Cyclic m-DCI-groups and m-CI-groups[*]

István Kovács[†] ⬤, Luka Šinkovec[‡]

UP IAM, University of Primorska, Muzejski trg 2 and
UP FAMNIT, University of Primorska, Glagoljaška ulica 8, SI-6000 Koper, Slovenia

Abstract

Based on the earlier work of Li from 1997 and Dobson from 2008, in this paper we complete the classification of cyclic m-DCI-groups and m-CI-groups. For a positive integer m such that $m \geq 3$, we show that the group $\mathbb{Z}_n$ is an m-DCI-group if and only if n is not divisible by 8 nor by p^2 for any odd prime $p < m$. Furthermore, if $m \geq 6$, then we show that $\mathbb{Z}_n$ is an m-CI-group if and only if either $n \in \{8, 9, 18\}$, or $n \notin \{8, 9, 18\}$ and n is not divisible by 8 nor by p^2 for any odd prime $p < \frac{m-1}{2}$.

Keywords: Cayley graph, cyclic group, m-CI-group, m-DCI-group.

Math. Subj. Class.: 05C25, 20B25

1 Introduction

Let G be a finite group and $S \subset G$ be a subset not containing the identity element of G. The *Cayley digraph* $\mathrm{Cay}(G, S)$ is defined to have vertex set G and arcs in the form (g, sg), where $g \in G$ and $s \in S$. In the case when S is also inverse-closed, i.e., for every $x \in S$, $x^{-1} \in S$, the pair of arcs (g, sg) and (sg, g) can be identified with the undirected edge $\{g, sg\}$, in which case $\mathrm{Cay}(G, S)$ is regarded as an undirected graph and referred to as a *Cayley graph*. Every automorphism $\sigma \in \mathrm{Aut}(G)$ induces an isomorphism between the (di)graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G, S^\alpha)$, in which case σ is called a *Cayley isomorphism*. The converse is not true in general, examples of Cayley (di)graphs are known which are isomorphic but there exists no Cayley isomorphism mapping one onto

the other. A (di)graph $\mathrm{Cay}(G, S)$ is called a *CI-(di)graph* if for any $\mathrm{Cay}(G, T)$, whenever $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$, we have $S^\sigma = T$ for some $\sigma \in \mathrm{Aut}(G)$. For a positive integer m, the group G has the *m-DCI-property* (*m-CI-property*, resp.) if all Cayley digraphs (Cayley graphs, resp.) on G of valency m are CI-digraphs (CI-graphs, resp.) (see [11, Definition 1.1]). By the valency of a Cayley digraph $\mathrm{Cay}(G, S)$ we mean its in-valency, which is equal to the cardinality $|S|$ and coincides with its out-valency. Furthermore, G is called an *m-(D)CI-group* if it has the i-(D)CI property for every $i \leq m$ and a *D(CI)-group* when it has the i-(D)CI property for every positive integer i.

The study of finite groups with the m-(D)CI property was initiated by Li et al. [11]. Both properties attracted considerable attention in the late 90's, in particular, it was shown that the finite m-DCI-groups belong to a relatively restricted list of groups, and a similar list was also derived containing the finite m-CI-groups. For the results from this period, we refer to the survey paper [10].

In this paper, we aim to complete the classification of cyclic m-DCI- and m-CI-groups. We review next the known results. In 1967, Ádám [1] made a conjecture stating that every cyclic group is a DCI-group. This conjecture was shown to be false soon after it has been published and remarkably, the question as to which cyclic groups are DCI-groups was answered only 30 years later by Muzychuk [12].

Theorem 1.1 ([12])**.**

(1) *The group $\mathbb{Z}_n$ is a DCI-group if and only if $n = k$ or $2k$, where k is square-free.*

(2) *The group $\mathbb{Z}_n$ is a CI-group if and only if either $n \in \{8, 9, 18\}$, or $n = k$ or $2k$, where k is square-free.*

A few papers were devoted to cyclic m-(D)CI-groups for small m (see [3, 4, 7, 8, 14, 15, 16]), in particular, Sun [14] showed that every cyclic group is a 2-DCI-group and Li [8] showed that every cyclic group is a 5-CI-group. At this point we would like to emphasize the difference between the m-DCI- and the m-CI-property for cyclic groups, which lies in the fact that by the former property one concerns digraphs, whereas by the latter property one concerns only undirected graphs. For example, it is known that $\mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\})$ is not a CI-digraph [6], showing that $\mathbb{Z}_8$ does not have the 3-DCI-property. On the other hand, as $\mathbb{Z}_n$ is a 5-CI-group for every n, $\mathbb{Z}_8$ has the 3-CI-property (this can be easily checked by simply looking at the possible Cayley graphs on $\mathbb{Z}_8$ of valency 3).

In [9], Li determined the positive integers m for which $\mathbb{Z}_{p^2}$ has the m-DCI-property. The following result was also shown, we present it here as it is stated in [10, Theorem 7.2].

Theorem 1.2 ([10])**.** *Let G be a cyclic group, and let G_p be the Sylow p-subgroup of G. Suppose that G has the m-DCI-property. If $|G|$ is not a prime-square and $p + 1 \leq m \leq (|G| - 1)/2$, then $G_p \cong \mathbb{Z}_p$ or $\mathbb{Z}_4$.*

The above theorem provides necessary conditions for a cyclic group to be an m-DCI-group, but it does not yield the complete classification of cyclic m-DCI-groups. In his survey, Li wrote (see [10, page 319]):

'A natural question is, for a positive integer m, which cyclic groups are m-DCI-groups, and which cyclic groups are m-CI-groups?'

Motivated by Theorem 1.2, he also proposed a conjecture, which contains sufficient conditions for a cyclic group to be an m-DCI- and m-CI-group, respectively (see [10, Conjecture 7.3]). This conjecture was proved later by Dobson [5] and it reads as follows.

Theorem 1.3 ([5])**.** *Let $n = n_1 n_2 \in \mathbb{N}$ such that $\gcd(n_1, n_2) = 1$ and n_1 divides $4k$, where k is odd and square-free.*

(1) *If $p > m$ for every prime divisor p of n_2, then $\mathbb{Z}_n$ is an m-DCI-group.*

(2) *If $p > 2m$ for every prime divisor p of n_2, then $\mathbb{Z}_n$ is a $2m$-CI-group.*

However, it turns out that in order to classify the cyclic m-DCI- and m-CI-groups, the sufficient conditions in Theorem 1.3 need to be strengthened. Our main result is the following generalization.

Theorem 1.4. *Let $n = n_1 n_2 \in \mathbb{N}$ such that $\gcd(n_1, n_2) = 1$ and n_1 divides $4k$, where k is odd and square-free.*

(1) *If $p \geq m$ for every prime divisor p of n_2, then $\mathbb{Z}_n$ is an m-DCI-group.*

(2) *If $2p + 1 \geq m$ for every prime divisor p of n_2, then $\mathbb{Z}_n$ is an m-CI-group.*

Combining these stronger sufficient conditions with the known necessary conditions, we complete the classification of cyclic m-DCI- and m-CI-groups.

Theorem 1.5.

(1) *If $m \in \mathbb{N}$ and $m \geq 3$, then the group $\mathbb{Z}_n$ is an m-DCI-group if and only if n is not divisible by 8 nor by p^2 for any odd prime $p < m$.*

(2) *If $m \in \mathbb{N}$ and $m \geq 6$, then the group $\mathbb{Z}_n$ is an m-CI-group if and only if either $n \in \{8, 9, 18\}$, or $n \notin \{8, 9, 18\}$ and it is not divisible by 8 nor by p^2 for any odd prime $p < \frac{m-1}{2}$.*

Remark 1.6. The necessity part of Theorem 1.5 follows directly from known constructions of non-CI-digraphs and graphs discovered in [2, 6, 11]. All these examples will appear in the course of the proof of Theorem 1.5.

Remark 1.7. Comparing Theorem 1.5 with the classification of cyclic DCI- and CI-groups given in Theorem 1.1, we obtain that the group $\mathbb{Z}_n$ is an m-DCI-group for $m \geq 3$ but not a DCI-group if there exist a prime p such that $p \geq m$ and $p^2 \mid n$; and also that $\mathbb{Z}_n$ is an m-CI-group for $m \geq 6$ but not a CI-group if $n \notin \{8, 9, 18\}$, and there exists a prime p such that $p \geq (m-1)/2$ and $p^2 \mid n$.

Dobson [5] obtained Theorem 1.3 using permutation group theoretical techniques. Our proof of Theorem 1.4 is independent, it relies on a necessary and sufficient criterion for two circulant digraphs to be isomorphic due to Muzychuk [13]. In the next section we give a short overview of Muzychuk's criterion, Theorems 1.4 and 1.5 will then be derived in Section 3.

2   Isomorphic circulant digraphs

2.1   Key spaces

For $n \in \mathbb{N}$, we use the symbol $[n]$ to denote the set $\{1, \ldots, n\}$. Let $n = p_1^{t_1} \cdots p_l^{t_l}$ be the prime decomposition of n. In what follows, $\mathbb{Z}_n$ will be identified with the direct sum $\mathbb{Z}_{p_1^{t_1}} \oplus \cdots \oplus \mathbb{Z}_{p_l^{t_l}}$. Therefore, an element $x \in \mathbb{Z}_n$ will also be represented as the l-tuple $x = (x_1, \ldots, x_l)$, where $x_i \in \mathbb{Z}_{p_i^{t_i}}$ for every $i \in [l]$.

Definition 2.1. The *key space* $\mathbf{K}_n$ is the direct product

$$\mathbf{K}_n := \mathbf{K}_{p_1^{t_1}} \times \cdots \times \mathbf{K}_{p_l^{t_l}},$$

where for a prime power p^t, $t \geq 1$, $\mathbf{K}_{p^t}$ consists of the t-tuples $(k_1, \ldots, k_t) \in \mathbb{N}_0^t$ such that,

- $\forall i \in [t]$, $0 \leq k_i < i$,

- $\forall i \in [t-1]$, $k_i \leq k_{i+1}$.

The elements of $\mathbf{K}_n$ are called *keys*. Thus a key $\mathbf{k} \in \mathbf{K}_n$ is a two-dimensional integer array, which will be written as

$$\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_l) = (k_{ij})_{i \in [l], j \in [t_i]},$$

where $\mathbf{k}_i = (k_{i1}, \ldots, k_{it_i}) \in \mathbf{K}_{p_i^{t_i}}$.

The *zero key* $\mathbf{z}$ in $\mathbf{K}_n$ is defined as $\mathbf{z} = (z_{ij})_{i \in [l], j \in [t_i]}$ with $z_{ij} = 0$ for every $i \in [l], j \in [t_i]$. If $n \equiv 4 \pmod 8$, then the *almost zero key* $\mathbf{z}_*$ in $\mathbf{K}_n$ is defined as $\mathbf{z}_* = (z_{ij})_{i \in [l], j \in [t_i]}$ with

$$z_{ij} = \begin{cases} 1 & \text{if } p_i^{t_i} = 4 \text{ and } j = 2, \\ 0 & \text{otherwise.} \end{cases}$$

For two keys $\mathbf{k}, \mathbf{m} \in \mathbf{K}_n$, we write $\mathbf{k} \leq \mathbf{m}$ if $k_{ij} \leq m_{ij}$, for every $i \in [l]$ and $j \in [t_i]$. The relation $\leq$ is a partial order on $\mathbf{K}_n$. The poset $(\mathbf{K}_n, \leq)$ is a lattice with meet $\wedge$ and join $\vee$ operations defined as

$$\forall i \in [l], \ \forall j \in [t_i], \ (\mathbf{k} \wedge \mathbf{m})_{ij} = \min(k_{ij}, m_{ij}) \text{ and } (\mathbf{k} \vee \mathbf{m})_{ij} = \max(k_{ij}, m_{ij}).$$

2.2   Key partitions

The set of all partitions of $\mathbb{Z}_n$ will be denoted by $\mathrm{Part}(\mathbb{Z}_n)$. For two partitions $\Sigma, \Delta \in \mathrm{Part}(\mathbb{Z}_n)$, Δ is said to be a *refinement* of Σ, denoted by $\Sigma \sqsubseteq \Delta$, if every class of Σ is union of classes of Δ. The relation $\sqsubseteq$ is a partial order on $\mathrm{Part}(\mathbb{Z}_n)$. The poset $(\mathrm{Part}(\mathbb{Z}_n), \sqsubseteq)$ is a lattice. We write $\Sigma \wedge \Delta$ for the meet and $\Sigma \vee \Delta$ for the join of the partitions Σ and Δ.

Definition 2.2. Let $n = p^t$ for a prime p and let $\mathbf{k} = (k_1, \ldots, k_t) \in \mathbf{K}_{p^t}$. The *key partition* $\Sigma(\mathbf{k})$ is the partition of $\mathbb{Z}_{p^t}$ defined as

$$\Sigma(\mathbf{k}) = \big\{\{0\}\big\} \cup \big\{ P_{k_{\alpha(x)}} + x \mid x \in \mathbb{Z}_{p^t} \setminus \{0\} \big\},$$

where for $x \in \mathbb{Z}_{p^t} \setminus \{0\}$, $\alpha(x)$ is the number in $[t]$ defined by the property that $p^{\alpha(x)}$ is the order of x as an element in the group $(\mathbb{Z}_{p^t}, +)$; and for $j \in \{0, 1, \ldots, t\}$, P_j is the subgroup of $\mathbb{Z}_{p^t}$ of order p^j.

Definition 2.3. Let $n \in \mathbb{N}$ be a number greater than 1 with prime decomposition $n = p_1^{t_1} \cdots p_l^{t_l}$ and let $\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_l) \in \mathbf{K}_n$. Then the *key partition* $\Sigma(\mathbf{k})$ is the partition of $\mathbb{Z}_n$ defined as

$$\Sigma(\mathbf{k}) = \big\{ (S_1, \ldots, S_l) \mid S_i \in \Sigma(\mathbf{k}_i), i \in [l] \big\}.$$

Proposition 2.4 ([13, Proposition 2.2]). *Let $n \in \mathbb{N}$ and $\mathbf{k}, \mathbf{m} \in \mathbf{K}_n$. If $\mathbf{k} \leq \mathbf{m}$ then $\Sigma(\mathbf{m}) \sqsubseteq \Sigma(\mathbf{k})$.*

Definition 2.5. Let $n \in \mathbb{N}$ and let $\Pi \in \text{Part}(\mathbb{Z}_n)$ be an arbitrary partition of $\mathbb{Z}_n$. The *key partition of* Π is the coarsest key partition $\Sigma(\mathbf{m})$ that refines Π; or more formally,

- $\Pi \sqsubseteq \Sigma(\mathbf{m})$.

- If $\Pi \sqsubseteq \Sigma(\mathbf{k})$ for some $\mathbf{k} \in \mathbf{K}_n$, then $\Sigma(\mathbf{m}) \sqsubseteq \Sigma(\mathbf{k})$.

The above key $\mathbf{m}$ is referred to as the *key of* Π.

Definition 2.6. Let $n \in \mathbb{N}$ and S be a nonempty subset of $\mathbb{Z}_n$. The *key of* S, denoted by $\mathbf{k}(S)$, is the key of the partition $\{S, \mathbb{Z}_n \setminus S\}$.

2.3 Generalized multipliers

We consider first the generalized multipliers of cyclic groups of prime power order.

Definition 2.7. Let $p \in \mathbb{N}$ be a prime and $t \in \mathbb{N}$. A *generalized multiplier* of $\mathbb{Z}_{p^t}$ is a t-tuple $\vec{m} = (m_1, \ldots, m_t) \in \mathbb{N}^t$ such that $\gcd(m_i, p) = 1$ for every $i \in [t]$.

The set of all generalized multipliers of $\mathbb{Z}_{p^t}$ is denoted by $\mathbb{Z}_{p^t}^{**}$. We associate next a permutation of $\mathbb{Z}_{p^t}$ with any generalized multiplier in $\mathbb{Z}_{p^t}^{**}$.

Definition 2.8. Let $p \in \mathbb{N}$ be a prime and $t \in \mathbb{N}$. For $\vec{m} = (m_1, \ldots, m_t) \in \mathbb{Z}_{p^t}^{**}$, the *generalized multiplier function* $f_{\vec{m}}$ is the permutation of $\mathbb{Z}_{p^t}$, defined as

$$\forall x \in \mathbb{Z}_{p^t}, \ x^{f_{\vec{m}}} = \sum_{i=0}^{t-1} m_{t-i} x_i p^i \ (\text{mod } p^t),$$

where $\sum_{i=0}^{t-1} x_i p^i$ is the p-adic decomposition of x, i.e., $x_i \in \{0, \ldots, p-1\}$ for every $i \in \{0, \ldots, t-1\}$.

It follows from the above definition that, if $\vec{m} = (m_1, \ldots, m_t)$ and $\vec{m'} = (m_1', \ldots, m_t')$ are two generalized multipliers of $\mathbb{Z}_{p^t}$ such that

$$\forall i \in [t], \ m_i \equiv m_i' \ (\text{mod } p^i),$$

then $f_{\vec{m}} = f_{\vec{m'}}$. Thus, to have all generalized multiplier functions, it is sufficient to consider only those generalized multipliers $\vec{m} = (m_1, \ldots, m_t)$, which satisfy $m_i \in [p^i - 1]$ for every $i \in [t]$.

Fix a key $\mathbf{k} \in \mathbf{K}_{p^t}$. We define a subset $\mathbb{Z}_{p^t}^{**}(\mathbf{k}) \subseteq \mathbb{Z}_{p^t}^{**}$ as follows. If $t > 1$, then let

$$\mathbb{Z}_{p^t}^{**}(\mathbf{k}) = \left\{ (m_1, \ldots, m_t) \in \mathbb{Z}_{p^t}^{**} \mid \forall i \in [t-1], \ m_{i+1} \equiv m_i \ (\text{mod } p^{i-k_{i+1}}) \right\};$$

and if $t = 1$, then let $\mathbb{Z}_p^{**}(\mathbf{k}) = \mathbb{Z}_p^{**}$.

A $\Sigma(\mathbf{k})$-class different from $\{0\}$ is in the form $P_{k_i} + x$, where P_{k_i} is the subgroup of $\mathbb{Z}_{p^t}$ of order p^{k_i}, and x is a non-zero element of order p^i in $(\mathbb{Z}_{p^t}, +)$. It is easy to see that for every $\vec{m} = (m_1, \ldots, m_t) \in \mathbb{Z}_{p^t}^{**}(\mathbf{k})$, $x^{f_{\vec{m}}}$ has order p^i, and

$$(P_{k_i} + x)^{f_{\vec{m}}} = P_{k_i} + x^{f_{\vec{m}}}.$$

These show that $f_{\vec{m}}$ induces a permutation of $\Sigma(\mathbf{k})$. Furthermore, one can show that, if $\vec{m}' = (m_1', \ldots, m_t')$ is another generalized multiplier from $\mathbb{Z}_{p^t}^{**}(\mathbf{k})$ such that $m_i' \equiv m_i$ (mod p^{i-k_i}), then $(P_{k_i} + x)^{f_{\vec{m}}} = (P_{k_i} + x)^{f_{\vec{m}'}}$. In view of this, to have all permutations of $\Sigma(\mathbf{k})$ induced by the generalized multipliers in $\mathbb{Z}_{p^t}^{**}(\mathbf{k})$, it suffices to consider only those generalized multipliers $\vec{m} = (m_1, \ldots, m_t) \in \mathbb{Z}_{p^t}^{**}(\mathbf{k})$, which satisfy $m_i \in [p^{i-k_i} - 1]$ for every $i \in [t]$. We refer to the latter generalized multipliers as *genuine* and denote their set by $\mathbb{Z}_{p^t}^{**}(\mathbf{k})^{\circ}$. More formally,

$$\mathbb{Z}_{p^t}^{**}(\mathbf{k})^{\circ} = \left\{ (m_1, \ldots, m_t) \in \mathbb{Z}_{p^t}^{**}(\mathbf{k}) \mid \forall i \in [t],\ m_i \in [p^{i-k_i} - 1] \right\}.$$

Let $n \in \mathbb{N}$ be an arbitrary number with prime decomposition $n = p_1^{t_1} \cdots p_l^{t_l}$, and let $\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_l) \in \mathbf{K}_n$ be an arbitrary key. The above concepts are generalized to $\mathbb{Z}_n$ as follows:

$$\mathbb{Z}_n^{**} = \mathbb{Z}_{p_1^{t_1}}^{**} \times \cdots \times \mathbb{Z}_{p_l^{t_l}}^{**},$$
$$\mathbb{Z}_n^{**}(\mathbf{k}) = \mathbb{Z}_{p_1^{t_1}}^{**}(\mathbf{k}_1) \times \cdots \times \mathbb{Z}_{p_l^{t_l}}^{**}(\mathbf{k}_l),$$
$$\mathbb{Z}_n^{**}(\mathbf{k})^{\circ} = \mathbb{Z}_{p_1^{t_1}}^{**}(\mathbf{k}_1)^{\circ} \times \cdots \times \mathbb{Z}_{p_l^{t_l}}^{**}(\mathbf{k}_l)^{\circ}.$$

For $\vec{m} = (\vec{m}_1, \ldots, \vec{m}_t) \in \mathbb{Z}_n^{**}$, the generalized multiplier function $f_{\vec{m}}$ is the permutation of $\mathbb{Z}_n$ acting as

$$\forall (x_1, \ldots, x_l) \in \mathbb{Z}_n,\ (x_1, \ldots, x_l)^{f_{\vec{m}}} = \left(x_1^{f_{\vec{m}_1}}, \ldots, x_l^{f_{\vec{m}_l}} \right).$$

Definition 2.9. Let $n \in \mathbb{N}$ and let $\mathbf{k} \in \mathbf{K}_n$. The *solving set* $P(\mathbf{k})$ is the following set of permutations of $\mathbb{Z}_n$:

$$P(\mathbf{k}) = \{ f_{\vec{m}} \mid \vec{m} \in \mathbb{Z}_n^{**}(\mathbf{k})^{\circ} \}.$$

The example below is meant to illustrate all the concepts introduced in this section.

Example 2.10. We determine below the solving sets $P(\mathbf{k})$, where $\mathbf{k} \in \mathbf{K}_{p^2}$ and p is a fixed prime.

Due to Definition 2.1, $\mathbf{K}_{p^2}$ consists of two keys: $(0, 0)$ and $(0, 1)$. Let $\vec{m} = (m_1, m_2) \in \mathbb{Z}_{p^2}^{**}((0, i))^{\circ}$, where $i \in \{0, 1\}$. Then

$$m_1 \in [p - 1],\ m_2 \in [p^{2-i} - 1],\ \gcd(m_2, p) = 1 \text{ and } m_2 \equiv m_1 \pmod{p^{1-i}}.$$

Due to Definition 2.8, $(x_0 + x_1 p)^{f_{\vec{m}}} = m_2 x_0 + m_1 x_1 p$. Note that, if $i = 0$, then m_1 is uniquely determined by m_2. Moreover, $m_1 p \equiv m_2 p \pmod{p^2}$, and hence we have $(x_0 + x_1 p)^{f_{\vec{m}}} = m_2(x_0 + x_1 p)$. We conclude that

$$P((0,0)) = \left\{ x \mapsto mx \mid m \in [p^2 - 1], \gcd(m, p) = 1 \right\} = \mathrm{Aut}(\mathbb{Z}_{p^2}),$$
$$P((0,1)) = \left\{ x_0 + x_1 p \mapsto m_2 x_0 + m_1 x_1 p \mid m_1, m_2 \in [p - 1] \right\}. \tag{2.1}$$

$\square$

In the next lemma we generalize the above example to solving sets $P(\mathbf{z})$, where $\mathbf{z}$ is the zero key in $\mathbf{K}_{p^t}$, i.e., $\mathbf{z} = (0, \ldots, 0)$.

Lemma 2.11. *Let p be a prime and $t \in \mathbb{N}$. For the zero key $\mathbf{z} \in \mathbf{K}_{p^t}$, $P(\mathbf{z}) = \mathrm{Aut}(\mathbb{Z}_{p^t})$.*

Proof. Let $f_{\vec{m}} \in P(\mathbf{z})$, where $\vec{m} = (m_1, \ldots, m_t) \in \mathbb{Z}_{p^t}^{**}(\mathbf{z})^\circ$. Note that, for every $i \in [t], m_i \in [p^i - 1]$ and $\gcd(m_i, p) = 1$. We are going to show that $x^{f_{\vec{m}}} \equiv m_t x \pmod{p^t}$ holds for every $x \in \mathbb{Z}_{p^t}$.

Fix an arbitrary $x \in \mathbb{Z}_{p^t}$ and let $x = \sum_{i=0}^{t-1} x_i p^i$ be its p-adic decomposition. Due to Definition 2.8,

$$x^{f_{\vec{m}}} = m_t x_0 + m_{t-1} x_1 p + \cdots + m_1 x_{t-1} p^{t-1}. \tag{2.2}$$

On the other hand, it follows from the definition of $\mathbb{Z}_{p^t}^{**}(\mathbf{z})^\circ$ that,

$$\forall i \in [t-1], \ m_{i+1} \equiv m_i \pmod{p^i}.$$

This yields

$$\forall i \in [t], \ m_t \equiv m_i \pmod{p^i}.$$

Thus, $m_t p^{t-i} \equiv m_i p^{t-i} \pmod{p^t}$ for every $i \in [t]$, and then substituting this in (2.2), we obtain that $x^{f_{\vec{m}}} \equiv m_t x \pmod{p^t}$, as required. □

2.4 Muzychuk's criterion

Now we are prepared to present Muzychuk's criterion for two circulant digraphs to be isomorphic.

Theorem 2.12 ([13]). *Let $n \in \mathbb{N}$ such that $n > 1$ and let $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ be two circulant digraphs. Then we have the following.*

(1) *If $\mathbf{k}(S) \neq \mathbf{k}(T)$, then $\mathrm{Cay}(\mathbb{Z}_n, S) \not\cong \mathrm{Cay}(\mathbb{Z}_n, T)$.*

(2) *If $\mathbf{k}(S) = \mathbf{k}(T) = \mathbf{k}$, then the following statements are equivalent.*

  (i) *$\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$.*

  (ii) *There exists a permutation $f_{\vec{m}} \in P(\mathbf{k})$ such that*

$$\mathrm{Cay}(\mathbb{Z}_n, S)^{f_{\vec{m}}} = \mathrm{Cay}(\mathbb{Z}_n, T).$$

  (iii) *There exists a permutation $f_{\vec{m}} \in P(\mathbf{k})$ such that $S^{f_{\vec{m}}} = T$.*

Using the above theorem, we obtain the following sufficient condition for a circulant digraph to be CI.

Lemma 2.13. *Let $n \in \mathbb{N}$ such that $n > 1$ and $S \subseteq \mathbb{Z}_n \setminus \{0\}$ be a subset such that $\mathbf{k}(S) = \mathbf{z}$ or $\mathbf{z}_*$ (i.e., the zero key or the almost zero key, resp. in $\mathbb{Z}_n$). Then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a CI-digraph.*

Proof. Suppose that $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$ for some subset $T \subset \mathbb{Z}_n$. We have to show that $S^\sigma = T$ for some $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$.

By Theorem 2.12, $\mathbf{k}(T) = \mathbf{k}(S)$ and there exists $f_{\vec{m}} \in P(\mathbf{k})$, such that $S^{f_{\vec{m}}} = T$. Let n have prime decomposition $n = p_1^{t_1} \cdots p_l^{t_l}$. Then $\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_l) \in \mathbf{K}_{p_1^{t_1}} \times \cdots \times \mathbf{K}_{p_l^{t_l}}$, and the action of $f_{\vec{m}}$ on $\mathbb{Z}_n$ can be described as

$$(x_1, \ldots, x_l)^{f_{\vec{m}}} = \left(x_1^{f_{\vec{m}_1}}, \ldots, x_l^{f_{\vec{m}_l}} \right),$$

where for every $i \in [l]$, $f_{\vec{m}_i} \in P(\mathbf{k}_i)$. If $\mathbf{k}_i$ is the zero key in $\mathbf{K}_{p_i^{t_i}}$, then $f_{\vec{m}_i} \in \mathrm{Aut}(\mathbb{Z}_{p_i^{t_i}})$ by Lemma 2.11. On the other hand, as $\mathbf{k} = \mathbf{z}$ or $\mathbf{k} = \mathbf{z}_*$, we conclude that $\mathbf{k}_i$ is the zero key, unless $p_i^{t_i} = 4$ and $\mathbf{k}_i = (0, 1)$. In the later case, we see in (2.1) that $f_{\vec{m}_i}$ is the identity permutation of $\mathbb{Z}_4$. We conclude that $f_{\vec{m}} \in \mathrm{Aut}(\mathbb{Z}_n)$. □

3   Proof of the main results

Lemma 3.1 ([11, Lemma 2.1])**.** *Let G be a finite group, and let $S, T \subseteq G \setminus \{1_G\}$. Then* $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, T)$ *if and only if* $\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\langle T \rangle, T)$.

Lemma 3.2. *For every subset $S \subseteq \mathbb{Z}_n \setminus \{0\}$, $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a CI-digraph if and only if* $\mathrm{Cay}(\langle S \rangle, S)$ *is a CI-digraph.*

Proof. ($\Longrightarrow$) Suppose that $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a CI-digraph and $\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\langle S \rangle, T)$ for some subset $T \subset \langle S \rangle$. Since $\mathrm{Cay}(\langle S \rangle, S)$ is connected, it follows that $\mathrm{Cay}(\langle S \rangle, T)$ is also connected and thus $\langle T \rangle = \langle S \rangle$. By Lemma 3.1, $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$. As $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a CI-digraph, there exists a Cayley isomorphism $\sigma \in \mathrm{Aut}(\mathbb{Z}_n)$ between $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$. The automorphism σ maps $\langle S \rangle$ to itself, hence its restriction to $\langle S \rangle$ induces a Cayley isomorphism between $\mathrm{Cay}(\langle S \rangle, S)$ and $\mathrm{Cay}(\langle S \rangle, T)$, and so $\mathrm{Cay}(\langle S \rangle, S)$ is indeed a CI-digraph.

($\Longleftarrow$) Suppose that $\mathrm{Cay}(\langle S \rangle, S)$ is a CI-digraph and $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$ for some subset $T \subset \mathbb{Z}_n$. By Lemma 3.1, $\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\langle T \rangle, T)$. Since $\mathbb{Z}_n$ is a cyclic group, $\langle S \rangle = \langle T \rangle$. As $\mathrm{Cay}(\langle S \rangle, S)$ is a CI-digraph, there exists a Cayley isomorphism $\sigma \in \mathrm{Aut}(\langle S \rangle)$ between $\mathrm{Cay}(\langle S \rangle, S)$ and $\mathrm{Cay}(\langle S \rangle, T)$. It is not hard to show that σ can be extended to an automorphism of $\mathbb{Z}_n$, or in other words, there exists an automorphism $\sigma' \in \mathrm{Aut}(\mathbb{Z}_n)$ such that its restriction to $\langle S \rangle$ is equal to σ. We obtain that σ' is a Cayley isomorphism between $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$, so $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a CI-digraph. $\square$

The following lemma follows from [5, Lemma 25].

Lemma 3.3. *Let $H \leq \mathbb{Z}_n$ be a subgroup and let $s \in \mathbb{Z}_n$ be any element outside H. Then* $\mathrm{Cay}(\mathbb{Z}_n, H + s)$ *is a CI-digraph and* $\mathrm{Cay}(\mathbb{Z}_n, (H + s) \cup (H - s))$ *is a CI-graph.*

Lemma 3.4. *Let $n \in \mathbb{N}$ be an even number and let p be an odd prime such that $p^2 \mid n$. Suppose that $S = (P + s) \cup (P - s) \cup \{\frac{n}{2}\}$, where $P \leq \mathbb{Z}_n$ is the subgroup of order p, $P + s \neq P - s$ and $\langle S \rangle = \mathbb{Z}_n$. Then $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a CI-graph.*

Proof. For the sake of simplicity we set $\Gamma = \mathrm{Cay}(\mathbb{Z}_n, S)$. If $n = 18$, then Γ is a CI-graph by Theorem 1.1, hence in the rest of the proof we assume that $n > 18$. Call an edge $\{x, y\}$ of Γ a *half edge* if $y - x = \frac{n}{2}$.

Claim. *An edge of Γ is contained in a subgraph isomorphic to $K_{p,p}$ if and only if it is not a half edge.*

Let e be a half edge of Γ, i.e., $e = (x, x + \frac{n}{2})$ for some $x \in \mathbb{Z}_n$. Assume for the moment that e is contained in a subgraph isomorphic to $K_{p,p}$. Then the latter subgraph contains a 4-cycle in the form $(x, x + \frac{n}{2}, y_1, y_2)$ with no half edge besides e. This means that there are elements $z, z_1, z_2 \in P$ satisfying one of the following equalities:

$$x + z \pm s = y_2 = y_1 + z_2 \pm s = x + \frac{n}{2} + z_1 \pm s + z_2 \pm s.$$

This shows that $s + \frac{n}{2} \in P$ or $3s + \frac{n}{2} \in P$, and hence $2s \in P$ or $6s \in P$. If $2s \in P$, then the order of s is a divisor of $2p$, and as $\mathbb{Z}_n = \langle S \rangle$, we get $n = 2p$. This contradicts that $p^2 \mid n$. If $6s \in P$, then the order of s is a divisor of $6p$. Using also that $p^2 \mid n$, we find that $p = 3$ and $n = 18$. This, however, is excluded.

Suppose second that $e = \{x, y\}$ is not a half edge, i.e., $y = x + z + \varepsilon s$, where $z \in P$ and $\varepsilon \in \{1, -1\}$. It is straightforward to check that the subgraph of Γ induced by the set $(P + x) \cup (P + y)$ contains e and it is isomorphic to $K_{p,p}$. This completes the proof of the claim.

The above argument also shows that the biparts of the subgraphs of Γ isomorphic to $K_{p,p}$ partition the vertex set $\mathbb{Z}_n$ into the P-cosets, which therefore, form an $\mathrm{Aut}(\Gamma)$-invariant partition.

Now suppose that $\mathrm{Cay}(\mathbb{Z}_n, S) \cong \mathrm{Cay}(\mathbb{Z}_n, T)$ for some subset $T \subset \mathbb{Z}_n$. It follows in turn that, the partition of $\mathbb{Z}_n$ into the P-cosets is also $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_n, T))$-invariant, $T \setminus \{\frac{n}{2}\} = (P + t) \cup (P - t)$ for a suitable element $t \in \mathbb{Z}_n$, and

$$\mathrm{Cay}(\mathbb{Z}_n, (P + s) \cup (P - s)) \cong \mathrm{Cay}(\mathbb{Z}_n, (P + t) \cup (P - t)).$$

By Lemma 3.3, $T \setminus \{\frac{n}{2}\} = (S \setminus \{\frac{n}{2}\})^\sigma$ for some automorphism σ of $\mathbb{Z}_n$, and hence $T = S^\sigma$. □

We are ready to derive our main theorems. Given a positive integer k, in the proofs below we denote by $\pi(k)$ the set of all prime divisors of k. For a prime p, the *p-part* of k is the largest power of p dividing k.

Proof of Theorem 1.4. If $n_2 = 1$, then Theorem 1.4 follows from Theorem 1.1. Thus for the rest of the proof we assume that $n_2 > 1$. Let $S \subset \mathbb{Z}_n$ such that $0 \notin S$ and $|S| \leq m$. By Lemma 3.2, it suffices to show that $\mathrm{Cay}(\langle S \rangle, S)$ is a CI-(di)graph. We derive this in three steps. Write $\langle S \rangle = \mathbb{Z}_{n'}$.

Step 1. $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a CI-(di)graph, unless n_2 is odd.

Assume that n_2 is even. Then $|S| \leq 2$ if $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a digraph and $|S| \leq 5$ if it is a graph. Thus the claim in Step 1 follows from the known facts that every cyclic group is 2-DCI-group [14] and also a 5-CI-group [8].

For the rest of the proof we assume that n_2 is odd. Let p be the smallest prime divisor of n_2 and P be the subgroup of $\mathbb{Z}_n$ of order p.

Step 2. $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a CI-(di)graph, unless $p^2 \mid n'$ and one of the following holds:

(i) $S = P + s$, for some $s \in \mathbb{Z}_{n'}$,

(ii) $S = (P + s) \cup (P - s)$, for some $s \in \mathbb{Z}_{n'}$ such that $P + s \neq P - s$,

(iii) n' is even and $S = (P+s) \cup (P-s) \cup \{\frac{n'}{2}\}$, for some $s \in \mathbb{Z}_{n'}$ such that $P + s \neq P - s$.

Assume that S is none of the sets described in the cases (i) − (iii) above. We show below that $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a CI-(di)graph.

Let n' have prime decomposition $n' = p_1^{t_1} \cdots p_l^{t_l}$. Let $\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_l) = \mathbf{k}(S)$ be the key of the set S. Suppose that $\mathbf{k}_i \neq \mathbf{z}$, the zero key in $\mathbf{K}_{p_i^{t_i}}$. Then $t_i > 1$. Assume for the moment that $p_i > 2$. Since $p_i^2 \mid n'$, it follows that $p_i \in \pi(n_2)$. As $\langle S \rangle = \mathbb{Z}_{n'}$, there is an element $s \in S$ such that the order of s in the group $\mathbb{Z}_{n'}$ has p_i-part $p_i^{t_i}$. Let $\mathbf{m} = (\mathbf{m}_1, \ldots, \mathbf{m}_l)$ be the key of $\mathbb{Z}_{n'}$ defined as for every $j \in [l]$,

$$\mathbf{m}_j = \begin{cases} (0, \ldots, 0) & \text{if } j \neq i, \\ (0, \ldots, 0, 1) & \text{if } j = i. \end{cases}$$

The cell of $\Sigma(\mathbf{m})$ containing s is equal to $P_i + s$, where $P_i \leq \mathbb{Z}_{n'}$ and $|P_i| = p_i$. Also, $\mathbf{m} \leq \mathbf{k}$, hence by Proposition 2.4, $\Sigma(\mathbf{k}) \sqsubseteq \Sigma(\mathbf{m})$. Let C be the cell of $\Sigma(\mathbf{k})$ containing s. It follows from the definition of $\mathbf{k} = \mathbf{k}(S)$ that

$$P_i + s \subseteq C \subseteq S \implies p_i \leq |S|.$$

Suppose first that $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a digraph. Since $p_i \in \pi(n_2)$, it follows that $|S| \leq p_i$ also holds, and we conclude that $S = P_i + s$. If $p_j \in \pi(n_2)$ and $p_j \neq p_i$, then $p_i = |S| \leq p_j$. Thus $p_i = p$, the smallest prime divisor of n_2, and so S is a set described in case (i) , which is impossible.

Suppose now that $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a graph. Then $S = -S$, and so

$$(P_i + s) \cup (P_i - s) \subseteq C \subseteq S \implies 2p_i \leq |S|.$$

For the last implication observe that $P_i + s \neq P_i - s$, for otherwise, $2s \in P_i$, contradicting that the order of s has p_i-part $p_i^{t_i} > p_i$. As $p_i \in \pi(n_2)$, $|S| \leq 2p_i + 1$ also holds, so we conclude that $S = (P_i + s) \cup (P_i - s)$ or n' is even and $S = (P_i + s) \cup (P_i - s) \cup \{\frac{n'}{2}\}$. If $p_j \in \pi(n_2)$ and $p_j \neq p_i$, then $2p_i \leq |S| \leq 2p_j + 1$. It follows that $p_i = p$ and S is a set in the form given in either case (ii) or case (iii) , which is again impossible. We obtain that $p_i = 2$. But as n_2 is odd, 2 must be a divisor of n_1, and so $t_i = 2$.

We conclude that $\mathbf{k} = \mathbf{z}$, the zero key of $\mathbb{Z}_{n'}$, or the 2-part of n' is 4 and $\mathbf{k} = \mathbf{z}_*$, the almost zero key in $\mathbf{K}_{n'}$. By Lemma 2.13, $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a CI-(di)graph.

Step 3. $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a CI-(di)graph.

In view of Step 2, we may assume that $p^2 \mid n'$. If $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a digraph, then S is a set described in case (i) of Step 2, and the statement follows from Lemma 3.3. Suppose that $\mathrm{Cay}(\mathbb{Z}_{n'}, S)$ is a graph. If S is a set described in case (ii) of Step 2, then the statement follows again from Lemma 3.3; while if it is a set described in case (iii) , then the statement follows from Lemma 3.4. □

Proof of case (1) *in* Theorem 1.5. ($\implies$) This is equivalent to the following implication: If $8 \mid n$ or $p^2 \mid n$ for some odd prime $p < m$, then $\mathbb{Z}_n$ is not an m-DCI-group.

Suppose first that $8 \mid n$. Then there is a subset $S \subset \mathbb{Z}_n$ such that $\langle S \rangle \cong \mathbb{Z}_8$ and

$$\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\mathbb{Z}_8, \{1, 2, 5\}),$$

the non-CI-digraph discussed in [6]. By Lemma 3.2, $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a non-CI-digraph, and so $\mathbb{Z}_n$ is not an m-DCI-group (recall that $m \geq 3$).

Now suppose that $p^2 \mid n$ for some odd prime $p < m$. Then there is a subset $S \subset \mathbb{Z}_n$ such that $\langle S \rangle \cong \mathbb{Z}_{p^2}$ and

$$\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}(\mathbb{Z}_{p^2}, (\langle p \rangle + 1) \cup \{p\}),$$

the non-CI-digraph discussed in [11] (see the proof of [11, Theorem 1.4]). By Lemma 3.2, $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a non-CI-digraph, and so $\mathbb{Z}_n$ is not an m-DCI-group.

($\impliedby$) Define n_2 to be 1 if there is no odd prime $p \in \pi(n)$ such that p^2 divides n, and let $n_2 = \prod_{\substack{p \in \pi(n) \\ 2 < p < n_p}} n_p$ otherwise, where n_p denotes the p-part of n. Let $n_1 = \frac{n}{n_2}$. It follows that $\gcd(n_1, n_2) = 1$ and $n_1 \mid 4k$, where k is odd and square-free. Note that, for every $p \in \pi(n_2)$, $p^2 \mid n$, implying that $p \geq m$. Thus Theorem 1.4 can be applied to $\mathbb{Z}_n$ and this gives that $\mathbb{Z}_n$ is an m-DCI-group. □

Proof of case (2) *in* Theorem 1.5. ($\Longrightarrow$) This is equivalent to the following implication: If $n \notin \{8, 9, 18\}$ and $8 \mid n$ or $p^2 \mid n$ for some odd prime $p < \frac{m-1}{2}$, then $\mathbb{Z}_n$ is not an m-CI-group.

If $8 \mid n$, then the graph

$$\mathrm{Cay}\left(\mathbb{Z}_n, \left\{1, n-1, 2, n-2, \frac{n}{2}-1, \frac{n}{2}+1\right\}\right)$$

is a non-CI-graph as shown in [2, Example 1.22]. Thus $\mathbb{Z}_n$ is not an m-CI-group (recall that $m \geq 6$).

Now suppose that $p^2 \mid n$ for some odd prime $p < \frac{m-1}{2}$. Let $p = 3$ (so $m \geq 8$). The graph

$$\mathrm{Cay}\left(\mathbb{Z}_n, \left\{1, n-1, 3, n-3, \frac{n}{3}+1, \frac{n}{3}-1, \frac{2n}{3}+1, \frac{2n}{3}-1,\right\}\right)$$

is a non-CI-graph as shown in [2, Example 1.23], and hence $\mathbb{Z}_n$ is not an m-CI-group.

Let $p \geq 5$ (so $m \geq 2p + 2$). In this case, there is a subset $S \subset \mathbb{Z}_n$ such that $\langle S \rangle \cong \mathbb{Z}_{p^2}$ and

$$\mathrm{Cay}(\langle S \rangle, S) \cong \mathrm{Cay}\left(\mathbb{Z}_{p^2}, (\langle p \rangle + 1) \cup (\langle p \rangle - 1) \cup \{p, -p\}\right),$$

the non-CI-graph discussed in [11] (see the proof of [11, Theorem 1.5]). By Lemma 3.2, $\mathrm{Cay}(\mathbb{Z}_n, S)$ is a non-CI-graph, and so $\mathbb{Z}_n$ is not an m-CI-group.

($\Longleftarrow$) If $n \in \{8, 9, 18\}$, then $\mathbb{Z}_n$ is a CI-group, so the statement holds. Assume that $n \notin \{8, 9, 18\}$. Define n_2 to be 1 if there is no odd prime $p \in \pi(n)$ such that p^2 divides n, and let $n_2 = \prod_{\substack{p \in \pi(n) \\ 2 < p < n_p}} n_p$ otherwise, where n_p denotes the p-part of n. Let $n_1 = \frac{n}{n_2}$. It follows that $\gcd(n_1, n_2) = 1$ and $n_1 \mid 4k$, where k is odd and square-free. Note that, for every $p \in \pi(n_2)$, $p^2 \mid n$, implying that $2p + 1 \geq m$. Thus Theorem 1.4 can be applied to $\mathbb{Z}_n$ and this gives that $\mathbb{Z}_n$ is an m-CI-group. $\qquad\square$

ORCID iDs

István Kovács https://orcid.org/0009-0001-5199-2850

References

[1] A. Ádám, Research problem 2–10, *J. Comb. Theory* **1** (1967), 309.

[2] B. Alspach, Isomorphism and Cayley graphs on abelian groups, in: G. Hahn and G. Sabidussi (eds.), *Graph symmetry: algebraic methods and applications. Proceedings of the NATO Advanced Study Institute and séminaire de mathématiques supérieures, Montréal, Canada, July 1-12, 1996*, Kluwer Academic Publishers, Dordrecht, pp. 1–22, 1997.

[3] F. Boesch and R. Tindell, Circulants and their connectivities, *J. Graph Theory* **8** (1984), 487–499, doi:10.1002/jgt.3190080406, https://doi.org/10.1002/jgt.3190080406.

[4] C. Delorme, O. Favaron and M. Mahéo, Isomorphisms of Cayley multigraphs of degree 4 on finite Abelian groups, *Eur. J. Comb.* **13** (1992), 59–61, doi:10.1016/0195-6698(92)90067-A, https://doi.org/10.1016/0195-6698(92)90067-A.

[5] E. Dobson, On isomorphisms of circulant digraphs of bounded degree, *Discrete Math.* **308** (2008), 6047–6055, doi:10.1016/j.disc.2007.11.024, https://doi.org/10.1016/j.disc.2007.11.024.

[6] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, *J. Comb. Theory* **9** (1970), 297–307, doi:10.1016/S0021-9800(70)80068-0, https://doi.org/10.1016/S0021-9800(70)80068-0.

[7] X. Fang and M. Xu, On isomorphisms of Cayley graphs of small valency, *Algebra Colloq.* **1** (1994), 67–76.

[8] C. H. Li, Isomorphisms and classification of Cayley graphs of small valencies on finite abelian groups, *Australas. J. Comb.* **12** (1995), 3–14.

[9] C. H. Li, The cyclic groups with the m-DCI property, *Eur. J. Comb.* **18** (1997), 655–665, ej960130, doi:10.1006/eujc.1996.0130, https://doi.org/10.1006/eujc.1996.0130.

[10] C. H. Li, On isomorphisms of finite Cayley graphs—a survey, *Discrete Math.* **256** (2002), 301–334, doi:10.1016/S0012-365X(01)00438-1, https://doi.org/10.1016/S0012-365X(01)00438-1.

[11] C. H. Li, C. E. Praeger and M. Y. Xu, On finite groups with the Cayley isomorphism property, *J. Graph Theory* **27** (1998), 21–31, doi:10.1002/(SICI)1097-0118(199801)27:1⟨21::AID-JGT5⟩ 3.0.CO;2-I, https://doi.org/10.1002/(SICI)1097-0118(199801)27:1<21::AID-JGT5>3.0.CO;2-I.

[12] M. Muzychuk, On Ádám's conjecture for circulant graphs, *Discrete Math.* **167-168** (1997), 497–510, doi:10.1016/S0012-365X(96)00251-8, https://doi.org/10.1016/S0012-365X(96)00251-8.

[13] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, *Proc. Lond. Math. Soc. (3)* **88** (2004), 1–41, doi:10.1112/S0024611503014412, https://doi.org/10.1112/S0024611503014412.

[14] L. Sun, Isomorphisms of circulants with degree 2, *J. Beijing Ins. Technol.* **9** (1984), 42—-46.

[15] L. Sun, Isomorphisms of circulants graphs, *Chinese Ann. Math.* **9A** (1988), 259—266.

[16] S. Toida, A note on Ádám's conjecture, *J. Comb. Theory, Ser. B* **23** (1977), 239–246, doi:10.1016/0095-8956(77)90036-3, https://doi.org/10.1016/0095-8956(77)90036-3.