{0, 1, 3\}, k \in \{1, 4, 7\}\} \cup \{a^{-1}z^3, az^6\}.$$

Then $S^{-1} = S$, $T^{-1} = T$ and $|S| = |T| = 20$. Set $\Gamma = \mathsf{Cay}(G, S)$ and $\Sigma = \mathsf{Cay}(G, T)$.

Let $\tau = (3\,6)(4\,7)(5\,8) \in \mathrm{S}_9$, and define a permutation ϕ of G as follows:

$$\phi : \ a^i z^j \longmapsto a^i z^{j^\tau}, \ \text{ where } 0 \le i \le p-1 \text{ and } 0 \le j \le 8.$$

We claim that ϕ is an isomorphism from Γ to Σ. In the following, for an integer k, k^τ denotes k_0^τ, where $k \equiv k_0 \,(\mathsf{mod}\ 9)$ and $0 \le k_0 \le 8$. For any $g = a^i z^j \in G$, noting that $l^3 \equiv 1 \,(\mathsf{mod}\ p)$, straightforward calculation shows that

$$\begin{aligned}(Sg)^\phi &= \{a^{m+il}z^{(j+k)^\tau}, a^{(i-m)l^{-1}}z^{(j-k)^\tau} \mid m = 0,1,3,\ k = 1,4,7\} \bigcup \\ &\quad \{a^{i+1}z^{(j+3)^\tau},\ a^{i-1}z^{(j+6)^\tau}\},\\ Tg^\phi &= \{a^{m+il}z^{j^\tau+k}, a^{(i-m)l^{-1}}z^{j^\tau-k} \mid m = 0,1,3,\ k = 1,4,7\} \bigcup \\ &\quad \{a^{i-1}z^{j^\tau+3}, a^{i+1}z^{j^\tau+6}\}.\end{aligned}$$

Then further calculation shows that, for $0 \le j \le 8$,

$$\begin{array}{l}\{(j+t)^\tau \mid t = 1,4,7,-1,-4,-7\} \equiv \{j^\tau + t \mid t = 1,4,7,-1,-4,-7\},\\ (j+3)^\tau \equiv j^\tau + 6, \quad (j+6)^\tau \equiv j^\tau + 3.\end{array} \quad (\mathsf{mod}\ 9).$$

It follows that $(Sg)^\phi = Tg^\phi$. Therefore, ϕ is an isomorphism from Γ to Σ.

Now assume by way of contradiction that there exists an automorphism $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$. The automorphism σ has the form $a^\sigma = a^r$, $z^\sigma = a^s z^{1+3t}$ for $1 \le r \le p-1$, $0 \le s \le p-1$, $0 \le t \le 2$. If we fix r, s, t then

$$S^\sigma = \{(a^{m'}z^{k'})^{\pm 1} \mid m' \in \{s, r+s, 3r+s\},\ k' \in \{1,4,7\}\} \cup \{a^r z^3, a^{-r}z^6\}.$$

Comparing S^σ with T we must have $\{s, r+s, 3r+s\} \equiv \{0,1,3\}$ and $r \equiv -1 \,(\mathsf{mod}\ p)$. It leads to $p \le 5$, which is a contradiction. Thus Γ is not a CI-graph, and hence G is not a CI-group. □

4. An explicit list of candidates for CI-groups

This section is devoted to proving Theorem 1.2. A group G is said to be *coprime-indecomposable* if whenever $G = A \times B$ with $(|A|, |B|) = 1$ then $A = 1$ or $B = 1$. We first treat a special case.

Lemma 4.1. *Let $G \cong \mathbb{Z}_p^d \rtimes \mathbb{Z}_n$, where p is a prime, $d \ge 1$, $n \ge 2$ and $(p,n) = 1$, be a coprime-indecomposable CI-group. Then G is isomorphic to $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$ ($\cong \mathrm{A}_4$), $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$, or $\mathsf{E}(\mathbb{Z}_p^d, n)$ with $n \in \{2,3,4,8\}$; in particular, $G \in \mathcal{CI}$.*

Proof. Write $G = N \rtimes L$, where $N \cong \mathbb{Z}_p^d$ and $L = \langle z \rangle \cong \mathbb{Z}_n$. It is easily shown using Lemma 2.1 and the coprime-indecomposable assumption that $N \cap \mathbf{Z}(G) = 1$, and hence $\mathbf{Z}(G) = \mathbf{C}_L(N)$.

Assume first that there exists an element $a \in N$ such that z does not normalise $\langle a \rangle$. Let $b := a^z$ and $c \in N \setminus (\langle a \rangle \cup \langle b \rangle)$; let $S = \{a, a^{-1}, b, b^{-1}\}$, and $T = \{a, a^{-1}, c, c^{-1}\}$. Then $\langle S \rangle \cong \langle T \rangle$, and $\mathsf{Cay}(\langle S \rangle, S) \cong \mathsf{Cay}(\langle T \rangle, T)$. Thus $\mathsf{Cay}(G, S) \cong \mathsf{Cay}(G, T)$. Since G is a CI-group, $S^\sigma = T$ for some $\sigma \in \mathsf{Aut}(G)$. Now $z^\sigma = fz^i$ for some $f \in N$ and some integer i, and so $z^{-i}a^\sigma z^i = (z^{-1}az)^\sigma = b^\sigma$. Thus $\{a^\sigma, (a^\sigma)^{-1}, b^\sigma, (b^\sigma)^{-1}\} = S^\sigma = T = \{a, a^{-1}, c, c^{-1}\}$. It follows that $\{c, c^{-1}\}$ is conjugate by z^i or z^{-i} to $\{a, a^{-1}\}$. Thus, letting $\Delta = \{\{x, x^{-1}\} \mid x \in N \setminus \{1\}\}$, we have that $L = \langle z \rangle$ acts by conjugation transitively on Δ. The kernel of the L-action on Δ contains $\mathbf{C}_L(N) = \mathbf{Z}(G)$. Thus $\langle \overline{z} \rangle := \langle z \rangle / \mathbf{Z}(G)$ is transitive on Δ, and so $|\Delta| = \frac{p^d - 1}{(p-1,2)}$ divides the order of $\langle \overline{z} \rangle$.

Since N is a characteristic subgroup of G, N is invariant under $\mathsf{Aut}(G)$. Let A and I be the groups of automorphisms of N induced by $\mathsf{Aut}(G)$ and $\mathsf{Inn}(G)$, respectively. Then $\langle \overline{z} \rangle = I \lhd A \le \mathrm{GL}(d,p)$. It follows that $A \le \mathbf{N}_{\mathrm{GL}(d,p)}(I) \cong \Gamma\mathrm{L}(1, p^d) \cong \mathbb{Z}_{p^d-1} \rtimes \mathbb{Z}_d$, see [15, II, 7.3]. In particular, $|A|$ is divisor of $(p^d - 1)d$.

Let $\Omega = \{\{x, x^{-1}, y, y^{-1}\} \mid x, y \in N,\ \langle x, y\rangle \cong \mathbb{Z}_p^2\}$. Then for each tuple $\{x, x^{-1}, y, y^{-1}\}$ in Ω, the Cayley graph $\mathsf{Cay}(G, \{x, x^{-1}, y, y^{-1}\})$ is isomorphic to $\mathsf{Cay}(G, S)$. Since G is a CI-group, $\{x, x^{-1}, y, y^{-1}\}$ is conjugate in $\mathsf{Aut}(G)$ to S. It follows that A is transitive on Ω. Thus $|\Omega|$ divides $|A|$. Now $|A|$ divides $(p^d - 1)d$, and

$$|\Omega| = \begin{cases} (2^d - 1)(2^d - 2), & \text{if } p = 2; \\ \frac{p^d-1}{2}(\frac{p^d-1}{2} - \frac{p-1}{2}) = \frac{(p^d-1)(p^d-p)}{4}, & \text{if } p \text{ is odd.} \end{cases}$$

Therefore, if $p = 2$, then $(2^d-1)(2^d-2)$ divides $(2^d-1)d$, so that $d = 2$; while if p is odd, then $\frac{(p^d-1)(p^d-p)}{4}$ divides $(p^d - 1)d$, which is not possible. Thus $(p, d) = (2, 2)$. Since G is coprime-indecomposable, L is a cyclic 3-group. By Lemma 2.3, $L \cong \mathbb{Z}_3$ or $\mathbb{Z}_9$. Thus $G = \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3 \cong \mathrm{A}_4$, or $G = \mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ with centre of order 3.

Assume next that z normalises every cyclic subgroup of N. Since G is coprime-indecomposable, $\mathbf{C}_L(N) = \mathbf{Z}(G)$ contains no Sylow subgroups of L.

Take an arbitrary element $x \in N \setminus \{1\}$. Suppose that $\mathbf{C}_L(x)$ contains a Sylow q-subgroup L_q of L, where q is a prime divisor of n, that is, $L_q \le \mathbf{C}_L(x)$. Then x lies in the centre $\mathbf{Z}(F)$ of the subgroup $F := N \rtimes L_q$. Now F is a CI-group, and hence all subgroups of F of order p are conjugate in $\mathsf{Aut}(F)$. Since $\mathbf{Z}(F)$ is a characteristic subgroup of F, it follows that $N \le \mathbf{Z}(F)$, so F is abelian, which is a contradiction since G is coprime-indecomposable. Thus no Sylow subgroup of L centralises x; in particular, z does not centralise x.

Let $H = \langle x, z\rangle$, and let $\overline{H} = H/\mathbf{Z}(H) = \langle \overline{x}\rangle \rtimes \langle \overline{z}\rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_m$, where m is the order of the image $\overline{z}$. Then $\mathbf{Z}(\overline{H}) = 1$, and by the conclusion given in the previous paragraph, each prime divisor of n divides m. Now $\overline{H}$ is a CI-group, and so a subgroup of $\mathsf{Aut}(\overline{H})$ is transitive on the set $\{\{\overline{z}^i, \overline{z}^{-i}\} \mid (i, m) = 1\}$. By Lemma 2.6, an automorphism $\sigma \in \mathsf{Aut}(\overline{H})$ is such that $\overline{z}^\sigma = \overline{x}^j\overline{z}$ for some j. Thus the set $\{\{\overline{z}^i, \overline{z}^{-i}\} \mid (i, m) = 1\}$ contains only one element, and so $m = 2, 3, 4$ or 6. By Theorem 1.1, we have $m = 2$ or 3, and by Lemma 2.3, $o(z) \in \{2, 3, 4, 8, 9\}$. Further, if $o(z)$ is even, then z inverts all elements of N; while if $o(z) = 3$ or 9, then $x^z = x^l$ where $l^3 \equiv 1 \pmod p$, and $l \not\equiv 1 \pmod p$. By Theorem 1.1, $o(z) \ne 9$. Therefore, since x is an arbitrary element of N, we conclude that $G = \mathsf{E}(\mathbb{Z}_p^d, n)$ for some $n \in \{2, 3, 4, 8\}$. □

Lemma 4.2. *If G is a finite CI-group and P is a Sylow p-subgroup of G, then either P is normal in G, or $p \le 3$ and P is cyclic.*

Proof. We know (see [16]) that G is soluble. Let $\mathsf{F}(G)$ denote the Fitting subgroup of G. Let us assume that P is not normal, so $P \not\le \mathsf{F}(G)$.

First suppose that P is elementary abelian. Then by Lemma 2.1 all subgroups of order p are conjugate under $\mathsf{Aut}(G)$, hence we see that $P \cap \mathsf{F}(G) = 1$. In particular, $(p, |\mathsf{F}(G)|) = 1$. In a soluble group $\mathbf{C}_G(\mathsf{F}(G)) \le \mathsf{F}(G)$, hence P does not centralise $\mathsf{F}(G)$. Then there exists a prime $r \ne p$ such that $R = \mathbf{O}_r(G) \le \mathsf{F}(G)$ is not centralised by P. Let $H = RP$. By Lemma 2.2 H is a CI-group as well, hence the previous argument yields that $\mathsf{F}(H) = R$. Thus $|P|$ divides $|\mathsf{Aut}(R)|$. So R cannot be a cyclic 2-group. If R is a cyclic 3-group, then $|P| = 2$. If $R \cong \mathrm{Q}_8$, then $|P| = 3$, since $|\mathsf{Aut}(\mathrm{Q}_8)| = 24$. If $R \cong \mathbb{Z}_2^2$, then again $|P| = 3$. So in these cases $p = 2$ or 3, and P is cyclic, as we have claimed. Therefore, we may assume that R is an elementary abelian group of order at least 5. Let $1 \ne z \in P$, then z acts nontrivially on R. Then $L = R \rtimes \langle z\rangle$ is a coprime-indecomposable CI-group, hence

Lemma 4.1 yields that $L \cong \mathsf{E}(R, n)$ with $n \in \{2, 3, 4, 8\}$. So we see that $p = 2$ or 3. Moreover, any other nontrivial element $z' \in P$ acts on R the same way as z or z^{-1} does, hence P is cyclic, since otherwise $z^{-1}z'$ or zz' would act trivially on R, contrary to $\mathbf{C}_H(R) = \mathbf{C}_H(\mathsf{F}(H)) \leq \mathsf{F}(H) = R$.

If P is not elementary abelian, then by Lemma 2.3 it is either cyclic of order 4, 8, or 9, or P is the quaternion group. We have to exclude the last possibility. We can proceed similarly as in the previous paragraph, the only difference is that considering subgroups of order 4 we can deduce just that $|\mathsf{F}(G) \cap P| \leq 2$ and so 4 must divide $|\mathsf{Aut}(R)|$, and further, $\mathsf{F}(G)$ is not a 2-group. $\square$

Lemma 4.3. *If G is a CI-group and P is a normal Sylow p-subgroup of G, then either $|G : \mathbf{C}_G(P)| \leq 3$, or P is the quaternion group and $G = P \times H$ with a normal subgroup H of odd order.*

Proof. First let us consider the case when P is the quaternion group. Let H be a complement to P in G. Then $|H|$ is odd and $|H : \mathbf{C}_H(P)|$ divides $|\mathsf{Aut}(P)| = 24$. Hence either H centralises P and so $G = P \times H$, or there is an element z of 3-power order in H not centralizing P. By Lemma 2.3, z has order 3 or 9, hence $P \rtimes \langle z \rangle$ is isomorphic to one of the groups $\mathrm{Q}_8 \rtimes \mathbb{Z}_3$ or $\mathrm{Q}_8 \rtimes \mathbb{Z}_9$. However, these groups are not CI-groups (see [7]).

Now let P be a normal abelian Sylow p-subgroup of G. If P is a cyclic 2-group, then $\mathbf{C}_G(P) = G$. If $P \cong \mathbb{Z}_2^2$, then $|G : \mathbf{C}_G(P)|$ divides 3. If $P \cong \mathbb{Z}_3$ or $\mathbb{Z}_9$, then $|G : \mathbf{C}_G(P)| \leq 2$. So we may assume that P is elementary abelian of order at least 5. Let H be a complement to P in G, and let $z \in H$ be an element not centralizing P and take $L = P \rtimes \langle z \rangle$. Then $L/\mathbf{Z}(L)$ is a coprime-indecomposable CI-group, hence Lemma 4.1 yields that $L/\mathbf{Z}(L) \cong \mathsf{E}(P, n)$ for some $n \in \{2, 3, 4, 8\}$. Therefore, for every $z \in H$ there is a k such that $z^{-1}xz = x^k$ for all $x \in P$ and either $k = -1$ or $k^3 \equiv 1 \pmod{p}$. So the group of automorphisms induced by G on P is cyclic and every induced automorphism has order at most 3. Thus we have $|G : \mathbf{C}_G(P)| \leq 3$. $\square$

As usual, let $\mathbf{O}^{p'}(G)$ denote the smallest normal subgroup of index not divisible by p. Obviously, $\mathbf{O}^{p'}(G)$ is a characteristic subgroup; it is the subgroup generated by all Sylow p-subgroups of G. Clearly, $\mathbf{O}^{p'}(\mathbf{O}^{p'}(G)) = \mathbf{O}^{p'}(G)$ and $\mathbf{O}^{p'}(G)$ has no non-trivial direct product decompositions with a p'-factor. Recall that H is a Hall subgroup in G if $|H|$ and $|G : H|$ are coprime.

Lemma 4.4. *If G is a CI-group, then $\mathbf{O}^{2'}(G)$ and $\mathbf{O}^{3'}(G)$ are Hall subgroups in G.*

Proof. Let $p = 2$ or 3, let r be a prime divisor of $|\mathbf{O}^{p'}(G)|$ and R a Sylow r-subgroup of G. We have to show that $R \leq \mathbf{O}^{p'}(G)$. If $r = p$, then $\mathbf{O}^{p'}(G)$ contains all Sylow p-subgroups of G by definition. Let $r \neq p$. If R is elementary abelian, then we can use Lemma 2.1 to see that $\mathbf{O}^{p'}(G)$ contains all elements of order r. So we may assume that R is not elementary abelian, that is, either R is cyclic of order 4, 8, or 9, or $R \cong \mathrm{Q}_8$. The last case is impossible, since by Lemmas 4.2 and 4.3 we would have $G = R \times H$, and so $\mathbf{O}^{3'}(G) \leq H$ would have odd order.

Let P be a Sylow p-subgroup of G. The lemma follows if P is normal. So we may assume that P is not normal in G in which case Lemma 4.2 gives that P is also cyclic. Let N be the product of all normal Sylow s-subgroups of G for

$s \geq 5$ (cf. Lemma 4.2). Then G/N is a $\{2,3\}$-group and now both the Sylow 2-subgroup and the Sylow 3-subgroup of G/N are cyclic. Hence G/N is either cyclic, or $G/N \cong \mathbb{Z}_{3^i} \rtimes \mathbb{Z}_{2^j}$ and is not cyclic. In either case $\mathbf{O}^{3'}(G)$ has odd order, hence $p = 2$, $r = 3$ and $i = 2$. In the first case $|\mathbf{O}^{2'}(G)|$ is not divisible by 3, so the second case occurs, and then $\mathbf{O}^{2'}(G)$ does indeed contain a Sylow 3-subgroup of G. □

Lemma 4.5. *If G is a CI-group, then either $\mathbf{O}^{2'}(G) \cap \mathbf{O}^{3'}(G) = 1$, or one of these subgroups contains the other.*

Proof. Using the previous lemma, we see that if 3 divides $|\mathbf{O}^{2'}(G)|$, then $\mathbf{O}^{3'}(G) \leq \mathbf{O}^{2'}(G)$. Symmetrically, 2 dividing $|\mathbf{O}^{3'}(G)|$ implies that $\mathbf{O}^{2'}(G) \leq \mathbf{O}^{3'}(G)$. So let us suppose that neither of these occurs, that is, the order of the intersection $I = \mathbf{O}^{2'}(G) \cap \mathbf{O}^{3'}(G)$ is not divisible by 2 and 3.

Assume by way of contradiction that I is nontrivial. We know that I is a normal Hall subgroup of G. Let r be a prime divisor of $|I|$ and R a Sylow r-subgroup in G. Then $r \geq 5$, and Lemma 4.2 yields that R is normal in G. By Lemma 4.3 $|G : \mathbf{C}_G(R)| \leq 3$. Suppose that $|G : \mathbf{C}_G(R)| = 3$. Then $\mathbf{C}_G(R) \geq \mathbf{O}^{2'}(G)$, so R lies in the centre of $\mathbf{O}^{2'}(G)$. Let K_2 be a complement to R in $\mathbf{O}^{2'}(G)$, then $\mathbf{O}^{2'}(G) = R \times K_2$, a contradiction. Similarly, $|G : \mathbf{C}_G(R)| = 2$ leads to a direct decomposition $\mathbf{O}^{3'}(G) = R \times K_3$; and $|G : \mathbf{C}_G(R)| = 1$ implies $G = R \times K_1$. □

Lemma 4.6. *If G is a CI-group with $\mathbf{O}^{2'}(G) = G$, then G is one of the following groups: $\mathbb{Z}_2^n$, $\mathbb{Z}_4$, $\mathbb{Z}_8$, Q_8, $\mathsf{E}(M, 2^j)$ $(j = 1, 2, 3)$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_2$, $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$.*

Proof. Let P be a Sylow 2-subgroup of G. If P is normal in G, then $G = \mathbf{O}^{2'}(G) = P$ and Lemma 2.3 gives the result. Otherwise, Lemma 4.2 yields that P is cyclic. It is well-known that groups with cyclic Sylow 2-subgroups contain a normal 2-complement N, that is $G = N \rtimes P$. Let $r \geq 5$ be a prime divisor of $|G|$ and R a Sylow r-subgroup of G. Then R is normal in G and $|G : \mathbf{C}_G(R)| \leq 3$ (see Lemmas 4.2 and 4.3). Arguing as in the proof of Lemma 4.5, we obtain that $|G : \mathbf{C}_G(R)| = 2$. So R lies in the centre of N. Hence also the Sylow 3-subgroup of N is normal and N is the direct product of its Sylow subgroups. The Sylow 3-subgroup is either elementary abelian, or it is cyclic of order 9. By Lemma 2.3 a CI-group cannot contain elements of order $9k$ for $k \geq 3$. Hence N is either a direct product of elementary abelian groups or $N \cong \mathbb{Z}_9$. Let us choose a generator $z \in P$. Applying Lemma 4.1 to $R \rtimes P$ for each Sylow subgroup R of N we obtain that $z^{-1}xz = x^{-1}$ for every $x \in N$, and thus $G \cong \mathsf{E}(N, 2^j)$ or $\mathbb{Z}_9 \rtimes \mathbb{Z}_{2^j}$ for $j = 1$, 2, or 3. In fact, $\mathbb{Z}_9 \rtimes \mathbb{Z}_8$ cannot occur, since it contains elements of order 36. □

Lemma 4.7. *If G is a CI-group with $\mathbf{O}^{3'}(G) = G$, then G is one of the following groups: $\mathbb{Z}_3^n$, $\mathbb{Z}_9$, $\mathsf{E}(M, 3)$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$, $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$.*

Proof. Let P be a Sylow 3-subgroup of G. If P is normal in G, then $\mathbf{O}^{3'}(G) = P$ and Lemma 2.3 gives the result. Otherwise, Lemma 4.2 yields that P is cyclic.

If a Sylow 2-subgroup of G is cyclic, then G has a normal subgroup of index 2, contrary to the assumption $\mathbf{O}^{3'}(G) = G$. Now Lemma 4.2 yields that the Sylow 2-subgroup of G is normal. If it is isomorphic to the quaternion group, then Lemma 4.3 gives a contradiction. So the Sylow 2-subgroup of G is elementary abelian and of order at least 4.

Let $r \neq 3$ be a prime divisor of $|G|$ and let R be a Sylow r-subgroup in G. Then $R \lhd G$. Since $\mathbf{O}^{3'}(G) = G$, we conclude that RP is coprime-indecomposable. Then Lemma 4.1 gives that RP is either $\mathsf{E}(R, 3)$ (if $r \neq 2$) or $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_{3^j}$ ($j = 1$ or 2). It remains to show that a prime $r \geq 5$ and 2 cannot simultaneously divide the order of G.

Suppose that $|G|$ is even and $|G|$ has a prime divisor $r \geq 5$. Then, by the previous argument, we may write $G = (\mathbb{Z}_2^2 \times M) \rtimes \mathbb{Z}_3$, and so there exist elements $a_0, a_1, b, z \in G$ such that $o(a_0) = o(a_1) = 2$, $o(b) = r$, $o(z) = 3$ and $a_0^z = a_1$ and $b^z = b^l$ where $l^3 \equiv 1$ and $l \not\equiv 1 \pmod{r}$. Set $S = \{a_0 b^l, (a_0 b^l)^{-1}, a_1 b, (a_1 b)^{-1}\}$ and $T = \{a_0 b, (a_0 b)^{-1}, a_1 b^l, (a_1 b^l)^{-1}\}$. Then $\langle S \rangle = \langle T \rangle = \langle a_0, a_1, b \rangle = \mathbb{Z}_2^2 \times \mathbb{Z}_r$, and there exists $\sigma \in \mathsf{Aut}(\langle S \rangle) \cong \mathsf{Aut}(\mathbb{Z}_2^2) \times \mathsf{Aut}(\mathbb{Z}_r)$ such that $(a_1 b)^\sigma = a_0 b$ and $(a_0 b^l)^\sigma = a_1 b^l$. Thus $\mathsf{Cay}(\langle S \rangle, S) \cong \mathsf{Cay}(\langle T \rangle, T)$ and so $\mathsf{Cay}(G, S) \cong \mathsf{Cay}(G, T)$. Since G is a CI-group, $S^\rho = T$ for some $\rho \in \mathsf{Aut}(G)$. Thus $(a_0 b^l, a_1 b)^\rho = ((a_0 b)^\varepsilon, (a_1 b^l)^{\varepsilon'})$ or $((a_1 b^l)^{\varepsilon'}, (a_0 b)^\varepsilon)$ where $\varepsilon, \varepsilon' = \pm 1$. It follows that either

$$(a_0, a_1)^\rho = (a_0, a_1) \text{ and } (b^l, b)^\rho = (b^\varepsilon, b^{l\varepsilon'}), \text{ or}$$
$$(a_0, a_1)^\rho = (a_1, a_0) \text{ and } (b^l, b)^\rho = (b^{l\varepsilon'}, b^\varepsilon).$$

If the first line above holds, then $b^\rho = b^{l\varepsilon'}$, and $b^\varepsilon = (b^l)^\rho = (b^\rho)^l = b^{l^2\varepsilon'}$ which implies that $r = o(b)$ divides $l^2 \pm 1$, which is a contradiction. Hence the second line holds, and since $z^\rho = cz^i$ for some $c \in \mathbb{Z}_2^2 \times M$ and some $i = 1$ or -1, we have that $a_0 = a_1^\rho = (z^{-1} a_0 z)^\rho = (cz^i)^{-1} a_1 c z^i = z^{-i} a_1 z^i$. Thus $i = -1$, and thus $b^{l\varepsilon'} = (b^l)^\rho = (z^{-1} b z)^\rho = (cz^{-1})^{-1} b^\varepsilon c z^{-1} = z b^\varepsilon z^{-1} = b^{l^2 \varepsilon}$. Therefore, r divides $l^2 - l\varepsilon'$, which is not possible. □

Now we are ready to prove Theorem 1.2.

Proof of Theorem 1.2: If $\mathbf{O}^{2'}(G) \geq \mathbf{O}^{3'}(G) > 1$, then let $H_2 = \mathbf{O}^{2'}(G)$ and $H_3 = 1$. If $\mathbf{O}^{3'}(G) \geq \mathbf{O}^{2'}(G) > 1$, then let $H_3 = \mathbf{O}^{3'}(G)$ and $H_2 = 1$. Otherwise, we know from Lemma 4.5 that $\mathbf{O}^{2'}(G) \cap \mathbf{O}^{3'}(G) = 1$. In this case, if $\mathbf{O}^{2'}(G)$ is nonabelian, then let $H_2 = \mathbf{O}^{2'}(G)$, else put $H_2 = 1$, and if $\mathbf{O}^{3'}(G)$ is nonabelian, then let $H_3 = \mathbf{O}^{3'}(G)$, else put $H_3 = 1$. So we have defined H_2 and H_3 in all cases. Note that both of them are Hall subgroups of G. If r is a prime not dividing $|H_2 H_3|$, then either $r = 2$ or 3 and $\mathbf{O}^{r'}(G)$ is an abelian Sylow r-subgroup of G, or $r \geq 5$. In all cases the Sylow r-subgroup is normal in G. Finally, let H_1 be the product of these Sylow subgroups.

Then it is clear, using Lemmas 4.4 and 4.5, that the orders of H_1, H_2, and H_3 are pairwise coprime, and G is the direct product of these subgroups. One can see that H_1 is abelian, while H_2 and H_3 are either nonabelian or trivial.

Let us assume first that G does not contain elements of order 8 or 9. Then the Sylow subgroups of H_1 are elementary abelian, except that the Sylow 2-subgroup can also be $\mathbb{Z}_4$. The structure of H_2 as described in Theorem 1.2(a) follows from Lemma 4.6, and for H_3 from Lemma 4.7.

If G contains elements of order 8, then it cannot contain any elements of order $8k$ with $k \geq 2$ (see Lemma 2.3). Exactly one of the direct factors must contain an element of order 8, hence the group is directly indecomposable. From Lemma 4.7 we see that H_3 cannot contain any element of order 8. Hence either $G = H_1 \cong \mathbb{Z}_8$, or $G = H_2 \cong \mathsf{E}(M, 8)$, as follows from Lemma 4.6. Thus we obtain part (b) of Theorem 1.2.

If G contains elements of order 9, then it cannot contain any elements of order $9k$ with $k \geq 3$, see Lemma 2.3. If H_3 contains elements of order 9, then $G = H_3 \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$ by Lemma 4.7. If H_2 contains elements of order 9, then $G = H_2 \cong \mathbb{Z}_9 \rtimes \mathbb{Z}_{2^j}$ ($j = 1$ or 2) by Lemma 4.6. Finally, if H_1 contains elements of order 9, then H_2 could only contain elements of order 2, but then it would be abelian, contrary to the construction, so $H_2 = 1$ in this case. Hence $G = H_1 = \mathbb{Z}_9 \times \mathbb{Z}_2^n$ for some n. By the result of Nowitz [25], $n \leq 5$. Thus we have proved part (c) of Theorem 1.2 as well. □

5. Proof of Theorem 1.3

It is known that the groups $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ and $\mathbb{Z}_3 \rtimes \mathbb{Z}_8$ are CI-groups, see Royle [29]. Let $p \geq 5$ be a prime throughout this section, and let

$$G = \langle a, z \mid a^p = 1, z^8 = 1, z^{-1}az = a^{-1} \rangle.$$

Let $\Gamma = \mathsf{Cay}(G, S)$ be an undirected Cayley graph, and let $A = \mathsf{Aut}\Gamma$.

Assume that $S \subset \langle a, z^2 \rangle \cong \mathbb{Z}_{4p}$. Then by [23], $\mathsf{Cay}(\langle S \rangle, S)$ is a CI-graph of $\langle S \rangle$. It is easily shown that every automorphism of $\langle a, z^2 \rangle$ can be extended to an automorphism of G. It then follows that Γ is a CI-graph of G.

Thus we assume that $S \not\subseteq \langle a, z^2 \rangle$. Also, replacing Γ by its complementary graph if necessary, we may assume that $|S| < 4p$.

Let P be a Sylow p-subgroup of A with $\hat{a} \in P$. Consider the action of P on $V\Gamma$. It is easily shown that either P has exactly 8 orbits in $V\Gamma$, all of which are of length p, or $p = 5$ or 7, and P has exactly one orbit of length p^2 and $8 - p$ orbits of length p. Accordingly, we use different subsections to treat separate cases.

5.1. $|P| = p$**.** To treat this case, we need a property about the symmetric group S_8. It is easily shown that S_8 has exactly $3^2 \cdot 5 \cdot 7$ Sylow 2-subgroups, all 8-cycles are conjugate in S_8, and $\mathbf{C}_{\mathrm{S}_8}(\pi) = \langle \pi \rangle$ for an 8-cycle π of S_8. Hence the number of 8-cycles in S_8 is $2^4 \cdot 3^2 \cdot 5 \cdot 7$, and each Sylow 2-subgroup of S_8 contains at least sixteen 8-cycles. Moreover, the following lemma shows that each Sylow 2-subgroup of S_8 contains exactly sixteen 8-cycles, and so any pair of Sylow 2-subgroups contain no common 8-cycles.

Lemma 5.1. *Let $\mu = (0\,2\,4\,6)$, $\nu = (1\,2)(3\,4)(5\,6)(7\,0)$ and $\tau = (2\,6)$. Set $R = \langle \mu, \tau, \nu \rangle$. Then R is a Sylow 2-subgroup of S_8, and R contains exactly four cyclic subgroups of order 8, which are $\langle \pi \rangle$, $\langle \pi^\tau \rangle$, $\langle \pi^{\tau\pi} \rangle$ and $\langle \pi^\rho \rangle$, where $\pi = \mu\nu = (0\,1\,2\,3\,4\,5\,6\,7)$ and $\rho = \tau\tau^\pi = (2\,6)(3\,7)$.*

Proof. Straightforward calculation shows that R is a Sylow 2-subgroup of S_8, and R contains four cyclic subgroups of order 8, say, $\langle \pi \rangle$, $\langle \pi^\tau \rangle$, $\langle \pi^{\tau\pi} \rangle$ and $\langle \pi^\rho \rangle$, where $\pi = \mu\nu = (0\,1\,2\,3\,4\,5\,6\,7)$ and $\rho = \tau\tau^\pi = (2\,6)(3\,7)$. Further, these four subgroups contain sixteen different 8-cycles.

Since $R < \mathrm{S}_4 \wr \mathrm{S}_2 < \mathrm{S}_8$, we may write $R \cong \mathrm{D}_8 \wr \mathrm{S}_2$. Now we need only to show $\mathrm{D}_8 \wr \mathrm{S}_2$ contains at most sixteen elements of order 8. Set $\mathrm{D}_8 = \langle a, b \mid a^4 = b^2 = 1, bab = a^{-1} \rangle$, and $\mathrm{S}_2 = \langle \eta \rangle$. Let $\theta \in \mathrm{D}_8 \wr \mathrm{S}_2$ be of order 8. Then $\theta = (x, y; \eta)$ for some $x, y \in D_8$, and hence $\theta^2 = (xy, yx; 1)$ is of order 4. Thus, either $x, y \in \langle a \rangle$, or $x, y \in \mathrm{D}_8 \setminus \langle a \rangle$. We first assume that $x, y \in \langle a \rangle$. Then $x = a^i$ and $y = a^j$ for some integers i and j, and so $xy = a^{i+j} = yx$. It follows that a^{i+j} is of order 4, and hence $i + j$ is odd, where $0 \leq i, j \leq 3$. Therefore, in this case, (x, y) has at most 8 choices. Now $x, y \in \mathrm{D}_8 \setminus \langle a \rangle$. Then $x = a^i b$ and $y = a^j b$ for some integers i and

j, and so $xy = a^{i-j} = (yx)^{-1}$. It follows that a^{i-j} is of order 4, and hence $i-j$ is odd. Thus, if $x, y \in \mathrm{D}_8 \setminus \langle a\rangle$, then (x, y) has at most 8 choices. Then, the above argument indicates that $\mathrm{D}_8 \wr \mathrm{S}_2$ contains at most sixteen elements of order 8. This completes the proof. $\square$

The next lemma shows that if $|P| = p$ then Γ is a CI-graph.

Lemma 5.2. *Assume that $A = \mathsf{Aut}\Gamma$ contains another regular subgroup $\tilde{G} = \langle\tilde{a}\rangle \rtimes \langle\tilde{z}\rangle \cong \hat{G}$. If $\langle\hat{a}\rangle$ and $\langle\tilde{a}\rangle$ are conjugate in A, then $\hat{G}$ and $\tilde{G}$ are also conjugate in A. In particular, if $|P| = p$ then Γ is a CI-graph.*

Proof. Suppose that $\langle\hat{a}\rangle$ and $\langle\tilde{a}\rangle$ are conjugate in A. Then, replacing $\tilde{G}$ by a suitable conjugate if necessary, we may assume that $\tilde{a} = \hat{a}$, and thus $\hat{z}, \tilde{z} \in \mathbf{N}_A(\langle\hat{a}\rangle)$ and $\hat{a}^{\hat{z}} = \hat{a}^{-1} = \hat{a}^{\tilde{z}}$. Let Q be a Sylow 2-subgroup of $\mathbf{N}_A(\langle\hat{a}\rangle)$ such that $z, \tilde{z} \in Q$. Then the length of any orbit of Q is $2^r \geq 8$, and hence there exists an orbit Λ of length 8. Since $\langle\hat{z}\rangle$ and $\langle\tilde{z}\rangle$ are semi-regular, they are transitive on Λ. Since $\hat{G}$ is transitive on $V\Gamma$, we may assume that $\mathbf{1} \in \Lambda$, so that $\Lambda = \{\mathbf{1}, z, z^2, \cdots, z^7\}$.

Let π and $\tilde{\pi}$ be the permutations on the set $\{0, 1, \cdots, 7\}$ induced by the actions of $\hat{z}$ and $\tilde{z}$ on Λ such that $(z^i)^{\hat{z}} = z^{i^\pi}$ and $(z^i)^{\tilde{z}} = z^{i^{\tilde{\pi}}}$, respectively. Then $\pi = (0\,1\,2\,3\,4\,5\,6\,7)$. Consider the action of $\tilde{z}$ on $V\Gamma$. For integers i and j, since $(z^ia^j)^{\tilde{z}} = (z^i)^{\hat{a}^j\tilde{z}} = (z^i)^{\tilde{z}\hat{a}^{-j}} = ((z^i)^{\tilde{z}})^{\hat{a}^{-j}} = z^{i^{\tilde{\pi}}}a^{-j}$, the action of $\tilde{z}$ on Λ is independent of j. Hence $\tilde{\pi}$ uniquely determines the action of $\tilde{z}$ on $V\Gamma$, and so uniquely determines the element $\tilde{z}$ of $\tilde{G}$. By Lemma 5.1, a Sylow 2-subgroup of S_8 contains exactly four cyclic subgroups of order 8, $\langle\pi\rangle$, $\langle\pi^\tau\rangle$, $\langle\pi^{\tau\pi}\rangle$ and $\langle\pi^\rho\rangle$, where $\tau = (2\,6)$ and $\rho = \tau\tau^\pi = (2\,6)(3\,7)$. Then we may assume that $\langle\tilde{\pi}\rangle$ is one of these four subgroups.

Next we prove that $\hat{G}$ and $\tilde{G}$ are conjugate in A. For $\omega \in \mathrm{S}_8$, let $f_\omega \in \mathrm{Sym}(V\Gamma)$ be such that for any integers i and j, $(z^ia^j)^{f_\omega} = z^{i^\omega}a^j$. Then $(z^ia^j)^{f_\omega^{-1}\hat{a}f_\omega} = (z^ia^j)^{\hat{a}}$ and $(z^ia^j)^{f_\omega f_{\omega'}} = z^{i^{\omega\omega'}}a^j = (z^ia^j)^{f_{\omega\omega'}}$, for all integers i, j, and so $\hat{a}^{f_\omega} = f_\omega^{-1}\hat{a}f_\omega = \hat{a}$ and $f_\omega f_{\omega'} = f_{\omega\omega'}$, for any $\omega, \omega' \in \mathrm{S}_8$. In particular, $f_\omega^{-1} = f_{\omega^{-1}}$ for $\omega \in \mathrm{S}_8$, f_τ and f_ρ centralise $\hat{a}$, and further, $\langle\tilde{z}\rangle$ is one of $\langle\hat{z}\rangle$, $\langle\hat{z}^{f_\tau}\rangle$, $\langle\hat{z}^{f_{\tau\pi}}\rangle$ and $\langle\hat{z}^{f_\rho}\rangle$. Without loss of generality, we assume $\hat{G} \neq \tilde{G}$. Then, replacing $\tilde{z}$ by a power of $\tilde{z}$ if necessary, we may assume that $\tilde{z} = \hat{z}^{f_\tau}$, $\hat{z}^{f_{\tau\pi}}$ or $\hat{z}^{f_\rho}$.

Assume first that $\tilde{z} = \hat{z}^{f_\tau}$. Then $f_\tau^{-1}\hat{G}f_\tau = \tilde{G}$; in particular, $f_\tau^{-1}\hat{z}f_\tau \in \tilde{G} \leq A$. Thus we only need to show $f_\tau \in A$. For integers i and j, we have $(z^ia^j)^{f_\tau^{-1}\hat{z}f_\tau\hat{z}^{-1}} = (z^{i^\tau}a^jz)^{f_\tau\hat{z}^{-1}} = (z^{i^\tau+1}a^{-j})^{f_\tau\hat{z}^{-1}} = (z^{i^{\tau\pi}}a^{-j})^{f_\tau\hat{z}^{-1}} = (z^{i^{\tau\pi\tau}}a^{-j})^{\hat{z}^{-1}} = z^{i^{\tau\pi\tau\pi^{-1}}}a^j = (z^ia^j)^{f_\sigma}$, and hence $f_\tau^{-1}\hat{z}f_\tau\hat{z}^{-1} = f_\sigma$ with $\sigma = \tau\pi\tau\pi^{-1} = (1\,5)(2\,6)$, and $f_\sigma \in A_{\mathbf{1}}$. Further, $f_{\sigma^{\pi^k}} = \hat{z}^{-k}f_\sigma\hat{z}^k \in A_{\mathbf{1}}$, where $k \in \{0, 1, 2, 3\}$, and hence $S^{f_{\sigma^{\pi^k}}} = S$. It follows that $z^ia^j \in S$ if and only if $z^{i+4}a^j \in S$. Take $z^ia^j, z^{i'}a^{j'} \in V\Gamma$, we have $(z^{i'}a^{j'})(z^ia^j)^{-1} = z^{i'-i}a^{(-1)^i(j'-j)}$ and $(z^{i'}a^{j'})^{f_\tau}((z^ia^j)^{f_\tau})^{-1} = z^{i'^\tau-i^\tau}a^{(-1)^{i^\tau}(j'-j)}$. Noting that $(i')^\tau - i^\tau \equiv i' - i \pmod 4$ and $(-1)^{i^\tau} = (-1)^i$, we see that $z^{i'-i}a^{(-1)^i(j'-j)} \in S$ if and only if $z^{(i')^\tau-i^\tau}a^{(-1)^{i^\tau}(j'-j)} \in S$. It follows that $f_\tau \in A$.

Assume now that $\tilde{z} = \hat{z}^{f_{\tau\pi}}$. Calculation shows that $\hat{z}^{f_{\tau\pi}} = (\hat{z}^{f_\tau})^{\hat{z}}$. Then $\tilde{G} = \langle\tilde{a}, \tilde{z}\rangle = \langle\hat{a}, \hat{z}^{f_{\tau\pi}}\rangle = \langle\hat{a}, (\hat{z}^{f_\tau})^{\hat{z}}\rangle = \hat{G}^{f_\tau\hat{z}}$. By the previous paragraph, $f_\tau \in A$ and so $f_\tau\hat{z} \in A$. Hence $\tilde{G}$ and $\hat{G}$ are conjugate in A.

Assume finally that $\tilde{z} = \hat{z}^{f_\rho}$. Then f_ρ centralises $\hat{a}$, and hence $\hat{G}^{f_\rho} = \tilde{G}$. Moreover, we have $f_\rho^{-1}\hat{z}f_\rho\hat{z}^{-1} = f_{\sigma'}$ with $\sigma' = (1\,5)(3\,7)$ and $\hat{z}^{-1}f_\rho^{-1}\hat{z}f_\rho = f_{\rho'}$ with

$\rho' = (0\,4)(2\,6)$. It is easily known that $f_{\sigma'}, f_{\rho'} \in A_{\mathbf{1}}$. A similar argument as above leads to $f_\rho \in A$.

Therefore, in all the cases, $\hat{G}$ and $\tilde{G}$ are conjugate in A.

In particular, if $|P| = p$, then $\langle \hat{a} \rangle$ and $\langle \tilde{a} \rangle$ are two Sylow p-subgroups of A, hence they are conjugate (in A). It follows that $\hat{G}$ and $\tilde{G}$ are conjugate (in A), and so Γ is a CI-graph. □

5.2. $|P| > p$ **and** P **has exactly** 8 **orbits, of length** p**.** Hereafter, we assume that $|P| = p^n$ for some integer $n > 1$.

Lemma 5.3. *Assume that $|P| > p$ and P has 8 orbits of length p. Then Γ is a CI-graph.*

Proof. By the assumption, $\hat{a} \in P$, and $|P| = p^n$ for some $n > 1$. Let $\mathcal{B} = \{B_0, B_1, \ldots, B_7\}$ be the set of the 8 orbits of P. Then $\langle \hat{a} \rangle$ is transitive on each B_i, and further, $\langle \hat{z} \rangle$ is regular on $\mathcal{B}$. Without loss of generality, assume that $B_i^{\hat{z}} = B_{i+1}$ (reading the subscripts modulo 8).

Let $\Phi(P)$ be the Frattini subgroup of P. Since $\hat{a} \in P$ and P has exactly 8 orbits on $V\Gamma$, all of which have length p, the subgroup $\Phi(P)$ fixes all vertices of Γ. Thus $\Phi(P) = 1$, and so $P \cong \mathbb{Z}_p^n$ is elementary abelian.

Let P_i be the kernel of P acting on B_i, for $0 \le i \le 7$. Then $P_i \cong \mathbb{Z}_p^{n-1}$, and $P = \langle \hat{a} \rangle P_i$. Further, $P^{\hat{z}} = \langle \hat{a} \rangle^{\hat{z}} P_i^{\hat{z}} = \langle \hat{a} \rangle P_{i+1} = P$, and so $\hat{z}$ normalises P.

Let $M = \mathbf{N}_A(P)$. Then $\hat{G} \le M$, and in particular, M is transitive on $V\Gamma$. Since P is normal in M, $\mathcal{B}$ is an M-invariant partition of $V\Gamma$.

Let K be the kernel of M acting on $\mathcal{B}$. Then $\langle \hat{a} \rangle \le P \le K \lhd M$; in particular, K is transitive on each B_i. Let K_i be the kernel of K acting on B_i, where $0 \le i \le 7$. Then $P_i \le K_i = K_0^{\hat{z}^i}$; in particular $|K_i| = |K_0|$, for $0 \le i \le 7$, and p^{n-1} divides $|K_i|$. In particular, $K_i \ne 1$. Since $|B_i| = p$ and $K_0 \lhd K$, the action of K_0 on B_i is either transitive or trivial. Suppose that K_0 is trivial on B_i for some i. Then $K_0 \le K_i$, and hence $K_0 = K_i = K_0^{\hat{z}^i}$. If i is odd, then it follows that $K_0 = K_j$ for all $j \in \{0, 1, \ldots, 7\}$, so K_0 fixes all vertices of Γ, which is not possible. Thus i is even, and so K_0 is transitive on B_j for $j = 1, 3, 5$ or 7. It follows that $S \cap B_j = \emptyset$ or B_j, where $j \in \{1, 3, 5, 7\}$. Noting that $|S| < 4p$, $S \not\subseteq \langle a, z^2 \rangle$, $B_1^{-1} = B_7$ and $B_3^{-1} = B_5$, we conclude that exactly one of $B_1 \cup B_7$ and $B_3 \cup B_5$ is contained in S, say $B_1 \cup B_7 \subseteq S$. Then we may write $S = B_1 \cup B_7 \cup S_0$, where $S_0 = S \cap \langle a, z^2 \rangle$.

Let $\Gamma_1 = \mathsf{Cay}(G, B_1 \cup B_7)$ and $\Gamma_0 = \mathsf{Cay}(G, S_0)$. Then Γ is an edge-disjoint union of Γ_1 and Γ_0. Since $K_0 \le M_{\mathbf{1}}$ (the stabilizer of $\mathbf{1}$ in M) and K_0 is transitive on B_1, the subgraph Γ_1 is M-edge-transitive. Since $|S| < 4p$, the subgraph Γ_0 has valency less than $2p$, and hence Γ_0 is an edge-disjoint union of M-edge-transitive subgraphs of Γ.

Let $T \subset G$ be such that $\Sigma := \mathsf{Cay}(G, T) \cong \Gamma$, and let $Y = \mathsf{Aut}\Sigma$. Let Q be a Sylow p-subgroup of Y which contains $\hat{a}$, and let $N = \mathbf{N}_Y(Q)$. Arguing as above, we have that $T = (B_i \cup B_{8-i}) \cup T_0$, where $i = 1$ or 3, and $T_0 \subset \langle a, z^2 \rangle$, such that $\Sigma_1 := \mathsf{Cay}(G, B_i \cup B_{8-i})$ is N-edge-transitive, and $\Sigma_0 := \mathsf{Cay}(G, T_0)$ is an edge-disjoint union of N-edge-transitive subgraphs of Σ and has valency less than $2p$.

Let σ be an isomorphism from Γ to Σ. Then $\sigma \in \mathrm{Sym}(V\Gamma)$ is such that $\sigma^{-1} A \sigma = Y$. Since $\sigma^{-1} P \sigma$ and Q are Sylow p-subgroups of Y, there exists $y \in Y$ such that $y^{-1}\sigma^{-1} P \sigma y = Q$. Since N is transitive on $V\Sigma$, there exists $x \in N$ such that

$(1^{\sigma y})^x = 1$. Let $\tau = \sigma yx$. Then τ is an isomorphism from Γ to Σ such that $1^\tau = 1$, and $\tau^{-1}P\tau = Q$. Thus $\tau^{-1}M\tau = N$. Note that Γ_1 is the unique M-edge-transitive subgraph of Γ and Σ_1 is the unique N-edge-transitive subgraph of Σ, of valency $2p$. We conclude that $\Gamma_1^\tau = \Sigma_1$. Hence also $\Gamma_0^\tau = \Sigma_0$.

Since $S_0, T_0 \subset H := \langle a, z^2\rangle$, it follows that $\mathsf{Cay}(H, S_0) \cong \mathsf{Cay}(H, T_0)$. Since $H \cong \mathbb{Z}_{4p}$ is a CI-group, there exists $\alpha_0 \in \mathsf{Aut}(H)$ such that $S_0^{\alpha_0} = T_0$. It is easily shown that there exists $\alpha \in \mathsf{Aut}(G)$ such that the restriction of α to H equals α_0, so $S_0^\alpha = T_0$. Obviously, $(B_1 \cup B_7)^\alpha = B_1 \cup B_7$ or $B_3 \cup B_5$.

Let $\rho \in \mathsf{Aut}(G)$ be such that $a^\rho = a^{-1}$ and $z^\rho = z^3$. Then $(B_1 \cup B_7)^\rho = B_3 \cup B_5$, and for each $g \in H$, we have $g^\rho = g^{-1}$. Since $T_0 = T_0^{-1}$, we conclude that $T_0^\rho = T_0$, and so $(B_1 \cup B_7 \cup T_0)^\rho = (B_3 \cup B_5 \cup T_0)$. It then follows that either $S^\alpha = T$, or $S^{\alpha\rho} = T$. So Γ is a CI-graph. □

5.3. $|P| > p$ **and** P **has an orbit of length** p^2**.** In this case, it is easily shown that $p = 5$ or 7. This subsection proves the following lemma.

Lemma 5.4. *Assume that $|P| > p$ and that P has an orbit of length p^2. Then Γ is a CI-graph.*

Proof. Suppose that A is primitive on $V\Gamma$. Since Γ is not a complete graph, then A is not 2-transitive on $V\Gamma$. Now $|V\Gamma| = 8p = 40$ or 56. By [8, Appendix B], either $p = 5$ and $\mathsf{soc}(A) = \mathrm{PSL}(4,3)$ or $\mathrm{PSU}(4,2)$, or $p = 7$ and $\mathsf{soc}(A) = \mathrm{A}_8$ or $\mathrm{PSL}(3,4)$. In either case, it follows that p^2 does not divide $|A|$, which is a contradiction. Thus A is imprimitive.

Let $\mathcal{B} := \{B_0, B_1, \cdots, B_{t-1}\}$ be a non-trivial A-invariant partition of $V\Gamma$ such that $\mathbf{1} \in B_0$. Let Λ be the orbit of P of length p^2, and let $\mathcal{C} := \{B_0, B_1, \cdots, B_{s-1}\}$ be the orbit of P on $\mathcal{B}$ such that $\Lambda \subseteq \cup_{i=0}^{s-1} B_i$. Then s is a power of p, and as $2p^2 > 8p$, we have $s \le t < 2p$. Thus $s = p$. For each element $x \in P$ and each $i < s$, $(B_i \cap \Lambda)^x = B_i^x \cap \Lambda^x = B_j \cap \Lambda$ for some $j < s$. Since P is transitive on Λ and $\mathcal{C}$, it follows that P acts transitively on $\{B_i \cap \Lambda \mid 0 \le i < s\}$. In particular, $|B_i \cap \Lambda| = |B_0 \cap \Lambda|$ for all $i < s$. Now $p^2 = |\Lambda| = |\cup_{i=0}^{s-1} (B_i \cap \Lambda)| = s|B_0 \cap \Lambda| = p|B_0 \cap \Lambda|$. Hence $|B_0 \cap \Lambda| = p$, and it then follows that $|B_0| = p$ or 8. Since $|B_0 \cap \Lambda| = p$, we know that P_{B_0} is non-trivial on B_0, and so $A_{B_0}^{B_0}$ contains an element of order p. Further, since $\mathcal{B}$ is G-invariant, it follows that $\hat{a}$ or $\hat{z}$ lies in A_{B_0}, and hence $A_{B_0}^{B_0}$ contains a cyclic regular subgroup. It follows that $A_{B_0}^{B_0}$ is primitive. Since A is transitive on $\mathcal{B}$, A_B^B is primitive for each $B \in \mathcal{B}$. Since $s = p$, P is non-trivial on $\mathcal{B}$, and so $A^{\mathcal{B}}$ contains elements of order p. Further, it is easily shown that $A^{\mathcal{B}}$ contains a cyclic regular subgroup. It implies that $A^{\mathcal{B}}$ is primitive. It is known that the primitive permutation groups X containing a cyclic regular subgroup of order $m = p$ or 8 are as follows, see for example [18, Corollary 1.2]:

(i) $m = p$, and X is one of the groups: $\mathbb{Z}_p{:}\mathbb{Z}_l$ with l divides $p-1$, $\mathrm{GL}(3,2)$ with $p = 7$, A_p or S_p;

(ii) $m = 8$, and $X = \mathrm{PGL}(2,7)$ or S_8.

We observe that each non-trivial normal subgroup of X is primitive.

Let K be the kernel of A acting on $\mathcal{B}$. Then $G/G \cap K \cong GK/K < A^{\mathcal{B}}$, and it follows that $\hat{a}$ or $\hat{z}^2$ lies in K; so in particular, $K \ne 1$. It then follows that $1 \ne K^B \lhd A_B^B$ for each $B \in \mathcal{B}$, and hence K^B is primitive.

Assume that $K \cong K^B$, where $B \in \mathcal{B}$. Then either $A = K.A^{\mathcal{B}} = K \times L$ where $L \cong A^{\mathcal{B}}$, or $A = K.A^{\mathcal{B}} \cong (K \times L).\mathbb{Z}_2$ where L is a subgroup of $A^{\mathcal{B}}$ of index 2. Let

$\tilde{G} = \langle\tilde{a}\rangle \rtimes \langle\tilde{z}\rangle \cong G$ be a regular subgroup of A. Note that $K \times L$ is transitive on $V\Gamma$, the set of orbits of L form a non-trivial A-invariant partition of $V\Gamma$ and none of A/K and A/L has a subgroup isomorphic to $\mathbb{Z}_p \rtimes \mathbb{Z}_8$ with centre $\mathbb{Z}_4$. Then, in either case, $\hat{a}$ and $\tilde{a}$ lie in one of K and L, and hence $\langle\hat{a}\rangle$, $\langle\tilde{a}\rangle$ are conjugate in K or L, and of course, in A. By Lemma 5.2, all regular subgroups of A isomorphic to G are conjugate. Thus Γ is a CI-graph.

Assume now that K acts unfaithfully on B_i. Let K_i be the kernel of K acting on B_i, where $0 \leq i \leq |\mathcal{B}|$. Since G is transitive on $V\Gamma$ and normalises K, we have $K_i = K_0^x$ for some $x \in G$. In particular $|K_i| = |K_0|$. Since $K_0 \neq 1$, we have that $K_0^{B_j} \neq 1$ for some j, and as $K_0^{B_j} \lhd K^{B_j}$ and K^{B_j} is primitive, $K_0^{B_j}$ is transitive. Thus the subgraph $[B_0, B_j]$, with vertex set $B_0 \cup B_j$ and edge set $\{\{u,v\} \in E\Gamma \mid u \in B_0, v \in B_j\}$, contains no edge or is isomorphic to the complete bipartite graph $\mathsf{K}_{b,b}$, where $b = |B_j|$. Suppose that $|B_j| = p$. Then $A^{\mathcal{B}}$ is a 2-transitive permutation group of degree $|\mathcal{B}| = 8$, and the quotient graph $\Gamma_{\mathcal{B}} \cong \mathsf{K}_8$. It follows that $[B_0, B] \cong \mathsf{K}_{p,p}$ for all $B \in \mathcal{B} \setminus \{B_0\}$. Thus Γ has valency at least $7p$, which is a contradiction. Hence $|B_j| = 8$.

Then $A^{\mathcal{B}}$ is primitive of degree p, and the quotient graph $\Gamma_{\mathcal{B}}$ has valency 2, 4 or 6. Further, K_0^B is transitive for all $B \in \mathcal{B} \setminus \{B_0\}$. Since the valency of Γ is less than $4p$ which is less than 32, it follows that $\Gamma_{\mathcal{B}}$ is of valency 2, and $\Gamma_{\mathcal{B}} \cong \mathbf{C}_p$. Note that K is 2-transitive on each $B \in \mathcal{B}$. Then the subgraph $[B]$, with vertex set B and edge set $\{\{u,v\} \in E\Gamma \mid u, v \in B\}$, contains no edge or is isomorphic to the complete graph K_8. It is easily shown that $\Gamma \cong \mathbf{C}_p[8\mathsf{K}_1]$ or $\mathbf{C}_p[\mathsf{K}_8]$, and hence $S = a^i\langle z\rangle \cup a^{-i}\langle z\rangle$, or $a^i\langle z\rangle \cup a^{-i}\langle z\rangle \cup \langle z\rangle \setminus \{1\}$, where $1 \leq i \leq 3$. Let $T \subset G$ be such that $\mathsf{Cay}(G,T) \cong \mathsf{Cay}(G,S)$. Then similarly we have $T = a^j\langle z\rangle \cup a^{-j}\langle z\rangle$, or $a^j\langle z\rangle \cup a^{-j}\langle z\rangle \cup \langle z\rangle \setminus \{1\}$, respectively, where $1 \leq i \leq 3$. It is now easily shown that there exists $\sigma \in \mathsf{Aut}(G)$ such that $S^\sigma = T$. Thus Γ is a CI-graph. $\square$

5.4. **Proof of Theorem 1.3.** Here is a summary of the argument for proving Theorem 1.3.

Proof of Theorem 1.3: Let $G = \langle a\rangle \rtimes \langle z\rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_8$ with centre of order 4, where p is an odd prime. If $p = 3$, then Γ is a CI-graph, see [29]. Thus we assume that $p \geq 5$. Let $\Gamma = \mathsf{Cay}(G,S)$ be a Cayley graph of G. As observed in the beginning of this section, if $S \subset \langle a, z^2\rangle \cong \mathbb{Z}_{4p}$ then Γ is a CI-graph. Also we may assume that Γ has valency less than $4p$. Let P be a Sylow p-subgroup of $\mathsf{Aut}\Gamma$ containing $\hat{a}$. Since $\langle\hat{a}\rangle$ is semi-regular on $V\Gamma$, P has at most 8 orbits in $V\Gamma$. If $|P| = p$, then by Lemma 5.2, Γ is a CI-graph. Assume that $|P| > p$. If P has exactly 8 orbits in $V\Gamma$, then each of them has length p. Thus by Lemma 5.3, Γ is a CI-graph. If P has less than 8 orbits, then P has at least one orbit of length p^2. It then follows that $p = 5$ or 7. By Lemma 5.4, Γ is a CI-graph. Therefore, all Cayley graphs of G are CI-graphs, and so G is a CI-group.

Let $H \cong \mathbb{Z}_p \rtimes \mathbb{Z}_4$ with centre of order 2, where p is an odd prime. Then H is isomorphic to the factor group of G modulo the characteristic subgroup $\mathbb{Z}_2$. By Lemma 2.2, H is a CI-group. This completes the proof of Theorem 1.3. $\square$

6. Proof of Theorem 1.4.

Let p be a prime, and G be a Frobenius group of order $3p$. Write $G = \langle a, z \mid z^{-1}az = a^l\rangle$, where $l \not\equiv 1 \,(\mathsf{mod}\ p)$ and $l^3 \equiv 1 \,(\mathsf{mod}\ p)$. Let $S \subseteq G\setminus\{1\}$ be such that $S^{-1} = S$, and let $\Gamma = \mathsf{Cay}(G, S)$ and $A = \mathsf{Aut}\,\Gamma$.

Assume first that p^2 divides $|A|$. Let $N = \mathbf{N}_A(\langle\hat{a}\rangle)$. Then $\hat{G} \le N$ and p^2 divides $|N|$. Now N is transitive on $V\Gamma$, and since $\langle\hat{a}\rangle$ is normal in N, the N-action is imprimitive. Let $\mathcal{B} = \{B_1, B_2, \cdots, B_m\}$ be an N-invariant partition of $V\Gamma$. It follows since p^2 divides $|N|$ that $m = 3$, $|B_i| = p$, and $\Gamma = K_3[\Sigma]$ or 3Σ, where $\Sigma = \mathsf{Cay}(\mathbb{Z}_p, S_0)$ for some $S_0 \subseteq \mathbb{Z}_p \setminus \{0\}$. It is now easily proved that Γ is a CI-graph.

Assume now that p^2 does not divide $|A|$. Let $\tilde{G}$ be a subgroup of A which is isomorphic to $\hat{G}$ and regular on $V\Gamma$. Then $\tilde{G} \cong \mathbb{Z}_p \rtimes \mathbb{Z}_3$. By the Sylow Theorem, to prove that $\tilde{G}$ is conjugate to $\hat{G}$, we may assume that $\langle\hat{a}\rangle < \tilde{G}$ so that $\tilde{G} = \langle\hat{a}\rangle \rtimes \langle y\rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_3$ for some $y \in A$ of order 3. Let $N = \mathbf{N}_A(\langle\hat{a}\rangle)$. Then $\hat{G} \le N$ and $\tilde{G} \le N$. Let $h \in N$ be such that both $\tilde{y} := y^h$ and $\hat{z}$ lie in the same Sylow 3-subgroup N_3 of N. Then $\tilde{G}^h = \langle\hat{a}\rangle \rtimes \langle\tilde{y}\rangle$. Since $\tilde{G} \cong \hat{G}$, we may further assume that $\hat{a}^{\tilde{y}} = \hat{a}^l$. In fact, if necessary, we may replace $\tilde{y}$ with $\tilde{y}^2$.

Consider the actions of N_3, $\hat{z}$ and $\tilde{y}$ on $V\Gamma$. We know that N_3 has a orbit Δ of length 3, and $\tilde{y}^\Delta = \hat{z}^\Delta$ or $(\hat{z}^\Delta)^{-1}$. Without loss of generality, we may assume that $\mathbf{1} \in \Delta$, and set $\Delta = \{\mathbf{1}, z, z^{-1}\}$. We have

$$(z^ia^j)^{\tilde{y}} = ((z^i)^{\hat{a}^j})^{\tilde{y}} = (z^i)^{\hat{a}^j\tilde{y}} = ((z^i)^{\tilde{y}})^{\hat{a}^{jl}} = (z^i)^{\tilde{y}^\Delta}a^{jl}, \text{ for } i = 0,\ 1,\ -1.$$

If $\tilde{y}^\Delta = \hat{z}^\Delta$, then $(z^ia^j)^{\tilde{y}} = z^{i+1}a^{jl} = (z^ia^j)^{\hat{z}}$, so $\tilde{y} = \hat{z}$, hence $\tilde{G}^h = \langle\hat{a}\rangle \rtimes \langle\tilde{y}\rangle = \langle\hat{a}\rangle \rtimes \langle\hat{z}\rangle = \hat{G}$.

Suppose that $\tilde{y}^\Delta = (\hat{z}^\Delta)^{-1}$. Then $(z^ia^j)^{\tilde{y}} = z^{i-1}a^{jl}$. Set $\tau : z^ia^j \longmapsto z^{-i}a^{-j}$. Then $\tau^{-1}\hat{a}\tau = \hat{a}^{-1}$ and $\tau^{-1}\hat{z}\tau = \tilde{y}$. It follows that $\hat{G}^{\tau h^{-1}} = \tilde{G}$. Since $h \in N \le A$, we have to show $\tau \in A$. Let $\sigma = (\tilde{y}\hat{z})^2$. Then $1^\sigma = 1$ and $\sigma \in A$, hence $S^\sigma = S$. For $g_1 = z^ia^j$ and $g_2 = z^{i'}a^{j'}$, we have

$$\begin{aligned} g_2^\tau(g_1^\tau)^{-1} &= (z^{i'}a^{j'})^\tau((z^ia^j)^\tau)^{-1} = z^{i-i'}a^{l^i(j-j')} = (z^{i-i'}a^{(j-j')l^{-i'}})^{\sigma^{i'+i}} \\ &= ((z^ia^j)(z^{i'}a^{j'})^{-1})^{\sigma^{i'+i}} = ((g_2g_1^{-1})^{-1})^{\sigma^{i'+i}}. \end{aligned}$$

It follows that $g_2^\tau(g_1^\tau)^{-1} \in S$ if and only if $g_2g_1^{-1} \in (S^{-1})^{\sigma^{-(i+i')}}$=S. Therefore, τ is an automorphism of Γ. This completes the proof. $\square$

References

[1] A. Ádám, Research problem 2-10, *J. Combin. Theory* **2** (1967), 309.

[2] B. Alspach, Isomorphisms of Cayley graphs on abelian groups, in *Graph Symmetry: Algebraic Methods and Applications*, NATO ASI Ser. C **497** (1997), 1–23.

[3] B. Alspach and T. D. Parsons, Isomorphisms of circulant graphs and digraphs, *Discrete Math.* **25** (1979), 97–108.

[4] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336.

[5] L. Babai and P. Frankl, Isomorphisms of Cayley graphs I, *Colloq. Math. Soc. J. Bolyai, 18. Combinatorics, Keszthely,* 1976*; North-Holland, Amsterdam*, 1978; 35–52.

[6] L. Babai and P. Frankl, Isomorphisms of Cayley graphs II, *Acta Math. Acad. Sci. Hungar.* **34** (1979), 177–183.

[7] M. Conder and C. H. Li, On isomorphisms for finite Cayley graphs, *European J. Combin.* **19** (1998), 911–919.

[8] J. D. Dixon and B. Mortimer, *Permutation Groups*, Springer-Verlag New York, 1996.
[9] D. Z. Djokovic, Isomorphism problem for a special class of graphs, *Acta Math. Acad. Sci. Hungar.* **21** (1970), 267–270.
[10] E. Dobson, Isomorphism problem for Cayley graph of $\mathbb{Z}_p^3$, *Discrete Math.* **147** (1995), 87–94.
[11] E. Dobson, Isomorphism problem for metacirculant graphs of order a product of distinct primes, *Canad. J. Math.* **50** (1998), 1176–1188.
[12] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Combin. Theory* **9** (1970), 297–307.
[13] C. D. Godsil, On Cayley graph isomorphisms, *Ars Combin.* **15** (1983), 231–246.
[14] M. Hirasaka and M. Muzychuk, The elementary abelian group of odd order and rank 4 is a CI-group, *J. Combin. Theory Ser. A* **94** (2001), no. 2, 339–362.
[15] B. Huppert, *Endliche Gruppen*, Springer, Berlin, 1967.
[16] C. H. Li, Finite CI-groups are soluble, *Bull. London Math. Soc.* **31** (1999), 419–423.
[17] C. H. Li, On Cayley isomorphism of finite Cayley graphs – a survey, *Discrete Math.* **256** (2002), no. 1-2, 301–334.
[18] C. H. Li, The finite primitive permutation groups containing an abelian regular subgroup, *Proc. London Math. Soc.* **87** (2003), no. 3, 725–747.
[19] C. H. Li and C. E. Praeger, The finite simple groups with at most two fusion classes of every order, *Comm. Algebra* **24** (1996), 3681–3704.
[20] C. H. Li and C. E. Praeger, On finite groups in which any two elements of the same order are fused or inverse-fused, *Comm. Algebra* **25** (1997), 3081–3118.
[21] C. H. Li and C. E. Praeger, On the isomorphism problem for finite Cayley graphs of bounded valency, *European J. Combin.* **20** (1999), 279–292.
[22] M. Muzychuk, Ádám's conjecture is true in the square-free case, *J. Combin. Theory (A)* **72** (1995), 118–134.
[23] M. Muzychuk, On Ádám's conjecture for circulant graphs, *Discrete Math.* **167/168** (1997), 497–510.
[24] M. Muzychuk, An elementary abelian group of large rank is not a CI-group, *Discrete Math.* **264** (2003), no. 1-3, 167–185.
[25] L. A. Nowitz, A non Cayley-invariant Cayley graph of the elementary Abelian group of order 64, *Discrete Math.* **110** (1992) 223–228.
[26] P. P. Pàlfy, On regular pronormal subgroups of symmetric groups, *Acta Math. Acad. Sci. Hungar.* **34** (1979), 187–292.
[27] P. P. Pàlfy, Isomorphism problem for relational structures with a cyclic automorphism, *European J. Combin.* **8** (1987), 35–43.
[28] C. E. Praeger, Finite transitive permutation groups and finite vertex-transitive graphs, in *Graph Symmetry: Algebraic Methods and Applications*, NATO ASI Ser. C **497**(1997), pp. 277–318.
[29] G. Royle, Constructive enumeration of graphs, PhD Thesis, University of Western Australia, 1987.

Department of Mathematics, Ohio State University, Columbus, OH 43210, USA

School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia
E-mail address: `li@maths.uwa.edu.au`

Center for Combinatorics, LPMC, Nankai University, Tianjin 300071, P. R. China
E-mail address: `zaipinglu@sohu.com`

Department of Algebra and Number Theory, Eötvös University, Budapest, P.O.Box 120, H–1518 Hungary
E-mail address: `ppp@cs.elte.hu`