Journal of Algebraic Combinatorics **8** (1998), 205–215

On Cayley Graphs of Abelian Groups

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

Received March 9, 1995; Revised April 18, 1997

Abstract. Let G be a finite Abelian group and $\mathrm{Cay}(G, S)$ the Cayley (di)-graph of G with respect to S, and let $A = \mathrm{Aut}\,\mathrm{Cay}(G, S)$ and A_1 the stabilizer of 1 in A. In this paper, we first prove that if A_1 is unfaithful on S then S contains a coset of some nontrivial subgroup of G, and then characterize $\mathrm{Cay}(G, S)$ if A_1^S contains the alternating group on S. Finally, we precisely determine all m-DCI p-groups for $2 \le m \le p + 1$, where p is a prime.

Keywords: Cayley graph, isomorphism, CI-subset, m-DCI group

1. Introduction

Let G be a finite group and S a *Cayley subset* of G, that is, S does not contain the identity of G. The *Cayley (di)-graph* $\mathrm{Cay}(G, S)$ of G with respect to S has the elements of G as vertices and the pairs $(g, sg), g \in G, s \in S$, as edges. Given a Cayley subset S of G, if, for any Cayley subset T of G, $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ implies $T = S^\sigma$ for some $\sigma \in \mathrm{Aut}(G)$, then S is called a *CI-subset* (CI stands for *Cayley Isomorphism*). A finite group G is called an *m-DCI group* if all of its Cayley subsets of G of size at most m are CI-subsets; G is called a *DCI-group* if it is a $|G|$-DCI group. Similarly, G is called an *m-CI group* if all Cayley subsets S of G of size at most m with $S = S^{-1}$ are CI-subsets, G is called a *CI-group* if G is an $|G|$-CI group. The problem of determining which groups are m-DCI groups and m-CI groups has been investigated for a long time, see [6, 10, 12] for references. Recently, all m-DCI groups and all m-CI groups for $m \ge 2$ have been classified in [10] and [9], respectively, in the sense that all the possibilities for such groups are explicitly listed. However, it is still a difficult question to determine which of them are really m-DCI (m-CI) groups. Babai and Frankl [2] asked whether the elementary abelian group Z_p^d for any p and d was an m-CI group for all $m \le |G|$ (in other words, Z_p^d is a CI-group). Godsil [6] and Dobson [4] proved this to be true for $d = 2, 3$, respectively. However, recently Nowitz [11] gave a negative answer to the question by proving that Z_2^6 is not a 31-CI group. It is not known if this the answer of the question is positive for odd prime p and $d \ge 4$. The main aims of this paper are to characterize Cayley graphs $\mathrm{Cay}(G, S)$ of abelian groups by the action of A_1 on S, where A_1 is the stabilizer of 1 in $\mathrm{Aut}\,\mathrm{Cay}(G, S)$, and to determine precisely m-DCI p-groups for $2 \le m \le p + 1$, which implies that the answer of Babai and Frankl's question is positive for any p, d and $m \le p + 1$.

Notation In this paper, Z_n denotes a cyclic group of order n, Q_8 is the quaternion group of order 8. Recall that a group is called *homocylic* if it is a direct product of some cyclic groups of the same order. For groups G and H, $H \leq G$ denotes that H is a subgroup of G, and $G \rtimes H$ denotes a semidirect product of G by H. For a positive integer n, C_n denotes the directed cycle of length n, K_n denotes the complete graph on n vertices and $K_{n,n}$ denotes the complete-bipartite graph on $2n$ vertices. For a directed graph $\Gamma = (V, E)$, its *complement* $\bar{\Gamma} = (V, \bar{E})$ is the directed graph with vertex set V such that $(a, b) \in \bar{E}$ if and only if $(a, b) \notin E$. The *direct product* $\Gamma_1 \times \Gamma_2$ of two directed graphs $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ is the directed graph with vertex set $V_1 \times V_2$ such that $((a_1, a_2), (b_1, b_2))$ is an edge if and only if either $(a_1, b_1) \in E_1$ and $a_2 = b_2$, or $(a_2, b_2) \in E_2$ and $a_1 = b_1$. The *lexicographic product* $\Gamma_1[\Gamma_2]$ of two directed graphs $\Gamma_1 = (V_1, E_1)$ 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 edge 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 any vertex x of graph $\mathrm{Cay}(G, S)$, the neighborhood $\Gamma(x)$ of x in $\mathrm{Cay}(G, S)$ equals $xS = \{xa_i \mid 1 \leq i \leq m\}$. Let $\Gamma_i(x) = \{y \in G \mid d(x, y) = i\}$, where $d(x, y)$ denotes the distance from x to y in $\mathrm{Cay}(G, S)$. Note that $\Gamma(x) = \Gamma_1(x)$.

In Section 2, we quote some results which are used in the following sections. Section 3 characterizes some Cayley graphs on Abelian groups, and Section 4 precisely determines m-DCI p-groups for certain values of m.

2. Preliminaries

In this section, we quote some results which we need in the following sections. Let G be a finite group, S a Cayley subset of G and let $A = \mathrm{Aut}\,\mathrm{Cay}(G, S)$. Babai [1] gave a criterion for a subset of G to be a CI-subset.

Theorem 2.1 ([1]) *For a given group G and a Cayley subset S of G, S is a CI-subset if and only if for any $\tau \in \mathrm{Sym}(G)$ with $\tau G \tau^{-1} \leq A$, there exists $\alpha \in A$ such that $\alpha G \alpha^{-1} = \tau G \tau^{-1}$, where $\mathrm{Sym}(G)$ is the symmetric group on G.*

The normalizer of G in A is often useful for characterizing $\mathrm{Cay}(G, S)$.

Lemma 2.2 ([5]) *Let $A = \mathrm{Aut}\,\mathrm{Cay}(G, S)$ and $\mathrm{Aut}(G, S) = \{\alpha \in \mathrm{Aut}(G) \mid S^\alpha = S\}$. Then $\mathrm{N}_A(G)$ equals a semidirect product of G by $\mathrm{Aut}(G, S)$, that is, $N_A(G) = G \rtimes \mathrm{Aut}(G, S)$.*

All finite m-DCI groups for $m \geq 2$ have been explicitly listed in [10], in particular, we have

Lemma 2.3 ([10, Proposition 3.1]) *Let G be a finite m-DCI p-group, where $m \geq 2$ and p is a prime.*

(1) *If p is odd and $2 \leq m \leq p - 1$, then G is homocyclic.*

(2) *If $m = p$, then either G is elementary Abelian, cyclic, or $G = Q_8$.*

(3) *If $m = p + 1$, then either G is elementary Abelian, or $G = Z_4$ or Q_8.*

Lemma 2.4 ([16]) *The quaternion group Q_8 is a DCI-group.*

3. Cayley graphs of Abelian groups

In this section, we characterize some properties of Cayley graphs of Abelian groups. Let G be a finite group, $S = \{a_1, a_2, \ldots, a_m\}$ be a Cayley subset of G and $\Gamma = \mathrm{Cay}(G, S)$. Let A be the full automorphism group of Γ and A_1 the stabilizer of 1 in A. For h distinct elements $a_{i_1}, a_{i_2}, \ldots, a_{i_h} \in S$ and $y \in G$, let

$$\begin{cases} \Gamma\big(ya_{i_1}, \ldots, ya_{i_h}\big) = \Gamma\big(ya_{i_1}\big) \cap \cdots \cap \Gamma\big(ya_{i_h}\big), \\ \Gamma^*\big(ya_{i_1}, \ldots, ya_{i_h}\big) = \Gamma\big(ya_{i_1}, \ldots, ya_{i_h}\big) \setminus \bigcup_{x\in R} \Gamma(yx), \end{cases}$$

where $R = S\backslash\{a_{i_1}, \ldots, a_{i_h}\}$, that is, $\Gamma^*(ya_{i_1}, \ldots, ya_{i_h})$ is the set of all vertices of Γ which are joined to every element of $\{ya_{i_1}, \ldots, ya_{i_h}\}$ and to no element of yR. Let

$$\Gamma_i^* = \max\{|\Gamma^*(u_1, \ldots, u_i)| \mid u_1, \ldots, u_i \in S\}.$$

If $R = \{u_1, \ldots, u_i\} \subseteq S$, then denote $\Gamma^*(u_1, \ldots, u_i)$ by $\Gamma^*(R)$ sometimes.

Lemma 3.1 *Suppose that G is an Abelian group. Then*

(i) $1 \in \Gamma^*(W)$ *for* $W \subseteq S$ *if and only if* $W = W^{-1}$ *and* $(S\backslash W) \cap (S\backslash W)^{-1} = \emptyset$;

(ii) $\Gamma^*(xx_1, \ldots, xx_k) = x\Gamma^*(x_1, \ldots, x_k)$ *for any* $x \in G$ *and any* $x_1, \ldots, x_k \in S$;

(iii) $\Gamma_k^* \leq k$ *for every* $k \geq 1$;

(iv) *every element of* $\Gamma_2(1)$ *lies in* $\Gamma^*(x_1, \ldots, x_k)$ *for some* $x_1, \ldots, x_k \in S$.

Proof: By the definition of $\Gamma^*(x_1, \ldots, x_k)$, part (i) is clear. Again by definition, we have

$$\begin{aligned} y \in \Gamma^*(xx_1, \ldots, xx_k) &\Leftrightarrow y \in \Gamma^*(xx_1) \cap \cdots \cap \Gamma^*(xx_k)\setminus\bigcup_{z\in R}\Gamma(xz) \\ &\Leftrightarrow x^{-1}y \in \Gamma(x_1) \cap \cdots \cap \Gamma(x_k)\setminus\bigcup_{z\in R}\Gamma(z) \\ &\Leftrightarrow y \in x\big(\Gamma(x_1) \cap \cdots \cap \Gamma(x_k)\setminus\bigcup_{z\in R}\Gamma(z)\big) \\ &\quad= x\Gamma^*(x_1, \ldots, x_k), \end{aligned}$$

where $R = S\backslash\{x_1, \ldots, x_k\}$. Thus part (ii) is true. Now suppose that $\Gamma_k^* = |\Gamma^*(x_1, \ldots, x_k)|$ for some $x_1, \ldots, x_k \in S$. By definition, $x_1x \notin \Gamma^*(x_1, \ldots, x_k)$ for any $x \in S\backslash\{x_1, \ldots, x_k)$, so $\Gamma^*(x_1, \ldots, x_k) \subseteq \{x_1x_1, \ldots, x_1x_k\}$. Hence $\Gamma_k^* = |\Gamma^*(x_1, \ldots, x_k)| \leq k$ as in (iii). Finally, for any $y \in \Gamma_2(1)$, let $\{x_1, \ldots, x_k\} = \{x \in S \mid y \in \Gamma(x)\}$. Then $y \in \Gamma^*(x_1, \ldots, x_k)$ is as in (iv). □

It is clear that if $\mathrm{Cay}(G, S) \cong C_l[\bar{K}_m]$ for $m > 1$ then A_1 is not faithful on S. Conversely, the following theorem shows that if A_1 is not faithful on S then $\mathrm{Cay}(G, S)$ contains such a subgraph.

Theorem 3.2 *Let G be an Abelian group and $\Gamma = Cay(G, S)$ for some $S \subset G$ such that $G = \langle S \rangle$. Let $A = Aut\,\Gamma$ and A_1 the stabilizer of 1 in A. Then either A_1 is faithful on S, or S contains a coset of some nontrivial subgroup of G and Γ has a subgraph isomorphic to $C_l[\bar{K}_n]$ for some integers l and n.*

Proof: Let $S = \{a_1, a_2, \ldots, a_m\}$. Assume first that for any integer $h \geq 1$ and any h elements $x_1, \ldots, x_h \in S$, $|\Gamma^*(x_1, \ldots, x_h)| \leq 1$. We claim that A_1 is faithful on S. For any $y \in \Gamma_2(1)$, let $\{a_{i_1}, \ldots, a_{i_h}\} = \{x \in S \mid y \in \Gamma(x)\}$. Then y is the unique element of $\Gamma^*(a_{i_1}, \ldots, a_{i_h})$. If $\alpha \in A_1$ such that $x^\alpha = x$ for all $x \in S$, then α fixes $a_{i_1}, \ldots, a_{i_h}$. Thus α fixes $\Gamma^*(a_{i_1}, \ldots, a_{i_h})$, and so α fixes y. Hence $x^\alpha = x$ for all $x \in \Gamma_2(1)$. Since $\langle S \rangle = G$, $\mathrm{Cay}(G, S)$ is connected, and it follows that $x^\alpha = x$ for all $x \in V\Gamma$. Hence $\alpha = 1$ and A_1 is faithful on S.

Assume now that there are some h vertices $a_{i_1}, \ldots, a_{i_h}$ such that $|\Gamma^*(a_{i_1}, \ldots, a_{i_h})| \geq 2$. Let $w, y \in \Gamma^*(a_{i_1}, \ldots, a_{i_h})$. Without loss of generality, we may assume that $\{i_1, \ldots, i_h\} = \{1, \ldots, h\}$. By the definition of $\Gamma^*(a_1, \ldots, a_h)$, there exist $u_1, \ldots, u_h$, $v_1, \ldots, v_h \in \{a_1, \ldots, a_h\}$ such that

$$\begin{cases} a_1u_1 = a_2u_2 = \cdots = a_hu_h = w, \\ a_1v_1 = a_2v_2 = \cdots = a_hv_h = y, \end{cases}$$

where $u_i \neq v_i$ and $\{u_1, \ldots, u_h\} = \{v_1, \ldots, v_h\} = \{a_1, \ldots, a_h\}$. Since $\{u_1, \ldots, u_h\} = \{v_1, \ldots, v_h\}$, there exist $i_1 \neq 1$, $i_2 \neq i_1, \ldots, i_k \neq i_{k-1}$ for some $k \leq h$ such that $v_1 = u_{i_1}, v_{i_1} = u_{i_2}, \ldots, v_{i_{k-1}} = u_{i_k}$ and $v_{i_k} = u_1$. Thus

$$\begin{cases} a_1u_1 = a_{i_1}u_{i_1} = \cdots = a_{i_k}u_{i_k}, \\ a_1u_{i_1} = a_{i_1}u_{i_2} = \cdots = a_{i_k}u_1. \end{cases}$$

For convenience, without loss of generality, we may assume that $i_1 = 2, i_2 = 3, \ldots, i_k = k+1$. Then we have

$$\begin{cases} a_1u_1 = a_2u_2 = \cdots = a_{k+1}u_{k+1}, \\ a_1u_2 = a_2u_3 = \cdots = a_{k+1}u_1. \end{cases}$$

Thus $a_1u_1a_iu_{i+1} = a_1u_2a_iu_i$ for $i \leq k$ and $a_1u_1a_{k+1}u_1 = a_1u_2a_{k+1}u_{k+1}$. Therefore, $u_1u_{i+1} = u_2u_i$ for $i \leq k$ and $u_1^2 = u_2u_{k+1}$. Let $U = \{u_1, \ldots, u_{k+1}\}$. Then $u_1U = u_2U$. Similarly, we have $u_1U = \cdots = u_{k+1}U$. We claim that $a_1^{-1}U$ is a subgroup of G. In fact, for any i, j with $1 \leq i, j \leq k+1$, there exists an integer l such that $u_1u_i = u_ju_l$ because $u_1U = u_jU$. Thus $u_iu_j^{-1} = u_1^{-1}u_l$ and so

$$u_1^{-1}u_i \cdot \left(u_1^{-1}u_j\right)^{-1} = u_iu_j^{-1} = u_1^{-1}u_l \in u_1^{-1}U.$$

Therefore, $u_1^{-1}U$ is a subgroup of G and U is a coset of the subgroup $u_1^{-1}U$. Now $\mathrm{Cay}(\langle U \rangle, U) \cong C_l[\bar{K}_{|U|}]$ is a subgraph of $\mathrm{Cay}(G, S)$ as in the theorem. This completes the proof of the theorem. □

Next we are going to characterize Cayley graphs $\mathrm{Cay}(G, S)$ for which A_1^S is the alternating group or the symmetric group of degree $|S|$. To do this, we first prove the following lemma.

Lemma 3.3 *Let G be an Abelian group, and let S, T be two Cayley subsets of G such that $G = \langle S \rangle$ and $Cay(G, S) \cong Cay(G, T)$. If $\Gamma^*(x, y) = \{xy\}$ for all $x, y \in S$ and $\Gamma^*(u, v) = \{uv\}$ for all $u, v \in T$, then every isomorphism preserving 1 between $Cay(G, S)$ and $Cay(G, T)$ induces an automorphism of G.*

Proof: Let $S = \{a_1, a_2, \ldots, a_m\}$ and $T = \{b_1, b_2, \ldots, b_m\}$. Without loss of generality, assume that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$ such that $1 \to 1$, $a_i \to b_i$ for $i = 1, 2, \ldots, m$. Then for any $i \neq j$,

$$\rho : \{a_i a_j\} = \Gamma^*(a_i, a_j) \mapsto \Gamma^*(b_i, b_j) = \{b_i b_j\}.$$

We claim that ρ is an automorphism of G. To prove this, we need only verify that for all integers $n_1, n_2, \ldots, n_m \geq 0$,

$$\left(a_1^{n_1} a_2^{n_2} \cdots a_m^{n_m}\right)^\rho = b_1^{n_1} b_2^{n_2} \cdots b_m^{n_m}, \tag{1}$$

by induction on $n_1 + n_2 + \cdots + n_m$. Since

$$\rho : \begin{cases} a_i \to b_i, & \text{for } 1 \leq i \leq m, \\ a_i a_j \to b_i b_j, & \text{for } i \neq j, \end{cases}$$

we have ρ:

$$\left\{a_i^2\right\} = \Gamma(a_i) \backslash \{a_i a_j \mid j \neq i\} \mapsto \Gamma(b_i) \backslash \{b_i b_j \mid j \neq i\} = \left\{b_i^2\right\}$$

for all $i = 1, 2, \ldots, m$. In other words, (1) holds for $n_1 + n_2 + \cdots + n_m \leq 2$. Now assume inductively that the equality (1) holds for $n_1 + n_2 + \cdots + n_m \leq N$, where $N \geq 2$. Let

$$a = \prod_{j=1}^{m} a_j^{n'_j}, \quad \text{where } \sum_{j=1}^{m} n'_j = N - 1.$$

By the induction assumption, we have

$$\rho : \begin{cases} a \to b = \prod_{j=1}^{m} b_j^{n'_j}, & \\ a a_i \to b b_i, & \text{for } 1 \leq i \leq m. \end{cases}$$

Since G is Abelian, for any $x \in \langle S \rangle$, $y \in \langle T \rangle$ and any $i \neq j$, we have $\Gamma^*(x a_i, x a_j) = \{x a_i a_j\}$ and $\Gamma^*(y b_i, y b_j) = \{y b_i b_j\}$. Hence ρ:

$$\begin{cases} \{a a_i a_j\} = \Gamma^*(a a_i, a a_j) \mapsto \Gamma^*(b b_i, b b_j) = \{b b_i b_j\}, & \text{for } 1 \leq i \neq j \leq m, \\ \left\{a a_i^2\right\} = \Gamma(a a_i) \backslash \{a a_i a_j \mid j \neq i\} \mapsto \Gamma(b b_i) \backslash \{b b_i b_j \mid j \neq i\} = \left\{b b_i^2\right\}. & \end{cases}$$

Therefore, the equality (1) holds for $n_1+n_2+\cdots+n_m = N+1$. By induction, the equality (1) holds for all $n_1, n_2, \ldots, n_m \geq 0$. Hence ρ is an automorphism of G sending S to T. □

To prove our next theorem, we need some notation. If $a, b \in S$ and $b \neq a^{-1}$, then the product ab (in G) is said to be a *word* of length 2 on S. Let $w(ab)$ be the number of all words of length 2 on S which are equal to ab, that is, $w(ab) = |\{uv \mid uv = ab \text{ and } u, v \in S\}|$. For $Y \subseteq \Gamma_2(1)$, let $w(Y)$ be the number of all words of length 2 on S which are equal to an element of Y, that is, $w(Y) = \sum_{y\in Y} w(y)$.

Lemma 3.4 *Using the notation defined above, we have*

(i) *if* $1 \neq ab \in \Gamma^*(u_1, u_2, \ldots, u_i)$, *then* $w(ab) = i$ *for any* $u_1, u_2, \ldots, u_i \in S$;

(ii) *if* $|\Gamma^*(u_1, \ldots, u_i)| = j$ *then*

$$w(\Gamma^*(u_1, \ldots, u_i)) = \begin{cases} ij & \text{if } 1 \notin \Gamma^*(u_1, \ldots, u_i), \\ i(j-1) & \text{if } 1 \in \Gamma^*(u_1, \ldots, u_i); \end{cases}$$

(iii) $|\Gamma_2(1)| \leq w(\Gamma_2(1))$ *and if* $1 \in \Gamma^*(R)$ *then* $w(\Gamma_2(1)) = m^2 - |R|$ *for any* $R \subseteq S$;

(iv) *if* $A_1^S \geq Alt(|S|)$, *then* $1 \in \Gamma^*(R)$ *for* $R \subseteq S$ *implies* $R = S$.

Proof: By definition, part (i) is clear. It follows that part (ii) holds. Now let $S = \{a_1, \ldots, a_m\}$. Then $\Gamma_2(1) = \{a_i a_j \mid 1 \leq i, j \leq m\} \backslash \{1\}$. It follows that part (iii) is true. Noting that A_1^S is $(m-2)$-transitive on S, in particular, transitive and 2-set-transitive on S, part (iv) is clearly true. □

Now we can prove our next result.

Theorem 3.5 *Let G be an Abelian group, and let S be a generating subset of G of size m. Let $\Gamma = Cay(G, S)$, and let $A = Aut\,\Gamma$ and A_1 the stabilizer of 1 in A. If $A_1^S \geq Alt(m)$, the alternating group of degree m, then one of the following holds*:

(i) $S = G\backslash\{1\}$ *and* $\Gamma \cong K_{m+1}$;

(ii) $S = aH$ *for some* $H \leq G$, *and* $\Gamma \cong K_{m,m}$ *or* $C_{|G|/m}[\bar{K}_m]$;

(iii) $S = bH\backslash\{b\}$ *for some* $H \leq G$, $\Gamma \cong C_{|G|/(m+1)}[\bar{K}_{m+1}] - \frac{|G|}{o(b)} C_{o(b)}$;

(iv) $S = a^L$ *for some* $a \in S$ *and some* $L \leq Aut(G, S)$, *and* $G \lhd A$;

(v) *either G is cyclic, or $G = Z_n \times B$, where n is odd and B is a 2-group of exponent 4, and* $\Gamma_2(1) = \bigcup_{u,v\in S} \Gamma^*(u, v) \cup \Gamma^*(S)\backslash\{1\}$.

Proof: First assume that $m = 2$ and $S = \{a, b\}$. If $b = a^{-1}$ then $G = \langle a \rangle$ is cyclic and Γ is a cycle of length $n := o(a)$. Thus $A \cong D_{2n}$, and so part (iv) holds in this case. Suppose that $b \neq a^{-1}$. If $|\Gamma^*(a, b)| = 1$, then $a^2 \neq b^2$ and so $\Gamma^*(a, b) = \{ab\}$. It follows from Lemma 3.3 that part (iv) holds. If $|\Gamma^*(a, b)| = 2$ then $\Gamma^*(a, b) = \{ab = ba, a^2 = b^2\}$. Thus $\{1, a^{-1}b\}$ is a subgroup of G of order 2, and $S = a\{1, a^{-1}b\}$ as in part (ii). Hence $\Gamma_i(1) = a^i\{1, a^{-1}b\}$ for all $i \geq 1$. Hence $|\Gamma_i(1)| = 2$, and it follows that $\mathrm{Cay}(G, S) \cong C_{|G|/2}[\bar{K}_2]$.

In the following, assume that $m \geq 3$ and $S = \{a_1, a_2, \ldots, a_m\}$. Since $A_1^S \geq \mathrm{Alt}(m)$, A_1^S is $(m-2)$-transitive on S, in particular, A_1^S is 2-set-transitive on S. By Lemma 3.1(iv), any element of $\Gamma_2(1)$ belongs to $\Gamma^*(R)$ for some $R \subseteq S$. Since either $\Gamma^*(a_i) = \emptyset$ or $\Gamma^*(a_i) = \{a_i^2\}$ and $a_i^2 \neq a_j a_k$ for any $j, k \neq i$, there is at least one $n \in \{2, \ldots, m\}$ such that $\Gamma_n^* \geq 1$.

(1) Assume that there exists an integer n with $3 \leq n \leq m-2$ such that $\Gamma_n^* = r \geq 1$. Then there are n vertices $c_1, \ldots, c_n \in S$ such that $|\Gamma^*(c_1, \ldots, c_n)| = r$. Thus $\Gamma^*(c_1, \ldots, c_n)$ contains exactly r elements of $\Gamma_2(1)$. By Lemma 3.4(ii) and (iv), $w(\Gamma^*(c_1, c_2, \ldots, c_n)) = rn$. Since A_1 is $(m-2)$-transitive on S, for any n elements $x_1, \ldots, x_n$ of S, $w(\Gamma^*(x_1, \ldots, x_n)) = rn$. Hence

$$m^2 \geq w(\Gamma_2(1)) \geq \sum_{x_1,\ldots,x_n \in S} w(\Gamma^*(x_1, \ldots, x_n)) = rn\binom{m}{n}.$$

However, it is easy to see that $rn\binom{m}{n} > m^2$ since $3 \leq n \leq m-2$, a contradiction. Thus $\Gamma_n^* = 0$ for $3 \leq n \leq m-2$.

(2) Assume that $\Gamma_2^* = \Gamma_{m-1}^* = 0$. Then $\Gamma_2(1) = (\Gamma^*(S)\backslash\{1\}) \cup \Gamma^*(a_1) \cup \cdots \cup \Gamma^*(a_m) \subseteq (\Gamma^*(S)\backslash\{1\}) \cup \{a_1^2, \ldots, a_m^2\}$. Thus $a_i a_j \in \Gamma^*(S)$ for any $a_i \neq a_j$. Since no two of $a_1 a_2, \ldots, a_1 a_m$ are equal, $|\Gamma^*(S)| \geq m-1 \geq 2$. Thus for any $i, j \neq 1$, there are integers h, k such that $a_1 a_i = a_j a_h$ and $a_1 a_j = a_i a_k$. It follows that $a_1^2 = a_h a_k$ and so $\Gamma^*(a_1) = \emptyset$. Thus $\Gamma^*(S)\backslash\{1\} = \Gamma_2(1)$. Hence every vertex in $\Gamma_2(1)$ is joined to all vertices in $\Gamma(1) = S$. Thus if $1 \in \Gamma^*(S)$ then $\mathrm{Cay}(G, S) \cong K_{m,m}$; if $1 \notin \Gamma^*(S)$ then $\mathrm{Cay}(G, S) \cong C_{\frac{|G|}{m}}[\bar{K}_m]$ where $|G| > 2m$. It follows that $a_i S = a_j S$ for any $a_i, a_j \in S$. Thus $H = a_1^{-1}S$ is a subgroup of G and $S = a_1 H$. This case is as in part (ii).

(3) Suppose that $\Gamma_2^* = r \geq 1$. By Lemma 3.1(iii), $r \leq 2$. If $r = 2$, then since A_1 is 2-set-transitive on S, for any $u, v \in S$, $|\Gamma^*(u, v)| = 2$ and so $\Gamma^*(u, v) = \{uv = vu, u^2 = v^2\}$. It follows that $a_1^2 = a_2^2$ and $a_2^2 = a_3^2$, a contradiction. Thus $r = 1$. Since A_1 is 2-set-transitive on S, $|\Gamma^*(u, v)| = 1$ for any $u, v \in S$. Hence $\Gamma^*(u, v) = \{uv = vu\}$ or $\{u^2 = v^2\}$. By Lemma 3.4(iv), $1 \notin \Gamma^*(u, v)$ and so $w(\Gamma^*(u, v)) = 2$.

First assume that there are two elements $a, b \in S$ such that $\Gamma^*(a, b) = \{a^2 = b^2\}$. Then $\Gamma^*(a) = \emptyset$ and $ab \notin \Gamma^*(a, b)$, so $ab = cd$ for some $c, d \in S\backslash\{a, b\}$. Thus $ab \in \Gamma^*(x_1, \ldots, x_i)$ for some $x_1, \ldots, x_i \in S$ where $i > 2$. Since $\Gamma_n^* = 0$ for $3 \leq n \leq m-2$ shown in (1), $i \geq m-1$ and so $w(ab) \geq m-1$. Thus $\Gamma_{m-1}^* \neq 0$ or $\Gamma_m^* \neq 0$. Since $w(\Gamma^*(u, v)) = 2$ for all $u, v \in S$ where $u \neq v$, $\sum_{u,v \in S} w(\Gamma^*(u, v)) = 2\binom{m}{2} = m(m-1)$. If $\Gamma_{m-1}^* = s \neq 0$ then since A_1^S is transitive on S, $|\Gamma^*(S\backslash\{u\})| = s$ for all $u \in S$. Thus $w(\Gamma^*(S\backslash\{u\})) = s(m-1)$ and so $\sum_{u \in S} w(\Gamma^*(S\backslash\{u\})) = ms(m-1)$. Since $1 \notin \Gamma^*(S\backslash\{u\})$, we have

$$\begin{aligned} w(\Gamma_2(1)) &\geq \sum_{u,v \in S} w(\Gamma^*(u, v)) + \sum_{u \in S} w(\Gamma^*(S\backslash\{u\})) \\ &= (s+1)m(m-1) > m^2 \geq w(\Gamma_2(1)), \end{aligned}$$

a contradiction. Thus $\Gamma_{m-1}^* = 0$, so $\Gamma_m^* = s \neq 0$ and $\Gamma_2(1) = \bigcup_{u,v \in S} \Gamma^*(u, v) \cup \Gamma^*(S)\backslash\{1\}$. Without loss of generality, suppose that $a = a_1$ and $b = a_2$, and let $a_i = o_i e_i$ such that $o_i \in G_{2'}$ and $e_i \in G_2$, where G_2 is a Sylow 2-subgroup and $G_{2'}$ is a Hall $2'$-subgroup of G. Since $a_1^2 = a_2^2$, $o_1 = o_2 =: o$ and $e_1^2 = e_2^2$. For any $a_i \in S$ with $i \neq 1, 2$, since $a_1 a_2 \in \Gamma^*(S)$, there is an a_j such that $a_1a_2 = a_ia_j$. If $j = i$ then $o_i^2 = o_1o_2 = o^2$ and $e_i^2 = e_1e_2$, so $o_i = o$. If $j \neq i$ then since $a_ia_j = a_1a_2$, $a_ia_j \notin \Gamma^*(a_i, a_j)$. Since $\Gamma^*(a_i, a_j) \neq \emptyset$, we have $\Gamma^*(a_i, a_j) = \{a_i^2 = a_j^2\}$. It follows that $o_i = o_j$ and $e_i^2 = e_j^2$. Since $a_ia_j = a_1a_2 = o^2e_1e_2$, we have $o_i = o$ and $e_ie_j = e_1e_2$. Thus, whether $j = i$ or not, we have $o_i = o$ and $e_i^4 = (e_ie_j)^2 = (e_1e_2)^2 = e_1^4$. Hence $o_1 = o_2 = \cdots = o_m$ and $e_1^4 = e_2^4 = \cdots = e_m^4$. Note that $G = \langle S\rangle$, so $G_{2'} = \langle o\rangle$ and $G_2 = \langle e_1, e_2, \ldots, e_m\rangle$. If $e_1^4 \neq 1$ then G_2 has only one subgroup of order 2. By [14, p. 59], G_2 is cyclic; if $e_1^4 = 1$ then G_2 is of exponent 4. This case is as in part (v).

Now assume that $\Gamma^*(u, v) = \{uv\}$ for any $u, v \in S$ and that G is not as in part (v). For any $T \subseteq S\backslash\{1\}$, by the previous paragraph, $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ implies that $\Gamma^*(u', v') = \{u'v'\}$ for any $u', v' \in T$ with $u' \neq v'$. By Lemma 3.3, S is conjugate in $\mathrm{Aut}(G)$ to T and so S is a CI-subset. For any $\rho \in A_1$, let $b_i = a_i^\rho$ and $T = \{b_1, \ldots, b_m\}$. Then $\mathrm{Cay}(G, S) = \mathrm{Cay}(G, T)$. By Lemma 3.3, ρ induces an automorphism of G. Thus $A_1 \leq \mathrm{Aut}(G)$, so $A_1 = \mathrm{Aut}(G, S)$ and $A = GA_1 = G \rtimes \mathrm{Aut}(G, S)$, which is as in part (iv).

(4) Assume that $\Gamma_2^* = 0$ and $\Gamma_{m-1}^* = r \geq 1$. Then $m \geq 4$. Since A_1 is transitive on S, we have $|\Gamma^*(S\backslash\{x\})| = r$ for every $x \in S$. If $r \geq 2$, then since $1 \notin \Gamma^*(S\backslash\{x\})$ for any $x \in S$,

$$w(\Gamma_2(1)) \geq \sum_{x\in S} w(\Gamma^*(S\backslash\{x\})) = rm(m-1) > m^2 \geq w(\Gamma_2(1)),$$

a contradiction. Thus $r = 1$. Let $v(x)$ be the unique element of $\Gamma^*(S\backslash\{x\})$. If $v(a_1) = a_1$, then for any a_i, we have $v(a_i) = a_i$ because A_1 is transitive on S. Thus $\mathrm{Cay}(G, S) \cong K_{m+1}$ as in part (i). Now suppose that $v(a_1) \neq a_1$. Then $v(a_1) \in \Gamma(x)$ for all $x \in S\backslash\{a_1\}$. Let $b = a_1^{-1}v(a_1)$ and $S^* = S \cup \{b\}$. We shall prove that $b^{-1}S^*$ is a subgroup of G. To do this, we need to prove that $b^{-1}a_i \cdot (b^{-1}a_j)^{-1} \in b^{-1}S^*$ for any $i \neq j$. Since $i \neq j$, we may assume that $j \neq 1$. Then $v(a_1) \in \Gamma(a_j)$ and so $v(a_1) = a_ja_k$ for some $a_k \in S$. Thus

$$\begin{aligned} b^{-1}a_i \cdot (b^{-1}a_j)^{-1} &= b^{-1} \cdot b \cdot a_ia_j^{-1} \\ &= b^{-1} \cdot a_1^{-1}v(a_1) \cdot a_ia_j^{-1} \\ &= b^{-1} \cdot a_1^{-1}a_ja_k \cdot a_ia_j^{-1} \\ &= b^{-1}a_1^{-1}a_ia_k. \end{aligned}$$

If $a_ia_k \in \Gamma(a_1)$, that is, $a_ia_k = a_1a_{k'}$ for some $a_{k'} \in S$, then $b^{-1}a_i(b^{-1}a_j)^{-1} = b^{-1}a_1^{-1}a_ia_k = b^{-1}a_{k'} \in b^{-1}S^*$. Hence $H := b^{-1}S^*$ is a subgroup of G and S^* is a coset of H. Thus $S = S^*\backslash\{b\} = bH\backslash\{b\}$, and $\mathrm{Cay}(G, S) = \mathrm{Cay}(G, S^*) - \mathrm{Cay}(G, \{b\}) \cong C_{\frac{|G|}{m+1}}[\bar{K}_{m+1}] - \frac{|G|}{k}C_k$ where $k = o(b)$, which are as in part (iii) of the theorem. Thus, in the following, we only need to prove that $a_ia_k \in \Gamma(a_1)$. Since $i \neq j$, $a_ia_k \neq a_ja_k = v(a_1)$. If $i \neq k$, then since $\Gamma_n^* = 0$ for $2 \leq n \leq m-2$, $a_ia_k \in \Gamma^*(S) \cup \Gamma^*(S\backslash\{x\})$ for some $x \in S\backslash\{a_1\}$ and so $a_ia_k \in \Gamma(a_1)$. Thus we may assume that $i = k$, so $a_ia_k = a_k^2$. If $a_k^2 = a_1^2$ then $a_k^2 \in \Gamma(a_1)$. Hence suppose that $a_k^2 \neq a_1^2$. Since $a_ja_k = v(a_1) \in \Gamma^*(S\backslash\{a_1\})$, there exist $a_h, a_l \in S\backslash\{a_j, a_k\}$ such that $a_ja_k = a_ha_l$. If $l = h$ then $a_h^2 = a_ja_k$ and so $\Gamma^*(a_h) = \emptyset$. Since A_1 is transitive on S, $\Gamma^*(a_k) = \emptyset$ and so $a_k^2 \in \Gamma^*(S) \cup \Gamma^*(S\backslash\{x\})$ for some $x \in S$.

Since $a_k^2 \neq \upsilon(a_1)$, we have $a_k^2 \in \Gamma(a_1)$. If $l \neq h$, then at least one of $a_k a_h$ and $a_k a_l$ does not belong to $\Gamma^*(S\backslash\{a_j\})$, say, $a_k a_h \notin \Gamma^*(S\backslash\{a_j\})$. Thus $a_k a_h \in \Gamma^*(S) \cup \Gamma^*(S\backslash\{x\})$ for some $x \in S\backslash\{a_j\}$, and so $a_k a_h = a_j a_{l'}$ for some l', which, together with $a_j a_k = a_h a_l$, implies $a_k^2 = a_l a_{l'}$. Thus $\Gamma^*(a_k) = \emptyset$ and so $a_k^2 \in \Gamma^*(S) \cup \Gamma^*(S\backslash\{x\})$ for some $x \in S$. Since $a_k^2 \neq \upsilon(a_1)$, $a_k^2 \notin \Gamma^*(S\backslash\{a_1\})$ and so $a_k^2 \in \Gamma(a_1)$. This completes the proof of the theorem. □

Theorem 3.5 gives an application to Babai and Frankl's question.

Corollary 3.6 *Let G be an elementary Abelian p-group, p a prime, and S a Cayley subset. Let $A = \mathrm{Aut\,Cay}(G, S)$. If $A_1^S \geq \mathrm{Alt}(S)$, then S is a CI-subset of G.*

Proof: Since any subgroup of G is still elementary Abelian group and each isomorphism between any two subgroups can be extended as an automorphism of G, we may assume that $\langle S \rangle = G$. By Theorem 3.5, Cay(G, S) satisfies parts (i)–(iv). It is easy to check that S is a CI-subset of G. □

Remark By Theorem 3.5, the graphs in parts (i)–(iii) have been completely characterized. The graphs Cay(G, S) in part (iv) satisfies a very strong condition $\mathrm{Aut\,Cay}(G, S) \leq G \rtimes \mathrm{Aut}(G)$'s.

4. Finite *m*-DCI *p*-groups, *p* a prime

By definition, a finite group G is a 1-DCI group if and only if all elements of G of the same order are conjugate in Aut(G). Suppose that G is a 1-DCI p-group. If p is an odd prime then G is homocyclic by the result of Shult [13]; if $p = 2$ then by [7], G is a homocyclic group or the quaternion group Q_8, or G satisfies the following conditions:

(i) $G' = \Phi(G)$ is homocyclic of rank n;
(ii) G/G' is of order 2^n or 2^{2n};
(iii) the centre $\mathbf{Z}(G)$ of G consists of the identity and all the involutions of G;
(iv) either $\mathbf{Z}(G) = G'$, or $\mathbf{C}_G(G') = G'$ with $\mathbf{Z}(G) = \Phi(G')$.

It is easy to see that homocyclic groups and Q_8 are 1-DCI groups, however, it is still difficult to characterize precisely 1-DCI 2-groups, see [7]. For $m \geq 2$, the problem of determining m-DCI groups is very different from the case $m = 1$. By Lemma 2.4, we need to consider mainly Abelian p-groups. We first prove a property of Cayley graphs of arbitrary Abelian p-groups.

Proposition 4.1 *Let G be an Abelian p-group, S a Cayley subset of G such that $\langle S \rangle = G$ and $A = \mathrm{Aut\,Cay}(G, S)$. If $p^2 \nmid |A_1|$ then either S is a CI-subset, or $p \parallel |A_1|$ and S contains a coset of some subgroup of G, where A_1 is the stabilizer of* 1 *in A.*

Proof: Suppose that $|G| = p^d$. If $p \nmid |A_1|$, then G is a Sylow p-subgroup of A. By Sylow Theorem and Theorem 2.1, S is a CI-subset. Thus assume that $p \parallel |A_1|$. Let P be a Sylow p-subgroup of A containing G. Then $|P : G| = p$ and $P_1 \cong Z_p$ where P_1 is the stabilizer of 1 in P, and so P is non-Abelian, see [15, 4.4]. Assume that S is not a CI-subset of G. By Theorem 2.1, there is a $\tau \in \mathrm{Sym}(G)$ such that $G^\tau < A$ and G^τ is not conjugate to G. Let $g \in A$ such that $(G^\tau)^g < P$. Then $G^{\tau g} \neq G$ and $P \geq \langle G^{\tau g}, G\rangle > G$. Hence $P = \langle G^{\tau g}, G\rangle = G^{\tau g}G$ as $|P : G| = p$. Since any element in $G^{\tau g} \cap G$ commutes with all elements of $G^{\tau g}$ and G, we have $G^{\tau g} \cap G \leq \mathbf{Z}(\langle G^{\tau g}, G\rangle) = \mathbf{Z}(P)$. Further

$$|G^{\tau g} \cap G| = \frac{|G^{\tau g}||G|}{|G^{\tau g}G|} = \frac{p^d \cdot p^d}{p^{d+1}} = p^{d-1}.$$

Since P is non-Abelian, $G^{\tau g} \cap G = \mathbf{Z}(P)$. For any $a \in \mathbf{Z}(P)$, $P_a = P_{1^a} = P_1^a = P_1$, so P_1 fixes all vertices in $\mathbf{Z}(P)$. Now $\langle \mathbf{Z}(P), P_1\rangle$ is an Abelian subgroup of index p in P. Hence $\langle \mathbf{Z}(P), P_1\rangle \lhd P$ and $\langle \mathbf{Z}(P), P_1\rangle$ has orbits $\{x\mathbf{Z}(P) \mid x \in G\}$ on $V\Gamma = G$. Thus P_1 fixes every $x\mathbf{Z}(P)$ setwise. Moreover, $P_1 = \langle\alpha\rangle$ has an orbit O on S of length p. If $a \in O \subseteq S$, then since P_1 fixes $x\mathbf{Z}(P)$ setwise for each $x \in G$, $a^\alpha \in a\mathbf{Z}(P)$, so $a^\alpha = az$ for some $z \in \mathbf{Z}(P)$. Thus $O = a^{\langle\alpha\rangle} = \{a, az, az^2, \ldots, az^{p-1}\} = a\langle z\rangle$. Thus the proposition holds. □

This result has been generalized in [8] to general abelian groups under certain conditions. The following lemma enables us to focus our attention on connected graphs.

Lemma 4.2 *Assume that G is a homocyclic p-group and that S is a Cayley subset of G. If S is a CI-subset of $\langle S\rangle$ and for any subset T of G, Cay$(\langle T\rangle, T) \cong$ Cay$(\langle S\rangle, S)$ implies $\langle T\rangle \cong \langle S\rangle$, then S is a CI-subset of G.*

Proof: Assume that S is a CI-subset of $\langle S\rangle$ and that T is a Cayley subset of G such that $\mathrm{Cay}(\langle T\rangle, T) \cong \mathrm{Cay}(\langle S\rangle, S)$. Then $\langle T\rangle \cong^\sigma \langle S\rangle$ for some isomorphism σ from $\langle T\rangle$ to $\langle S\rangle$. Let $T' = T^\sigma$. Then $\mathrm{Cay}(\langle S\rangle, T') \cong \mathrm{Cay}(\langle T\rangle, T) \cong \mathrm{Cay}(\langle S\rangle, S)$. Since S is a CI-subset of $\langle S\rangle$, there is $\alpha \in \mathrm{Aut}(\langle S\rangle)$ such that $T'^\alpha = S$. Thus $\beta = \sigma\alpha$ is an isomorphism from $\langle T\rangle$ to $\langle S\rangle$ such that $T^\beta = (T^\sigma)^\alpha = T'^\alpha = S$. Since G is a homocyclic p-group, it is easy to show that every isomorphism between any two isomorphic subgroups of G can be extended as an automorphism of G. Let $\rho \in \mathrm{Aut}(G)$ be an extension of β. Then $T^\rho = T^\beta = S$, so S is a CI-subset of G. □

Now we can determine m-DCI p-groups for $2 \leq m \leq p + 1$.

Theorem 4.3 *Let G be a finite p-group, where p is prime. Then*
(1) *G is an m-DCI group for $2 \leq m \leq p - 1$ if and only if $p \geq 3$ and G is homocyclic*;
(2) *G is a p-DCI group if and only if G is elementary Abelian, cyclic, or $G = Q_8$*;
(3) *G is a $(p + 1)$-DCI group if and only if G is elementary Abelian, or $G = Z_4, Q_8$.*

Proof:

(1) By Lemmas 2.3 and 2.4, we only need to prove that homocyclic p-groups are m-DCI groups. Let S be a Cayley subset of G of size m. By [8, Theorem 1.1], S is a CI-subset of $\langle S\rangle$. Thus by Lemma 4.2, S is a CI-subset of G and G is an m-DCI group.

(2) By Lemmas 2.4 and 4.2, we only need to prove that elementary Abelian p-groups and cyclic p-groups are p-DCI groups. By [8, Theorem 1.1], S is a CI-subset of $\langle S\rangle$. Thus by Lemma 4.2, S is a CI-subset of G and G is a p-DCI group.

(3) By Lemmas 2.4 and 4.2, we only need to prove that elementary Abelian p-groups are $(p+1)$-DCI groups. Let $G = Z_p^d$ and let S be a Cayley subset of G such that $|S| \leq p+1$. By parts (1) and (2), we only need to consider the case where $|S| = p+1$. Since G is elementary Abelian, any two subgroups of G of the same order are isomorphic. Thus, by Lemma 4.2, we may assume that $\langle S\rangle = G$.

If $p = 2$, then by [3, Theorem 1], G is a 3-DCI group. Thus assume $p \geq 3$ in the following. Suppose first that S contains a coset aH of some subgroup H of G for some $a \in S$. Since $|S| = p + 1$, we have $|H| = p$ and $S = aH \cup \{b\}$ for some $b \in S$. If $b \in \langle aH\rangle$ then $G = \langle a, H\rangle$ is of order p^2, and thus by [6], S is a CI-subset. If $b \notin \langle aH\rangle$ then $G = \langle aH\rangle \times \langle b\rangle \cong Z_p^3$, and thus by [4], again S is a CI-subset. Suppose now that S does not contain any coset of subgroups of G. By Theorem 3.2, A_1 is faithful on S. Since $|S| = p + 1$, it follows that $p^2 \nmid |A_1|$. By Proposition 4.1, S is a CI-subset and so G is a $(p+1)$-DCI group. This completes the proof of the theorem. □

Acknowledgments

The author gratefully acknowledges the support of an Overseas Postgraduate Research Scholarship of the Australian Department of Education, Employment and Training and a University Postgraduate Award from the University of Western Australia.

References

1. L. Babai, "Isomorphism problem for a class of point-symmetric structures," *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336.
2. L. Babai and P. Frankl, "Isomorphisms of Cayley graphs I," *Colloq. Math. Soc. J. Bolyai* **18** (*Combinatorics*, Keszthely, 1976), North-Holland, Amsterdam, 1978, 35–52.
3. 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.
4. E. Dobson, "Isomorphism problem for Cayley graph of $\mathbb{Z}_p^3$," *Disc. Math.* **147** (1995), 87–94.
5. C.D. Godsil, "On the full automorphism group of a graph," *Combinatorica* **1** (1981), 243–256.
6. C.D. Godsil, "On Cayley graph isomorphisms," *Ars Combin.* **15** (1983), 231–146.
7. F. Gross, "2-automorphic 2-groups," *J. Algebra* **40** (1976), 348–353.
8. C.H. Li, "On isomorphisms of connected Cayley graphs," *Disc. Math.* **178** (1998), 109–122.
9. C.H. Li and C.E. Praeger, "On the isomorphism problem for finite Cayley graphs of bounded valency," preprint, 1997.
10. C.H. Li, C.E. Praeger, and M.Y. Xu, "Isomorphisms of finite Cayley digraphs of bounded valency," *J. Combin. Theory*, series, to appear.
11. L.A. Nowitz, "A non-Cayley-invariant Cayley graph of the elementary Abelian group of order 64," *Disc. Math.* **110** (1992), 223–228.
12. P.P. Pálfy, "Isomorphism problem for relational structures with a cyclic automorphism," *Europ. J. Combin.* **8** (1987), 35–43.
13. E.E. Shult, "On finite automorphic algebras," *Illinois J. Math.* **13** (1969), 625–653.
14. M. Suzuki, *Groups Theory II*, Spring-Verlag, New York, 1982.
15. H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.
16. M.Y. Xu, "On isomorphisms of Cayley digraphs and graphs of groups of order p^3," preprint.