Europ. J. Combinatorics (1997) **18,** 655–665

The Cyclic Groups with the m-DCI Property

CAI HENG LI

For a finite group G and a subset S of G which does not contain the identity of G, let $\mathrm{Cay}(G, S)$ denote the Cayley graph of G with respect to S. If, for all subsets S, T of G of size m, $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ implies $S^{\alpha} = T$ for some $\alpha \in \mathrm{Aut}(G)$, then G is said to have the m-DCI property. In this paper, a classification is presented of the cyclic groups with the m-DCI property, which is reasonably complete.

1. INTRODUCTION

Let G be a finite group and set $G^{\#} = G \backslash \{1\}$. For a subset S of $G^{\#}$, the *Cayley graph* $\mathrm{Cay}(G, S)$ of G with respect to S is the directed graph Γ with vertex set $V\Gamma = G$ and edge set $E\Gamma = \{(a, b) \mid a, b \in G,\ ba^{-1} \in S\}$. If $S = S^{-1} := \{s^{-1} \mid s \in S\}$, then the adjacency relation is symmetric and so $\mathrm{Cay}(G, S)$ may be viewed as an undirected graph.

The problem of determining whether any two Cayley graphs of a group G are isomorphic is a long-standing open problem. If $\sigma \in \mathrm{Aut}(G)$, then σ induces an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, S^{\sigma})$. However, it is of course possible that there exist a group G and subsets S and T of $G^{\#}$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ but S is not conjugate under $\mathrm{Aut}(G)$ to T. A Cayley graph $\mathrm{Cay}(G, S)$ is called a *CI-graph* (CI stands for *Cayley Invariant*) of G if, for any subset T of $G^{\#}$, $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ implies $S^{\alpha} = T$ for some $\alpha \in \mathrm{Aut}(G)$. If all Cayley graphs of G of valency m are CI-graphs, then G is said to have the *m-DCI property*. Recently, Praeger, Xu and the author in [12] proposed to characterize finite groups with the m-DCI property. A group G has the 1-DCI property iff all elements of G of the same order are conjugate under $\mathrm{Aut}(G)$. Zhang [17] gave a good description for such groups. The author [9] completely classified the finite groups which have the 2-DCI property but do not have the 1-DCI property. It is proved in [10] that all Sylow subgroups of an abelian group with the m-DCI property are homocyclic. (A group is said to be *homocyclic* if it is a direct product of cyclic groups of the same order.) In [12], all finite abelian groups with the m-DCI property for $m \leq 4$ were completely classified, and a general investigation was made of the structure of Sylow subgroups of groups with the m-DCI property for certain values of m. However, this seems very far from obtaining a 'good' characterization of arbitrary groups with the m-DCI property. In this paper, we focus on the cyclic groups.

A. Ádám [1] conjectured that if G is cyclic then, for any S and T, $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ implies $S = T^{\sigma}$ for some $\sigma \in \mathrm{Aut}(G)$. This conjecture was disproved in [6]. However, it has been proved in many cases: it is true for graphs of valency not greater than 5 (see [5, 8, 16]), and of order n where $n = 4p$ [3, 7] or n is square-free [13]. On the other hand, it is also known that the conjecture fails if n is divisible by 8 or by an odd prime-square. In this paper, it will be shown that if n is not a prime-square and n is divisible by 8 or by an odd prime-square then $\mathbb{Z}_n$ does not have the m-DCI property for any value of m which is greater than the largest prime divisor of n. More precisely, the aim of this paper is to obtain a reasonably complete classification of cyclic groups with the m-DCI property where m is a positive integer.

0195-6698/97/060655 + 11 $25.00/0 ej960130

For convenience, if $\mathrm{Cay}(G, S)$ is a CI-graph of G, then the subset S is called a *CI-subset* of G. From the definition it easily follows that a subset S of $G^{\#}$ is a CI-subset of G iff $G^{\#}\backslash S$ is a CI-subset. Thus, for any positive integer $m < |G|$, G has the m-DCI property iff G has the $(|G^{\#}| - m)$-DCI property. Therefore, we shall always assume that $m \leqslant (|G| - 1)/2$.

The first result of this paper determines for which positive integers m the cyclic groups of order p^2 have the m-DCI property, where p is a prime. It is trivial to show that $\mathbb{Z}_4$ has the m-DCI property for all values of m, so we only consider the case in which p is odd.

THEOREM 1.1. *Let G be a cyclic group of order p^2, where p is an odd prime, and let m be a positive integer with $1 \leqslant m \leqslant (p^2 - 1)/2$. Then G has the m-DCI property iff either $m < p$, or $m \equiv 0$ or $-1 \pmod p$.*

The next result presents a classification of all cyclic groups with the m-DCI property.

THEOREM 1.2. *Let G be a cyclic group, and let p be a prime divisor of $|G|$ and G_p, the Sylow p-subgroup of G. Suppose that G has the m-DCI property, where $p + 1 \leqslant m \leqslant (|G| - 1)/2$. Then one of the following holds*:
(i) $G = \mathbb{Z}_{p^2}$ *and* $m \equiv 0$ *or* $-1 \pmod p$;
(ii) *p is odd and* $G_p = \mathbb{Z}_p$;
(iii) $p = 2$ *and* $G_2 = \mathbb{Z}_2$ *or* $\mathbb{Z}_4$.

REMARK. Let m be a positive integer. A group G is called an *m-DCI-group* if G has the k-DCI property for any positive integer $k \leqslant m$. Let G be a cyclic group with the m-DCI property. If m is greater than the largest prime divisor of $|G|$ and $G_2 \neq \mathbb{Z}_4$, then, by Theorem 1.2, $|G|$ is square-free. Consequently, by [13], G is a $|G|$-DCI-group and so G has the m-DCI property. On the other hand, if m is less than the least prime divisor of $|G|$, then it follows from [11, Theorem 1.1] that G is an m-DCI-group and so G has the m-DCI property. Therefore, we suggest the following.

CONJECTURE 1.3. *The converse of Theorem* 1.2 *is true.*

If the conjecture were true, then Theorems 1.1 and 1.2 would provide a complete classification of cyclic groups with the m-DCI property.

Finally, we discuss the undirected Cayley graphs. For a positive integer m, a group G is said to have the *m-CI property* if all undirected Cayley graphs of G of valency m are CI-graphs of G. For undirected graphs, a similar conclusion should hold, so we propose the following problem.

PROBLEM 1.4. Characterize the cyclic groups $\mathbb{Z}_n$ and integers $m \geqslant 2$ such that $\mathbb{Z}_n$ has the *m-CI* property.

2. Preliminaries

In this section we quote some preliminary results that will be used in the proofs of Theorems 1.1 and 1.2. The normalizer of G in $\mathrm{Aut}\,\mathrm{Cay}(G, S)$ is often useful for characterizing $\mathrm{Cay}(G, S)$.

LEMMA 2.1 ([7, Lemma 2.1]). *Let G be a finite group and let S be a subset of $G^{\#}$. Let $A = \mathrm{Aut}\,\mathrm{Cay}(G, S)$ and $\mathrm{Aut}(G, S) = \{\alpha \in \mathrm{Aut}(G) \mid S^{\alpha} = S\}$. Then $\mathbf{N}_A(G) = G \rtimes \mathrm{Aut}(G, S)$, a semidirect product of G by $\mathrm{Aut}(G, S)$.*

This property is especially useful for groups of prime-power order, because of the following conclusion.

LEMMA 2.2 ([15, p. 88]). *Let H be a proper subgroup of a p-group G, where p is a prime. Then $\mathbf{N}_G(H) > H$. In particular, if $|[G: H]| = p$, then $H \lhd G$.*

Next, we have a criterion for a Cayley graph to a be a CI-graph, which will be used in the next section.

LEMMA 2.3 (Alspach and Parsons [2, Theorem 1], or Babai [3, Lemma 3.1]). *Let Γ be a Cayley graph of a finite group G and let A be the automorphism group of Γ. Let G_R denote the subgroup of A consisting of right multiplications $g: x \to xg$ by elements $g \in G$. Then Γ is a CI-graph of G iff for any $\tau \in \mathrm{Sym}(G)$ with $G_R^{\tau} \leqslant A$, there exists $\alpha \in A$ such that $G_R^{\alpha} = G_R^{\tau}$.*

The next simple lemma gives some properties about subsets of a cyclic group.

LEMMA 2.4 ([10, 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 $i = 1$.*

For a digraph $\Gamma = (V, E)$, its *complement* $\bar{\Gamma} = (V, \bar{E})$ is the graph with vertex set V such that $(a, b) \in \bar{E}$ 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 $((a_1, a_2), (b_1, b_2))$ is an arc iff 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 vertex-disjoint copies of Γ. The final lemma concerns the structure of graphs coming from lexicographic product of graphs.

LEMMA 2.5 ([10, 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 less than $|G/H|$. Set $\bar{G} := G/H$, $\bar{R} := R/H$ and $\Sigma := \mathrm{Cay}(\bar{G}, \bar{R})$. Then $\mathrm{Cay}(G, R) = \Sigma[\bar{K}_m]$, where $m = |H|$. Furthermore, if $S = R \cup R_0$, where R_0 is a subset of $H^{\#}$, then $\mathrm{Cay}(G, S) = \Sigma[\Gamma_0]$, where $\Gamma_0 = \mathrm{Cay}(H, R_0)$.*

The terminology and notation used in this paper are standard (see, for example, [4, 15]). In particular, for a positive integer n, C_n denotes the (directed or undirected) cycle of length n. For a group and an element $g \in G$, denote by $|G|$ and $o(g)$ the orders of G and g, respectively. For a group G and a pair of subsets S, T of $G^{\#}$, if $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ but S is not conjugate under $\mathrm{Aut}(G)$ to T, then $\{S, T\}$ is called an *NCI-pair* of G.

3. The m-DCI property of $\mathbb{Z}_{p^2}$

In this section, we will prove Theorem 1.1.

Proof of Theorem 1.1. Suppose that $m > p$ and $m \not\equiv 0, -1 \pmod p$. Since $p < m \leqslant (p^2-1)/2$, we may write $m = kp + j$ such that $1 \leqslant k \leqslant (p-1)/2$ and $1 \leqslant j \leqslant p-2$. We will prove that G does not have the m-DCI property. Let $G = \langle a \rangle$, and set

$$\begin{cases} S = \{a, \ldots, a^k\}\langle a^p \rangle \cup \{a^p, \ldots, a^{jp}\}, \\ T = \{a, \ldots, a^k\}\langle a^p \rangle \cup \{a^{-p}, \ldots, a^{-jp}\}. \end{cases}$$

Clearly, $\Gamma_1 := \mathrm{Cay}(\langle a^p \rangle, \{a^p, \ldots, a^{jp}\}) \cong \mathrm{Cay}(\langle a^p \rangle, \{a^{-p}, \ldots, a^{-jp}\})$. Let $\bar{G} := G/\langle a^p \rangle$, $\bar{S} := S\langle a^p \rangle/\langle a^p \rangle \backslash \{1\}$ and $\bar{T} := T\langle a^p \rangle / \langle a^p \rangle \backslash \{1\}$. Then $\bar{S} = \{\bar{a}, \ldots, \bar{a}^k\} = \bar{T}$. Let $\Gamma_2 = \mathrm{Cay}(\bar{G}, \bar{S})$ $(= \mathrm{Cay}(\bar{G}, \bar{T}))$. By Lemma 2.5, $\mathrm{Cay}(G, S) \cong \Gamma_2[\Gamma_1] \cong \mathrm{Cay}(G, T)$. If G has the m-DCI property, then there exists $\alpha \in \mathrm{Aut}(G)$ mapping S to T. Since $a \in S$ we have $a^\alpha \in T$, and since $o(a^\alpha) = o(a)$, we have $a^\alpha \in \{a, \ldots, a^k\}\langle a^p \rangle$. Thus $a^\alpha = a^{i+hp}$ for some integers i, h with $1 \leqslant i \leqslant k$. Let $\bar{\alpha}$ be the automorphism of $\bar{G}$ induced by α. Then $\{\bar{a}^i, \ldots, \bar{a}^{ik}\} = \bar{S}^{\bar{\alpha}} = \bar{T} = \{\bar{a}, \ldots, \bar{a}^k\}$. By Lemma 2.4, $i \equiv 1 \pmod p$ and since $1 \leqslant i \leqslant k < p$, we have $i = 1$. Therefore, $(a^p)^\alpha = (a^{1+hp})^p = a^p$. Since $1 \leqslant j \leqslant p-2$, $a^p \notin T$, so $(a^p)^\alpha \in S^\alpha \backslash T$, which is a contradiction.

Conversely, we need to prove that G has the m-DCI property for $m < p$ or $m \equiv 0, -1 \pmod p$. Let $G = \langle a \rangle \cong \mathbb{Z}_{p^2}$, and let S be a subset of $G^\#$ of size m. Our goal is to show that S is a CI-subset. Let $\Gamma = \mathrm{Cay}(G, S)$ and $A = \mathrm{Aut}\,\Gamma$, and let A_1 be the stabilizer of 1 in A. If $p \nmid |A_1|$, then G is a Sylow p-subgroup of A. By Sylow's Theorem and Lemma 2.3, S is a CI-subset. Thus we may assume that $p \mid |A_1|$.

First, assume that $m < p$. If $\langle S \rangle = G$, then $p \nmid |A_1|$, which is a contradiction. Thus $\langle S \rangle < G$ and so $\langle S \rangle = \langle a^p \rangle$. Let $B = \mathrm{Aut}\,\mathrm{Cay}(\langle a^p \rangle, S)$ and let B_1 be the stabilizer of 1 in B. Since $m < p, p \nmid |B_1|$, so S is a CI-subset of $\langle a^p \rangle$ (arguing as in the previous paragraph). For any subset T of $G^\#$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, we have $\langle T \rangle = \{a^p\}$ and $\mathrm{Cay}(\langle a^p \rangle, S) \cong \mathrm{Cay}(\langle a^p \rangle, T)$, and, therefore, since S is a CI-subset of $\langle a^p \rangle$, there exists $\alpha \in \mathrm{Aut}(\langle a^p \rangle)$ satisfying $S^\alpha = T$. Furthermore, there exists $\beta \in \mathrm{Aut}(G)$ such that the restriction of β to $\langle a^p \rangle$ is equal to α. Hence $S^\beta = T$ and so S is a CI-subset of G.

Next, suppose that $m \geqslant p$ and $m \equiv 0$ or $-1 \pmod p$; that is, $m = kp$ or $kp + (p-1)$ for some k such that $p \leqslant m \leqslant (p^2-1)/2$. Since $p \mid |A_1|$, a Sylow p-subgroup of A has order at least p^3. By Sylow's Theorem, there exists a Sylow p-subgroup P of A which contains G as a subgroup. By Lemma 2.2, $\mathbf{N}_A(G) \geqslant \mathbf{N}_P(G) > G$. First, we study the structure of S. From Lemma 2.1, it follows that there exists $\alpha \in \mathrm{Aut}(G)$ of order p such that $S^\alpha = S$. It is easy to see that $a^\alpha = a^{1+jp}$ for some $1 \leqslant j \leqslant p-1$. Thus, for any integer k, $(a^k)^\alpha = a^{k+kjp}$, so $(a^k)^\alpha = a^k$ iff $p \mid k$, which is equivalent to $a^k \in \langle a^p \rangle$. Therefore, α fixes every element of S of order p and fixes no elements of S of order p^2. Moreover, if $a^k \in S$ and $(a^k)^\alpha \neq a^k$, then $a^k\langle a^p \rangle = a^k \langle a^{kjp} \rangle = \{a^k, a^{k+kjp}, \ldots, a^{k+(p-1)kjp}\} = \{a^k, (a^k)^\alpha, \ldots, (a^k)^{\alpha^{p-1}}\} = (a^k)^{\langle \alpha \rangle} \subset S$. Since α is of order p, every non-trivial $\langle \alpha \rangle$-orbit (on S) has length p. Since G has exactly $p-1$ elements of order p, it follows that there is a subset Q of $G \backslash \langle a^p \rangle$ of size k such that, if $m = kp$, then $S = Q\langle a^p \rangle$, and if $m = kp + (p-1)$ then $S = Q\langle a^p \rangle \cup \langle a^p \rangle^\#$.

Let T be a subset of $G^\#$ such that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$. It follows from the arguments in the previous paragraph that if $m = kp$ then $T = Q'\langle a^p \rangle$, and if $m = kp + (p-1)$ then $T = Q'\langle a^p \rangle \cup \langle a^p \rangle^\#$, for some subset Q' of $G \backslash \langle a^p \rangle$ of size k. We want to prove that S is conjugate under $\mathrm{Aut}(G)$ to T. Let $\bar{G} = G/\langle a^p \rangle$ and $\bar{S} = S\langle a^p \rangle / \langle a^p \rangle$, and let $\Sigma = \mathrm{Cay}(\bar{G}, \bar{S})$. By Lemma 2.5, if $m = kp$, then $\Gamma \cong \Sigma[\bar{K}_p]$; if $m = kp + (p-1)$, then $\Gamma = \Sigma[K_p]$. Thus A preserves the unique non-trivial imprimitive system $\{x\langle a^p\rangle \mid x \in G\}$ of $V\Gamma$ consisting of p blocks of size p. Similarly, setting $\Gamma' = \mathrm{Cay}(G, T)$, also $\mathrm{Aut}\,\Gamma'$ has the unique imprimitive system $\{x\langle a^p\rangle \mid x \in G\}$. Therefore, if ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$, then $\{x\langle a^p\rangle \mid x \in G\}^\rho = \{x\langle a^p\rangle \mid x \in G\}$. Hence ρ induces an isomorphism from $\mathrm{Cay}(\bar{G}, \bar{S})$ to $\mathrm{Cay}(\bar{G}, \bar{T})$, where $\bar{T} = T\langle a^p\rangle/\langle a^p\rangle$. Since $V\Sigma$ is of size p, $\bar{G}$ is a Sylow p-subgroup of $\mathrm{Aut}\,\Sigma$. All subgroups of $\mathrm{Aut}\ \Sigma$ which act regularly on $V\Sigma$ are cyclic of order p and hence are conjugate by Sylow's Theorem. So, by Lemma 2.3, $\bar{S}$ is a CI-subset of $\bar{G}$. Hence there exists $\tau \in \mathrm{Aut}(\bar{G})$ such that $\bar{S}^\tau = \bar{T}$, so $\bar{a}^\tau = \bar{a}^r$ for some integer $r \in \{1, 2, \ldots, p-1\}$. Write $\bar{S} = \{\bar{a}^{i_1}, \bar{a}^{i_2}, \ldots, \bar{a}^{i_k}\}$, and then $\bar{T} = \bar{S}^\tau = \{\bar{a}^{i_1 r}, \bar{a}^{i_2 r}, \ldots, \bar{a}^{i_k r}\}$. Therefore, $S = a^{i_1}\langle a^p\rangle \cup a^{i_2}\langle a^p\rangle \cup \ldots \cup a^{i_k}\langle a^p\rangle$ and $T = a^{i_1 r}\langle a^p\rangle \cup a^{i_2 r}\langle a^p\rangle \cup \ldots \cup a^{i_k r}\langle a^p\rangle$. Since r is coprime to p, $a \to a^r$ induces an automorphism σ of G. Now $S^\sigma = T$, so S is a CI-subset of G. Therefore, G has the m-DCI property. □

4. Proof of Theorem 1.2

This section is devoted to proving Theorem 1.2. Let G be a cyclic group with the m-DCI property, and let p be a prime divisor of $|G|$. If G is of order p^2, then we have completely determined the m-DCI property in Theorem 1.1. Thus here we only consider the other cases; that is, we assume that G is not of order p^2.

Proof of Theorem 1.2. Let $G = \langle z\rangle$ with order n, and let $G_p = \langle a\rangle \cong \mathbb{Z}_{p^d}$ be the Sylow p-subgroup of G. If $G = \mathbb{Z}_{p^2}$ then, by Theorem 1.1, $m \equiv 0$ or $-1 \pmod p$, as in part (i). Suppose that $G \neq \mathbb{Z}_{p^2}$, and that if p is odd then $d \geqslant 2$, and if $p = 2$ then $d \geqslant 3$. To prove the theorem, we shall construct an NCI-pair of size m for every $m \in \{p+1,\ p+2, \ldots, (|G|-1)/2\}$.

Case 1. Suppose that p is odd and that $d \geqslant 2$. Let $n' = n/p$ and let $a_0 = z^{n'}$. Then a_0 is of order p, and since $p \mid n'$, $a_0^{n'} = 1$. Write $m = kp + j$, where $0 \leqslant j \leqslant p-1$, $k \geqslant 1$, and if $j = 0$ then $k > 1$.

Step 1. Assume that $1 \leqslant j \leqslant p-2$. Set $S_0 = \{a_0, \ldots, a_0^j\}$ and $T_0 = \{a_0^{-1}, \ldots, a_0^{-j}\}$, and let

$$\begin{cases} S = \{z, \ldots, z^k\}\langle a_0\rangle \cup S_0, \\ T = \{z, \ldots, z^k\}\langle a_0\rangle \cup T_0. \end{cases}$$

Let $\bar{G} = G/\langle a_0\rangle$, $\bar{S} = S\langle a_0\rangle/\langle a_0\rangle$ and $\bar{T} = T\langle a_0\rangle/\langle a_0\rangle$. Then $\bar{S} = \bar{T} = \{\bar{z}, \ldots, \bar{z}^k\}$. Let $\Gamma_1 = \mathrm{Cay}(\bar{G}, \bar{S})$ and $\Gamma_2 = \mathrm{Cay}(\langle a_0\rangle, S_0)$. Then $\Gamma_2 \cong \mathrm{Cay}(\langle a_0\rangle, T_0)$, and hence, by Lemma 2.5, $\mathrm{Cay}(G, S) = \Gamma_1[\Gamma_2] \cong \mathrm{Cay}(G, T)$. Since G has the m-DCI property, there exists $\alpha \in \mathrm{Aut}(G)$ such that $S^\alpha = T$. Since $o(z^\alpha) = o(z) = n$ and $o(a_0) < n$, we have $z^\alpha \in z^i\langle a_0\rangle$ for some $1 \leqslant i \leqslant k$. Thus $\bar{z}^{\bar{\alpha}} = \bar{z}^i$, where $\bar{\alpha}$ is the automorphism of $\bar{G}$ induced by α. Therefore, $\{\bar{z}^i, \ldots, \bar{z}^{ki}\} = \{\bar{z}, \ldots, \bar{z}^k\}^{\bar{\alpha}} = \bar{S}^{\bar{\alpha}} = \bar{T} = \{\bar{z}, \ldots, \bar{z}^k\}$. By Lemma 2.4, $i \equiv 1 \pmod{n'}$; that is, $z^\alpha = za_0^h$ for some integer h. Since $1 \leqslant j \leqslant p-2$, $a_0 \notin T$. However, since $z^{n'} = a_0$ and $a_0^{n'} = 1$, we have $a_0^\alpha = (z^{n'})\alpha = (za_0^h)^{n'} = a_0 \in S^\alpha$, which is a contradiction. Therefore, $\{S, T\}$ is an NCI-pair of G.

Step 2. Assume that $j = p-1$, so that $m = kp + (p-1)$. First, suppose that $G \ncong \mathbb{Z}_{p^d}$. Then $z^{p^d} \neq 1$ and $G = \langle a\rangle \times \langle z^{p^d}\rangle$. Set $S' = \{a_0, \ldots, a_0^{p-2}\} \cup \{z^{p^d}\}$ and $T' = \{a_0^{-1}, \ldots, a_0^{-(p-2)}\} \cup \{z^{p^d}\}$. If $p^d > k$, then let

$$\begin{cases} S = \{z, \ldots, z^k\}\langle a_0\rangle \cup S', \\ T = \{z, \ldots, z^k\}\langle a_0\rangle \cup T'; \end{cases}$$

if $p^d \leqslant k$, then let

$$\begin{cases} S = (\{z, \ldots, z^{k+1}\}\backslash\{z^{p^d}\})\langle a_0\rangle \cup S', \\ T = (\{z, \ldots, z^{k+1}\}\backslash\{z^{p^d}\})\langle a_0\rangle \cup T'. \end{cases}$$

It is easy to see that $K := \langle S'\rangle = \langle T'\rangle = \langle a_0, z^{p^d}\rangle = \langle a_0\rangle \times \langle z^{p^d}\rangle$ and $G = K \cup zK \cup \cdots \cup z^{p^{d-1}-1}K$. Thus z^iK is the vertex-set of the connected component of both $\mathrm{Cay}(G, S')$ and $\mathrm{Cay}(G, T')$ containing the vertex z^i. Let C_i and D_i denote the connected components of $\mathrm{Cay}(G, S')$ and of $\mathrm{Cay}(G, T')$, respectively, with vertex set z^iK. Clearly, there exists $\sigma \in \mathrm{Aut}(K)$ such that $a_0^\sigma = a_0^{-1}$ and $(z^{p^d})^\sigma = z^{p^d}$, which satisfies $S'^\sigma = T'$. Thus σ induces an isomorphism from $\mathrm{Cay}(K, S')$ to $\mathrm{Cay}(k, T')$. Let ρ be a map from G to G defined by

$$\rho\colon z^iu \to z^iu^\sigma, \qquad \text{where } i \in \{0, 1, \ldots, p^{d-1}-1\} \quad \text{and} \quad u \in K.$$

Then $(z^iK)^\rho = z^iK$, and ρ induces an isomorphism from C_i to D_i for every i. Thus ρ preserves adjacency from $\mathrm{Cay}(G, S')$ to $\mathrm{Cay}(G, T')$.

We want to prove that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Write $l = n/p^d$, $z' = z^{p^d}$ and $K = \langle a_0\rangle \cup z'\langle a_0\rangle \cup \cdots \cup z'^{l-1}\langle a_0\rangle$. Since $\langle a_0\rangle^\sigma = \langle a_0\rangle$ and $z'^\sigma = z'$, we have $(z'^i\langle a_0\rangle)^\sigma = z'^i\langle a_0\rangle$ for $i = 0, 1, \ldots, l-1$. Furthermore, write G as the union of cosets of $\langle a_0\rangle$ by

$$G = \bigcup_{0\leqslant s\leqslant p^{d-1}-1} \bigcup_{0\leqslant t\leqslant l-1} z^sz'^t\langle a_0\rangle.$$

Then we have $(z^sz'^t\langle a_0\rangle)^\rho = z^s(z'^t\langle a_0\rangle)^\sigma = z^sz'^t\langle a_0\rangle$, so ρ maps $z^i\langle a_0\rangle$ to $z^i\langle a_0\rangle$ for all $i \in \{0, 1, \ldots, k+1\}$. Consequently, ρ also preserves adjacency from $\mathrm{Cay}(G, S\backslash S')$ to $\mathrm{Cay}(G, T\backslash T')$. It follows that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Since G has the m-DCI property, there is $\alpha \in \mathrm{Aut}(G)$ such that $S^\alpha = T$. Now $z^\alpha = z^i$ for some integer $i \in \{1, \ldots, n-1\}$. Since $\langle a_0\rangle^\alpha = \langle a_0\rangle$, we have, for any integer h, $(z^h\langle a_0\rangle)^\alpha = z^{hi}\langle a_0\rangle$. Consequently, $(\{z, \ldots, z^k\}H)^\alpha = \{z, \ldots, z^k\}\langle a_0\rangle$ and $((\{z, \ldots, z^{k+1}\}\backslash \{z^{p^d}\})\langle a_0\rangle)^\alpha = (\{z, \ldots, z^{k+1}\}\backslash\{z^{p^d}\})\langle a_0\rangle$. It follows that $S'^\alpha = T'$. Since z^{p^d} is a unique element of $S' \cup T'$ of order coprime to p, $(z^{p^d})^\alpha = z^{p^d}$, so $(z^{p^d}\langle a_0\rangle)^\alpha = z^{p^d}\langle a_0\rangle$. Therefore,

$$\{z^i, \ldots, z^{ik}\}\langle a_0\rangle = (\{z, \ldots, z^k\}\langle a_0\rangle)^\alpha = \{z, \ldots, z^k\}\langle a_0\rangle, \qquad \text{if } p^d > k;$$

or

$$\{z^i, \ldots, z^{i(k+1)}\}\langle a_0\rangle = (\{z, \ldots, z^{k+1}\}\langle a_0\rangle)^\alpha = \{z, \ldots, z^{k+1}\}\langle a_0\rangle, \qquad \text{if } p^d \leqslant k.$$

By Lemma 2.4, in either case $i \equiv 1 \pmod{n/p}$; that is, $z^\alpha = za_0^h$ for some integer h. Therefore, $a_0^\alpha = (z^{n'})^\alpha = (za_0^h)^{n'} = z^{n'} = a_0 \in S^\alpha\backslash T$, a contradiction. Thus $\{S, T\}$ is an NCI-pair.

Now suppose that $G = \mathbb{Z}_{p^d}$, where $d \geqslant 3$. Set $S' = \{a_0, \ldots, a_0^{p-2}\} \cup \{z^{p^{d-2}}\}$ and $T' = \{a_0, \ldots, a_0^{p-2}\} \cup \{z^{p^{d-2}+p^{d-1}}\}$. If $p^{d-2} > k$, then let

$$\begin{cases} S = \{z_1, \ldots, z^k\}\langle a_0\rangle \cup S', \\ T = \{z, \ldots, z^k\}\langle a_0\rangle \cup T'; \end{cases}$$

if $p^{d-2} \leqslant k$, then let

$$\begin{cases} S = (\{z, \ldots, z^{k+1}\}\backslash\{z^{p^{d-2}}\})\langle a_0\rangle \cup S', \\ T = (\{z, \ldots, z^{k+1}\}\backslash\{z^{p^{d-2}}\})\langle a_0\rangle \cup T'. \end{cases}$$

Now $K := \langle S'\rangle = \langle T'\rangle = \langle z^{p^{d-2}}\rangle \cong \mathbb{Z}_{p^2}$, and $G = K \cup zK \cup \cdots \cup z^{p^{d-2}-1}K$. Then z^iK is the vertex-set of the connected component of both $\mathrm{Cay}(G, S')$ and $\mathrm{Cay}(G, T')$ containing the vertex z^i. Let C_i and D_i denote the connected components of $\mathrm{Cay}(G, S')$ and of $\mathrm{Cay}(G, T')$, respectively, with vertex set z^iK. There is $\sigma \in \mathrm{Aut}(K)$ such that

$(z^{p^{d-2}})^{\sigma} = z^{p^{d-2}+p^{d-1}}$, which fixes $a_0(=z^{p^{d-1}})$. Therefore, $S'^{\sigma} = T'$ and so σ induces an isomorphism from $\mathrm{Cay}(K, S')$ to $\mathrm{Cay}(K, T')$. Let ρ be a map from $\langle z\rangle$ to $\langle z\rangle$ defined by

$$\rho\colon z^i u \to z^i u^{\sigma}, \qquad \text{where } i \in \{0, 1, \ldots, p^{d-2}-1\} \quad \text{and} \quad u \in K.$$

Then $(z^iK)^{\rho} = z^iK$, and ρ induces an isomorphism from C_i to D_i for every i. Thus ρ preserves adjacency from $\mathrm{Cay}(G, S')$ to $\mathrm{Cay}(G, T')$.

We want to prove that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Write $z' = z^{p^{d-2}}$ and $K = \langle a_0\rangle \cup z'\langle a_0\rangle \cdots \cup z'^{p-1}\langle a_0\rangle$. Since $(z^{hp^{d-2}}\langle a_0\rangle)^{\sigma} = z^{h(p^{d-2}+p^{d-1})}\langle a_0\rangle = z^{hp^{d-2}}\langle a_0\rangle$ for $h = 0, 1, \ldots, p-1$, we have $(z'^i\langle a_0\rangle)^{\sigma} = z'^i\langle a_0\rangle$ for $i = 0, 1, \ldots, p-1$. Furthermore, write G as the union of cosets of $\langle a_0\rangle$ by

$$G = \bigcup_{0\leqslant s\leqslant p^{d-2}-1}\ \bigcup_{0\leqslant t\leqslant p-1} z^s z''\langle a_0\rangle.$$

Now $(z^s z''\langle a_0\rangle)^{\rho} = z^s(z''\langle a_0\rangle)^{\sigma} = z^s z''\langle a_0\rangle$, and, consequently, ρ maps $z^i\langle a_0\rangle$ to $z^i\langle a_0\rangle$ for all $i \in \{0, 1, \ldots, p^{d-1}-1\}$. Thus ρ also preserves adjacency from $\mathrm{Cay}(G, S\backslash S')$ to $\mathrm{Cay}(G, T\backslash T')$. It follows that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Since G has the m-DCI property, there is $\alpha \in \mathrm{Aut}(G)$ such that $S^{\alpha} = T$. Let $z^{\alpha} = z^i$ for some integer i. Since $\langle a_0\rangle$ is a characteristic subgroup of $\langle z\rangle$, $\langle a_0\rangle^{\alpha} = \langle a_0\rangle$, so

$$\{a_0^i, \ldots, a_0^{i(p-2)}\} = \{a_0, \ldots, a_0^{p-2}\}^{\alpha} = \{a_0, \ldots, a_0^{p-2}\}.$$

Thus $i \equiv 1 \pmod p$; namely, $i = 1 + lp$ for some integer l. Therefore, $(z^{p^{d-2}})^{\alpha} = z^{ip^{d-2}} = z^{(1+lp)p^{d-2}} = z^{p^{d-2}+lp^{d-1}}$. Thus $(z^{p^{d-2}}\langle a_0\rangle)^{\alpha} = z^{p^{d-2}}\langle a_0\rangle$, and so

$$\{z^i, \ldots, z^{ik}\}\langle a_0\rangle = (\{z, \ldots, z^k\}\langle a_0\rangle)^{\alpha} = \{z, \ldots, z^k\}\langle a_0\rangle, \qquad \text{if } p^{d-2} > k;$$

or

$$\{z^i, \ldots, z^{i(k+1)}\}\langle a_0\rangle = (\{z, \ldots, z^{k+1}\}\langle a_0\rangle)^{\alpha} = \{z, \ldots, z^{k+1}\}\langle a_0\rangle, \qquad \text{if } p^{d-2} \leqslant k.$$

By Lemma 2.4, in either case $i \equiv 1 \pmod{p^{d-1}}$, so p^{d-1} divides lp. In particular, since $d \geqslant 3$, p^2 divides lp. Therefore, $(z^{p^{d-2}})^{\alpha} = (z^{1+lp})^{p^{d-2}} = z^{p^{d-2}+lp\cdot p^{d-2}} = z^{p^{d-2}}$, which is not in T, a contradiction. Thus $\{S, T\}$ is an NCI-pair of G.

Step 3. Assume that $j = 0$; namely, $m = kp$. First, suppose that G is neither $\mathbb{Z}_{p^d}$ nor $\mathbb{Z}_{2p^d}$. Then z^{p^d} is of order greater than 2. Set $S' = \{a_0, \ldots, a_0^{p-2}\} \cup \{z^{p^d}, z^{-p^d}\}$ and $T' = \{a_0^{-1}, \ldots, a_0^{-(p-2)}\} \cup \{z^{p^d}, z^{-p^d}\}$. If $p^d \geqslant k$, then let

$$\begin{cases} S = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup S', \\ T = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup T'; \end{cases}$$

if $p^d \leqslant k-1$, then let

$$\begin{cases} S = (\{z, \ldots, z^k\}\backslash\{z^{p^d}\})\langle a_0\rangle \cup S', \\ T = (\{z, \ldots, z^k\}\backslash\{z^{p^d}\})\langle a_0\rangle \cup T'. \end{cases}$$

Arguing as for the case $G \neq \mathbb{Z}_{p^d}$ in Step 2, we know that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, but S is not conjugate under $\mathrm{Aut}(G)$ to T, so $\{S, T\}$ is an NCI-pair.

Next suppose that $G = \mathbb{Z}_{p^d}$, where $d \geqslant 3$. Then $z^{p^{d-2}+p^{d-1}} \notin \{z^{p^{d-2}}, z^{-p^{d-2}}\}$. Set $S' = \{a_0, \ldots, a_0^{p-2}\} \cup \{z^{p^{d-2}}, z^{-p^{d-2}}\}$ and $T' = \{a_0, \ldots, a_0^{p-2}\} \cup \{z^{p^{d-2}+p^{d-1}}, z^{-p^{d-2}-p^{d-1}}\}$. If $p^{d-2} \geqslant k$ then let

$$\begin{cases} S = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup S', \\ T = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup T'; \end{cases}$$

if $p^{d-2} \leqslant k-1$, then let

$$\begin{cases} S = (\{z, \ldots, z^k\}\backslash\{z^{p^{d-2}}\})\langle a_0\rangle \cup S', \\ T = (\{z, \ldots, z^k\}\backslash\{z^{p^{d-2}}\})\langle a_0\rangle \cup T'. \end{cases}$$

Arguing as for the case $G=\mathbb{Z}_{p^d}$ in Step 2, we know that $\mathrm{Cay}(G,S)\cong\mathrm{Cay}(G,T)$, but S and T are not conjugate under $\mathrm{Aut}(G)$, so $\{S,T\}$ is an NCI-pair.

Finally, suppose that $G=\mathbb{Z}_{2p^d}$, where p is an odd prime and $d\geqslant 2$. Then $z^{p^{d-1}}\neq z^{-p^{d-1}}$. Set $S'=\{a_0,\ldots,a_0^{p-2}\}\cup\{z^{p^{d-1}},z^{-p^{d-1}}\}$ and $T'=\{a_0^{-1},\ldots,a_0^{-(p-2)}\}\cup\{z^{p^{d-1}},z^{-p^{d-1}}\}$. If $p^{d-1}>k$ then let

$$\begin{cases}S=\{z,\ldots,z^{k-1}\}\langle a_0\rangle\cup S',\\ T=\{z,\ldots,z^{k-1}\}\langle a_0\rangle\cup T',\end{cases}$$

if $p^{d-2}\leqslant k-1$, then let

$$\begin{cases}S=(\{z,\ldots,z^{k}\}\backslash\{z^{p^{d-1}}\})\langle a_0\rangle\cup S',\\ T=(\{z,\ldots,z^{k}\}\backslash\{z^{p^{d-1}}\})\langle a_0\rangle\cup T'.\end{cases}$$

Arguing as for the case $G\neq\mathbb{Z}_{p^d}$ in Step 2, $\mathrm{Cay}(G,S)\cong\mathrm{Cay}(G,T)$, but S and T are not conjugate under $\mathrm{Aut}(G)$, so $\{S,T\}$ is an NCI-pair.

Case 2. Suppose that $p=2$ and $d\geqslant 3$. If $m=3$, then let $S=\{a,a^5,a^2\}$ and $T=\{a,a^5,a^6\}$. It is easy to show that $\{S,T\}$ is an NCI-pair (see the following arguments). Assume that $m\geqslant 4$.

First, we treat the case $d=3$. Let $G=\langle a\rangle\times X$, where $\langle a\rangle=\mathbb{Z}_8$ and $|X|$ is odd. Write $m=4r+s$ such that $r\geqslant 1$ and $s=0$, 1, 2 or 3. Take R, $R_0\subseteq X\backslash\{1\}$ such that $|R|=r$ and $|R_0|=s$, and set

$$\begin{cases}S=\{a,a^5,a^2,a^4\}R\cup R_0,\\ T=\{a,a^5,a^6,a^4\}R\cup R_0.\end{cases}$$

Let ρ be a map from G to G, defined by

$$a^{2j+k}x\to a^{6j+k}x,\qquad \text{where } 0\leqslant j\leqslant 3,\ k=0 \text{ or } 1, \text{ and } x\in X.$$

We are going to prove that ρ is an isomorphism from $\mathrm{Cay}(G,S)$ to $\mathrm{Cay}(G,T)$. Every element of G can be written as a^ix for some integer $u\in\{0,1,\ldots,7\}$ and some $x\in X$. By definition, $(a^ix)^\rho=a^{i'}x$ for some integer $i'\in\{0,1,\ldots,7\}$. Taking two adjacent vertices $v_1=a^{i_1}x_1$ and $v_2=a^{i_2}x_2$ of $\mathrm{Cay}(G,S)$, we have $a^{i_2-i_1}x_1^{-1}x_2=v_1^{-1}v_2\in S$. Thus $a^{i_2-i_1}\in\{a,a^5,a^2,a^4\}$ and $x_1^{-1}x_2\in R$. Now $v_1^\rho=a^{i_1'}x_1$ and $v_2^\rho=a^{i_2'}x_2$. To prove that ρ is an isomorphism, we need only prove that $(v_1^\rho)^{-1}v_2^\rho=a^{i_2'-i_1'}x_1^{-1}x_2\in T$. Since $x_1^{-1}x_2\in R$, we need only prove that $a^{i_2'-i_1'}\in\{a,a^5,a^6,a^4\}$. Now ρ induces a function on $\{0,1,\ldots,7\}$ (mod 8). Without loss of generality, we may consider ρ as this function, so $(2j+k)^\rho\equiv 6j+k\pmod 8$. Write $i_1=2j_1+k_1$ such that $k_1=0$ or 1. Then $i_1^\rho=6j_1+k_1$. If $k_1=0$, then $i_1=2j_1$ and

$$i_2=\begin{cases}2j_1+1,\\ 2j_1+5=2(j_1+2)+1,\\ 2j_1+2=2(j_1+1),\\ 2j_1+4=2(j_1+2).\end{cases}$$

Therefore, $i_1^\rho=6j_1$ and

$$i_2^\rho=\begin{cases}6j_1+1,\\ 6(j_1+2)+1=6j_1+13,\\ 6(j_1+1)=6j_1+6,\\ 6(j_1+2)=6j_1+4.\end{cases}$$

Consequently, $i_2^\rho - i_1^\rho \equiv 1,\ 5,\ 6$ or $4 \pmod 8$, as required. If $k_1 = 1$, then $i_1 = 2j_1 + 1$ and

$$i_2 = \begin{cases} 2j_1 + 1 + 1 = 2(j_1 + 1), \\ 2j_1 + 1 + 5 = 2(j_1 + 3), \\ 2j_1 + 1 + 2 = 2(j_1 + 1) + 1, \\ 2j_1 + 1 + 4 = 2(j_1 + 2) + 1. \end{cases}$$

Therefore, $i_1^\rho = 6j_1 + 1$ and

$$i_2^\rho = \begin{cases} 6(j_1 + 1) = 6j_1 + 6, \\ 6(j_1 + 3) = 6j_1 + 18, \\ 6(j_1 + 1) + 1 = 6j_1 + 7, \\ 6(j_1 + 2) + 1 = 6j_1 + 5. \end{cases}$$

Consequently, $i_2^\rho - i_1^\rho \equiv 5,\ 1,\ 6$ or $4 \pmod 8$, as required. Thus ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Since G has the m-DCI property, there exists $\alpha \in \mathrm{Aut}(G)$ such that $S^\alpha = T$. Consider $\bar{G} = G/X$. We have $\bar{S} = SX/X = \{\bar{a}, \bar{a}^5, \bar{a}^2, \bar{a}^4\}$ and $\bar{T} = TX/X = \{\bar{a}, \bar{a}^5, \bar{a}^6, \bar{a}^4\}$. Let $\bar{\alpha}$ be the element of $\mathrm{Aut}(\bar{G})$ induced by α. Then $\bar{S}^{\bar{\alpha}} = \bar{T}$; that is, $\{\bar{a}, \bar{a}^5, \bar{a}^2, \bar{a}^4\}^{\bar{\alpha}} = \{\bar{a}, \bar{a}^5, \bar{a}^6, \bar{a}^4\}$. Thus $\bar{a}^{\bar{\alpha}} = \bar{a}$ or $\bar{a}^5$, and so $(\bar{a}^2)^{\bar{\alpha}} = \bar{a}^2$ or $\bar{a}^{10}(=\bar{a}^2)$, respectively, which is not in T, a contradiction. Therefore, $\{S, T\}$ is an NCI-pair.

Now assume that $d \geqslant 4$. Let $n' = n/4$ and let $a_0 = a^{2^{d-2}}$. Then $a_0 = z^{n'}$ is of order 4, and since $4 \mid n'$, $a_0^{n'} = 1$. Write $m = 4k + j$, where $0 \leqslant j \leqslant 3$, $k \geqslant 1$, and if $j = 0$ then $k > 1$. We use a method similar to that in Case 1 to construct NCI-pairs. (In fact, this case can be treated with the case in which p is odd in a uniform way. The reason why we treat them separately here is only so that the arguments will be more readable.)

Step 1. Assume that $j = 1$ or 2. Set $S_0 = \{a_0, a_0^j\}$ and $T_0 = \{a_0^{-1}, a_0^{-j}\}$, and let

$$\begin{cases} S = \{z, \ldots, z^k\}\langle a_0\rangle \cup S_0, \\ T = \{z, \ldots, z^k\}\langle a_0\rangle \cup T_0. \end{cases}$$

Arguing as in Step 1 of Case 1, $\{S, T\}$ is an NCI-pair of G.

Step 2. Assume that $j = 3$; namely, $m = 4k + 3$. First, suppose that $G \neq \langle a\rangle\ (\cong \mathbb{Z}_{2^d})$. Then $z^{2^d} \neq 1$ and $G = \langle a\rangle \times \langle z^{2^d}\rangle$. If $2^d > k$, then let

$$\begin{cases} S = \{z, \ldots, z^k\}\langle a_0\rangle \cup \{a_0, a_0^2, z^{2^d}\}, \\ T = \{z, \ldots, z^k\}\langle a_0\rangle \cup \{a_0^{-1}, a_0^{-2}, z^{2^d}\}; \end{cases}$$

if $2^d \leqslant k$, then let

$$\begin{cases} S = (\{z, \ldots, z^{k+1}\}\backslash\{z^{2^d}\})\langle a_0\rangle \cup \{a_0, a_0^2, z^{2^d}\}, \\ T = (\{z, \ldots, z^{k+1}\}\backslash\{z^{2^d}\})\langle a_0\rangle \cup \{a_0^{-1}, a_0^{-2}, z^{2^d}\}. \end{cases}$$

Arguing as in Step 2 of Case 1, $\{S, T\}$ is an NCI-pair.

Now suppose that $G = \mathbb{Z}_{2^d}$ for $d \geqslant 4$. If $2^{d-2} > k$, then let

$$\begin{cases} S = \{z, \ldots, z^k\}\langle a_0\rangle \cup \{a_0, a_0^2, z^{2^{d-2}}\}, \\ T = \{z, \ldots, z^k\}\langle a_0\rangle \cup \{a_0, a_0^2, z^{2^{d-2}+2^{d-1}}\}; \end{cases}$$

if $2^{d-2} \leqslant k$, then let

$$\begin{cases} S = (\{z, \ldots, z^{k+1}\}\backslash\{z^{2^{d-2}}\})\langle a_0\rangle \cup \{a_0, a_0^2, z^{2^{d-2}}\}, \\ T = (\{z, \ldots, z^{k+1}\}\backslash\{z^{2^{d-2}}\})\langle a_0\rangle \cup \{a_0, a_0^2, z^{2^{d-2}+2^{d-1}}\}. \end{cases}$$

Arguing as in Step 2 of Case 1, $\{S, T\}$ is an NCI-pair of G.

Step 3. Assume that $j = 0$; namely $m = 4k$. First, suppose that $G \neq \mathbb{Z}_{2^d}$. Then z^{2^d} is of order greater than 2. Set $S' = \{a_0, a_0^2\} \cup \{z^{2^d}, z^{-2^d}\}$ and $T' = \{a_0^{-1}, a_0^{-2}\} \cup \{z^{2^d}, z^{-2^d}\}$. If $2^d \geqslant k$, then let

$$\begin{cases} S = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup S', \\ T = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup T'; \end{cases}$$

if $2^d \leqslant k-1$, then let

$$\begin{cases} S = (\{z, \ldots, z^{k}\}\backslash\{z^{2^d}\})\langle a_0\rangle \cup S', \\ T = (\{z, \ldots, z^{k}\}\backslash\{z^{2^d}\})\langle a_0\rangle \cup T'. \end{cases}$$

Arguing as for the case $G \neq \mathbb{Z}_{2^d}$ in Step 3 of Case 1, we know that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, but S is not conjugate under $\mathrm{Aut}(G)$ to T, so $\{S, T\}$ is an NCL-pair.

Next, suppose that $G = \mathbb{Z}_{2^d}$. Then $z^{2^{d-3}+2^{d-1}} \notin \{z^{2^{d-3}}, z^{-2^{d-3}}\}$. Set $S' = \{a_0, a_0^2\} \cup \{z^{2^{d-3}}, z^{-2^{d-3}}\}$ and $T' = \{a_0, a_0^2\} \cup \{z^{2^{d-3}+2^{d-1}}, z^{-2^{d-3}-2^{d-1}}\}$. If $2^{d-3} \geqslant k$, then let

$$\begin{cases} S = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup S', \\ T = \{z, \ldots, z^{k-1}\}\langle a_0\rangle \cup T', \end{cases}$$

if $2^{d-3} \leqslant k-1$, then let

$$\begin{cases} S = (\{z, \ldots, z^{k}\}\backslash\{z^{2^{d-3}}\})\langle a_0\rangle \cup S', \\ T = (\{z, \ldots, z^{k}\}\backslash\{z^{2^{d-3}}\})\langle a_0\rangle \cup T'. \end{cases}$$

Arguing as for the case $G = \mathbb{Z}_{2^d}$ in Step 3 of Case 1, we know that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, but S and T are not conjugate under $\mathrm{Aut}(G)$, so $\{S, T\}$ is a NCI-pair. This completes the proof of the theorem. □

Acknowledgements

The author thanks Professor Cheryl E. Praeger and the referee for the numerous helpful comments which improved the paper. The support of an Overseas Postgraduate Research Scholarship from Australia and a University Postgraduate Award from the University of Western Australia is also gratefully acknowledged.

References

1. A. Ádám, Research problem 2.10, *J. Combin. Theory,* **2** (1967), 309.
2. B. Alspach and T. D. Parsons, Isomorphism of circulant graphs and digraphs, *Discr. Math.,* **25** (1979), 97–108.
3. L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.,* **29** (1977), 329–336.
4. N. Biggs, *Algebraic Graph Theory,* Cambridge University Press, New York, 1974.
5. C. Delorme, O. Favaron and M. Mahéo, Isomorphisms of Cayley multigraphs of degree 4 on finite abelian groups, *Europ. J. Combin.,* **13** (1992), 59–61.
6. B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Combin. Theory,* **9** (1970), 297–307.
7. C. D. Godsil, On the full automorphism group of a graph, *Combinatorica,* **1** (1981), 243–256.
8. C. H. Li. Isomorphisms and classification of Cayley graphs of small valencies on finite abelian groups, *Australas. J. Combin.,* **12** (1995), 3–14.
9. C. H. Li, The finite groups with the 2-DCI property, *Communs Algebra,* **24** (5) (1996), 1749–1757.
10. C. H. Li, Finite abelian groups with the m-DCI property, *Ars Combin.,* to appear.
11. C. H. Li, On isomorphisms of connected Cayley graphs, *Discr. Math.,* to appear.
12. C. H. Li, C. E. Praeger and M. Y. Xu, On finite groups with the Cayley isomorphism property, submitted.
13. M. Muzychuk, Ádám's conjecture is true inthe square-free case, *J. Combin. Theory, Ser. A,* **72** (1995), 118–134.
14. P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, *Europ. J. Combin.,* **8** (1987), 35–43.

15. M. Suzuki, *Group Theory I,* Springer-Verlag, New York, 1986.
16. S. Toida, A note on Ádám's conjecture, *J. Combin. Theory, Ser. B,* **23** (1977), 239–246.
17. 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.

Received 9 April 1996 and accepted in revised form 3 December 1996

CAI HENG LI
Department of Mathematics,
University of Western Australia,
Nedlands W A 6907, Australia
E-mail: li@maths.uwa.edu.au