Journal of Combinatorial Theory, Series B **86**, 38–53 (2002)
doi:10.1006/jctb.2002.2111

On the Isomorphisms of Cayley Graphs of Abelian Groups[1]

Yan-Quan Feng, Yan-Pei Liu

Department of Mathematics, Northern Jiaotong University, Beijing 100044, People's Republic of China
E-mail: yqfeng@cneter.njtu.edu.cn

and

Ming-Yao Xu

Department of Mathematics, Peking University, Beijing 100871, People's Republic of China
E-mail: xumy@math.pku.edu.cn

Received November 17, 1998; published online July 10, 2002

Let G be a finite group, S a subset of $G\setminus\{1\}$, and let Cay (G,S) denote the Cayley digraph of G with respect to S. If, for any subset T of $G\setminus\{1\}$, $\mathrm{Cay}(G,S)\cong\mathrm{Cay}(G,T)$ implies that $S^\alpha=T$ for some $\alpha\in\mathrm{Aut}(G)$, then S is called a *CI-subset*. The group G is called a *CIM-group* if for any minimal generating subset S of G, $S\cup S^{-1}$ is a CI-subset. In this paper, CIM-abelian groups are characterized. © 2002 Elsevier Science (USA)

Key Words: Cayley digraph; CI-subset; CIM-group.

1. INTRODUCTION

Let G be a finite group and let S be a subset of $G\setminus\{1\}$. The *Cayley digraph* $X=\mathrm{Cay}(G,S)$ of G with respect to S is defined to have vertex set $V(X)=G$ and edge set $E(X)=\{(g,sg)\mid g\in G,s\in S\}$. It is seen that X is connected if and only if S generates the group G. If $S=S^{-1}$ then $X=\mathrm{Cay}(G,S)$, called a *Cayley graph*, is viewed as an undirected graph by identifying two oppositely directed edges with one undirected edge. A subset S of $G\setminus\{1\}$ is said to be a *CI-subset* of G if for any subset T of $G\setminus\{1\}$, $\mathrm{Cay}(G,S)\cong\mathrm{Cay}(G,T)$ implies that there is an automorphism α of G such that $S^\alpha=T$.

The study of CI-subsets has received considerable attention for more than 30 years. In 1967 Ádám [1] posed the conjecture that each finite cyclic group is a DCI-group (a finite group G is called a *DCI-group* if each subset of

[1]Supported by the NSFC(10071002) and PD154-NJTU.

$G \setminus \{1\}$ is a CI-subset). The conjecture was disproved in 1970 by Elspas and Turner [6] but it is true if the number n of vertices is either a prime [4], or a product of two primes [17] or satisfies the condition $(n, \phi(n)) = 1$, where ϕ is Euler's function [27]. It is known that the conjecture fails if n is divisible by 8 or by an odd square, and Páley [27] conjectured that Ádám's conjecture is true for all other values of n. This was proved by Muzychuk [25, 26]. Also, a lot of other important work has been done about DCI-groups [2, 3, 5, 10]. However, DCI-groups are rare and CI-subsets have been investigated under various additional conditions, for example, m-DCI groups and m-CI-groups, see [7, 19–24]. This paper is devoted to the study of the following question posed by the third author [29].

QUESTION 1.1 [29, Problem 6]. *Let G be a finite group and let S be a minimal generating subset of G.*

(1) *Is S a CI-subset?*
(2) *Is $S \cup S^{-1}$ a CI-subset?*

Here, a minimal generating subset S of G means that S generates G and for any $s \in S$, $S \setminus \{s\}$ does not generate G. Both questions (1) and (2) were answered in the affirmative for cyclic groups [13–15] and for abelian groups with cyclic Sylow 2-subgroups [9]. Also, the question (1) was answered in the affirmative for minimum generating subsets (minimal generating subsets with least cardinality) of abelian groups [8]. However, Li and Zhou [24] gave infinite families of examples which show that the answers to questions (1) and (2) are negative in general.

Meng and Xu [18] defined the so-called DCIM- and CIM-groups: a finite group G is called a *DCIM*- and a *CIM-group* if for each minimal generating subset S of G, S and $S \cup S^{-1}$ are CI-subsets, respectively. Meng and Xu [18] characterized DCIM-abelian groups (see also Li and Zhou [24]), and they proposed the following question.

QUESTION 1.2 [18, Problem 1]. *Characterize CIM-abelian groups.*

The purpose of this paper is to give an answer for the above question.

THEOREM 1.3. *A finite abelian group G is a CIM-group if and only if Sylow 2-subgroups of G are elementary abelian or have no direct factor isomorphic to $\mathbb{Z}_2$.*

Let u be a vertex of an undirected graph X. We denote by $X_1(u)$ the neighborhood of u in X, that is, the vertices adjacent to u. For the group theoretic and graph theoretic notation and terminology not defined here we refer the reader to [12, 16].

2. PRELIMINARY RESULTS

In this section we give some preliminary results which will be used later.

PROPOSITION 2.1 [18, Theorem 7]. *A finite abelian group G is a DCIM-group if and only if G is a 2-group or G has no direct factor isomorphic to the type $\mathbb{Z}_2 \times \mathbb{Z}_{2^p}$ $(p \geqslant 2)$.*

Independently, this proposition was proved by Li and Zhou [24]. The following is the basic inclusion and exclusion formula (see also [11, Sect. 2.1]).

PROPOSITION 2.2 [28, Chap. 2, Theorem 1.1]. *Let $A_1, A_2, \dots, A_n$ be subsets of S and let r be a non-negative integer. Let $f(n,r)$ denote the number of the elements of S that belong to exactly r of A_i. Then*

$$f(n,r) = \sum_{k=r}^{n} (-1)^{k-r} \binom{k}{r} \sum_{\substack{K \subseteq M \\ |K|=k}} \left| \bigcap_{i \in k} A_i \right|,$$

where $M = \{1, 2, \dots, n\}$.

LEMMA 2.3. *Let*

$$p_n = \begin{cases} -n + \sum_{i=1}^{\frac{n-2}{2}} \left[2i \binom{n}{2i+1} - 2i \binom{n}{2i} \right], & n \text{ even} \\ \sum_{i=1}^{\frac{n-1}{2}} \left[2i \binom{n}{2i} - 2i \binom{n}{2i+1} \right], & n \text{ odd}. \end{cases}$$

If $n \geqslant 2$ then $p_n \neq 0$.

Proof. It is easy to check $p_n \neq 0$ for $n = 2$ and 3. Let $n \geqslant 4$. We divide the proof into four cases: $n = 4k$, $4k+2$, $4k+1$, or $4k+3$ (k a positive integer). If $n = 4k$, then

$$\begin{aligned} p_n = & -n + (n-2)\binom{n}{n-1} - \left[(n-2)\binom{n}{n-2} + 2\binom{n}{2} \right] \\ & + \left[(n-4)\binom{n}{n-3} + 2\binom{n}{3} \right] \end{aligned}$$

$$- \cdots - \left[\left(\frac{n}{2}+2\right)\binom{n}{\frac{n}{2}+2} + \left(\frac{n}{2}-2\right)\binom{n}{\frac{n}{2}-2} \right]$$

$$+ \left[\frac{n}{2}\binom{n}{\frac{n}{2}+1} + \left(\frac{n}{2}-2\right)\binom{n}{\frac{n}{2}-1} \right] - \frac{n}{2}\binom{n}{\frac{n}{2}}$$

$$= -n + (n-2)\binom{n}{1} - n\binom{n}{2} + (n-2)\binom{n}{3} - \cdots - n\binom{n}{\frac{n}{2}-2}$$

$$+ (n-2)\binom{n}{\frac{n}{2}-1} - \frac{n}{2}\binom{n}{\frac{n}{2}}$$

$$= -2\binom{n}{1} - 2\binom{n}{3} - \cdots - 2\binom{n}{\frac{n}{2}-1} - \frac{n}{2}\left[2\binom{n}{0}\right.$$

$$\left. - 2\binom{n}{1} + \cdots + 2\binom{n}{\frac{n}{2}-1} - \binom{n}{\frac{n}{2}} \right]$$

$$= -2\binom{n}{1} - 2\binom{n}{3} - \cdots - 2\binom{n}{\frac{n}{2}-1} < 0.$$

Similarly, if $n = 4k+2$ then $p_n = -2\binom{n}{1} - 2\binom{n}{3} - \cdots - 2\binom{n}{n/2-2} - \binom{n}{n/2} < 0.$ If $n = 4k+1$, then

$$p_n = (n-1)^2 - \left[(n-3)\binom{n}{n-2} - 2\binom{n}{2} \right]$$

$$+ \left[(n-3)\binom{n}{n-3} - 2\binom{n}{3} \right]$$

$$- \cdots - \left[\frac{n+3}{2}\binom{n}{\frac{n+5}{2}} - \frac{n-5}{2}\binom{n}{\frac{n-5}{2}} \right]$$

$$+ \left[\frac{n+3}{2}\binom{n}{\frac{n+3}{2}} - \frac{n-5}{2}\binom{n}{\frac{n-3}{2}} \right]$$

$$= (n-1)^2 - \left[(n-5)\binom{n}{2} - (n-5)\binom{n}{3}\right]$$

$$- \cdots - \left[4\binom{n}{\frac{n-5}{2}} - 4\binom{n}{\frac{n-3}{2}}\right]$$

$$= (n-1)^2 - \sum_{k=1}^{\frac{n-5}{4}} (n-4k-1)\left[\binom{n}{2k} - \binom{n}{2k+1}\right].$$

By the unimodality of the binomial coefficients, we have $p_n > 0$.

Similarly, if $n = 4k+3$ then $p_n = (n-1)^2 - \sum_{k=1}^{(n-3)/4}(n-4k-1)[\binom{n}{2k} - \binom{n}{2k+1}] > 0$. ∎

3. PROOF OF MAIN RESULT

In this section, we shall prove Theorem 1.3.

LEMMA 3.1. *Let* $G = \mathbb{Z}_2 \times \mathbb{Z}_{2^n} = \langle a \rangle \times \langle b \rangle (n \geqslant 2)$, $S = \{b, b^{-1}, ab^{2^{n-2}}, (ab^{2^{n-2}})^{-1}\}$, *and* $T = \{b, b^{-1}, a, ab^{2^{n-1}}\}$. *Then* $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ *and* S *is not a CI-subset of* G.

Proof. Let $X = \mathrm{Cay}(G, S)$ and $Y = \mathrm{Cay}(G, T)$. Define a map $\sigma : G \to G$ by

$$a^i b^j \to a^i b^{j - i \cdot 2^{n-2}}, \qquad i = 0 \text{ or } 1,\ 0 \leqslant j < 2^n.$$

Remember that for any $g \in G$, $X_1(g)$ and $Y_1(g)$ denote the neighborhoods of g in X and Y, respectively. Then we have $X_1(a^i b^j) = \{a^i b^{j+1}, a^i b^{j-1}, a^{i+1} b^{j+2^{n-2}}, a^{i+1} b^{j-2^{n-2}}\}$. By the definition of σ, considering $i = 0, 1$, respectively we obtain that $Y_1((a^i b^j)^\sigma) = [X_1(a^i b^j)]^\sigma$, and hence σ is an isomorphism from X to Y. Since there are two involutions in T but not in S, S is not a CI-subset of G. ∎

Hereafter we assume that G is a finite abelian group and S is a minimal generating subset of G. Let σ be an isomorphism from $X = \mathrm{Cay}(G, S \cup S^{-1})$ to $Y = \mathrm{Cay}(G, T)$ with $1^\sigma = 1$. Then $(S \cup S^{-1})^\sigma = T$. Assume that Sylow 2-subgroups of G are elementary abelian or have no direct factor isomorphic to $\mathbb{Z}_2$. We shall prove that there exists an $\alpha \in \mathrm{Aut}(G)$ such that $(S \cup S^{-1})^\alpha = T$, that is, $S \cup S^{-1}$ is a CI-subset of G.

LEMMA 3.2. *If Sylow 2-subgroups of G are elementary abelian, then $S \cup S^{-1}$ is a CI-subset of G.*

Proof. Define an equivalence relation $\sim$ on $S \cup S^{-1}$ by the rule

$$s_1 \sim s_2 \Leftrightarrow s_1^2 = s_2^2, \qquad \text{for any } s_1, s_2 \in S \cup S^{-1}.$$

Then the set of all involutions in $S \cup S^{-1}$, say S_0, is an equivalence class under $\sim$. If S_i is an equivalence class then it is easy to show that S_i^{-1} is also an equivalence class, and moreover if $S_i \neq S_0$ then $S_i^{-1} \neq S_i$ because G has no element of order 4. Thus, we may assume that $S \cup S^{-1} = S_0 \cup S_1 \cup \cdots \cup S_\ell \cup S_1^{-1} \cup \cdots \cup S_\ell^{-1}$ where $S_0, S_1, \ldots, S_\ell$, $S_1^{-1}, \ldots, S_\ell^{-1}$ are all equivalence classes of $\sim$ on $S \cup S^{-1}$.

The proof of Lemma 3.2 will be carried out over a series of three claims. We show $(S_i^{-1})^\sigma = (S_i^\sigma)^{-1}$ in Claim 2 and hence we may assume $T = T_0 \cup T_1 \cup \cdots \cup T_\ell \cup T_1^{-1} \cup \cdots \cup T_\ell^{-1}$ where $T_i = S_i^\sigma$. By Claim 3 we have $\mathrm{Cay}(G, S_0 \cup S_1 \cup \cdots \cup S_\ell) \cong \mathrm{Cay}(G, T_0 \cup T_1 \cup \cdots \cup T_\ell)$. Note that $S_0 \cup S_1 \cup \cdots \cup S_\ell$ is a minimal generating subset of G. Thus, by Proposition 2.1 there exists an $\alpha \in \mathrm{Aut}(G)$ such that $(S_0 \cup S_1 \cup \cdots \cup S_\ell)^\alpha = T_0 \cup T_1 \cup \cdots \cup T_\ell$ and it follows that $(S \cup S^{-1})^\alpha = T$, that is, $S \cup S^{-1}$ is a CI-subset of G. To prove Claim 2 and Claim 3, we need to know the intersection of the neighborhoods of gs_1 and gs_2 for any $g \in G$ and $s_1, s_2 \in S \cup S^{-1}$, which will be computed in Claim 1.

For convenience of statement, we assume that $S_0, S_1, \ldots, S_k$ are all the equivalence classes of $\sim$ on $S \cup S^{-1}$ and let $T_i = S_i^\sigma$ $(i = 0, 1, \ldots, k)$, where S_0 has the same meaning as above. Then $T = T_0 \cup T_1 \cup \cdots \cup T_k$.

CLAIM 1. *Let $s_1, s_2 \in S \cup S^{-1}$, $g \in G$ and let $s_1 \neq s_2^{\pm 1}$. Then we have*

(1) $X_1(gs_1) \cap X_1(gs_2) = \begin{cases} \{g, gs_1s_2\}, & s_1 \nsim s_2 \\ \{g, gs_1^2, gs_1s_2, gs_1s_2^{-1} = gs_2s_1^{-1}\}, & s_1 \sim s_2; \end{cases}$

(2) *Let $s_1 \in S_t \neq S_0$. Then $X_1(gs_1) \cap X_1(gs_1^{-1}) = \{gs_1s \mid s \in S_t^{-1}\} = X_1(gs_1) \cap X_1(gS_t^{-1})$ where $X_1(gS_t^{-1}) = \bigcup_{s \in S_t^{-1}} X_1(gs)$.*

Proof. If $\{x_1, x_2, \ldots, x_n\}$ is a minimal generating subset of G then $\{x_1^{\delta_1}, x_2^{\delta_2}, \ldots, x_n^{\delta_n}\}$ $(\delta_i = 1$ or -1, $i = 1, 2, \ldots, n)$ are also minimal generating subsets of G. To prove (1), we may assume that $S = \{s_1, s_2, \ldots, s_n\}$ since $s_1 \neq s_2^{\pm 1}$.

Assume that for some $s_i, s_j \in S$, $s_1 s_i^{\delta_i} = s_2 s_j^{\delta_j}$ $(\delta_i, \delta_j = 1$ or $-1)$. By the minimality of $\{s_1^{\delta_1}, s_2^{\delta_2}, \ldots, s_n^{\delta_n}\}$, we have $i = 1$ or 2 and $j = 1$ or 2. Furthermore, if $i = 1$ then $j = 2$ and if $i = 2$ then $j = 1$. Thus, it follows that

$$X_1(gs_1) \cap X_1(gs_2) \subseteq \begin{cases} \{g, gs_1s_2\}, & s_1^2 \neq s_2^2 \\ \{g, gs_1^2, gs_1s_2, gs_1s_2^{-1} = gs_2s_1^{-1}\}, & s_1^2 = s_2^2. \end{cases}$$

The inverse inclusion is obvious and (1) follows.

To prove (2), we assume that for some $s_i, s_j \in S$, $s_1 s_i^{\delta_i} = s_1^{-1} s_j^{\delta_j}$ ($\delta_i, \delta_j = 1$ or -1). By the minimality of $\{s_1^{\delta_1}, s_2^{\delta_2}, \ldots, s_n^{\delta_n}\}$, we have $i = j$. Since $s_1 \in S_t$ and $S_t \neq S_0$, we have $s_1^2 \neq 1$. Thus, $s_i^{\delta_i} = (s_j^{\delta_j})^{-1}$ and $s_1^2 = (s_j^{\delta_j})^2$, which forces $s_j^{\delta_j} \in S_t$ and $s_i^{\delta_i} \in S_t^{-1}$. Therefore, $X_1(gs_1) \cap X_1(gs_1^{-1}) \subseteq \{gs_1 s | s \in S_t^{-1}\}$. The inverse inclusion is also obvious. Since $S_t \neq S_0$, we have $S_t \neq S_t^{-1}$, which implies that $s_1 \nsim s_t^{-1}$ for any $s_t \in S_t$. By (1), if $s_t \neq s_1$ then $X_1(gs_1) \cap X_1(gs_t^{-1}) = \{g, gs_1 s_t^{-1}\}$, which is a subset of $X_1(gs_1) \cap X_1(gs_1^{-1}) = \{gs_1 s | s \in S_t^{-1}\}$. It follows that $X_1(gs_1) \cap X_1(gs_1^{-1}) = \{gs_1 s | s \in S_t^{-1}\} = X_1(gs_1) \cap X_1(gS_t^{-1})$. ∎

Claim 2. *$S_j = S_i^{-1}$ if and only if $T_j = T_i^{-1}$.*

Proof. Assume that $S_j = S_i^{-1}$. Let $i \neq 0$ and $t_i = s_i^\sigma \in T_i$ where $s_i \in S_i$. By $i \neq 0$, we have that $S_i^{-1} \neq S_i$ and so $j \neq i$. Claim 1 tells us that $|X_1(s_i) \cap X_1(S_j)| = |\{s_i s | s \in S_j\}| = |S_j|$ and it follows that $|Y_1(t_i) \cap Y_1(T_j)| = |S_j|$. Suppose that $t_i^{-1} \notin T_j$. Then $|Y_1(t_i) \cap Y_1(T_j)| \geqslant |\{1, t_i t | t \in T_j\}| = |T_j| + 1$. Thus, $|T_j| + 1 \leqslant |S_j|$. However, $T_j = S_j^\sigma$ implies that $|S_j| = |T_j|$, a contradiction. Therefore, $t_i^{-1} \in T_j$ and $T_i^{-1} = T_j$. Now we have proved that for any $i \neq 0$, $S_j = S_i^{-1}$ implies that $T_j = T_i^{-1}$. Consequently, $T_0 = T_0^{-1}$.

Assume that $T_j = T_i^{-1}$. We prove $S_j = S_i^{-1}$. Suppose to the contrary that $S_j \neq S_i^{-1}$. Then there exists some m ($m \neq j$) such that $S_m = S_i^{-1}$. By the above proof, we have $T_m = T_i^{-1}$. It follows that $T_m = T_j = T_i^{-1}$, contrary to the fact that $m \neq j$. ∎

Claim 3. *Let $s_1, s_2, \ldots, s_n \in S$ and $s_i \in S_{k_i}$ where $0 \leqslant k_i \leqslant k$ ($i = 1, 2, \ldots, n$). Then $(s_1 s_2 \cdots s_n)^\sigma = (s_1 s_2 \cdots s_{n-1})^\sigma t_n$ for some $t_n \in T_{k_n}$.*

Proof. For $n = 1$ the claim is obvious. Let $n \geqslant 2$ and set $x = s_1 s_2 \cdots s_{n-2}$ ($x = 1$ if $n = 2$). By induction on n, we may assume that $(xs_{n-1})^\sigma = x^\sigma t'_{n-1}$ and $(xs_n)^\sigma = x^\sigma t'_n$ for some $t'_{n-1} \in T_{k_{n-1}}$ and $t'_n \in T_{k_n}$. It suffices to prove that $(xs_{n-1}s_n)^\sigma = (xs_{n-1})^\sigma t_n$ for some $t_n \in T_{k_n}$.

Let $k_n \neq k_{n-1}$. We distinguish two cases: (i) $S_{k_n} \neq S_{k_{n-1}}^{-1}$ and (ii) $S_{k_n} = S_{k_{n-1}}^{-1}$. In the first case, we have $T_{k_n} \neq T_{k_{n-1}}^{-1}$ (Claim 2) and so $t'_{n-1} t'_n \neq 1$. Since $X_1(xs_{n-1}) \cap X_1(xs_n) = \{x, xs_{n-1}s_n\}$ (Claim 1) and $Y_1(x^\sigma t'_{n-1}) \cap Y_1(x^\sigma t'_n) \supseteq \{x^\sigma, x^\sigma t'_{n-1} t'_n\}$, it follows that $(xs_{n-1}s_n)^\sigma = x^\sigma t'_{n-1} t'_n = (xs_{n-1})^\sigma t'_n$ where $t'_n \in T_{k_n}$. In the second case, $T_{k_n} = T_{k_{n-1}}^{-1}$. Since $k_n \neq k_{n-1}$, we have $k_{n-1} \neq 0$. By Claim 1, we have $X_1(xs_{n-1}) \cap X_1(xS_{k_n}) = \{xs_{n-1}s | s \in S_{k_n}\}$. Clearly, $Y_1(x^\sigma t'_{n-1}) \cap Y_1(x^\sigma T_{k_n}) \supseteq \{x^\sigma t'_{n-1} t | t \in T_{k_n}\}$. Since $|S_{k_n}| = |T_{k_n}|$, there exists a $t_n \in T_{k_n}$ such that

$(xs_{n-1}s_n)^\sigma = x^\sigma t'_{n-1}t_n = (xs_{n-1})^\sigma t_n$. Combining these two cases, we have proved that for any $k_n \neq k_{n-1}$, $(xs_{n-1}s_n)^\sigma = (xs_{n-1})^\sigma t_n$ for some $t_n \in T_{k_n}$. Consequently, it is also true for $k_n = k_{n-1}$. ∎

Now we are ready to prove Lemma 3.2. Note that $S \cup S^{-1} = S_0 \cup S_1 \cup \cdots \cup S_\ell \cup S_1^{-1} \cup \cdots \cup S_\ell^{-1}$ where $S_0, S_1, \ldots, S_\ell$, $S_1^{-1}, \ldots, S_\ell^{-1}$ are all equivalence classes of $\sim$ on $S \cup S^{-1}$. By Claim 2, we may let $T = T_0 \cup T_1 \cup \cdots \cup T_\ell \cup T_1^{-1} \cup \cdots \cup T_\ell^{-1}$ where $T_i = S_i^\sigma$ for $0 \leqslant i \leqslant \ell$. Set $S' = S_0 \cup S_1 \cup \cdots \cup S_\ell$ and $T' = T_0 \cup T_1 \cup \cdots \cup T_\ell$. Then S' is a minimal generating subset of G and by Claim 3 we have $\mathrm{Cay}(G, S') \cong \mathrm{Cay}(G, T')$. By Proposition 2.1, S' is a CI-subset and so there is an $\alpha \in \mathrm{Aut}(G)$ such that $(S')^\alpha = T'$. It follows that $(S \cup S^{-1})^\alpha = (S' \cup (S')^{-1})^\alpha = T' \cup (T')^{-1} = T$ and so $S \cup S^{-1}$ is a CI-subset of G. ∎

LEMMA 3.3. *If Sylow* 2*-subgroups of G have no direct factor isomorphic to* $\mathbb{Z}_2$, *then* $S \cup S^{-1}$ *is a CI-subset of G.*

Proof. Denote by S_1 the set of all elements of order 4 in $S \cup S^{-1}$ and set $S_2 = (S \cup S^{-1}) \backslash S_1$, $T_1 = S_1^\sigma$ and $T_2 = S_2^\sigma$. Clearly, $S_1^{-1} = S_1$ and $S_2^{-1} = S_2$.

First we give an outline of the proof. The proof will also be carried out over a series of claims. Note that σ is an isomorphism from $X = \mathrm{Cay}(G, S \cup S^{-1})$ to $Y = \mathrm{Cay}(G, T)$ with $1^\sigma = 1$. In Claim 1 we show that the restriction of σ on $\langle S_2 \rangle$, say α, is a group isomorphism from $\langle S_2 \rangle$ to $\langle T_2 \rangle$. Hence, to prove the lemma it suffices to construct a group isomorphism, say β, from $\langle S_1 \rangle$ to $\langle T_1 \rangle$ such that $S_1^\beta = T_1$ and $u^\beta = u^\alpha$ for any $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$ (Claim 4) because the automorphism of G defined by $as \to a^\beta s^\alpha$ for any $a \in \langle S_1 \rangle$ and $s \in \langle S_2 \rangle$, maps $S \cup S^{-1}$ to T. Since Sylow 2-subgroups of G have no direct factor isomorphic to $\mathbb{Z}_2$, we may show $\langle S_1 \rangle = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle$ where $S_1 = \{a_1, a_2, \ldots, a_k\} \cup \{a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1}\}$. Thus to construct the above β such that $S_1^\beta = T_1$, we need to prove that T_1 consists of elements of order 4 and $\langle T_1 \rangle = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \times \langle b_k \rangle$ where $T_1 = \{b_1, b_2, \ldots, b_k\} \cup \{b_1^{-1}, b_2^{-1}, \ldots, b_k^{-1}\}$, which will be proved in Claim 2. For $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$, it is seen that $u = x_1^2 x_2^2 \cdots x_m^2$ (for $i \neq j$, $x_i \neq x_j$) where $x_i \in \{a_1, a_2, \ldots, a_k\}$, and $u^\alpha = y_1^2 y_2^2 \cdots y_m^2$ (for $i \neq j$, $y_i \neq y_j$) where $y_i \in \{b_1, b_2, \ldots, b_k\}$. We call $x_1, x_1, \ldots, x_m$ $(y_1, y_2, \ldots, y_m)$ the factors of $u(u^\alpha)$. To construct the above β such that $u^\alpha = u^\beta$ for any $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$, we need to prove that the number of common factors of $u_1, u_2, \ldots, u_n$ is equal to the number of common factors of $u_1^\alpha, u_2^\alpha, \ldots, u_n^\alpha$ for any $u_1, u_2, \ldots, u_n \in \langle S_1 \rangle \cap \langle S_2 \rangle$, which will be proved in Claim 3.

CLAIM 1. *The restriction of* σ *on* $\langle S_2 \rangle$ *is a group isomorphism from* $\langle S_2 \rangle$ *to* $\langle T_2 \rangle$ *and the restriction of* σ *on* $\langle S_1 \rangle$ *is a graph isomorphism from* $\mathrm{Cay}(\langle S_1 \rangle, S_1)$ *to* $\mathrm{Cay}(\langle T_1 \rangle, T_1)$.

Proof. Let $s_1, s_2 \in S \cup S^{-1}$ and $s_1 \neq s_2$. First we prove that $s_1^2 \neq s_2^2$, or $o(s_1) = 4$ and $s_2 = s_1^{-1}$. Let $s_1^2 = s_2^2$. Then $s_1^{-1}s_2$ is an involution. If $s_1, s_2 \in S$ then $G = \langle S \setminus \{s_1\}, s_1^{-1}s_2 \rangle$ and $G \neq \langle S \setminus \{s_1\} \rangle$ because S is a minimal generating subset of G, which implies that G has a direct factor isomorphic to $\mathbb{Z}_2$ ($\langle s_1^{-1}s_2 \rangle$), contrary to the hypothesis. Thus, s_1 and s_2 cannot be two elements of any minimal generating subset of G and so $s_2 = s_1^{-1}$. By $s_1^2 = s_2^2$, we have $o(s_1) = 4$.

Let $s_1, s_2 \in S \cup S^{-1}$ with $s_1 \neq s_2$. We have proved that $s_1^2 \neq s_2^2$, or $s_2 = s_1^{-1}$ and $o(s_1) = 4$. With this result, a similar argument to the proof of Claim 1 in Lemma 3.2 gives rise to the following formula for any $g \in G$:

$$X_1(gs_1) \cap X_1(gs_2) = \begin{cases} \{g\}, & s_2 = s_1^{-1} \text{ and } o(s_1) \neq 4 \\ \{g, gs_1^2\}, & s_2 = s_1^{-1} \text{ and } o(s_1) = 4 \\ \{g, gs_1s_2\}, & s_2 \neq s_1^{-1}. \end{cases}$$

Since $|X_1(gs_1) \cap X_1(gs_2)| = 1$ if and only if $s_2 = s_1^{-1}$ and $o(s_1) \neq 4$, we have $(s^{-1})^\sigma = (s^\sigma)^{-1}$ for any $s \in S_2$. Thus $T_2^{-1} = (S_2^\sigma)^{-1} = (S_2^{-1})^\sigma = T_2$ and $T_1^{-1} = T_1$. By a similar argument to the proof of Claim 3 in Lemma 3.2, we have that for any $s_1, s_2, \ldots, s_n \in S \cup S^{-1}$, $(s_1s_2 \cdots s_n)^\sigma = (s_1s_2 \cdots s_{n-1})^\sigma t_n$ where $t_n = s_n^\sigma$ if $s_n \in S_2$ and $t_n \in T_1$ if $s_n \in S_1$. This implies that the restriction of σ on $\langle S_2 \rangle$ is a group isomorphism from $\langle S_2 \rangle$ to $\langle T_2 \rangle$ and the restriction of σ on $\langle S_1 \rangle$ is a graph isomorphism from $\mathrm{Cay}(\langle S_1 \rangle, S_1)$ to $\mathrm{Cay}(\langle T_1 \rangle, T_1)$. ∎

If S_1 is empty then $S \cup S^{-1}$ coincides with S_2. By Claim 1, Lemma 3.2 is true. Thus, from now on we assume $|S_1| \geqslant 1$ and denote by α the isomorphism from $\langle S_2 \rangle$ to $\langle T_2 \rangle$ induced by the restriction of σ on $\langle S_2 \rangle$.

Let $S_1 = \{a_1, a_2, \ldots, a_k\} \cup \{a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1}\}$ with $\{a_1, a_2, \ldots, a_k\} \subseteq S$. Then $k \geqslant 1$. We claim $\langle S_1 \rangle = \langle a_1 \rangle \times \langle a_2 \rangle \times \cdots \times \langle a_k \rangle$. Otherwise, without loss of generality, we may suppose that $a_1^2 = (a_2^{\delta_2} a_3^{\delta_3} \cdots a_k^{\delta_k})^2$ by the minimality of S, where $\delta_i = 0, 1$ or -1 $(2 \leqslant i \leqslant k)$. Clearly, $\langle S_1 \rangle = \langle a_1^{-1} a_2^{\delta_2} \cdots a_k^{\delta_k}, a_2, a_3, \ldots, a_k \rangle$ and hence $\langle S \setminus \{a_1\}, a_1^{-1} a_2^{\delta_2} \cdots a_k^{\delta_k} \rangle = G$. Since $\langle S \setminus \{a_1\} \rangle \neq G$ and $o(a_1^{-1} a_2^{\delta_2} \cdots a_k^{\delta_k}) = 2$, G has a direct factor isomorphic to $\mathbb{Z}_2$ ($\langle a_1^{-1} a_2^{\delta_2} \cdots a_k^{\delta_k} \rangle$), contrary to the hypothesis.

Claim 2. *Each element of T_1 has order 4 and $\langle T_1 \rangle = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \langle b_k \rangle$ where $T_1 = \{b_1, b_2, \ldots, b_k\} \cup \{b_1^{-1}, b_2^{-1}, \ldots, b_k^{-1}\}$.*

Proof. Since $|S_1| \geqslant 1$, T_1 is not empty. Let $X_i = \mathrm{Cay}(\langle S_i \rangle, S_i)$ and $Y_i = \mathrm{Cay}(\langle T_i \rangle, T_i)$ $(i = 1, 2)$. By Claim 1, $X_i \cong Y_i$ $(i = 1, 2)$. If each element of T_1 has order 4 then we have $\langle T_1 \rangle = \langle b_1 \rangle \times \langle b_2 \rangle \times \cdots \langle b_k \rangle$ because $|S_1| = |T_1|$ and $|\langle S_1 \rangle| = |\langle T_1 \rangle|$. Thus, in order to prove the claim it suffices to prove that each element of T_1 has order 4. We consider three cases according to the orders of elements in T_1.

Case I. There is no element of order 3 in T_1.

Since X_1 has no triangle and $X_1 \cong Y_1$, Y_1 has no triangle and so T_1 contains no element of order 3.

Case II. There is no element of order greater than 4 in T_1.

Suppose to the contrary that there exists a $b_1 \in T_1$ and $o(b_1) > 4$. Let $u \in V(X_1)$ such that $d_{X_1}(1,u) = 2$, where $d_{X_1}(1,u)$ denotes the distance between 1 and u. It is seen that u and 1 lie on a cycle of length 4 in X_1 and so do 1 and b_1^2 in Y_1. Thus, there exist $b_2, b_3 \in T_1$ $(b_1 \neq b_2, b_3)$ such that $b_1^2 = b_2 b_3$. If $b_2 = b_3$ then $|Y_1(b_1) \cap Y_1(b_2)| \geqslant |\{1, b_1^2, b_1 b_2\}| = 3$ and if $b_2 \neq b_3$ then $|Y_1(b_1) \cap Y_1(b_2) \cap Y_1(b_3)| \geqslant |\{1, b_1^2\}| = 2$. Both are impossible since for any $a_1, a_2, a_3 \in S_1$ with $a_i \neq a_j$ $(i \neq j)$, $|X_1(a_1) \cap X_1(a_2)| = 2$ and $|X_1(a_1) \cap X_1(a_2) \cap X_1(a_3)| = 1$.

Case III. There is no element of order 2 in T_1.

Suppose to the contrary that $V \neq \phi$ is the set of all involutions in T_1. Set $U = T_1 \setminus V$. Then $T_1 = U \cup V$ and each element of U has order 4. Let $U = \{b_1, b_2, \ldots, b_\ell\} \cup \{b_1^{-1}, b_2^{-1}, \ldots, b_\ell^{-1}\}$ where $o(b_i) = 4$ $(1 \leqslant i \leqslant \ell)$. Noting that $S_1 = \{a_1, a_2, \ldots, a_k\} \cup \{a_1^{-1}, a_2^{-1}, \ldots, a_k^{-1}\}$ and $|S_1| = |T_1|$, we have $k > \ell$ since $V \neq \phi$.

Let $S_2 = \{s_1, s_2, \ldots, s_n\}$, $T_2 = \{t_1, t_2, \ldots, t_n\}$ and let $s_i^\alpha = t_i$ $(i = 1, 2, \ldots, n)$. We may assume that $s_i = e_i u_i$ and $t_i = f_i v_i$ such that $o(e_i)$, $o(f_i)$ are 2-powers and $o(u_i)$, $o(v_i)$ are odd. Since α is a group isomorphism from $\langle S_2 \rangle$ to $\langle T_2 \rangle$, we have $(e_i)^\alpha = f_i$. Denote by G_2 the Sylow 2-subgroup of G. Then, $G_2 = \langle \bigcup_{i=1}^n \{e_i\}, \bigcup_{i=1}^k \{a_i\} \rangle = \langle \bigcup_{i=1}^n \{f_i\}, \bigcup_{i=1}^\ell \{b_i\}, V \rangle$. Since G has no direct factor isomorphic to $\mathbb{Z}_2$, we have $V \subseteq \Phi(G_2)$ where $\Phi(G_2)$ is the Frattini subgroup of G_2. This implies that $G_2 = \langle \bigcup_{i=1}^n \{f_i\}, \bigcup_{i=1}^\ell \{b_i\} \rangle$. Clearly, $G_2 \neq \langle \bigcup_{i=1}^n \{e_i\}, \bigcup_{i=1}^k \{a_i\} \setminus \{a_j\} \rangle$ $(j = 1, 2, \ldots,$ or $k)$. If $e_n = e_1^{m_1} e_2^{m_2} \cdots e_{n-1}^{m_{n-1}} a$ for some $a \in \langle S_1 \rangle$, then $a^{-1} = e_1^{m_1} e_2^{m_2} \cdots e_{n-1}^{m_{n-1}} e_n^{-1} \in \langle S_1 \rangle \cap \langle S_2 \rangle$. Since α is an isomorphism from $\langle S_2 \rangle$ to $\langle T_2 \rangle$, we have $f_n = f_1^{m_1} f_2^{m_2} \cdots f_{n-1}^{m_{n-1}} a^\alpha$ where $a^\alpha \in \langle T_1 \rangle$. Thus, $G_2 = \langle \bigcup_{i=1}^{n-1} \{e_i\}, \bigcup_{i=1}^k \{a_i\} \rangle$ implies that $G_2 = \langle \bigcup_{i=1}^{n-1} \{f_i\}, \bigcup_{i=1}^\ell \{b_i\} \rangle$. Now we may assume that $G_2 = \langle \bigcup_{i=1}^m \{e_i\}, \bigcup_{i=1}^k \{a_i\} \rangle = \langle \bigcup_{i=1}^m \{f_i\}, \bigcup_{i=1}^\ell \{b_i\} \rangle$ $(m \leqslant n)$ such that $\{\bigcup_{i=1}^m \{e_i\}, \bigcup_{i=1}^k \{a_i\}\}$ is a minimal generating subset of G_2. Since any minimal generating subset of a p-group (p prime) is a minimum generating subset [16, 3.15 of Chapter III], we have $m + k \leqslant m + \ell$, which contradicts the fact that $k > \ell$. ∎

By Claim 2, there exists a group isomorphism λ, induced by $a_i \to b_i$ $(0 \leqslant i \leqslant k)$, from $\langle S_1 \rangle$ to $\langle T_1 \rangle$. Clearly, λ maps S_1 to T_1. If $\langle S_1 \rangle \cap \langle S_2 \rangle = 1$ then the automorphism of G, defined by $as \to a^\lambda s^\alpha$ for any $a \in S_1$, $s \in S_2$, maps $S \cup S^{-1}$ to T. Thus, Lemma 3.3 is true and so we assume $\langle S_1 \rangle \cap \langle S_2 \rangle \neq 1$ from now on.

Let $\bar{S}_1 = \{a_1, a_2, \ldots, a_k\}$ and $\bar{T}_1 = \{b_1, b_2, \ldots, b_k\}$. Then $\langle S_1 \rangle = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle$ and $\langle T_1 \rangle = \langle b_1 \rangle \times \cdots \times \langle b_k \rangle$ where $S_1 = \bar{S}_1 \cup (\bar{S}_1)^{-1}$ and $T_1 = \bar{T}_1 \cup (\bar{T}_1)^{-1}$. Remember that each element of S_1 is of order 4 and we have assumed $\bar{S}_1 \subseteq S$ before Claim 2. If $\langle S_1 \rangle \cap \langle S_2 \rangle$ has an element of order 4 then there exists at least one element of $\bar{S}_1$, say a_i, such that it is a product of elements in $S \backslash \{a_i\}$, which contradicts the minimality of S. Thus, $\langle S_1 \rangle \cap \langle S_2 \rangle$ is an elementary abelian 2-group. Let $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$ with $u \neq 1$. Then u can be written as a unique product $u = x_1^2 x_2^2 \cdots x_m^2$ (for $i \neq j,\ x_i \neq x_j$) where $x_i \in \bar{S}_1$. Since α is an isomorphism from $\langle S_2 \rangle$ to $\langle T_2 \rangle$, u^α has order 2 and hence u^α can be written as a unique product $u^\alpha = y_1^2 y_2^2 \cdots y_n^2$ (for $i \neq j,\ y_i \neq y_j$) where $y_i \in \bar{T}_1$. We call $x_1, x_2, \ldots, x_m$ (resp. $y_1, y_2, \ldots, y_n$) the *factors* of u (resp. u^α) and m (resp. n) the *factor number* of u (resp. u^α), denoted by $N(u)$ (resp. $N(u^\alpha)$). Since $\langle S_1 \rangle = \langle a_1 \rangle \times \cdots \times \langle a_k \rangle$ and $\langle T_1 \rangle = \langle b_1 \rangle \times \cdots \times \langle b_k \rangle$, we have that $d_{X_1}(1, u) = 2m$ and $d_{Y_1}(1, u^\alpha) = 2n$ where $d_{X_1}(1, u)$ (resp. $d_{Y_1}(1, u^\alpha)$) denotes the distance between 1 and u (resp. u^α) in X_1 (resp. Y_1). It follows that $m = n$ because $X_1 \cong Y_1$. Thus, $N(u) = N(u^\alpha)$ for any $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$ where we let $N(u) = 0$ for $u = 1$.

CLAIM 3. *Let* $u_1, u_2, \ldots, u_n \in \langle S_1 \rangle \cap \langle S_2 \rangle$ *and* $v_i = u_i^\alpha$ $(i = 1, 2, \ldots, n)$. *Then the number of common factors of* $u_1, u_2, \ldots, u_n$ *is equal to that of* $v_1, v_2, \ldots, v_n$.

Proof. The claim is true for $n = 1$. Let $n \geqslant 2$.

Let A_i (resp. B_i) be the set of all factors of u_i (resp. v_i) and let $f(n, r)$ (resp. $g(n, r)$) be the number of all elements in $\bar{S}_1$ (resp. $\bar{T}_1$) that belong to exactly r of A_i (resp. B_i). Then $\bigcap_{i=1}^n A_i$ (resp. $\bigcap_{i=1}^n B_i$) is the set of all common factors of $u_1, u_2, \ldots, u_n$ (resp. $v_1, v_2, \ldots, v_n$) and so $f(n, n) = |\bigcap_{i=1}^n A_i|$ (resp. $g(n, n) = |\bigcap_{i=1}^n B_i|$). To prove the claim, it suffices to prove that $f(n, n) = g(n, n)$.

Let x be a factor that belongs to exactly r of A_i. Then x is a factor of $u_1 u_2 \cdots u_n$ if r is odd, but not if r is even. Thus we have

$$N(u_1 u_2 \cdots u_n) = \begin{cases} \sum_{i=1}^n N(u_i) - n f(n, n) - \sum_{i=1}^{\frac{n-2}{2}} [2i f(n, 2i) \\ \quad + 2i f(n, 2i+1)], & n \text{ even} \\ \sum_{i=1}^n N(u_i) - \sum_{i=1}^{\frac{n-1}{2}} [2i f(n, 2i) + 2i f(n, 2i+1)], & n \text{ odd}. \end{cases}$$

Similarly,

$$N(v_1 v_2 \cdots v_n) = \begin{cases} \sum_{i=1}^n N(v_i) - n g(n, n) - \sum_{i=1}^{\frac{n-2}{2}} [2i g(n, 2i) + 2i g(n, 2i+1)], & n \text{ even} \\ \sum_{i=1}^n N(v_i) - \sum_{i=1}^{\frac{n-1}{2}} [2i g(n, 2i) + 2i g(n, 2i+1)], & n \text{ odd}. \end{cases}$$

By Proposition 2.2, we have

$$f(n,r)=\sum_{k=r}^{n}(-1)^{k-r}\binom{k}{r}\sum_{\substack{K\subseteq M\\|K|=k}}\left|\bigcap_{i\in K}A_i\right| = f_1(n,r)+(-1)^{n-r}\binom{n}{r}f(n,n),$$

where

$$f_1(n,r)=\sum_{k=r}^{n}(-1)^{k-r}\binom{k}{r}\sum_{\substack{K\subseteq M\\|K|=k}}\left|\bigcap_{i\in K}A_i\right|\ (r<n)\qquad\text{and}$$
$$M=\{1,2,\dots,n\}.$$

Similarly, $g(n,r)=g_1(n,r)+(-1)^{n-r}\binom{n}{r}g(n,n)$ where

$$g_1(n,r)=\sum_{k=r}^{n-1}(-1)^{k-r}\binom{k}{r}\sum_{\substack{k\subseteq M\\|K|=k}}\left|\bigcap_{i\in K}B_i\right|(r<n)\qquad\text{and}$$
$$M=\{1,2,\dots,n\}.$$

If n is even then $N(u_1u_2\cdots u_n)=\sum_{i=1}^{n}N(u_i)-nf(n,n)-\sum_{i=1}^{(n-2)/2}[2if(n,2i)+2if(n,2i+1)]=\sum_{i=1}^{n}N(u_i)-nf(n,n)-\sum_{i=1}^{(n-2)/2}[2if_1(n,2i)+(-1)^{n-2i}2i\binom{n}{2i}f(n,n)+2if_1(n,2i+1)+(-1)^{n-2i-1}2i\binom{n}{2i+1}f(n,n)]=\sum_{i=1}^{n}N(u_i)-\sum_{i=1}^{(n-2)/2}[2if_1(n,2i)+2if_1(n,2i+1)]+f(n,n)\{-n+\sum_{i=1}^{(n-2)/2}[2i\binom{n}{2i+1}-2i\binom{n}{2i}]\}=\sum_{i=1}^{n}N(u_i)-\sum_{i=1}^{(n-2)/2}[2if_1(n,2i)+2if_1(n,2i+1)]+p_nf(n,n)$, where p_n has the same meaning as in Lemma 2.3. Similarly, if n is odd then $N(u_1u_2\cdots u_n)=\sum_{i=1}^{n}N(u_i)-\sum_{i=1}^{(n-1)/2}[2if(n,2i)+2if(n,2i+1)]=\sum_{i=1}^{n}N(u_i)-\sum_{i=1}^{(n-1)/2}[2if_1(n,2i)+2if_1(n,2i+1)]+p_nf(n,n)$. Thus,

$$N(u_1u_2\cdots u_n)=\begin{cases}\sum_{i=1}^{n}N(u_i)-\sum_{i=1}^{\frac{n-2}{2}}[2if_1(n,2i)\\ \quad +2if_1(n,2i+1)]+p_nf(n,n), & n\text{ even}\\ \sum_{i=1}^{n}N(u_i)-\sum_{i=1}^{\frac{n-1}{2}}[2if_1(n,2i)\\ \quad +2if_1(n,2i+1)]+p_nf(n,n), & n\text{ odd.}\end{cases}$$

Similarly,

$$N(v_1 v_2 \cdots v_n) = \begin{cases} \sum_{i=1}^{n} N(v_i) - \sum_{i=1}^{\frac{n-2}{2}} [2ig_1(n,2i) + 2ig_1(n,2i+1)] \\ \quad + p_n g(n,n), & n \text{ even} \\ \sum_{i=1}^{n} N(v_i) - \sum_{i=1}^{\frac{n-1}{2}} [2ig_1(n,2i) + 2ig_1(n,2i+1)] \\ \quad + p_n g(n,n), & n \text{ odd.} \end{cases}$$

By induction on n, we may assume that $|\bigcap_{i\in T} A_i| = |\bigcap_{i\in T} B_i|$, where T is a proper subset of $M = \{1,2,\ldots,n\}$, that is, $|T|<n$. It implies that $f_1(n,r) = g_1(n,r)$ $(r<n)$. Since $(u_1u_2\cdots u_n)^\alpha = v_1v_2\cdots v_n$ and $u_i^\alpha = v_i$ $(1\leqslant i\leqslant n)$, we have that $N(u_1u_2\cdots u_n) = N(v_1v_2\cdots v_n)$ and $N(u_i) = N(v_i)$ $(1\leqslant i\leqslant n)$. Hence, $N(u_1u_2\cdots u_n) = N(v_1v_2\cdots v_n)$ implies that $p_n f(n,n) = p_n g(n,n)$. By Lemma 2.3, $p_n \neq 0$ and so $f(n,n) = g(n,n)$. ∎

CLAIM 4. *There exists a group isomorphism β from $\langle S_1\rangle$ to $\langle T_1\rangle$ such that $S_1^\beta = T_1$ and $u^\beta = u^\alpha$ for any $u \in \langle S_1\rangle \cap \langle S_2\rangle$.*

Proof. Let $1\leqslant i,j\leqslant k$. Define an equivalence relation $\approx$ on $\bar{S}_1 = \{a_1,a_2,\ldots,a_k\}$ by the rule

$a_i \approx a_j \Leftrightarrow$ both a_i and a_j are either factors of u or not for any $u \in \langle S_1\rangle \cap \langle S_2\rangle$.

We also define a similar equivalence relation on $\bar{T}_1 = \{b_1,b_2,\ldots,b_k\}$, also say $\approx$, by

$b_i \approx b_j \Leftrightarrow$ both b_i and b_j are either factors of v or not for any $v \in \langle T_1\rangle \cap \langle T_2\rangle$.

Let U_0 be the set of all elements in $\bar{S}_1$ that are not factors of any element in $\langle S_1\rangle \cap \langle S_2\rangle$. Clearly, if $U_0 \neq \phi$ then it is an equivalence class of $\approx$ on $\bar{S}_1$. We also have a similar subset of $\bar{T}_1$, say V_0.

Let $U_1,U_2,\ldots,U_l$ be all other equivalence classes of $\bar{S}_1$ different from U_0, and let $u_1,u_2,\ldots,u_{\ell_i}$ be all elements of $\langle S_1\rangle \cap \langle S_2\rangle$ which have a factor in U_i for some $1\leqslant i\leqslant \ell$. Since U_i is an equivalence class, every element in U_i is a factor of u_j for each $1\leqslant j\leqslant \ell_i$, and so there are no other elements in $\langle S_1\rangle \cap \langle S_2\rangle$ which have some factors in U_i. Clearly, U_i is the set of all common factors of $u_1,u_2,\ldots,$ and u_{ℓ_i}. By Claim 3, $u_1^\alpha,u_2^\alpha,\ldots,u_{\ell_i}^\alpha$ have $|U_i|$ common factors. Denote the set of these common factors by V_i. Then $|U_i| = |V_i|$. We prove that V_i is an equivalence class of $\bar{T}_1$.

Let $u_{\ell_i+1}^\alpha \in \langle T_1\rangle \cap \langle T_2\rangle$ and $u_{\ell_i+1}^\alpha \neq u_j^\alpha$ $(j = 1,2,\ldots,\ell_i)$ for some $u_{\ell_i+1} \in \langle S_1\rangle \cap \langle S_2\rangle$. It suffices to prove that $u_{\ell_i+1}^\alpha$ has no factor in V_i. Suppose to the contrary that $u_1^{\alpha}, u_2^{\alpha}, \ldots, u_{\ell_i}^{\alpha}, u_{\ell_i+1}^{\alpha}$ have at least one common factor. Claim 3 tells us that $u_1, u_2, \ldots, u_{\ell_i}, u_{\ell_i+1}$ have at least one common factor. Clearly, this common factor belongs to U_i, contrary to the fact that $u_1, u_2, \ldots, u_{\ell_i}$ are all elements of $\langle S_1 \rangle \cap \langle S_2 \rangle$ which have a factor in U_i. Hence, V_i is an equivalence class of $\bar{T}_1$.

Thus, we can make a one-one mapping $\bar{\beta}$ from $\bar{S}_1$ to $\bar{T}_1$ such that $(U_i)^{\bar{\beta}} = V_i$ $(i = 0, 1, 2, \ldots, \ell)$ and define a group isomorphism β from $\langle S_1 \rangle = \langle \bar{S}_1 \rangle$ to $\langle T_1 \rangle = \langle \bar{T}_1 \rangle$ by $a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k} \to (a_1^{\beta})^{m_1} (a_2^{\beta})^{m_2} \cdots (a_k^{\beta})^{m_k}$, where $m_1, m_2, \ldots, m_k$ are integers.

Let $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$ with $u \neq 1$. Then u has order 2. Assume that the set of all factors of u consist of r equivalence classes of $\bar{S}_1$, say $U_{t_1}, U_{t_2}, \ldots, U_{t_r}$. Then the set of all factors of u^{α} also consist of r equivalence classes of $\bar{T}_1$, that is, $V_{t_1}, V_{t_2}, \ldots, V_{t_r}$. Since $o(u) = 2$, we have that

$$u = \prod_{x \in U_{t_1} \cup U_{t_2} \cup \cdots U_{t_r}} x^2 \qquad \text{and} \qquad u^{\alpha} = \prod_{u \in V_{t_1} \cup V_{t_2} \cup \cdots V_{t_r}} y^2.$$

By the definition of β, we have $u^{\beta} = u^{\alpha}$ for any $u \in \langle S_1 \rangle \cap \langle S_2 \rangle$.

Now we are ready to prove Lemma 3.3. Define a map $\gamma : G \to G$ by $as \to a^{\beta} s^{\alpha}$ where $a \in \langle S_1 \rangle$ and $s \in \langle S_2 \rangle$. We claim that γ is an automorphism of G. Let $a_1 s_1 = a_2 s_2$ where $a_i \in \langle S_1 \rangle$ and $s_i \in \langle S_2 \rangle$ $(i = 1, 2)$. Then $a_1 a_2^{-1} = s_2 s_1^{-1} \in \langle S_1 \rangle \cap \langle S_2 \rangle$ and so $(a_1 a_2^{-1})^{\beta} = (s_2 s_1^{-1})^{\alpha}$. Since α, β are group isomorphisms, we have $\alpha_1^{\beta} s_1^{\alpha} = a_2^{\beta} s_2^{\alpha}$ which implies that γ is well defined. Now it is clear that γ is an automorphism of G and $(S \cup S^{-1})^{\gamma} = T$. Therefore, $S \cup S^{-1}$ is a CI-subset of G. ∎

Proof of Theorem 1.3. Let G_2 be a Sylow 2-subgroup of G. If G_2 is not elementary abelian and has a direct factor isomorphic to $\mathbb{Z}_2$, then we may assume that $G = \langle a \rangle \times \langle b \rangle \times \langle c_1 \rangle \times \cdots \times \langle c_m \rangle$ where $\langle a \rangle \cong \mathbb{Z}_2$ and $\langle b \rangle \cong \mathbb{Z}_{2^n}$ $(n \geqslant 2)$. Clearly, $S = \{b, ab^{2^{n-2}}, c_1, c_2, \ldots, c_m\}$ is a minimal generating subset of G. Set $T = \{b, b^{-1}, a, ab^{2^{n-1}}, c_1, c_2, \ldots, c_m, c_1^{-1}, c_2^{-1}, \ldots, c_m^{-1}\}$. By Lemma 3.1, it is easy to show that $\mathrm{Cay}(G, S \cup S^{-1}) \cong \mathrm{Cay}(G, T)$. But for any $\alpha \in \mathrm{Aut}(G)$, $(S \cup S^{-1})^{\alpha} \neq T$. This implies that $S \cup S^{-1}$ is not a CI-subset, and so G is not a CIM-group. Now we assume that G_2 is elementary abelian or has a direct factor isomorphic to $\mathbb{Z}_2$. Let S be a minimal generating subset of G. By Lemmas 3.2 and 3.3, $S \cup S^{-1}$ is a CI-subset and so G is a CIM-group. ∎

ACKNOWLEDGMENTS

The authors are indebted to the referee who spent a lot of time in correcting our English and made many useful suggestions.

REFERENCES

1. A. Ádám, Research problem 2-10, *J. Combin. Theory* **2** (1967), 393.
2. B. Alspach and T. D. Parsons, Isomorphisms of circulant graphs and digraphs, *Discrete 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. D. Ž. Djoković, Isomorphism problem for a special class of graphs, *Acta Math. Acad. Sci. Hungar.* **21** (1970), 267–270.
5. E. Dobson, Isomorphism problem for Cayley graphs of Z_p^3, *Discrete Math.* **147** (1995), 87–94.
6. B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Combin. Theory* **9** (1970), 297–307.
7. X. G. Fang, Abelian 3-DCI groups, *Ars Combin.* **32** (1992), 263–267.
8. Y. Q. Feng and M. Y. Xu, A note on isomorphisms of Cayley digraphs of abelian groups, *Australas. J. Combin.* **15** (1997), 87–90.
9. Y. Q. Feng and T. P. Gao, Automorphism groups and isomorphisms of Cayley digraphs of abelian groups, *Australas. J. Combin.* **16** (1997), 183–187.
10. C. D. Godsil, On Cayley graph isomorphisms, *Ars Combin.* **15** (1983), 231–246.
11. M. Hall, "*Combinatorial Theory*," 2nd ed., Wiley, New York, 1986.
12. F. Harary, "*Graph Theory*," Addison–Wesley, Reading, MA, 1969.
13. Q. X. Huang and J. X. Meng, Isomorphisms of circulant digraphs, *Appl. Math. J. Chinese Univ. Ser. B* **9** (1994), 405–409.
14. Q. X. Huang and J. X. Meng, Automorphism groups of Cayley digraphs, *in* "Combinatorics, Graph Theory, Algorithms and Applications" (Y. Alavi, D. R. Lick, and J. Q. Liu, Eds.), pp. 77–81, World Scientific, Singapore, 1994.
15. Q. X. Huang and J. X. Meng, On the isomorphisms and automorphism groups of circulants, *Graphs Combin.* **12** (1996), 179–187.
16. B. Huppert, "*Endliche Gruppen I*," Springer-Verlag, Berlin, 1979.
17. M. H. Klin and R. Pöschel, The König problem, the isomorphism problem for cyclic groups and the method of Schur rings, *in* "Algebraic Methods in Graph Theory, Szeged, 1978," *Colloq. Math. Soc. Janos Bolyai*, Vol. **25**, pp. 405–434, North-Holland, Amsterdam, 1981.
18. J. X. Meng and M. Y. Xu, On the isomorphism problem of Cayley graphs of abelian groups, *Discrete Math.* **187** (1998), 161–169.
19. C. H. Li, The finite groups with the 2-DCI property, *Comm. Algebra* **24** (1996), 1749–1757.
20. C. H. Li, Isomorphisms of connected Cayley graphs, II, *J. Combin. Theory Ser. B* **74** (1998), 28–34.
21. C. H. Li, On finite groups with the Cayley isomorphism property, II[1], *J. Combin. Theory Ser. A* **88** (1999), 19–35.
22. C. H. Li, Isomorphisms of finite Cayley digraphs of bounded valency, II[*], *J. Combin. Theory Ser. A* **87** (1999), 333–346.
23. C. H. Li, C. E. Praeger, and M. Y. Xu, Isomorphisms of finite Cayley digraphs of bounded valency, *J. Combin. Theory Ser. B* **73** (1998), 164–183.
24. C. H. Li and S. Zhou, On isomorphisms of minimal Cayley graphs and digraphs, *Graphs Combin.* **17** (2001), 307–314.
25. M. Muzychuk, Ádám's conjecture is true in the square-free case, *J. Combin. Theory Ser. A* **72** (1995), 118–134.
26. M. Muzychuk, On Ádám's conjecture for circulant graphs, *Discrete Math.* **176** (1997), 285–298.

27. P. P. Páley, Isomorphism problem for relational structures with a cyclic automorphism, *European J. Combin.* **8** (1987), 35–43.
28. H. J. Ryser, "*Combinatorial Mathematics*," Wiley, New York, 1963.
29. M. Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319.