BULL. AUSTRAL. MATH. SOC. 05C25
VOL. 56 (1997) [253-261]

ON FINITE GROUPS WITH THE CAYLEY INVARIANT PROPERTY

CAI HENG LI

A finite group G is said to have the *m-CI property* if, for any two Cayley graphs $\mathrm{Cay}(G,S)$ and $\mathrm{Cay}(G,T)$ of valency m, $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ implies $S^\sigma = T$ for some automorphism σ of G. In this paper, we investigate finite groups with the m-CI property. We first construct groups with the 3-CI property but not with the 2-CI property, and then prove that a nonabelian simple group has the 3-CI property if and only if it is A_5. Finally, for infinitely many values of m, we construct Frobenius groups with the m-CI property but not with the nontrivial k-CI property for any $k < m$.

1. INTRODUCTION

For a finite group G, set $G^\# = G \setminus \{1\}$ where 1 is the identity of G. For a subset S of $G^\#$, a Cayley (di)graph $\mathrm{Cay}(G,S)$ of G is the digraph with vertex-set G and edge-set $\{(a,b) \mid a,b \in G,\ a^{-1}b \in S\}$. If S is self-inverse, namely $S = S^{-1} := \{s^{-1} \mid s \in S\}$, then the adjacency relation is symmetric and $\mathrm{Cay}(G,S)$ may be viewed as an undirected graph. It is easily seen that $\mathrm{Cay}(G,S)$ is connected if and only if $\langle S \rangle = G$.

A Cayley (di)graph $\mathrm{Cay}(G,S)$ is called a *CI-graph* of G (CI stands for *Cayley Invariant*) if, for any $T \subseteq G^\#$, $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ implies $S^\sigma = T$ for some $\sigma \in \mathrm{Aut}(G)$. In this case, S is called a *CI-subset*. One long-standing open problem about Cayley graphs is the following: determine the groups G (or the types of Cayley graphs for a given group G) for which all Cayley graphs for G are CI-graphs. The investigation of this problem has received considerable attention in the literature (see [**13**] for references).

For a positive integer m, a group G is said to have the *m-DCI property* if every Cayley (di)graph of G of valency m is a CI-graph; G is said to have the *m-CI property* if every undirected Cayley graph of G of valency m is a CI-graph. Further, if a group G has the i-CI property for all $i \leqslant m$, then G is called an *m-CI-group*.

The problem of determining which groups are m-CI-groups has been investigated for a long time, see for example [**1, 2, 6, 9, 12, 13**]. In particular, a classification of 2-CI-groups has been obtained in [**9**], which is dependent on the classification of finite

Received 11th November, 1996
The author is very grateful to Cheryl Praeger and Peter Neumann for their helpful suggestions on the proofs of Theorems 1.2 and 1.4, and acknowledges partial support of an ARC small grant.

simple groups. Praeger, Xu and the author in [**11**] started to investigate finite groups with the m-(D)CI property, and proposed:

PROBLEM 1. Characterise finite groups with the *m-(D)CI* property.

A general investigation in [**11**] is made of the structure of Sylow subgroups of groups with the m-(D)CI property for certain values of m. However, it seems very hard to obtain a 'good' characterisation of the groups with the m-(D)CI property. For the directed graph case, namely the m-DCI property, there have been some further results. In [**8**], it is proved that if G is an Abelian group with the m-DCI property then every Sylow subgroup of G is homocyclic. The finite groups with the 2-DCI property but not with the 1-DCI property are completely classified in [**7**].

In this paper we study finite groups with the m-CI property for certain positive integers m. It is proved in [**11**] that a group with the 2-CI property is a 2-CI-group, and a classification of finite groups with the 2-CI property is therefore obtained as mentioned above. Because of this, the investigation of finite groups with the 3-CI property can be naturally divided into two problems. One is to determine 3-CI-groups, and the other is to determine the finite groups with the 3-CI property but not with the 2-CI property. A 3-CI-group is a 2-CI-group and so has been well-characterised (because of a classification of 2-CI-groups). For the second problem, the next theorem shows that there do exist groups with the 3-CI property but not with the 2-CI property. (In the following, we denote by A_n the alternating group of degree n.)

THEOREM 1.1. *Let H be a 2-CI-group of odd order such that 3 divides $|H|$, and let $G = H \times \mathrm{A}_4$. Then G has the 3-CI property but does not have the 2-CI property.*

It seems hard to obtain a complete characterisation of finite groups with the 3-CI property. However, the following theorem gives a complete classification of finite simple groups with the 3-CI property.

THEOREM 1.2. *Let G be a finite nonabelian simple group. Then G has the 3-CI property if and only if $G = \mathrm{A}_5$.*

To extend the investigation of the case $m = 3$ to the general case, we note that if G is of odd order, then $G^{\#}$ does not have self-inverse subsets of odd size and so the k-CI property for k odd is vacuously satisfied. Such a k-CI property will be said to be *trivial.* Now the following problem naturally arises:

PROBLEM 2. For a positive integer $m > 2$, characterise the finite groups which have the m-CI property but do not have the nontrivial k-CI property for any k with $2 \leqslant k < m$.

Then an immediate question we face is, for a positive integer m, whether there exist groups which have the m-CI property but do not have the nontrivial k-CI property for any k with $2 \leqslant k < m$. We shall positively answer this question in Theorem 1.4 by producing a family of such groups for infinitely many values of m. Examples of such groups are found in the class of Frobenius groups, which are described as follows. A

https://doi.org/10.1017/S0004972700030999 Published online by Cambridge University Press

group is said to be *homocyclic* if it is a direct product of some cyclic subgroups of the same order.

DEFINITION 1.3: Let $G = E(M,n) = M \rtimes \langle z \rangle$ be a finite group such that

(i) M is an Abelian group of odd order and all Sylow subgroups of M are homocyclic;

(ii) $\langle z \rangle \cong \mathbb{Z}_n$ where $n \geqslant 2$, and $(|M|, n) = 1$;

(iii) there exists an integer l such that for any $x \in M^{\#}$, $x^z = x^l$ and n is the least positive integer satisfying $l^n \equiv 1 \pmod{o(x)}$.

THEOREM 1.4. *Let $G = E(M,q)$ and $m = q-1$ where q is a prime and $q \geqslant 5$. Then G has the m-CI property but does not have the nontrivial k-CI property for any $k < m$.*

However, it is not known whether for every positive integer m there exist groups with the m-CI property but not with the nontrivial k-CI property for any k with $2 \leqslant k < m$. The smallest value of m in Theorem 1.4 is 4. We guess that a finite group with the 4-CI property but not with the nontrivial k-CI property for $k = 2, 3$ must be isomorphic to $E(M,5)$ for some M.

In Section 2 we establish our notation and give some preliminary results. Then in Section 3 we prove Theorems 1.1 and 1.2, and finally we prove Theorem 1.4 in Section 4.

2. PRELIMINARY RESULTS

This section draws together some preliminary results. The terminology and notation used in this paper are standard (see, for example, [**3, 15**]). In particular, for two positive integers m, n, we denote by $m \mid n$ that m divides n. For a positive integer n, C_n denotes the undirected cycle of length n, K_n denotes the complete graph of order n, and for n even, M_n denotes the graph Γ with

$$V\Gamma = \{0, 1, \ldots, n-1\} \text{ and } E\Gamma = \Big\{\{i,j\} \;\Big|\; |i-j| \equiv 1 \text{ or } n/2 \pmod{n}\Big\}.$$

For a graph Γ and a vertex $v \in V\Gamma$, denote by $\Gamma(v)$ the neighbours of v in Γ. For a finite group G, elements a, b of G are said to be *fused* if $a^\sigma = b$ for some $\sigma \in \mathrm{Aut}(G)$, and similarly, subsets S, T of G are said to be *fused* if $S^\sigma = T$ for some $\sigma \in \mathrm{Aut}(G)$.

Here we notice a simple fact which will be used often. For a group G and $S \subseteq G^{\#}$, $\mathrm{Cay}(G,S) = (|G| \,/\, |\langle S \rangle|)\mathrm{Cay}(\langle S \rangle, S)$. It follows that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ if and only if $\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\langle T \rangle, T)$. Next we have a simple property.

LEMMA 2.1. *Let Γ be a connected vertex transitive graph of valency m and let $G = \mathrm{Aut}\,\Gamma$ (the full automorphism group of Γ). Then any prime divisor of $|G_v|$ is at most m.*

https://doi.org/10.1017/S0004972700030999 Published online by Cambridge University Press

PROOF: Let $G_v^{\Gamma(v)}$ be the group induced by G_v on $\Gamma(v)$. For any $w \in V\Gamma$, since G is transitive on $V\Gamma$, there is $g \in G$ such that $w = v^g$. Thus $G_w^{\Gamma(w)} \cong G_v^{\Gamma(v)}$. Suppose that p is a prime dividing $|G_v|$, and let g be an element of G_v of order p. Then there exists $u \in V\Gamma$ which is not fixed by g. Since Γ is connected, there is a path from v to u: $v = v_0, v_1, \ldots, v_l = u$. Clearly there is some $k < l$ such that $v_i^g = v_i$ for all i with $0 \leqslant i \leqslant k$ and $v_{k+1}^g \neq v_{k+1}$. Thus $g \in G_{v_k}$, and since $v_{k+1} \in \Gamma(v_k)$, $v_{k+1}^g \in \Gamma(v_k)$. Let $g^* := g|_{\Gamma(v_k)}$ (the restriction of g to $\Gamma(v_k)$). Then $g^* \in G_{v_k}^{\Gamma(v_k)}$ and $v_{k+1}^{g^*} \neq v_{k+1}$. It follows that $o(g^*) = p$, so p divides $\left|G_{v_k}^{\Gamma(v_k)}\right| = \left|G_v^{\Gamma(v)}\right|$. Therefore, $p \leqslant m$. $\square$

Now we have a criterion for a Cayley graph to be a CI-graph.

LEMMA 2.2. (Alspach and Parsons [**1**, Theorem 1], or Babai [**2**, Lemma 3.1].) *For a group G and $S \subseteq G^{\#}$, let $\Gamma = \mathrm{Cay}(G,S)$ and $A = \mathrm{Aut}\,\Gamma$. Let $\mathrm{Sym}(G)$ be the symmetric group on G. Then $\mathrm{Cay}(G,S)$ is a CI-graph if and only if, for any $\tau \in \mathrm{Sym}(G)$ with $G^\tau \leqslant A$, there exists $\alpha \in A$ such that $G^\alpha = G^\tau$.*

The following result of Gross, together with Lemma 2.2, can provide a lot of examples of CI-graphs.

THEOREM 2.3. (Gross [**4**]) *Let G be a finite group and let π be a set of odd primes. If G has a Hall π-subgroup, then all Hall π-subgroups of G are conjugate in G.*

The proof of the following simple property is easy and omitted.

LEMMA 2.4. *Suppose that G is an Abelian group and all its Sylow subgroups are homocyclic. Let H, K be two isomorphic subgroups of G. Then any isomorphism from H to K can be extended to an automorphism of G.*

The Euler φ-function $\varphi(n)$ equals the number of positive integers less than n and relatively prime to n.

LEMMA 2.5. ([**10**, Lemma 2.4]) *Let m be a natural number. Then $\varphi(m) \geqslant \sqrt{m}/2$, and $\varphi(m) \geqslant \sqrt{m}$ whenever $m \neq 2$ or 6.*

3. THE 3-CI PROPERTY

This section is devoted to proving Theorems 1.1 and 1.2. First we prove Theorem 1.1.

PROOF OF THEOREM 1.1. Take an element $a \in H$ and $b \in \mathrm{A}_4$ such that $o(a) = o(b) = 3$, and set $S = \{a, a^{-1}\}$ and $T = \{b, b^{-1}\}$. Then $\mathrm{Cay}(G,S) \cong (|G|/3)C_3 \cong \mathrm{Cay}(G,T)$. Since $2 \,\big|\, |\mathbf{C}_G(a)|$ and $2 \nmid |\mathbf{C}_G(b)|$, it follows that S is not fused to T. So G does not have the 2-CI property. Next we must verify that G has the 3-CI property.

Let $S \subseteq G^{\#}$ be such that $|S| = 3$ and $S = S^{-1}$. If all elements of S are involutions, then S contains all the involutions of G. It follows that S is a CI-subset and $|\langle S\rangle| = 4$. Thus we may assume that $S = \{a, a^{-1}, b\}$ where $o(a) > 2$ and $o(b) = 2$. Let $T \subseteq G^{\#}$ be such that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ and so $\mathrm{Cay}(\langle S\rangle, S) \cong \mathrm{Cay}(\langle T\rangle, T)$. Then $|\langle T\rangle| =$

https://doi.org/10.1017/S0004972700030999 Published online by Cambridge University Press

$|\langle S\rangle| \neq 4$, and it follows that $T = \{a', a'^{-1}, b'\}$ where $o(a') > 2$ and $o(b') = 2$. Write $a = xy$ and $a' = x'y'$ where $x, x' \in H$ and $y, y' \in \mathrm{A}_4$.

Suppose first that $4 \nmid |\langle S\rangle|$. Then $y = 1$ or b, and since $\mathrm{Cay}(\langle S\rangle, S) \cong \mathrm{Cay}(\langle T\rangle, T)$, $4 \nmid |\langle T\rangle|$ and so $y' = 1$ or b'. If $y = 1$ then $\mathrm{Cay}(\langle S\rangle, S) \cong C_{o(a)} \times C_2$; if $y = b$ then $\mathrm{Cay}(\langle S\rangle, S) \cong M_{o(a)}$. It is easily checked that $C_{o(a)} \times C_2 \not\cong M_{2o(a)}$. Therefore, since $\mathrm{Cay}(\langle S\rangle, S) \cong \mathrm{Cay}(\langle T\rangle, T)$, it follows that $y = 1$ if and only if $y' = 1$ (so $y = b$ if and only if $y' = b'$). In particular, $o(a') = o(a)$. Since H is a 2-CI-group, there exists $\alpha \in \mathrm{Aut}(H)$ such that $\{a, a^{-1}\}^\alpha = \{a', a'^{-1}\}$. Clearly there exists $\beta \in \mathrm{Aut}(\mathrm{A}_4)$ such that $b^\beta = b'$. Hence $\rho = (\alpha, \beta) \in \mathrm{Aut}(G)$ sends S to T, so S is a CI-subset.

Suppose next that 4 divides $|\langle S\rangle|$. Then either $o(y) = 2$ and $y \neq b$, or $o(y) = 3$. Since $\mathrm{Cay}(\langle S\rangle, S) \cong \mathrm{Cay}(\langle T\rangle, T)$, 4 divides $|\langle T\rangle|$ and hence either $o(y') = 2$ and $y' \neq b'$, or $o(y') = 3$. In particular, neither $\langle S\rangle$ nor $\langle T\rangle$ is cyclic. We claim that $o(y) = o(y')$. Assume that $o(y) = 2$. Then $ab = ba$, and it follows that $\mathrm{Cay}(\langle S\rangle, S) \cong C_{o(a)} \times C_2$. Since $\mathrm{Cay}(\langle T\rangle, T) \cong \mathrm{Cay}(\langle S\rangle, S)$, $\mathrm{Cay}(\langle T\rangle, T) \cong C_{o(a)} \times C_2$. It follows that $a'b' = b'a'$ or $b'^{-1}a'$, and this implies that $o(y') = 2$. Conversely, if $o(y') = 2$ then similarly $o(y) = 2$. Therefore, $o(y) = 2$ if and only if $o(y') = 2$, and so $o(y) = 3$ if and only if $o(y') = 3$, namely, $o(y) = o(y')$ as claimed. It is easily checked that $\langle y, b\rangle = \langle y', b'\rangle$, $\langle S\rangle = \langle a, b\rangle = \langle x\rangle \times \langle y, b\rangle$ and $\langle T\rangle = \langle a', b'\rangle = \langle x'\rangle \times \langle y', b'\rangle$. Since $\mathrm{Cay}(\langle S\rangle, S) \cong \mathrm{Cay}(\langle T\rangle, T)$, $|\langle S\rangle| = |\langle T\rangle|$ and so $o(x) = o(x')$. Since H is a 2-CI-group, there exists $\alpha \in \mathrm{Aut}(H)$ such that $x^\alpha = x'^\varepsilon$ for some $\varepsilon = 1$ or -1. Noting that if $o(y') = 2$ then $y'^\varepsilon = y'$, it is clear that there exists $\beta \in \mathrm{Aut}(\mathrm{A}_4)$ such that $(y, b)^\beta = (y'^\varepsilon, b')$. Thus we have $\rho = (\alpha, \beta) \in \mathrm{Aut}(G)$ such that $S^\rho = \{xy, x^{-1}y^{-1}, b\}^\rho = \{x'^\varepsilon y'^\varepsilon, x'^{-\varepsilon}y'^{-\varepsilon}, b'\} = T$, so S is also a CI-subset. This completes the proof of the theorem. $\square$

Next we shall prove Theorem 1.2. First we determine the Sylow 2-subgroups of a group with the 3-CI property.

Lemma 3.1. *Let G be a finite group with the 3-CI property. Then a Sylow 2-subgroup of a 2-CI-group is elementary Abelian, cyclic, or generalised quaternion.*

Proof: Suppose that G is a finite group with the 3-CI property. If G is of odd order then the lemma is (trivially) true. So assume that G is of even order and let G_2 be a Sylow 2-subgroup of G. If G_2 has only one involution, then it follows from Sylow's Theorem that all involutions of G are conjugate. By [**16**, p.59], G_2 is either cyclic or generalised quaternion. Now suppose that G_2 has more than one involution. Then G_2 contains two involutions b, c such that $bc = cb$. Set $T := \{b, c, bc\}$. If G has an element a of order 4, and if we set $S := \{a, a^{-1}, a^2\}$, then $\mathrm{Cay}(\langle S\rangle, S) \cong K_4 \cong \mathrm{Cay}(\langle T\rangle, T)$, so $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$. However, clearly no automorphism of G maps S to T, which is a contradiction since G has the 3-CI property. Thus G_2 is of exponent 2 and so is elementary Abelian. $\square$

In the following, for a group G, let $\Omega(G, i) = \{\{a, a^{-1}\} \mid a \in G,\ o(a) = i\}$. We have a simple fact.

LEMMA 3.2. *Let G be a finite group such that $\mathrm{Aut}(G)$ is transitive on $\Omega(\langle z\rangle, o(z))$ for some $z \in G$. Then we have that $\mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)$ is transitive on the set $\Omega(\langle z\rangle, o(z))$ and $(1/2)\varphi(o(z))$ divides $\left|\mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)/\mathbf{C}_{\mathrm{Aut}(G)}(\langle z\rangle)\right|$.*

PROOF: For any i coprime to $o(z)$, $o(z) = o(z^i)$ and thus z is fused to z^i or z^{-i}, namely there exists $\alpha \in \mathrm{Aut}(G)$ such that $z^\alpha = z^i$ or z^{-i}. Thus $\alpha \in \mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)$. Consequently, $\mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)$ is transitive on $\Omega(\langle z\rangle, o(z))$, and so $(1/2)\varphi(o(z))$ $(= |\Omega(\langle z\rangle, o(z))|)$ divides $\left|\mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)/\mathbf{C}_{\mathrm{Aut}(G)}(\langle z\rangle)\right|$. ∎

Now we can prove Theorem 1.2.

PROOF OF THEOREM 1.2. By [**10**, Theorem 1.3], A_5 is a 3-CI-group and so A_5 has the 3-CI property.

Conversely, suppose that G is a finite nonabelian simple group with the 3-CI property. Then by Lemma 3.1, a Sylow 2-subgroup of G is elementary Abelian, cyclic or generalised quaternion. However, by [**14**, 10.2.2], a finite group with a cyclic or generalised quaternion Sylow 2-subgroup is not simple. Thus a Sylow 2-subgroup of G must be elementary Abelian. Therefore, by [**16**, p. 582], G is one of the following: J_1, $\mathrm{Ree}(3^{2n+1})$ (for some $n \geqslant 1$), $\mathrm{PSL}(2, 2^n)$ (for some $n \geqslant 2$) or $\mathrm{PSL}(2, q)$ with $q \equiv \pm 3 \pmod 8$. Now we need to prove $G = A_5$.

If $G = J_1$ then by the Atlas [**3**], $\mathrm{Aut}(G) = G$, G has a cyclic subgroup $\langle x\rangle$ of order 19, $\mathbf{N}_{\mathrm{Aut}(G)}(\langle x\rangle) \cong \langle x\rangle \rtimes \mathbb{Z}_6$, and x is conjugate to x^{-1} by an involution g. Let $S = \{x, x^{-1}, g\}$ and $T = \{x^i, x^{-i}, g\}$ where $2 \leqslant i \leqslant 18$. Then $\mathrm{Cay}(G,S) \cong (|G|/38)(C_{19} \times C_2) \cong \mathrm{Cay}(G,T)$. Since G has the 3-CI property, S is fused to T and so $\{x, x^{-1}\}$ is fused to $\{x^i, x^{-i}\}$. By Lemma 3.2, $9 = (1/2)\varphi(o(x))$ divides $\left|\mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)/\mathbf{C}_{\mathrm{Aut}(G)}(\langle z\rangle)\right| = 6$, which is a contradiction.

Assume that $G = \mathrm{Ree}(3^{2n+1})$ for some $n \geqslant 1$. By [**5**], G has a cyclic subgroup $\langle x\rangle$ of order $3^{2n+1} + 3^{n+1} + 1$, and $\mathbf{N}_{\mathrm{Aut}(G)}(\langle x\rangle) \cong \langle x\rangle \rtimes H$ where $|H|$ is even and divides $6(2n+1)$. Let g be an involution of H. Then g normalises $\langle x\rangle$. Let $y = x^i$ where i is coprime to $o(x)$. Let $S = \{x, x^{-1}, g\}$ and $T = \{x^i, x^{-i}, g\}$. It is easily checked that there exists $\alpha \in \mathrm{Aut}(\langle x, g\rangle)$ such that $S^\alpha = T$. It follows that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$. Since G has the 3-CI property, S is fused to T, and so $\{x, x^{-1}\}$ is fused to $\{y, y^{-1}\}$. By Lemma 3.2, we have $(1/2)\varphi(3^{2n+1} + 3^{n+1} + 1) \leqslant 6(2n+1)$. By Lemma 2.5, it follows that $3^n\sqrt{3} < \varphi(3^{2n+1} + 3^{n+1} + 1) \leqslant 12(2n+1)$. Consequently, $n \leqslant 3$. However, if $n = 2$ then $\varphi(3^5 + 3^3 + 1) = \varphi(271) = 270 \nleqslant 60$; if $n = 3$ then $\varphi(3^7 + 3^4 + 1) = \varphi(2269) = 2268 \nleqslant 86$. Thus $n = 1$ and $G = \mathrm{Ree}(27)$. By the Atlas [**3**], $|\mathrm{Out}(G)| = 3$, G contains 3 elements a, b, b^{-1} of order 3 such that no two of them are fused, and there exist involutions $g, h \in G$ such that $a^g = a^{-1}$ and $b^h = b$. Let $S = \{a, a^{-1}, g\}$ and $T = \{b, b^{-1}, h\}$. Then $\mathrm{Cay}(G,S) \cong (|G|/6)(C_3 \times C_2) \cong \mathrm{Cay}(G,T)$. Since G has the 3-CI property, S is fused to T and so a is fused to b or b^{-1}, which is not possible.

Assume that $G = \mathrm{PSL}(2,q)$ where either $q = 2^f$, or $q = p^f \equiv \pm 3 \pmod 8$ for some prime p. By [**15**, p. 417], G has a cyclic subgroup $\langle x\rangle \cong \mathbb{Z}_{(q+\varepsilon)/d}$, where $\varepsilon = \pm 1$ and $d = (q-1,2)$, and $\mathbf{N}_G(\langle x\rangle) = \langle x\rangle \rtimes \mathbb{Z}_2 \cong \mathrm{D}_{2o(x)}$ (a dihedral group). Arguing as in the previous paragraph, we have that $\{x, x^{-1}\}$ is fused to $\{x^i, x^{-i}\}$ for every i coprime to $o(x)$. Since $|\mathrm{Out}(G)| = df$, it follows that $\mathbf{N}_{\mathrm{Aut}(G)}(\langle x\rangle)/\mathbf{C}_{\mathrm{Aut}(G)}(\langle x\rangle)$ is of order dividing $2df$. By Lemma 3.2, $(1/2)\varphi((q+\varepsilon)/d)$ divides $2df$. Hence $4df$ is divisible by both $\varphi((q+1)/d)$ and $\varphi((q-1)/d)$. In particular, $\varphi((q+1)/d) \leqslant 4df$.

First suppose that $p = 2$. Then $d = 1$, and by Lemma 2.5, $\sqrt{2^f+1} \leqslant \varphi\big(2^f+1\big) \leqslant 4f$, whence $f \leqslant 10$. Since $(1/2)\varphi((q+\varepsilon)/d)$ divides $2df$ and $d = 1$, we have that both $\varphi\big(2^f+1\big)$ and $\varphi\big(2^f-1\big)$ divide $4f$. A straightforward calculation shows that $f \leqslant 4$. If $f = 4$ then $G = \mathrm{PSL}(2,16)$. By the Atlas [**3**], G has a cyclic subgroup $\langle x\rangle$ of order 17, and by the previous paragraph, x is conjugate to x^{-1} and $\{x, x^{-1}\}$ is fused to $\{x^i, x^{-i}\}$ for every positive integer $i \leqslant 16$. However, since $|\mathrm{Out}(G)| = 4$, it follows that $\mathbf{N}_{\mathrm{Aut}(G)}(\langle z\rangle)$ is not transitive on $\Omega(\langle z\rangle, 17)$, which is a contradiction to Lemma 3.2. Thus $f = 2$ or 3.

Now suppose that $p \geqslant 3$. Then $d = 2$. Assume first that f is even. Then $p^2-1 \,\big|\, p^f-1$. Since $p = 4k+1$ or $4k+3$ for some $k \geqslant 1$, 8 divides $(p+1)(p-1) = p^2-1$. Consequently, $p^f \equiv 1 \pmod 8$, a contradiction. Thus f is odd. If $f = 1$ then $p \equiv \pm 3 \pmod 8$, and we have that $\varphi((p+1)/2) \,\big|\, 8$ and $\varphi((p-1)/2) \,\big|\, 8$. Thus $(p+\varepsilon)/2 = 2^{r_1}3^{r_2}5^{r_3}$, where $r_1 \leqslant 4$ and $r_2, r_3 \leqslant 1$. It follows that $(p+\varepsilon)/2 \leqslant 30$ so $p \leqslant 61$. A straightforward calculation shows that $p = 5$ or 11 (since $p \equiv \pm 3 \pmod 8$). Finally suppose that $f \geqslant 3$. By Lemma 2.5, we have $(1/2)\sqrt{(p^f+1)/2} \leqslant \varphi\big(\big(p^f+1\big)/2\big) \leqslant 8f$, so $p^f + 1 \leqslant 512f^2$. It follows that $p \leqslant 13$, and if $p = 3$ then $f \leqslant 9$ so $f = 3, 5, 7$ or 9; if $p = 5$ then $f \leqslant 6$ so $f = 3$ or 5; if $7 \leqslant p \leqslant 13$ then $f \leqslant 4$ so $f = 3$. Recall that $p^f \equiv \pm 3 \pmod 8$, $\varphi\big(\big(p^f+1\big)2\big) \,\big|\, 8f$ and $\varphi\big(\big(p^f-1\big)/2\big) \,\big|\, 8f$. A straightforward calculation shows that $p^f = 27$. Thus we have that $p^f = 5, 11$ or 27.

Suppose that $p = 11$ or 27. Then by the Atlas [**3**], G has two fusion classes of order $(p-1)/2$ and if x is an element of order $(p-1)/2$ then x is conjugate to x^{-1} by an involution g. So $\{x, x^{-1}\}$ is not fused to $\{x^j, x^{-j}\}$ for some j with $1 < j < (p-1)/2$. Set $S = \{x, x^{-1}, g\}$ and $T = \{x^j, x^{-j}, g\}$. Then $\mathrm{Cay}(\langle S\rangle, S) \cong C_{(p-1)/2} \times C_2 \cong \mathrm{Cay}(\langle T\rangle, T)$, so $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$. Since G has the 3-CI property, S is fused to T. It follows that $\{x, x^{-1}\}$ is fused to $\{x^j, x^{-j}\}$, which is a contradiction.

Therefore, since $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong \mathrm{A}_5$, we have that $G = \mathrm{A}_5$ or $\mathrm{PSL}(2,8)$. By [**10**, Theorem 1.3], $\mathrm{PSL}(2,8)$ does not have the 3-CI property, and so $G = \mathrm{A}_5$. ∎

4. The m-CI property

This section is devoted to proving Theorem 1.4.

Proof of Theorem 1.4. As in Definition 1.3, write $G = M \rtimes \langle z\rangle$ where $\langle z\rangle \cong \mathbb{Z}_q$. By the definition, any non-identity element of $\langle z\rangle$ centralises no non-identity elements of M so that $\mathbf{C}_G(z) = \langle z\rangle$, and hence by [**14**, p. 299], G is a Frobenius group with

M the Frobenius kernel and $\langle z\rangle$ a Frobenius complement. In particular it follows from Definition 1.3 that any prime divisor of $|M|$ is greater than n, $(|M|, l) = 1$, and z normalises every cyclic subgroup of M.

First we show that G does not have the k-CI property for $k < m$, k even. Let $l = k/2$ and let $j = (q-1)/2$. Since k is even, we have $k \leqslant q - 3 = m - 2$. Thus $l = k/2 < (q-1)/2 = j$. Set

$$S = \{z, z^{-1}, \dots, z^l, z^{-l}\}, \text{ and } T = \{z^j, z^{-j}, \dots, z^{jl}, z^{-jl}\}.$$

Since $(j, q) = 1$, the map $z \to z^j$ induces an automorphism of $\langle z\rangle$, which maps S to T. Thus $\mathrm{Cay}(\langle z\rangle, S) \cong \mathrm{Cay}(\langle z\rangle, T)$, so $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$. If G has the k-CI property, then there is an element α of $\mathrm{Aut}(G)$ such that $S^\alpha = T$. Therefore, $z^\alpha = z^i$ for some integer $i \in \{j, -j, \dots, jl, -jl\}$. Let i_0 be the integer such that $i \equiv i_0 \pmod q$ and $0 < i_0 < q$. Then $z^\alpha = z^i = z^{i_0}$. For $a \in M$, let $a' = a^\alpha$. Then $z^{-i_0}a'z^{i_0} = (z^{-1}az)^\alpha = \left(a^l\right)^\alpha = (a')^l = z^{-1}a'z$. Thus $z^{-i_0+1}a'z^{i_0-1} = a'$. It follows from the definition of $E(M, q)$ that q divides $i_0 - 1$. Since $0 < i_0 < q$, we have $i_0 = 1$, that is, $S = S^\alpha = T$. However, since $l < j = (q-1)/2$, $z^j \in T \setminus S$, which is a contradiction.

Now we must verify that G has the m-CI property. Let $S \leqslant G \setminus \{1\}$ be such that $|S| = m$ and $S = S^{-1}$, and let $H = \langle S\rangle$. Let $\Gamma = \mathrm{Cay}(H, S)$, $A = \mathrm{Aut}\,\Gamma$ and let A_1 be the stabiliser of 1 in A. Since Γ is a connected graph of valency $m = q-1$, by Lemma 2.1, all prime divisors of $|A_1|$ are less than q. Since all prime divisors of G are at least q, $|H|$ and $|A_1|$ are coprime. Therefore, A_1 is a π-group and H is a Hall π'-subgroup of A, where π is the set of primes less than q. By Theorem 2.3, all Hall π'-subgroups of A are conjugate to H. Thus by Lemma 2.2, S is a CI-subset of H. For any $T \subset G$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, we have $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(\langle T\rangle, T)$. Let $K = \langle T\rangle$ and $B = \mathrm{Aut}\,\mathrm{Cay}(K, T)$, and let B_1 be the stabiliser of 1 in B. Then similarly K is a Hall π'-subgroup of B and $B \cong A$. Thus $K \cong H$. Let σ be an isomorphism from K to H and let $S' = T^\sigma$. Then $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(K, T) \cong \mathrm{Cay}(H, S')$. Since S is a CI-subset of H, $(S')^\tau = S$ for some $\tau \in \mathrm{Aut}(H)$. Thus $\rho := \sigma\tau$ is an isomorphism from K to H such that $T^\rho = T^{\sigma\tau} = (S')^\tau = S$.

Let $M_1 := K \cap M$ and $M_2 := H \cap M$. Then M_1, M_2 are characteristic subgroups of index 1 or q in K, H respectively. The isomorphism ρ: $K \to H$ induces an isomorphism ρ_0 from M_1 to M_2. By Lemma 2.4 there exists $\alpha \in \mathrm{Aut}(M)$ such that the restriction of α to M_1 is ρ_0. Note that since M is a characteristic subgroup of G, any automorphism of M can be induced by an automorphism of G. If $M_1 = K$ then there is nothing more to be done. Otherwise $K = M_1 \rtimes \langle z_1\rangle$ where z_1 has order q. Let $z_2 := z_1^\rho$. Then $H = M_2 \rtimes \langle z_2\rangle$. Now $\langle z_2\rangle$ and $\langle z_1^\alpha\rangle$ are Sylow q-subgroup of G and so they are conjugate by an element of M. Thus there is an inner automorphism β of G which fixes M pointwise and maps $\langle z_1^\alpha\rangle$ to $\langle z_2\rangle$. Then $\alpha\beta$ maps K to H, acts as ρ does on M_1, and maps $\langle z_1\rangle$ to $\langle z_1^\rho\rangle$. But then it is easy to see that $z_1^{\alpha\beta} = z_1^\rho$ (any automorphism of G induces the identity automorphism on G/M). Thus ρ is induced by an automorphism of G, and hence S is a CI-subset of G. Therefore, G has the m-CI property. This completes the proof of the theorem. $\square$

References

[1] B. Alspach and T.D. Parsons, 'Isomorphisms of circulant graphs and digraphs', *Discrete Math.* **25** (1979), 97–108.

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

[3] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker and R.A. Wilson, *Atlas of finite groups* (Clarendon Press, Oxford, 1985).

[4] F. Gross, 'Conjugacy of odd order Hall subgroups.', *Bull. London Math. Soc* **19** (1987), 311–319.

[5] P.B. Kleidman, 'The maximal subgroups of the Chevalley groups $G_2(q)$ with q odd, of the Ree groups ${}^2G_2(q)$, and their automorphism groups', *J. Algebra* **117** (1988), 30–71.

[6] C.H. Li, 'Isomorphisms and classification of Cayley graphs of small valencies on finite abelian groups', *Australas. J. Combin* **12** (1995), 3–14.

[7] C.H. Li, 'The finite groups with the 2-DCI property', *Comm. Algebra* **24** (1996), 1749–1757.

[8] C.H. Li, 'Finite abelian groups with the m-DCI property', *Ars Combin.* (to appear).

[9] C.H. Li, *Isomorphisms of finite Cayley graphs*, Ph.D. Thesis (The University of Western Australia, 1996).

[10] 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.

[11] C.H. Li, C.E. Praeger and M.Y. Xu, 'On finite groups with the Cayley isomorphism property', (preprint 1995).

[12] M. Muzychuk, 'Ádám's conjecture is true in the square-free case', *J. Combin. Theory (A)* **72** (1995), 118–134.

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

[14] D.J.S. Robinson, *A course in the theory of groups* (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

[15] M. Suzuki, *Group theory I* (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

[16] M. Suzuki, *Group theory II* (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

Department of Mathematics
University of Western Australia
Nedlands WA 6907
Australia
email: li@maths.uwa.edu.au