BULL. AUSTRAL. MATH. SOC. 05C25
VOL. 57 (1998) [181-188]

ISOMORPHISMS OF CAYLEY DIGRAPHS OF ABELIAN GROUPS

CAI HENG LI

For a finite group G and a subset S of G with $1 \notin S$, the Cayley graph $\mathrm{Cay}(G,S)$ is the digraph with vertex set G such that (x,y) is an arc if and only if $yx^{-1} \in S$. The Cayley graph $\mathrm{Cay}(G,S)$ is called a CI-graph if, for any $T \subset G$, whenever $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ there is an element $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$. For a positive integer m, G is called an m-DCI-group if all Cayley graphs of G of valency at most m are CI-graphs; G is called a connected m-DCI-group if all connected Cayley graphs of G of valency at most m are CI-graphs. The problem of determining Abelian m-DCI-groups is a long-standing open problem. It is known from previous work that all Abelian m-DCI-groups lie in an explicitly determined class $\mathcal{ADCI}(m)$ of Abelian groups. First we reduce the problem of determining Abelian m-DCI-groups to the problem of determining whether every subgroup of a member of $\mathcal{ADCI}(m)$ is a connected m-DCI-group. Then (for a finite group G, letting p be the least prime divisor of $|G|$,) we completely classify Abelian connected $(p+1)$-DCI-groups G, and as a corollary, we completely classify Abelian m-DCI-groups G for $m \leqslant p+1$. This gives many earlier results when $p = 2$.

1. INTRODUCTION

For a finite group G and a subset S of G not containing the identity of G, the associated *Cayley graph* $\mathrm{Cay}(G,S)$ of G is the directed graph with vertex set G and arc set $\{(x,y) \mid x,y \in G,\ yx^{-1} \in S\}$. It easily follows that $\mathrm{Cay}(G,S)$ is connected if and only if $\langle S \rangle = G$.

A Cayley graph $\mathrm{Cay}(G,S)$ is called a *CI-graph* (CI stands for *Cayley Isomorphism*) if, whenever $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$ there is $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$. One long-standing open problem about Cayley graphs is to determine which Cayley graphs for a given group are CI-graphs. In this paper we study the problem for the class of Abelian groups. For a positive integer m, if all Cayley graphs of G of valency at most m are CI-graphs, then G is called an *m-DCI-group*, in particular, if G is a $|G|$-DCI-group then G is called a *DCI-group*.

Received 3rd June, 1997
The author thanks Professor Cheryl Praeger for her helpful suggestions on the work of the paper.

The problem of determining m-DCI-groups has been investigated extensively over the past 30 years, stemming from a conjecture of Ádám [1] that all finite cyclic groups were DCI-groups. This conjecture was disproved by Elspas and Turner [7]. Since then, considerable energy has been devoted to seeking cyclic DCI-groups (see Babai [3], Alspach and Parsons [2], and Godsil [11]), and very recently, a complete classification of cyclic DCI-groups was finally obtained by Muzychuk [18, 19]. Babai and Frankl in [4] investigated isomorphisms of undirected Cayley graphs of odd order and posed a conjecture that all undirected Cayley graphs of elementary Abelian groups $\mathbb{Z}_p^d$ were CI-graphs. The conjecture has been proved for the case $d = 2$ by Godsil [11] and for the case $d = 3$ by Dobson [6]. It is actually proved that $\mathbb{Z}_p^d$ for $d \leqslant 3$ are DCI-groups. However, Nowitz [20] proved that $\mathbb{Z}_2^6$ is not a DCI-group.

On the other hand, m-DCI-groups have been studied for certain small values of m. A complete classification of the Abelian m-DCI-groups for $m \leqslant 4$ is obtained by the work of [21, 8, 9, 10, 12]. Recently, it is shown in [17] that if G is an m-DCI-group for $m \geqslant 2$ then $G = U \times V$ where $(|U|, |V|) = 1$, U is an Abelian group of which all Sylow subgroups are homocyclic (namely, the direct product of cyclic groups of the same order), and V belongs to an explicitly determined list of groups. In particular, it is shown that a Sylow q-subgroup G_q of an Abelian m-DCI-group G has the following properties (or see [14, Proposition 3.3]):

(i) if $q > m$ then G_q is homocyclic;

(ii) if $q = m$ then G_q is elementary Abelian or cyclic;

(iii) if $q < m$ then G_q is elementary Abelian or $\mathbb{Z}_4$.

We use $\mathcal{ADCI}(m)$ to denote the class of all Abelian groups of which all Sylow subgroups satisfy conditions (i)–(iii). Then $\mathcal{ADCI}(m)$ contains all candidates of Abelian m-DCI-groups, and therefore, the problem of determining Abelian m-DCI-groups becomes the following problem.

PROBLEM 1.1. Determine which groups in $\mathcal{ADCI}(m)$ are m-DCI-groups.

However, this is still a very difficult problem. For example, it is even not known whether $\mathbb{Z}_p^4$ with p a prime are m-DCI-groups for arbitrary m, see for example [6]. One of the main aims of this paper is to give a reduction for Problem 1.1.

A group G is called a *connected m-DCI-group* if all connected Cayley graphs of G of valency at most m are CI-graphs. It is easily shown that if a group G is an m-DCI-group then each subgroup of G is a connected m-DCI-group (see Lemma 2.1). Conversely, we have:

THEOREM 1.2. *Let m be a positive integer, and let G be a member of $\mathcal{ADCI}(m)$. Then G is an m-DCI-group if and only if all subgroups of G are connected m-DCI-groups.*

Thus the problem of determining Abelian m-DCI-groups is further reduced to the problem of determining Abelian connected m-DCI-groups which are subgroups of a member of $\mathcal{ADCI}(m)$. There have been some investigations on connected m-DCI-groups. It follows from [5] that an Abelian group G is a connected 2-DCI-group (also see [22]). Xu and Meng [22] obtain a complete classification of Abelian connected 3-DCI-groups. Some more general results are obtained in [14, 15], and in particular, it is shown in [14] that an Abelian group G with p the smallest prime divisor of $|G|$ is a connected m-DCI-group for $m \leqslant p$ but not necessarily a connected $(p+1)$-DCI-group. The next result gives a complete classification of Abelian connected $(p+1)$-DCI-groups:

Theorem 1.3. *Let G be an Abelian group, and let p be the smallest prime divisor of $|G|$. Then G is a connected p-DCI-group. Further, let G_p be the Sylow p-subgroup of G. Then G is a connected $(p+1)$-DCI-group if and only if one of the following holds:*

(i) *G is of rank at least 3;*

(ii) *G is of rank at most 2, and either G_p is homocyclic of rank 2, or $G_p \cong \mathbb{Z}_p$ or $\mathbb{Z}_4$.*

Combining Theorem 1.2 and Theorem 1.3, we have an immediate consequence:

Corollary 1.4. *Let G be a member of $\mathcal{ADCI}(m)$, and let p be the smallest prime divisor of $|G|$. If $m \leqslant p+1$ then G is an m-DCI-group.*

Taking $p = 2$, this corollary gives the results of [21, 8, 9, 10].

2. Proof of Theorem 1.2

If $\mathrm{Cay}(G,S)$ is a CI-graph, we shall call S a *CI-subset* for convenience. We use the following two lemmas to prove Theorem 1.2.

Lemma 2.1. *Assume that G is an m-DCI-group. Then all subgroups of G are connected m-DCI-groups.*

Proof: Let H be a subgroup of G which is generated by S where $|S| \leqslant m$. Let $T \subset H$ be such that $\mathrm{Cay}(H,S) \cong \mathrm{Cay}(H,T)$. Then $\langle T\rangle = H$ and $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$. Thus there exists $\sigma \in \mathrm{Aut}(G)$ such that $S^\sigma = T$. Now $H^\sigma = \langle S^\sigma\rangle = \langle T\rangle = H$, so σ induces an automorphism of H. Hence S is a CI-subset of H, and H is a connected m-DCI-group. ∎

Lemma 2.2. *Let G be a member of $\mathcal{ADCI}(m)$. Assume that every subgroup of G is a connected m-DCI-group. Then G is an m-DCI-group.*

Proof: Let S be a subset of G of size at most m, and let $H = \langle S\rangle$. Then S is a CI-subset of H. Let T be a subset of G such that $\mathrm{Cay}(G,S) \cong \mathrm{Cay}(G,T)$, and let $K = \langle T\rangle$. Then $\mathrm{Cay}(H,S) \cong \mathrm{Cay}(\langle T\rangle,T)$. Let $A = \mathrm{Aut}\,\mathrm{Cay}(H,S)$ and $B = \mathrm{Aut}\,\mathrm{Cay}(K,T)$. Then $A = HA_1$ with $H \cap A_1 = 1$, and $B = KB_1$ with $K \cap B_1 = 1$, where A_1, B_1 is the stabiliser of 1 in A, B, respectively. Since $\mathrm{Cay}(H,S) \cong \mathrm{Cay}(K,T)$, we have that $A \cong B$

and $|H| = |K|$. Since $|S|, |T| \leqslant m$, every prime divisor of $|A_1|$ (and of $|B_1|$) is at most m (see [**16**, Lemma 2.1]). Let q be a prime of $|H|$ and H_q a Sylow q-subgroup of H, and let K_q be a Sylow q-subgroup of K. We claim that $H_q \cong K_q$. If $q > m$ then H_q is a Sylow q-subgroup of A. Since $A \cong B$, $H_q \cong K_q$. Next assume that $q \leqslant m$. Then G_q is elementary Abelian or cyclic, and so any two subgroups of G_q of the same order are isomorphic. Since $|H| = |K|$, we have $|H_q| = |K_q|$, and so $H_q \cong K_q$. Consequently, $H_q \cong K_q$ for all q dividing $|H|$ and so $H \cong K$.

Let σ be an isomorphism from K to H and let $T' = T^\sigma$. Then $\mathrm{Cay}(H, T') \cong \mathrm{Cay}(K, T) \cong \mathrm{Cay}(H, S)$. Since S is a CI-subset of H, there is $\alpha \in \mathrm{Aut}(H)$ such that $(T')^\alpha = S$. Thus $\beta := \sigma\alpha$ is an isomorphism from K to H such that $T^\beta = (T^\sigma)^\alpha = (T')^\alpha = S$. Since all Sylow subgroups of G are homocyclic, it is easy to see that there exists an automorphism ρ of G such that $\beta = \rho|_K$, the restriction of ρ to K. Therefore, $T^\rho = T^\beta = S$, and so S is a CI-subset of G. $\square$

3. Proof of Theorem 1.3

In this section we prove Theorem 1.3. For a finite group G, we use p to denote the smallest prime divisor of $|G|$. The first lemma shows that if G is an Abelian connected $(p+1)$-DCI-group of rank 2 and a Sylow p-subgroup G_p of G is noncyclic then G_p must be homocyclic.

Lemma 3.1. *Let $G = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_{k_1 p^n} \times \mathbb{Z}_{k_2 p^m}$ where $(k_1 k_2, p) = 1$ and $n > m \geqslant 1$. Then $\langle x^{k_1 p^{n-1}} \rangle y \cup \{x\}$ is a generating subset and is not a CI-subset of G.*

Proof: Set $S := \langle x^{k_1 p^{n-1}} \rangle y \cup \{x\}$, and let $T = \langle x^{k_1 p^{n-1}} \rangle x^{k_1 p^{n-m-1}} y \cup \{x\}$. Then for any integer i, $o\left(x^{i k_1 p^{n-1}} y\right) = p^m$ and $o\left(x^{i k_1 p^{n-1}} x^{k_1 p^{n-m-1}} y\right) = p^{m+1}$. It follows that $S^\sigma \neq T$ for any $\sigma \in \mathrm{Aut}(G)$. To prove that S is not a CI-subset we only need to verify that $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$. Let $z = x^{k_1 p^{n-1}}$ and $y' = x^{k_1 p^{n-m-1}} y$. Then

$$G = \bigcup_{0 \leqslant i \leqslant k_2 p^m - 1} \bigcup_{0 \leqslant j \leqslant k_1 p^{n-1} - 1} \langle z \rangle y^i x^j = \bigcup_{0 \leqslant i \leqslant k_2 p^m - 1} \bigcup_{0 \leqslant j \leqslant k_1 p^{n-1} - 1} \langle z \rangle (y')^i x^j.$$

Let ρ be the map from G to G defined as follows:

$$z^h y^i x^j \to z^h (y')^i x^j \quad \text{for } 0 \leqslant h \leqslant p-1,\ 0 \leqslant i \leqslant k_2 p^m - 1 \text{ and } 0 \leqslant j \leqslant k_1 p^{n-1} - 1.$$

A straightforward calculation shows that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Hence S is not a CI-subset of G. $\square$

The next lemma shows that if a Sylow p-subgroup of an Abelian connected $(p+1)$-DCI-group of rank at most 2 is cyclic then it must be of order p or 4.

Lemma 3.2. *Let $G = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_{k_1 p^n} \times \mathbb{Z}_{k_2}$, where $(k_1 k_2, p) = 1$, and either $p \geqslant 3$ and $n \geqslant 2$, or $p = 2$ and $n \geqslant 3$. Let*

$$S = \begin{cases} \langle x^{k_1 p^{n-1}} \rangle x \cup \{y x^{k_1 p^{n-1}}\}, & \text{if } p \geqslant 3, \\ \langle x^{k_1 2^{n-1}} \rangle x \cup \{y x^{k_1 2^{n-2}}\}, & \text{if } p = 2. \end{cases}$$

Then S is a generating subset and is not a CI-subset of G.

https://doi.org/10.1017/S0004972700031579 Published online by Cambridge University Press

PROOF: Set

$$T = \begin{cases} \langle x^{k_1 p^{n-1}} \rangle x \cup \{y^{-1} x^{-k_1 p^{n-1}}\}, & \text{if } p \geqslant 3, \\ \langle x^{k_1 2^{n-1}} \rangle x \cup \{y^{-1} x^{-k_1 2^{n-2}}\}, & \text{if } p = 2. \end{cases}$$

Let $k_0 = \begin{cases} k_1 p^{n-1}, & \text{if } p \geqslant 3 \\ k_1 2^{n-2}, & \text{if } p = 2 \end{cases}$, and let $z = x^{k_0}$. Then $G = \bigcup_{0 \leqslant i \leqslant k_2 - 1} \bigcup_{0 \leqslant j \leqslant k_0 - 1} \langle z \rangle y^i x^j$. Let ρ be the map from G to G defined as follows:

$$z^h y^i x^j \to z^{-h} y^{-i} x^j \quad \text{for } 0 \leqslant h \leqslant p-1,\ 0 \leqslant i \leqslant k_2 - 1,\ 0 \leqslant j \leqslant k_0 - 1.$$

A straightforward calculation shows that ρ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, T)$. Suppose that there exists $\alpha \in \mathrm{Aut}(G)$ sending S to T. Now $o(x) = k_1 p^n$ and $o(y^{-1} z^{-1}) = k_2 p$ or $4k_2$ for $p > 2$ or $p = 2$, respectively. Thus $x^\alpha = x^{l k_1 p^{n-1}} x$ for some integer l, and so $z^\alpha = \left(x^{k_0}\right)^\alpha = \left(x^{l k_1 p^{n-1}} x\right)^{k_0} = z$. Therefore, $\left(\langle x^{k_1 p^{n-1}} \rangle x\right)^\alpha = \langle x^{k_1 p^{n-1}} \rangle x$ and $\{yz\}^\alpha = \left(S \setminus \langle x^{k_1 p^{n-1}} \rangle x\right)^\alpha = T \setminus \langle x^{k_1 p^{n-1}} \rangle x = \{y^{-1} z^{-1}\}$ so that $z^\alpha = z^{-1}$, which is a contradiction. Hence S is not a CI-subset of G. ∎

To complete the proof of Theorem 1.3, we need the following known results.

THEOREM 3.3. ([**13**, Theorem 3.2].) *Let G be an Abelian group and S a generating subset of G. Let $\Gamma = \mathrm{Cay}(G, S)$, and let $A = \mathrm{Aut}\,\Gamma$ and A_1 the stabiliser of 1 in A. Then either A_1 is faithful on S, or S contains a coset of some subgroup of G.*

PROPOSITION 3.4. ([**14**, Proposition 4.1].) *Let G be an Abelian group, and let p be the smallest prime divisor of $|G|$. Let S be a subset of G, and let $A = \mathrm{Aut}\,\mathrm{Cay}(G, S)$ and let A_1 be the stabiliser of 1 in A. If $(|A_1|, |G|) = 1$ then S is a CI-subset; if $(|A_1|, |G|) = p$, then either S is a CI-subset, or S contains a coset of some subgroup of G.*

Now we can complete the proof of Theorem 1.3.

PROOF OF THEOREM 1.3: Suppose that G is a connected $(p+1)$-DCI-group. If G is of rank at least 3 then G is as in part (i). Thus we assume that G has rank at most 2. By Lemmas 3.1 and 3.2, either G_p is homocyclic of rank 2, or $G_p \cong \mathbb{Z}_p$ or $\mathbb{Z}_4$, as in part (ii).

Conversely, assume that G is an Abelian group with p the least prime divisor of $|G|$ which satisfies part (i) or part (ii) of the theorem. We need to prove that G is a connected $(p+1)$-DCI-group. By [**14**, Theorem 1.1 (2)], G is a connected p-DCI-group. Thus assume that S is a generating subset of G of size $p+1$ with $1 \notin S$. Let $\Gamma = \mathrm{Cay}(G, S)$ and $A = \mathrm{Aut}\,\Gamma$. If $(|G|, |A_1|) = 1$ then by Proposition 3.4, S is a CI-subset. Thus we assume that $(|G|, |A_1|) \neq 1$. We need to prove that S is a CI-subset of G. By Xu and Meng [**22**], if $p = 2$ then S is a CI-subset. Thus we further assume that $p \geqslant 3$. Suppose that S contains no coset of a nontrivial subgroup of G. Then by Theorem 3.3, A_1 is faithful on S and it follows that $(|G|, |A_1|)$ divides p, and therefore, by Proposition 3.4, S is a CI-subset. Thus we suppose that S contains a coset of some nontrivial subgroup

https://doi.org/10.1017/S0004972700031579 Published online by Cambridge University Press

of G, so we may write $S = \langle c\rangle b \cup \{a\}$ for some $a, b, c \in G$ with $\langle c\rangle \cong \mathbb{Z}_p$. In particular, G is of rank at most 3.

We claim that $\langle c\rangle b$ and $\{a\}$ are two orbits of A_1 on S. Suppose that A_1 is transitive on S. Since $b^2\langle c\rangle \subseteq \Gamma(bc^i)$ for all i, $|\Gamma(bc^i) \cap \Gamma(bc^j)| \geqslant p \geqslant 3$ for any integers i, j, and hence we have that $|\Gamma(bc^i) \cap \Gamma(a)| \geqslant 3$. It follows that there exists an integer k such that $\left(a.bc^k\right) = \left(bc^i.bc^{j'}\right)$ for some integer j'. Therefore, $a = bc^{i+j'-k} \in b\langle c\rangle$, which is a contradiction. So A_1 is not transitive on S. On the other hand, since $p \,\big|\, |A_1|$, A_1 has an orbit of length p on S. Thus A_1 has exactly 2 orbits on S, one has length p and the other has length 1. It follows since $|\Gamma(bc^i) \cap \Gamma(a)| \leqslant 2$ for each i that $\langle c\rangle b$ and $\{a\}$ are the two orbits of A_1 on S, as claimed. Consequently, A has the two orbits on arcs of Γ; one is $(1, a)^A$ and the other is $(1, b)^A$. We shall call edges of Γ in these orbits a-edges and b-edges, respectively.

Let T be a subset of G such that $\Gamma \cong \mathrm{Cay}(G, T)$. Then $\mathrm{Cay}(G, T)$ is also not arc-transitive, and S is a CI-subset if and only if T is a CI-subset. Thus, similarly, we may write $T = \langle c'\rangle b' \cup \{a'\}$ for some $a', b', c' \in G$ with $\langle c'\rangle \cong \mathbb{Z}_p$. Further, $B := \mathrm{Aut}\,\mathrm{Cay}(G, T)$ has two orbits on the arcs of $\mathrm{Cay}(G, T)$; one is $(1, a')^B$, and the other is $(1, b')^B$. We shall call edges of $\mathrm{Cay}(G, T)$ in these orbits a'-edges and b'-edges, respectively. Since G_p is homocyclic, $\langle c\rangle$ is conjugate under $\mathrm{Aut}(G)$ to $\langle c'\rangle$, so we may assume that $\langle c'\rangle = \langle c\rangle$ so that $T = \langle c\rangle b' \cup \langle a'\rangle$. Let ρ be an isomorphism from Γ to $\mathrm{Cay}(G, T)$ such that $1^\rho = 1$. Then we have that ρ maps b-edges to b'-edges and a-edges to a'-edges. In particular, $\{b, cb, \dots, c^{p-1}b\}^\rho = (\langle c\rangle b)^\rho = \langle c\rangle b' = \{b', cb', \dots, c^{p-1}b'\}$ and $a^\rho = a'$, and if $x^\rho = x'$ (inductively) then

$$(ax)^\rho = a'x', \quad (\langle c\rangle bx)^\rho = \{bx, cbx, \dots, c^{p-1}bx\}^\rho = \{b'x', cb'x', \dots, c^{p-1}b'x'\} = \langle c\rangle b'x'.$$

By induction on $i + j$, we have

$$\left(a^i\right)^\rho = a'^i, \quad \left(\langle c\rangle b^i a^j\right)^\rho = \langle c\rangle (b')^i (a')^j, \quad \text{for all integers } i, j \geqslant 0.$$

Therefore, $o(a) = o(a')$, and ρ induces an automorphism β of $\overline{G} := G/\langle c\rangle$ such that $\left(\overline{b}^i\overline{a}^j\right)^\beta = \left(\overline{b}'\right)^i(\overline{a}')^j$, in particular, $\overline{S}^\beta = \{\overline{a}, \overline{b}\}^\beta = \{\overline{a}', \overline{b}'\} = \overline{T}$, $o(\overline{a}) = o(\overline{a}')$ and $o\left(\overline{b}\right) = o\left(\overline{b}'\right)$, where "$\overline{X}$" is the image of an object X (of G) under $G \to \overline{G}$.

If G is of rank 3, then $G = \langle S\rangle = \langle c, b, a\rangle$. If $\langle c\rangle \cap \langle b, a\rangle \neq 1$ then $c \in \langle b, a\rangle$ and so $G = \langle b, a\rangle$, which is a contradiction. Thus $\langle c\rangle \cap \langle b, a\rangle = 1$, and therefore, $G = \langle c\rangle \times \langle b, a\rangle \cong \langle c\rangle \times \overline{G}$. Thus the above-defined β may be viewed as an automorphism of $\langle b, a\rangle$ so that $(b, a)^\beta = (b', a')$. Let $\tau = (\varepsilon, \beta) \in \mathrm{Aut}(\langle c\rangle) \times \mathrm{Aut}(\langle b, a\rangle) \leqslant \mathrm{Aut}(G)$ where ε denotes the identity of $\mathrm{Aut}(\langle c\rangle)$. Then $S^\tau = (\langle c\rangle b \cup \{a\})^\tau = \langle c\rangle b' \cup \{a'\} = T$, so S is a CI-subset.

Thus we suppose that G is of rank at most 2 in the following. Let G_p be the Sylow p-subgroup and $G_{p'}$ the Hall p'-subgroup of G. Write $a = a_p a_{p'}$ and $b = b_p b_{p'}$ such that $a_p, b_p \in G_p$ and $a_{p'}, b_{p'} \in G_{p'}$, and write $a' = a'_p a'_{p'}$ and $b' = b'_p b'_{p'}$ such that $a'_p, b'_p \in G_p$ and $a'_{p'}, b'_{p'} \in G_{p'}$. Then $\overline{a}_p^\beta = \overline{a}'_p$ and $\overline{b}_p^\beta = \overline{b}'_p$. On the other hand, since $\overline{G}_{p'}^\beta = \overline{G}_{p'}$, β induces an automorphism β' of $\overline{G}_{p'}$, and since $\overline{G}_{p'} \cong G_{p'}$, β' may be viewed as an automorphism of $G_{p'}$. Thus $a_{p'}^{\beta'} = a'_{p'}$ and $b_{p'}^{\beta'} = b'_{p'}$.

Assume first that $G_p \cong \mathbb{Z}_p$. Then $G = \langle c\rangle \times G_{p'}$, and $b_p, b'_p \in \langle c\rangle$ and so $\langle c\rangle b = \langle c\rangle b_{p'}$ and $\langle c\rangle b' = \langle c\rangle b'_{p'}$. Let $\tau = (\alpha, \beta') \in \mathrm{Aut}(\langle c\rangle) \times \mathrm{Aut}(\langle b, a\rangle) \leqslant \mathrm{Aut}(G)$ such that $a_p^\alpha = a'_p$. Then

$$\begin{aligned} S^\tau &= (\langle c\rangle b \cup \{a\})^{(\alpha,\beta')} = (\langle c\rangle b_{p'} \cup \{a_p a_{p'}\})^{(\alpha,\beta')} \\ &= \langle c\rangle b_{p'}^{\beta'} \cup \{a_p^\alpha a_{p'}^{\beta'}\} = \langle c\rangle b'_{p'} \cup \{a'_p a'_{p'}\} = \langle c\rangle b' \cup \{a'\} = T. \end{aligned}$$

Thus S is a CI-subset.

Assume secondly that $G_p \cong \mathbb{Z}_p^2$. Then either $G_p = \langle a_p, c\rangle = \langle a'_p, c\rangle$, or $a = a_{p'}$, $a' = a'_{p'}$ and $G_p = \langle b_p, c\rangle = \langle b'_p, c\rangle$. First suppose that $G_p = \langle a_p, c\rangle = \langle a'_p, c\rangle$. Then $b_p = c^i a_p^j$ for some integers i, j, so $\overline{b}_p = \overline{a}_p^j$. Now $\overline{b}'_p = \overline{b}_p^\beta = \left(\overline{a}_p^j\right)^\beta = \left(\overline{a}'_p\right)^j$, so $b'_p = c^k\left(a'_p\right)^j$ for some integer k. Consequently, $\langle c\rangle b = \langle c\rangle b_p b_{p'} = \langle c\rangle c^i a_p^j b_{p'} = \langle c\rangle a_p^j b_{p'}$ and $\langle c\rangle b' = \langle c\rangle b'_p b'_{p'} = \langle c\rangle c^k\left(a'_p\right)^j b'_p = \langle c\rangle\left(a'_p\right)^j b'_{p'}$. Let $\tau = (\alpha, \beta') \in \mathrm{Aut}(G_p) \times \mathrm{Aut}(G_{p'}) \leqslant \mathrm{Aut}(G)$ such that $a_p^\alpha = a'_p$ and $c^\alpha = c$. Then

$$\begin{aligned} S^\tau &= (\langle c\rangle b \cup \{a\})^\tau = \left(\langle c\rangle a_p^j b_{p'} \cup \{a_p a_{p'}\}\right)^{(\alpha,\beta')} \\ &= \left(\langle c\rangle a_p^j\right)^\alpha b_{p'}^{\beta'} \cup \{a_p^\alpha a_{p'}^{\beta'}\} = \langle c\rangle\left(a'_p\right)^j b'_{p'} \cup \{a'_p a'_{p'}\} = \langle c\rangle b' \cup \{a'\} = T. \end{aligned}$$

Therefore, S is a CI-subset. Now suppose that $a = a_{p'}$, $a' = a'_{p'}$ and $G_p = \langle b_p, c\rangle = \langle b'_p, c\rangle$. Let $\tau = (\alpha, \beta') \in \mathrm{Aut}(G_p) \times \mathrm{Aut}(G_{p'}) \leqslant \mathrm{Aut}(G)$ such that $b_p^\alpha = b'_p$ and $c^\alpha = c$. Then

$$\begin{aligned} S^\tau &= (\langle c\rangle b \cup \{a\})^\tau = (\langle c\rangle b_p b_{p'} \cup \{a_{p'}\})^{(\alpha,\beta')} \\ &= (\langle c\rangle b_p)^\alpha b_{p'}^{\beta'} \cup \{a_{p'}^{\beta'}\} = \langle c\rangle b'_p b'_{p'} \cup \{a'_{p'}\} = \langle c\rangle b' \cup \{a'\} = T. \end{aligned}$$

Therefore, S is a CI-subset.

Assume, finally, that G_p is not elementary Abelian so that $G_p = \langle g_1\rangle \times \langle g_2\rangle \cong \mathbb{Z}_{p^n}^2$ with $n \geqslant 2$. Then $G_p = \langle b_p, a_p\rangle = \langle b'_p, a'_p\rangle$. Let τ be the map τ from G to G defined as follows:

$$\left(b^i a^j\right)^\tau = b'^i a'^j \quad \text{for all integers } i \text{ and } j.$$

Then τ induces the automorphism β of $G/\langle c\rangle$ defined before. In particular, β' (defined before) is the restriction of τ to $G_{p'}$. On the other hand, since G_p is of rank 2, τ induces an automorphism α of G_p. Therefore, $\tau = (\alpha, \beta')$ is an automorphism of G, and $\langle c\rangle^\tau = \overline{1}^\beta = \overline{1} = \langle c\rangle$ where $\overline{1}$ is the identity of $\overline{G}$. Consequently, we have that

$$S^\tau = (\langle c\rangle b \cup \{a\})^\tau = \langle c^\tau\rangle b^\tau \cup \{a^\tau\} = \langle c\rangle b' \cup \{a'\} = T.$$

Thus S is a CI-subset. This completes the proof of the theorem. $\square$

Combining Theorem 1.2 and Theorem 1.3, we can easily prove Corollary 1.4.

Proof of Corollary 1.4: Assume that G is a member of $\mathcal{ADCI}(m)$ with p the smallest prime divisor of $|G|$. Let S be a subset of G of size $m \leqslant p+1$. By Theorem 1.3, S is a CI-subset of $\langle S\rangle$, and so by Theorem 1.2, S is a CI-subset of G. Therefore, G is an m-DCI-group. $\square$

https://doi.org/10.1017/S0004972700031579 Published online by Cambridge University Press

References

[1] A. Adám, 'Research problem 2-10', *J. Combin. Theory* **2** (1967), 309.

[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. Hungary* **29** (1977), 329–336.

[4] L. Babai and P. Frankl, 'Isomorphisms of Cayley graphs I', *Colloq. Math. Soc. János Bolyai* **18** (1978), 35–52.

[5] C. Delorme, O. Favaron and M. Maheo, 'Isomorphisms of Cayley multigraphs of degree 4 on finite Abelian groups', *European J. Combin.* **13** (1992), 59–61.

[6] E. Dobson, 'Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$', *Discrete Math.* **147** (1995), 87–94.

[7] B. Elspas and J. Turner, 'Graphs with circulant adjacency matrices', *J. Combin. Theory* **9** (1970), 297–307.

[8] X.G. Fang, 'A characterization of finite Abelian 2-DCI groups', (in Chinese), *J. Math. (Wuhan)* **8** (1988), 315–317.

[9] X.G. Fang, 'Abelian 3-DCI groups', *Ars Combin.* **32** (1992), 263–267.

[10] X.G. Fang and M.Y. Xu, 'Abelian 3-DCI groups of odd order', *Ars Combin.* **28** (1988), 247–251.

[11] C.D. Godsil, 'On Cayley graph isomorphisms', *Ars Combin.* **15** (1983), 231–246.

[12] C.H. Li, 'Abelian 4-DCI groups', *J. Yunnan Normal University* **11** (1991), 24–27.

[13] C.H. Li, 'On Cayley graphs of Abelian groups', *J. Algebraic Combin.* (to appear).

[14] C.H. Li, 'On isomorphisms of connected Cayley graphs', *Discrete Math.* (to appear).

[15] C.H. Li, 'Isomorphisms of connected Cayley digraphs', *Graphs Combin.* (to appear).

[16] C.H. Li, 'The cyclic groups with the m-DCI property', *European J. Combin.* **18** (1997), 655–665.

[17] C.H. Li, C.E. Praeger and M.Y. Xu, 'Isomorphisms of finite Cayley digraphs of bounded valency', *J. Combin. Theory Ser. B* (to appear).

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

[19] M. Muzychuk, 'On Ádám's conjecture for circulant graphs', *Discrete Math.* **167/168** (1997), 497–510.

[20] L.A. Nowitz, 'A nonCayley-invariant Cayley graph of the elementary Abelian group of order 64', *Discrete Math.* **110** (1992), 223–228.

[21] L. Sun, 'Isomorphisms of circulant graphs', *Chinese Ann. Math. Ser. A* **9** (1988), 567–574.

[22] M.Y. Xu and J. Meng, 'Weakly 3-DCI Abelian groups', *Austral. J. Combin.* **13** (1996), 49–60.

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