Finite Abelian Groups with the m-DCI Property

Cai Heng Li*
Department of Mathematics
University of Western Australia
Nedlands W.A. 6907
Australia
email: li@maths.uwa.edu.au

Abstract

A Cayley digraph $Cay(G,S)$ of a finite group G is isomorphic to another Cayley digraph $Cay(G,S^\sigma)$ for each automorphism σ of G. We will call $Cay(G,S)$ a *CI-graph* if, for each Cayley digraph $Cay(G,T)$, whenever $Cay(G,S) \cong Cay(G,T)$ there exists an automorphism σ of G such that $S^\sigma = T$. Further, for a positive integer m, if all Cayley digraphs of G of out-valency m are CI-graphs, then G is said to have the *m-DCI property*. This paper shows that for any positive integer m if a finite abelian group G has the m-DCI property then all Sylow subgroups of G are homocyclic.

1 Introduction

Let G be a group, and set $G^\# := G \setminus \{1\}$ where 1 is the identity of G. For a subset S of $G^\#$, the *Cayley digraph* $\Gamma = Cay(G,S)$ of G with respect to S is defined as the directed graph with vertex set G and arc set $E\Gamma = \{(a,b) \mid a,b \in G, ba^{-1} \in S\}$. A Cayley digraph $Cay(G,S)$ is called a *CI-graph* (CI stands for *Cayley Isomorphism*) if, for any Cayley digraph $Cay(G,T)$, whenever $Cay(G,S) \cong Cay(G,T)$ there exists $\alpha \in Aut(G)$ such that $S^\alpha = T$. For a positive integer m, if all Cayley digraphs of a

*The author thanks his supervisor, Professor Cheryl E. Praeger, for her helpful suggestions on this paper, and acknowledges support of an Overseas Postgraduate Research Scholarship from Australia and a University Postgraduate Award from University of Western Australia. The author is grateful to the referee for his valuable comments.

group G of out-valency m are CI-graphs, then G is said to have the *m-DCI property*.

The problem of determining which Cayley digraphs are CI-graphs of the corresponding groups has been investigated for a long time, see for example [1, 3, 6, 7, 10, 11] and the references in these papers. Regarding this problem, Praeger, Xu and the author in [9] initiated to study finite groups with the m-DCI property. For a finite group G, elements a, b of G are said to be *fused* if $a^\sigma = b$ for some $\sigma \in Aut(G)$, and similarly, subsets S, T of G are said to be *fused* if $S^\sigma = T$ for some $\sigma \in Aut(G)$. A group G has the 1-DCI property if and only if all elements of G of the same order are fused. Zhang [13] gave a good description for such groups. The author [4] completely classified the finite groups which have the 2-DCI property but do not have the 1-DCI property. More recently, for infinitely many values of m, the author [8] constructed an infinite family of groups which have the m-DCI property but not the i-DCI property for any $i < m$. In [9], a general investigation was made of the structure of Sylow subgroups of groups with the m-DCI property for certain values of m; and moreover, a reasonable complete characterization for cyclic groups with the m-DCI property is given in [5]. However, it seems very hard to obtain a 'good' characterization of the groups with the m-DCI property. The aim of this paper is to characterize finite abelian groups with the m-DCI property.

We use $\mathbb{Z}_n$ to denote a cyclic group of order n, and we call a group G *homocyclic* if G is a direct product of cyclic groups of the same order. The main result of this paper is the following theorem.

Main Theorem *Let m be a positive integer and let G be an abelian group. If G has the m-DCI property then all Sylow subgroups of G are homocyclic.*

Remarks: Let G be an abelian group, and let m be a positive integer. By [9, Theorem 1.6], if $1 \leq m \leq 4$ then the m-DCI prop implies the k-DCI property for all $k < m$, and therefore, G has the m-DCI property if and only if G is an m-DCI-group (that is, G has the k-DCI property for all $k \leq m$). On the other hand, by [5], $\mathbb{Z}_{25}$ has the 9-DCI property but does not have the k-DCI property for $k = 6, 7$ or 8.

Question 1 *For abelian groups and $5 \leq m \leq 8$, does the m-DCI property imply the k-DCI property for all $k < m$?*

Assume that G is an abelian m-DCI-group and that G_q is a Sylow q-subgroup of G. Then by [10], G_q is homocyclic if $q > m$; G_q is elementary abelian or cyclic if $q = m$; G_q is elementary abelian or $\mathbb{Z}_4$ if $q < m$. Conversely, if $m \leq 4$ then this condition is sufficient for G to be an m-DCI-group. Therefore, the abelian groups which have the m-DCI property for $m \leq 4$ are completely classified. In particular, this shows that the converse of the Main Theorem is not true.

By [8], for infinitely many values of m, there exist groups which have the m-DCI property but do not have the i-DCI property for any $i < m$. However, it is easy to see that an abelian group with all Sylow subgroups homocyclic has the 1-DCI property, and therefore, by the Main Theorem, for abelian groups the m-DCI property implies the 1-DCI property for any positive integer m. We guess that for abelian groups, with a few exceptions, the m-DCI property implies the k-DCI property for all $k < m$. Thus we pose the following problem.

Problem 2 *Classify the finite abelian groups which have the m-DCI property but do not have the k-DCI property for some $k < m$.*

For this problem, the only known examples are the cyclic groups $\mathbb{Z}_{p^2}$ where p is a prime and $p \geq 5$. It is actually proved in [5] that $\mathbb{Z}_{p^2}$ has the m-DCI property if and only if either $m < p$, or $m \equiv 0$ or $-1 \pmod{p}$.

The 'm-DCI property' has a natural counterpart for undirected Cayley graphs, that is, a group G is said to have the *m-CI property* if all undirected Cayley graphs of G of valency m are CI-graphs. We conjecture that the conclusion of the Main Theorem is also true for the undirected case, namely,

Conjecture 3 *If G is an abelian group with the m-CI property then all Sylow subgroups of G are homocyclic.*

2 Preliminaries

This section quotes some preliminary results which will be used in the proof of the Main Theorem. The first lemma gives some properties of subsets of a cyclic group.

Lemma 2.1 *Let $G = \langle z \rangle$ be a cyclic group of order n, and assume that $i, m \in \{1, 2, \ldots, n-2\}$. Suppose that $\{z, z^2, \ldots, z^m\} = \{z^i, z^{2i}, \ldots, z^{mi}\}$. Then $i = 1$.*

Proof. Let $S = \{z, z^2, \ldots, z^m\}$ and $S^i = \{z^i, z^{2i}, \ldots, z^{mi}\}$. First we observe that i is coprime to n since $z \in S^i$, and that $1 \leq i \leq m$ since $1 \leq i \leq n-2$ and $z^i \in S$. Suppose that $i > 1$. Then there exists $l \in \{1, \ldots, m-1\}$ such that $li \leq m$ and $(l+1)i > m$.

Assume that $m \leq \frac{n}{2}$. Since $l+1 \leq m$, $z^{(l+1)i} \in S^i = S = \{z, z^2, \ldots, z^m\}$. Since $(l+1)i > m$ and $(l+1)i \equiv i_0 \pmod{n}$ such that $i_0 \in \{1, \ldots, m\}$, we have $(l+1)i > n$, and therefore, since $m \geq li \geq i$, $n \geq 2m \geq li + i = (l+1)i > n$, which is a contradiction. Thus $m > \frac{n}{2}$, and since $G = \langle z \rangle$, setting $x = z^{-1}$, $\{x, x^2, \ldots, x^{n-(m+1)}\} = \langle z \rangle^\# \setminus S = \langle z \rangle^\# \setminus S^i = \{x^i, x^{2i}, \ldots, x^{(n-(m+1))i}\}$. Since $n - (m+1) \leq \frac{n-2}{2}$, the argument above also deduces a contradiction. Thus $i = 1$.

For a digraph $\Gamma = (V, E)$, its *complement* $\overline{\Gamma} = (V, \overline{E})$ is the graph with vertex set V such that $(a, b) \in \overline{E}$ if and only if $(a, b) \notin E$. The *lexicographic product* $\Gamma_1[\Gamma_2]$ of two digraphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ is the graph with vertex set $V_1 \times V_2$ such that $\Big((a_1, a_2), (b_1, b_2)\Big)$ is an arc if and only if either $(a_1, b_1) \in E_1$ or $a_1 = b_1$ and $(a_2, b_2) \in E_2$. For a positive integer n, K_n denotes the complete digraph on n vertices. For a graph Γ, $n\Gamma$ denotes the graph which consists of n copies of Γ. The next lemma concerns the structure of graphs that come from lexicographic product of graphs.

Lemma 2.2 *Let $G = \langle a, H \rangle$ be an abelian group where H is a proper subgroup of G, and let $R = \{a^{i_1}, \ldots, a^{i_k}\}H$ where $\langle R \rangle = G$ and $i_1, \ldots, i_k$ are distinct positive integers. Set $\overline{G} := G/H$, $\overline{R} := R/H$ and $\Sigma := Cay(\overline{G}, \overline{R})$. Then $Cay(G, R) = \Sigma[\overline{K}_m]$ where $m = |H|$. Further, if $S = R \cup R_0$ where R_0 is a Cayley subset of H then $Cay(G, S) = \Sigma[\Gamma_0]$ where $\Gamma_0 = Cay(H, R_0)$.*

Proof. Let $\Gamma = Cay(G, R)$. Then the vertex set G of Γ is partitioned as $\bigcup_{i=0}^{n-1} V_i$, where $n = o(a) = |\overline{G}|$ and $V_i = a^i H =: \overline{a}^i$ such that for any $x \in V_i$, the neighbourhood $\Gamma(x) = V_{i+i_1} \cup \ldots \cup V_{i+i_k}$ (reading the subscripts modulo n). The vertex set $\overline{G}$ of Σ is $\bigcup_{i=0}^{n-1} \{\overline{V}_i\}$ where $\overline{V}_i = \overline{a}^i$ such that $\overline{V}_i$ has the neighbourhood $\Sigma(\overline{V}_i) = \{\overline{V}_{i+i_1}\} \cup \ldots \cup \{\overline{V}_{i+i_k}\}$. It follows from the definition of lexicographic product of graphs that $\Gamma = \Sigma[\overline{K}_m]$.

Next let $\Gamma = Cay(G, S)$. Now $Cay(G, R_0)$ consists of $\frac{|G|}{m}$ copies of Γ_0, that is, $Cay(G, R_0) = \frac{|G|}{m}\Gamma_0$, and has components (not necessarily connected) V_i, $0 \leq i \leq n$. It follows from definition that $\Gamma = \Sigma[\Gamma_0]$.

Finally, we give a simple lemma which will be used.

Lemma 2.3 *Let G be a finite group, and let $S, T \subseteq G^{\#}$. Then $Cay(G,S) \cong Cay(G,T)$ if and only if $Cay(\langle S\rangle, S) \cong Cay(\langle T\rangle, T)$.*

Proof. If $Cay(G,S) \cong Cay(G,T)$ then clearly $Cay(\langle S\rangle, S) \cong Cay(\langle T\rangle, T)$. Conversely, if $Cay(\langle S\rangle, S) \cong Cay(\langle T\rangle, T)$ then we have that $Cay(G,S) = \frac{|G|}{|\langle S\rangle|} Cay(\langle S\rangle, S) \cong \frac{|G|}{|\langle T\rangle|} Cay(\langle T\rangle, T) = Cay(G,T)$.

The terminology and notation used in this paper are standard (see, for example, [2, 12]). In particular, for a positive integer n, C_n denotes the (directed or undirected) cycle of length n. For convenient, if a Cayley digraph $Cay(G,S)$ is a CI-graph we will call the subset S a *CI-subset*. Finally, for a group G and a pair of subsets S, T of $G^{\#}$, if $Cay(G,S) \cong Cay(G,T)$ but S is not fused to T, then $\{S,T\}$ is called a *NCI-pair* of G.

3 Proof of the Main Theorem

It is clear from the definition that a Cayley subset S of G is a CI-subset if and only if $G^{\#} \setminus S$ is a CI-subset. Thus G has the m-DCI property if and only if G has the $(|G^{\#}| - |S|)$-DCI property. So we shall always assume that $m \leq \frac{|G|-1}{2}$.

Proof of the Main Theorem: Suppose that G has the m-DCI property, and suppose that p is a prime divisor of $|G|$ such that a Sylow p-subgroup G_p of G is not homocyclic. Then there exist $a, b \in G_p$ such that $o(a) < o(b)$ and

$$G = \langle a\rangle \times \langle b\rangle \times L,$$

where L is a subgroup of G. Let $o(a) = p^r$ and $o(b) = p^s$. Then $s = r + \tau$ for some integer $\tau \geq 1$. Let $b_0 = b^{p^\tau}$. Then $o(a) = o(b_0) = p^r$ and $\langle a, b_0\rangle = \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^r}$. To prove the theorem, we are going to construct a NCI-pair of size m for every $m \in \{1, \ldots, \frac{|G|-1}{2}\}$. First of all, we note the fact that $\langle a\rangle$ is not fused to $\langle b_0\rangle$ because an automorphism has to send a basis to a basis, in particular, a is not fused to b_0

Step 1: (Construct NCI-pairs of size m for $1 \leq m \leq p^r - 1$.) Assume that $m \leq p^r - 1$, and let

$$S = \{a, \ldots, a^m\}, \quad T = \{b_0, \ldots, b_0^m\}.$$

Now there exists an isomorphism σ from $\langle a\rangle$ to $\langle b_0\rangle$ with $a^\sigma = b_0$. Thus $S^\sigma = T$, and so $Cay(\langle a\rangle, S) \cong Cay(\langle b_0\rangle, T)$. By Lemma 2.3, $Cay(G,S) \cong Cay(G,T)$. Since G has the m-DCI property, there exists $\alpha \in Aut(G)$ such that $S^\alpha = T$ and so $\langle a\rangle^\alpha = \langle S^\alpha\rangle = \langle T\rangle = \langle b_0\rangle$. This is not possible as noted at the beginning of the proof. Therefore, we have a NCI-pair $\{S,T\}$ of size m for $1 \le m \le p^r - 1$.

Step 2: (Construct NCI-pairs of size m for $p^r \le m \le p^{2r} - 1$.) If $m = p^{2r} - 1$, then let

$$S = \langle a, b_0\rangle \setminus \{1\}, \quad T = \langle a^p, b^{p^{r-1}}\rangle \setminus \{1\}.$$

Then $Cay(\langle S\rangle, S) \cong K_{p^{2r}} \cong Cay(\langle T\rangle, T)$, and so by Lemma 2.3, $Cay(G,S) \cong Cay(G,T)$. However, S is not fused to T since $\langle S\rangle \cong \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^r} \ncong \mathbb{Z}_{p^{r-1}} \times \mathbb{Z}_{p^{r+1}} \cong \langle T\rangle$. Therefore, $\{S,T\}$ is a NCI-pair of size $p^{2r} - 1$.

Thus assume that $p^r \le m \le p^{2r} - 2$. Now $m = kp^r + j$, where $1 \le k \le p^r - 1$ and $0 \le j \le p^r - 1$. Let

$$\begin{cases} S = \{b_0, b_0^2, \ldots, b_0^k\}\langle a\rangle \cup \{a^i \mid 1 \le i \le j\}, \\ T = \{a, a^2, \ldots, a^k\}\langle b_0\rangle \cup \{b_0^i \mid 1 \le i \le j\}. \end{cases}$$

Clearly there exists $\sigma \in Aut(\langle a, b_0\rangle)$ such that $a^\sigma = b_0$ and $b_0^\sigma = a$. This σ is automatically an isomorphism from $Cay(\langle a, b_0\rangle, S)$ to $Cay(\langle a, b_0\rangle, T)$, and so by Lemma 2.3, $Cay(G,S) \cong Cay(G,T)$. Since G has the m-DCI property, there is an $\alpha \in Aut(G)$ such that $S^\alpha = T$. Thus $\langle a, b_0\rangle^\alpha = \langle S^\alpha\rangle = \langle T\rangle = \langle a, b_0\rangle$, so $a^\alpha = a^x b_0^y$ and $b_0^\alpha = a^u b_0^v$ for some integers x, y, u, v. Then

$$(b_0\langle a\rangle)^\alpha = a^u b_0^v \langle a^x b_0^y\rangle = \{a^{u+xh} b_0^{v+yh} \mid 0 \le h \le p^r - 1\}.$$

If $p \mid x$, then $a^\alpha = a^x b_0^y \in \Phi(G)$, the Frattini subgroup of G. However, $a \notin \Phi(G)$ and $\Phi(G)$ is characteristic in G, which is a contradiction. Thus x is coprime to p and so

$$\{u + xh \mid 0 \le h \le p^r - 1\} \equiv \{0, 1, \ldots, p^r - 1\} \pmod{p^r}.$$

It follows, since $(b_0\langle a\rangle)^\alpha \subseteq T$, that $k = p^r - 1$. Since $m \le p^{2r} - 2$, we have $j \le p^r - 2$ and so α maps $\langle a, b_0\rangle^\# \setminus S$ (a nonempty set of $\langle a\rangle^\#$) to $\langle a, b_0\rangle^\# \setminus T$ (a nonempty subset of $\langle b_0\rangle^\#$), which is a contradiction because the sets contain a^{-1} and b_0^{-1}. Thus $\{S,T\}$ is a NCI-pair of size m.

Step 3: (Construct NCI-pairs of size m for $p^{2r} \leq m \leq p^{r+s} - 2$.) If $m = p^{2r}$ then let

$$S = b^{p^{r-1}}\langle a, b_0\rangle, \quad T = a\langle a^p, b^{p^{r-1}}\rangle.$$

By Lemma 2.2, $Cay(\langle S\rangle, S) \cong C_p[\overline{K}_{p^{2r}}] \cong Cay(\langle T\rangle, T)$, and so by Lemma 2.3, $Cay(G, S) \cong Cay(G, T)$. However, S is not fused to T since all elements of S are of order p^{r+1} but the element a of T is of order p^r, a contradiction. Thus $\{S, T\}$ is a NCI-pair of size p^{2r}.

Assume that $p^{2r} + 1 \leq m \leq p^{r+s} - 2$. Now $m = kp^{2r} + j$, where $1 \leq k \leq p^r - 1$ and $0 \leq j \leq p^{2r} - 1$. Let $H = \langle a, b_0\rangle$.

Case 1. Suppose that $1 \leq j \leq p^{2r} - 2$. Let

$$S = \{b, \ldots, b^k\}H \cup S_0 \text{ and } T = \{b, \ldots, b^k\}H \cup T_0,$$

where $\{S_0, T_0\}$ is a NCI-pair of size j constructed in Steps 1 and 2 (so $S_0, T_0 \subset H$). Let $K = \langle a, b\rangle$ and $\overline{K} = K/H$. Let $\Gamma_1 = Cay(\overline{K}, \{\overline{b}, \ldots, \overline{b}^k\})$, and let $\Gamma_2 = Cay(H, S_0)$ and $\Gamma_2' = Cay(H, T_0)$. Then $\Gamma_2 \cong \Gamma_2'$, and so by Lemma 2.2,

$$Cay(K, S) = \Gamma_1[\Gamma_2] \cong \Gamma_1[\Gamma_2'] = Cay(K, T).$$

Thus by Lemma 2.3, $Cay(G, S) \cong Cay(G, T)$. Since G has the m-DCI property, there exists $\alpha \in Aut(G)$ such that $S^\alpha = T$. Thus $K^\alpha = \langle a, b\rangle^\alpha = \langle S^\alpha\rangle = \langle T\rangle = \langle a, b\rangle$. Note that all elements of S_0 and of T_0 are of order at most p^r, and all elements of $S \setminus S_0$ and of $T \setminus T_0$ are of order at least p^{r+1} (since $1 \leq k \leq p^r - 1$). So $S_0^\alpha = T_0$, which is a contradiction to Steps 1 and 2. Thus $\{S, T\}$ is a NCI-pair.

Case 2. Suppose that $j = 0$, that is, $m = kp^{2r}$ for some $k \geq 2$. First assume that $r = 1$. Then $o(b) = p^{r+1}$ and $H = \langle a, b^p\rangle$. Since $m \geq p^{2r} + 1$, $2 \leq k \leq p - 1$. Let $J = \langle a^p, b\rangle$, and let

$$S = \{b, \ldots, b^k\}H, \quad T = \{a, \ldots, a^k\}J.$$

Then $\langle S\rangle = \langle T\rangle = \langle a, b\rangle =: K$ and $K/H \cong K/J \cong \mathbb{Z}_p$. Now there exists an isomorphism σ from K/H to K/J such that $(bH)^\sigma = aJ$, and so $(S/H)^\sigma = T/J$. Therefore,

$$\Gamma_1 := Cay(K/H, S/H) \cong Cay(K/J, T/J) =: \Gamma_2$$

and by Lemma 2.2, we have $Cay(K,S) = \Gamma_1[\overline{K}_{p^{2r}}] \cong \Gamma_2[\overline{K}_{p^{2r}}] = Cay(K,T)$. Further, by Lemma 2.3, $Cay(G,S) \cong Cay(G,T)$. Since G has the m-DCI property, there is $\alpha \in Aut(G)$ such that $S^\alpha = T$. However, all elements of S are of order p^{r+1} and the element a of T is of order p^r, which is a contradictio. Hence $\{S,T\}$ is a NCI-pair.

Now assume that $r > 1$. Set $S' = H^\# \cup \{b^{p^{r-1}}\}$ and $T' = H^\# \cup \{b^{p^{r-1}+p^r}\}$. If $p^{r-1} \geq k$ then let

$$\begin{cases} S = \{b, \ldots, b^{k-1}\}H \cup S', \\ T = \{b, \ldots, b^{k-1}\}H \cup T'; \end{cases}$$

if $p^{r-1} < k$ then let

$$\begin{cases} S = (\{b, \ldots, b^k\}H \setminus b^{p^{r-1}}H) \cup S', \\ T = (\{b, \ldots, b^k\}H \setminus b^{p^{r-1}}H) \cup T'. \end{cases}$$

Now $F := \langle S' \rangle = \langle T' \rangle = \langle H, b^{p^{r-1}} \rangle = \langle a \rangle \times \langle b^{p^{r-1}} \rangle \cong \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^{r+1}}$, and

$$\begin{cases} F = H \cup b^{p^{r-1}}H \cup \ldots \cup b^{(p-1)p^{r-1}}H, \\ K := \langle a, b \rangle = \langle S \rangle = \langle T \rangle = F \cup bF \cup \ldots \cup b^{p^{r-1}-1}F. \end{cases}$$

Thus neither $Cay(K,S')$ nor $Cay(K,T')$ is connected, and moreover, both $Cay(K,S')$ and $Cay(K,T')$ have b^iF, $i = 0,1,\ldots,p^{r-1}-1$, as vertex sets of their connected components. We use C_i and D_i to denote the connected components of $Cay(K,S')$ and of $Cay(K,T')$ containing the vertex b^i, respectively. Clearly there is $\sigma \in Aut(F)$ such that $a^\sigma = a$ and $(b^{p^{r-1}})^\sigma = b^{p^{r-1}+p^r}$, which normalizes H and so $S'^\sigma = T'$. Thus σ automatically induces an isomorphism from $Cay(F,S')$ to $Cay(F,T')$ Let ρ be a map from K to K defined by

$$\rho: \quad b^if \to b^if^\sigma, \text{ where } i \in \{0,1,\ldots,p^{r-1}-1\} \text{ and } f \in F.$$

Then $(b^iF)^\rho = b^iF$ and ρ induces an isomorphism from C_i to D_i for every $i \in \{0,1,\ldots,p^{r-1}-1\}$. Thus ρ preserves adjacency from $Cay(K,S')$ to $Cay(K,T')$.

Now we are going to prove that ρ also induces an isomorphism from $Cay(K,S)$ to $Cay(K,T)$. Write K as a union of cosets by

$$K = \bigcup_{0 \leq x \leq p^{r-1}-1} \bigcup_{0 \leq y \leq p-1} b^x b^{yp^{r-1}} H.$$

For any x, y, we have

$$(b^x b^{yp^{r-1}} H)^\rho = b^x (b^{yp^{r-1}} H)^\sigma = b^x b^{y(p^{r-1}+p^r)} H = b^x b^{yp^{r-1}} H.$$

In particular, $(b^i H)^\rho = b^i H$ for every $1 \leq i \leq k$. Thus ρ also preserves adjacency from $Cay(K, S \setminus S')$ to $Cay(K, T \setminus T')$. Consequently, ρ is an isomorphism from $Cay(K, S)$ to $Cay(K, T)$, so $Cay(G, S) \cong Cay(G, T)$ (see Lemma 2.3).

Since G has the m-DCI property, there is $\alpha \in Aut(G)$ such that $S^\alpha = T$ and so $K^\alpha = \langle S^\alpha \rangle = \langle T \rangle = K$. Hence $b^\alpha = b^y a^x$ for some integers x, y. Note that all elements of $H^\#$ are of order at most p^r. Since $1 \leq k \leq p^r - 1$, every element of each of both $S \setminus H^\#$ and $T \setminus H^\#$ is of order at least p^{r+1}. Therefore, α must send $H^\#$ to $H^\#$ and $H^\alpha = H$. Thus for any integer i, $(b^i H)^\alpha = (b^i)^\alpha H^\alpha = b^{yi} a^{xi} H = b^{yi} H$. Consequently, $(\{b, \ldots, b^{k-1}\}H)^\alpha = \{b, \ldots, b^{k-1}\}H$ and $((\{b, \ldots, b^k\} \setminus \{b^{p^{r-1}}\})H)^\alpha = (\{b, \ldots, b^k\} \setminus \{b^{p^{r-1}}\})H$. It follows that $(b^{p^{r-1}})^\alpha = b^{p^{r-1}+p^r}$ and so $(b^{p^{r-1}} H)^\alpha = b^{p^{r-1}+p^r} H = b^{p^{r-1}} H$. Therefore,

$$\begin{aligned} \{b^y, \ldots, b^{(k-1)y}\}H = (\{b, \ldots, b^{k-1}\}H)^\alpha = \{b, \ldots, b^{k-1}\}H, & \quad \text{if } p^{r-1} \geq k; \\ \{b^y, \ldots, b^{ky}\}H = (\{b, \ldots, b^k\}H)^\alpha = \{b, \ldots, b^k\}H, & \quad \text{if } p^{r-1} < k. \end{aligned}$$

It follows from Lemma 2.1 that $y \equiv 1 \pmod{p^r}$, namely $b^\alpha = b^{1+p^r h} a^x$ for some integer h. So $(b^{p^{r-1}})^\alpha = (b^{1+p^r h} a^x)^{p^{r-1}} = b^{p^{r-1}+p^{2r-1}h} a^{xp^{r-1}} \neq b^{p^{r-1}+p^r}$, a contradiction. Thus $\{S, T\}$ is a NCI-pair of size kp^{2r}.

Case 3. Suppose that $j = p^{2r} - 1$, namely $m = kp^{2r} + (p^{2r} - 1)$. Set $S' = H^\# \setminus \{a\} \cup \{b^{p^{r-1}}\}$ and $T' = H^\# \setminus \{a\} \cup \{b^{p^{r-1}+p^r}\}$. If $p^{r-1} > k$ then let

$$\begin{cases} S = \{b, \ldots, b^k\}H \cup S', \\ T = \{b, \ldots, b^k\}H \cup T'; \end{cases}$$

if $p^{r-1} \leq k$ then let

$$\begin{cases} S = (\{b, \ldots, b^{k+1}\}H \setminus b^{p^{r-1}} H) \cup S', \\ T = (\{b, \ldots, b^{k+1}\}H \setminus b^{p^{r-1}} H) \cup T'. \end{cases}$$

Arguing as in Case 2, we have $Cay(G, S) \cong Cay(G, T)$ but S is not fused to T. Thus $\{S, T\}$ is a NCI-pair of size $kp^{2r} + (p^{2r} - 1)$.

By Steps 1, 2 and 3, we have constructed a NCI-pair of G with size m for every value of $m \in \{1, 2, \ldots, p^{r+s} - 2\}$. Hence, if $G = \langle a, b \rangle$ or $m \leq p^{r+s} - 2$, the theorem holds. To complete the proof of the theorem,

assume that $G \neq \langle a, b\rangle$ and $m \geq p^{r+s} - 1$. Then $G = \langle a, b\rangle \times L$ for some $L \neq 1$.

Step 4: (Construct NCI-pairs of size m for $m \geq p^{r+s} - 1$.) First assume that $p^{r+s} - 1 \leq m \leq |L|$. Then $m \geq 2^{1+2} - 1 = 7$. Set

$$S = \{a\} \cup R, \quad T = \{b_0\} \cup R,$$

where R is a Cayley subset of L of size $m - 1$ which is defined as follows: Write $L = \langle a_1\rangle \times \ldots \times \langle a_l\rangle$ such that each $o(a_i)$ is a prime-power. If $m \leq o(a_1)$ then let R be an arbitrary Cayley subset of $\langle a_1\rangle$ of size $m - 1$. Suppose that $m > o(a_1)$. Then there exists an integer i such that $|\langle a_1\rangle \times \ldots \times \langle a_i\rangle| \leq m - 1 \leq |\langle a_1\rangle \times \ldots \times \langle a_i\rangle \times \langle a_{i+1}\rangle|$. Set $M = \langle a_1\rangle \times \ldots \times \langle a_i\rangle$ and $m_0 = |M|$, and let $m - 1 = km_0 + j$ for some $k \geq 1$ and $0 \leq j < m_0$. Let R_0 be an arbitrary Cayley subset of M of size j (if $j = 0$ then $R_0 = \emptyset$), and let $R = \{a_{i+1}, \ldots, a_{i+1}^k\}M \cup R_0$. Then

$$\begin{aligned} Cay(\langle S\rangle, S) &= Cay(\langle a\rangle, \{a\}) \times Cay(\langle R\rangle, R) \\ &\cong Cay(\langle b_0\rangle, \{b_0\}) \times Cay(\langle R\rangle, R) = Cay(\langle T\rangle, T). \end{aligned}$$

Thus $Cay(G, S) \cong Cay(G, T)$ (by Lemma 2.3). Since G has the m-DCI property, there is $\alpha \in Aut(G)$ such that $S^\alpha = T$. It is straightforward to check that R cannot be written as $R = R' \cup \{c\}$ such that $\langle R\rangle = \langle R'\rangle \times \langle c\rangle$ for any $c \in R$. Consequently, $a^\alpha = b_0$, which is a contradiction. So $\{S, T\}$ is a NCI-pair of size m.

Now assume that $m > |L|$ and $m = k|L| + j$ where $1 \leq k \leq p^{r+s} - 2$ and $0 \leq j \leq |L| - 1$. Note that $m \leq \frac{|G|-1}{2} = \frac{p^{r+s}|L|-1}{2}$. Let $\{S_0, T_0\}$ be a NCI-pair of $\langle a, b\rangle$ of size k constructed in Steps 1–3. Let R be an arbitrary Cayley subset of L of size j. Set

$$S = S_0 L \cup R, \quad T = T_0 L \cup R.$$

Let $\Gamma_1 = Cay(L, R)$. By Lemma 2.2, we have

$$Cay(\langle S\rangle, S) = Cay(\langle S_0\rangle, S_0)[\Gamma_1] \cong Cay(\langle T_0\rangle, T_0)[\Gamma_1] = Cay(\langle T\rangle, T).$$

Thus $Cay(G, S) \cong Cay(G, T)$ (by Lemma 2.3). Since G has the m-DCI property, there is $\alpha \in Aut(G)$ such that $S^\alpha = T$. Let $\Gamma = Cay(G, S)$ and $\Sigma = Cay(G, T)$, and let $A = Aut\,\Gamma$ and $B = Aut\,\Sigma$. Then this α automatically induces an isomorphism from Γ to Σ so that $1^\alpha = 1$ and

$\Gamma(1)^\alpha = \Sigma(1)$. Now $\{xL \mid x \in \langle a, b\rangle\}$ is an imprimitive system of A on $V\Gamma$. It follows that for each $x \in S_0L$, x lies in an orbit of A_1^S of size at least $|L|$; for each $x \in R$, the orbit of A_1^S containing x has size at most $|R| < |L|$. Similarly, if $x \in T_0L$ then x lies in an orbit of B_1^T of size at least $|L|$; if $x \in R$ then the orbit of B_1^T containing x has size at most $|R| < |L|$. Consequently, $(S_0L)^\alpha = T_0L$ and $R^\alpha = R$. Let $\overline{\alpha}$ be the automorphism of $G/L \cong \langle a, b\rangle$ induced by α. Then it follows that S_0 is fused to T_0, a contradiction. This completes the proof of the Main Theorem.

References

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

[2] N. Biggs, *Algebraic Graph Theory*, (Cambridge Uni. Press, New York, 1974).

[3] C. Delorme, O. Favaron and M. Maheo, Isomorphisms of Cayley Multigraphs of degree 4 on finite abelian groups, *Europ. J. Combin.* **13** (1992), 59-61.

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

[5] C. H. Li, The cyclic groups with the m-DCI property, *Europ. J. Combin.* **18** (1997), 253-261.

[6] C. H. Li, On isomorphisms of connected Cayley graphs, *Discrete Math.* **178** (1998), 109-122.

[7] C. H. Li, On isomorphisms of connected Cayley graphs, II, *J. Combin. Theory (B)* **74** (1998), 28-34.

[8] C. H. Li, On finite groups with the Cayley isomorphism property, II, *J. Combin. Theory (A)* (to appear).

[9] C. H. Li, C. E. Praeger and M. Y. Xu, On finite groups with the Cayley isomorphism property, *J. Graph Theory* **27** (1998), 21-31.

[10] C. H. Li, C. E. Praeger and M. Y. Xu, Isomorphisms of finite Cayley digraphs of bounded valency, *J. Combin. Theory (B)* **73** (1998), 164-183.

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

[12] M. Suzuki, *Group Theory I*, (Springer-Verlag, New York, 1986).

[13] J. P. Zhang, On finite groups all of whose elements of the same order are conjugate in their automorphism groups, *J. Algebra* **153** (1992), 22-36.