ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 22 (2022) #P2.07 / 287–304
https://doi.org/10.26493/1855-3974.2443.02e
(Also available at http://amc-journal.eu)

Generalised dihedral CI-groups

Ted Dobson *

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

Mikhail Muzychuk

Department of Mathematics, Ben-Gurion University of the Negev, Israel

Pablo Spiga

Dipartimento di Matematica e Applicazioni, University of Milano-Bicocca,
Via Cozzi 55, 20125 Milano, Italy

Received 24 September 2020, accepted 16 August 2021, published online 27 May 2022

Abstract

In this paper, we find a strong new restriction on the structure of CI-groups. We show that, if R is a generalised dihedral group and if R is a CI-group, then for every odd prime p the Sylow p-subgroup of R has order p, or 9. Consequently, any CI-group with quotient a generalised dihedral group has the same restriction, that for every odd prime p the Sylow p-subgroup of the group has order p, or 9.

Keywords: CI-group, DCI-group, generalised dihedral, Cayley isomorphism.

Math. Subj. Class. (2020): 05E18, 05E30

1 Introduction

Let R be a finite group and let S be a subset of R. The *Cayley digraph* of R with connection set S, denoted $\mathsf{Cay}(R,S)$, is the digraph with vertex set R and with (x,y) being an arc if and only if $xy^{-1} \in S$. Now, $\mathsf{Cay}(R,S)$ is said to be a *DCI-graph* (here *CI* stands for *Cayley isomorphic while the D stands for directed)*, if whenever $\mathsf{Cay}(R,S)$ is isomorphic to $\mathsf{Cay}(R,T)$, there exists an automorphism φ of R with $S^\varphi = T$. Clearly,

*Corresponding author. This work is supported in part by the Slovenian Research Agency (research program P1-0285 and research projects N1-0062, J1-9108, J1-1695, N1-0140, N1-0160, J1-2451, N1-0208).

E-mail addresses: ted.dobson@upr.si (Ted Dobson), muzychuk@bgu.ac.il (Mikhail Muzychuk), pablo.spiga@unimib.it (Pablo Spiga)

$\mathsf{Cay}(R,S) \cong \mathsf{Cay}(R,S^\varphi)$ for every $\varphi \in \mathrm{Aut}(R)$ and hence, loosely speaking, for a DCI-graph $\mathsf{Cay}(R,S)$ deciding when a Cayley digraph over R is isomorphic to $\mathsf{Cay}(R,S)$ is theoretically and algorithmically elementary, but computationally efficient only if $\mathrm{Aut}(R)$ is small; that is, the solving set for $\mathsf{Cay}(R,S)$ is reduced to simply $\mathrm{Aut}(R)$ (for the definition of a solving set see for example [24, 26]). The group R is a *DCI-group* if $\mathsf{Cay}(R,S)$ is a DCI-graph for every subset S of R. Moreover, R is a *CI-group* if $\mathsf{Cay}(R,S)$ is a DCI-graph for every inverse-closed subset S of R. Thus every DCI-group is a CI-group.

After roughly 50 years of intense research, the classification of DCI- and CI-groups is still open. The current state of the art in this problem is as follows. There exist two rather short lists of candidates for DCI- and CI-groups and it is known that every DCI- and every CI-group must be a member of the corresponding list, see for instance [20]. Showing that a candidate on the lists of possible DCI- or CI-groups is actually a DCI- or CI-group, though, takes a considerable amount of effort. Just to give an example, the recent paper of Feng and Kovács [15] is a tour de force that shows that elementary abelian groups of rank 5 are DCI-groups.

In this paper we find an unexpected new restriction on which generalised dihedral groups are CI-groups, and significantly shorten the list of candidates for CI-groups.

Definition 1.1. Let A be an abelian group. The *generalised dihedral* group $\mathrm{Dih}(A)$ over A is the group $\langle A, x \mid a^x = a^{-1}, \forall a \in A\rangle$. A group is called generalised dihedral if it is isomorphic to $\mathrm{Dih}(A)$ for some A. When A is cyclic, $\mathrm{Dih}(A)$ is called a dihedral group.

Our main result is the following.

Theorem 1.2. *Let* $\mathrm{Dih}(A)$ *be a generalised dihedral group over the abelian group* A*. If* $\mathrm{Dih}(A)$ *is a* CI-*group, then, for every odd prime* p *the Sylow* p*-subgroup of* A *has order* p*, or* 9*. If* $\mathrm{Dih}(A)$ *is a* DCI-*group, then, in addition, the Sylow* 3-*subgroup has order* 3.

Generalised dihedral groups are amongst the most abundant members in the list of putative CI-groups. The importance of Theorem 1.2 is the arithmetical condition on the order of such groups, which greatly reduces even further the list of candidates for CI-groups. We believe that every generalised dihedral group satisfying this numerical condition on its order is a genuine CI-group. (This is in line with the partial result in [8].) Additionally, this result further reduces to two other groups on the list, whose definitions we now give.

Definition 1.3. Let A be an abelian group such that every Sylow p-subgroup of A is elementary abelian. Let $n \in \{2,4,8\}$ be relatively prime to $|A|$. Set $E(A,n) = A \rtimes \langle g \rangle$, where g has order n and $a^g = a^{-1}, \forall a \in A$.

Note that $E(A,2) = \mathrm{Dih}(A)$. The groups $E(A,4)$ and $E(A,8)$ have centres Z_1 and Z_2 of order 2 and 4, respectively, and $E(A,4)/Z_1 \cong E(A,8)/Z_2 \cong \mathrm{Dih}(A)$. Babai and Frankl [2, Lemma 3.5] showed that a quotient of a (D)CI-group by a characteristic subgroup is a (D)CI-group, while the first author and Joy Morris [7, Theorem 8] showed that a quotient of a (D)CI-group is a (D)CI-group. Applying either result and Theorem 1.2 we have the following.

Corollary 1.4. *If* $E(A,4)$ *or* $E(A,8)$ *is a* CI-*group, then, for every odd prime* p *the Sylow* p*-subgroup of* A *has order* p *or* 9*. If* $E(A,n), n \in \{2,4,8\}$ *is a* DCI-*group, then, in addition,* $n \neq 8$ *and the Sylow* 3-*subgroup of* A *has order* 3.

Not much is known about which of the groups under consideration in this paper are CI-groups. Let p be a prime. Babai [1, Theorem 4.4] showed D_{2p} is a CI-group. The first author [4, Theorem 22] extended this to some special values of square-free integers. With Joy Morris, the first and third authors [8] showed that D_{6p} is a CI-group, $p \geq 5$. Also, Li, Lu, and Pálfy showed $E(p, 4)$ and $E(p, 8)$ are CI-groups.

We have one other result of interest, for which we will need an additional definition.

Definition 1.5. Let G be a group, and $S \subseteq G$. A *Haar graph* of G with connection set S has vertex set $G \times \mathbb{Z}_2$ and edge set $\{\{(g, 0), (sg, 1)\} : g \in G \text{ and } s \in S\}$.

So a Haar graph is a bipartite analogue of a Cayley graph. There is a corresponding isomorphism problem for Haar graphs, and if the group A is abelian, it is equivalent to the isomorphism problem for Cayley graphs of generalised dihedral groups $\mathrm{Dih}(A)$ that are bipartite (for nonabelian groups the problems are not equivalent, as for non-abelian groups Haar graphs need not be transitive), see [17, Lemma 2.2]. If isomorphic bipartite Cayley graphs of $\mathrm{Dih}(A)$ are isomorphic by group automorphisms of A, we say A is a *BCI-group*. We will also show that $\mathbb{Z}_3^k$ is not a BCI-group for every $k \geq 3$, while it is known that $\mathbb{Z}_3^k$ is a CI-group for every $1 \leq k \leq 5$ [32].

1.1 Some notation

Babai [1, Lemma 3.1] has proved a very useful criterion for determining when a finite group is a DCI-group and, more generally, when $\mathsf{Cay}(R, S)$ is a DCI-graph.

Lemma 1.6. *Let R be a finite group, and let S be a subset of R. Then, $\mathsf{Cay}(R, S)$ is a DCI-graph if and only if $\mathrm{Aut}(\mathsf{Cay}(R, S))$ contains a unique conjugacy class of regular subgroups isomorphic to R.*

Let Ω be a finite set and let G be a permutation group on Ω. An *orbital graph* of G is a digraph with vertex set Ω and with arc set a G-orbit $(\alpha, \beta)^G = \{(\alpha^g, \beta^g) \mid g \in G\}$, where $(\alpha, \beta) \in \Omega \times \Omega$. In particular, each orbital graph has for its arcs one orbit on the ordered pairs of elements of Ω, under the action of G. Moreover, we say that the orbital graphs $(\alpha, \beta)^G$ and $(\beta, \alpha)^G$ are *paired*. When $(\alpha, \beta)^G = (\beta, \alpha)^G$, we say that the orbital graph is *self-paired*.

When G is transitive and $\omega_0 \in \Omega$, there exists a natural one-to-one correspondence between the orbits of G on $\Omega \times \Omega$ (a.k.a. orbitals or 2-orbits of G) and the orbits of the stabiliser G_{ω_0} on Ω (a.k.a. *suborbits* of G). Therefore, under this correspondence, we may naturally define paired and self-paired suborbits.

Two subgroups of the symmetric group $\mathsf{Sym}(\Omega)$ are called 2-*equivalent* if they have the same orbitals. A subgroup of $\mathsf{Sym}(\Omega)$ generated by all subgroups 2-equivalent to a given $G \leq \mathsf{Sym}(\Omega)$ is called the 2-*closure* of G, denoted $G^{(2)}$.

The group G is said to be 2-*closed* if $G = G^{(2)}$. It is easy to verify that $G^{(2)}$ is a subgroup of $\mathrm{Sym}(\Omega)$ containing G and, in fact, $G^{(2)}$ is the largest (with respect to inclusion) subgroup of $\mathrm{Sym}(\Omega)$ preserving every orbital of G.

2 Construction and basic results

Let q be a power of an odd prime and let $\mathbb{F}$ be a field of cardinality q. We let

$$G := \left\{ \begin{pmatrix} a & x & z \\ 0 & b & y \\ 0 & 0 & c \end{pmatrix} \mid x, y, z \in \mathbb{F}, a, b, c \in \{-1, 1\}, abc = 1 \right\},$$

$$D := \left\{ \begin{pmatrix} a & ax & ax^2/2 \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix} \mid x \in \mathbb{F}, a \in \{-1, 1\} \right\},$$

$$H := \left\{ \begin{pmatrix} a & 0 & x \\ 0 & a & y \\ 0 & 0 & 1 \end{pmatrix} \mid x, y \in \mathbb{F}, a \in \{-1, 1\} \right\},$$

$$K := \left\{ \begin{pmatrix} 1 & x & y \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \mid x, y \in \mathbb{F}, a \in \{-1, 1\} \right\}.$$

It is elementary to verify that G, D, H and K are subgroups of the special linear group $\mathrm{SL}_3(\mathbb{F})$. Moreover, D, H and K are subgroups of G, $|G| = 4q^3$, $|D| = 2q$ and $|H| = |K| = 2q^2$. We summarise in Proposition 2.1 some more facts.

Proposition 2.1. *The group D is generalised dihedral over the abelian group $(\mathbb{F}, +)$ and, H and K are generalised dihedral over the abelian group $(\mathbb{F} \oplus \mathbb{F}, +)$. The core of D in G is 1. Moreover,*

$$DK = DH = G = HD = KD \text{ and } D \cap H = 1 = D \cap K.$$

Proof. The first two assertions follow with easy matrix computations. Let

$$g := \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in G$$

and observe that

$$g^{-1} \begin{pmatrix} a & ax & ax^2/2 \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix} g = \begin{pmatrix} a & -ax & -ax^2/2 \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix}.$$

As the characteristic of $\mathbb{F}$ is odd, from this it follows that

$$D \cap D^g = \left\langle \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \right\rangle.$$

It is now easy to see that D is core-free in G.

It is readily seen from the definitions that $D \cap H = 1 = D \cap K$. Therefore, $|DH| = |D||H| = 4q^3$ and $|DK| = |D||K| = 4q^3$. As DH and DK are subsets of G and $|G| = 4q^3$, we deduce $DH = G = DK$ and hence also $HD = G = KD$. □

We let $D\backslash G := \{Dg \mid g \in G\}$ be the set of right cosets of D in G. In view of Proposition 2.1, G acts faithfully by right multiplication on $D\backslash G$ and H and K act regularly by right multiplication on $D\backslash G$.

Proposition 2.2. *The subgroups H and K are normal in G and, therefore, are in distinct G-conjugacy classes.*

Proof. The normality of H and K in G can be checked by direct computations. □

2.1 Schur notation

Since $G = DH$ and $D \cap H = 1$, for every $g \in G$, there exists a unique $h \in H$ with $Dg = Dh$. In this way, we obtain a bijection $\theta : D\backslash G \to H$, where $\theta(Dg) = h \in H$ satisfies $Dg = Dh$.

Using the method of Schur (see [33]), we may identify via θ the G-set $D\backslash G$ with H. Moreover, we may define an action of G on H via the following rule: for every $g \in G$ and for every $h \in H$,

$$h^g = h' \text{ if and only if } Dhg = Dh'.$$

A classic observation of Schur yields that the action of G on $D\backslash G$ is permutation isomorphic to the action of G on H. In the rest of the paper, we use both points of view.

In the action of G on H, D is a stabiliser of the identity $e \in H$, i.e. $G_e = D$, and H acts on itself via its right regular representation. Since H is normal in G, the action of the point stabiliser G_e on H is permutation equivalent to the action of G_e via conjugation on H (Proposition 20.2 [33]). More precisely, $h^g = g^{-1}hg$ for any $g \in G_e$ and $h \in H$.

In what follows, we represent the elements of H and D as pairs $[a, x]$ and $[a, \vec{w}]$, where $x \in \mathbb{F}$, $\vec{w} \in \mathbb{F}^2$ and $a \in \{\pm 1\}$. In particular, $[a, x]$ represents the matrix

$$\begin{pmatrix} a & ax & ax^2/2 \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix}$$

of D and, if $\vec{w} = (x, y)$, then $[a, \vec{w}]$ represents the matrix

$$\begin{pmatrix} a & 0 & x \\ 0 & a & y \\ 0 & 0 & 1 \end{pmatrix}$$

of H. Under this identification, the product in D and H greatly simplifies. Indeed, for every $[a, x], [b, y] \in D$ and for every $[a, \vec{v}], [b, \vec{w}] \in H$, we have

$$\begin{aligned} [a, x][b, y] &= [ab, bx + y], \\ [a, \vec{v}][b, \vec{w}] &= [ab, b\vec{v} + \vec{w}]. \end{aligned} \tag{2.1}$$

Using this identification, the action of D on H also becomes slightly easier. Indeed, for every $[a, \vec{v}] \in H$ (with $\vec{v} = (x, y)$) and for every $[b, z] \in D$, we have

$$[a, (x, y)]^{[b,z]} = [a, \big((1 - a)z^2/2 - byz + x, (-1 + a)z + by\big)]. \tag{2.2}$$

This equality can be verified observing that

$$\begin{pmatrix} a & 0 & x \\ 0 & a & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} b & bz & bz^2/2 \\ 0 & 1 & z \\ 0 & 0 & b \end{pmatrix} = \begin{pmatrix} b & bz & bz^2/2 \\ 0 & 1 & z \\ 0 & 0 & b \end{pmatrix} \begin{pmatrix} a & 0 & (1 - a)z^2/2 - byz + x \\ 0 & a & (-1 + a)z + by \\ 0 & 0 & 1 \end{pmatrix}.$$

2.2 One special case

Let $A := \langle e_1, e_2, e_3\rangle$, where $e_1 := (1\,2\,3)$, $e_2 := (4\,5\,6)$, $e_1 := (7\,8\,9)$, let $x := (1\,2)(4\,5)(7\,8)$ and let $R := \langle A, x\rangle$. Then R is a generalised dihedral group over the elementary abelian 3-group A of order $3^3 = 27$. Let

$$S := \{x,\, e_1x,\, e_2x,\, e_3x,\, e_1e_2x,\, e_1^2e_2^2x,\, e_2e_3x,\, e_2^2e_3^2x,\, e_1^2e_2^2e_3^2x\}$$

and define

$$\Gamma := \mathsf{Cay}(R, S).$$

It can be verified with the computer algebra system Magma that $\mathrm{Aut}(\Gamma)$ has order $46656 = 2^6 \cdot 3^6$, acts transitively on the arcs of Γ and (most importantly) contains two conjugacy classes of regular subgroups isomorphic to R and hence, via Babai's lemma, R is not a CI-group.

This example has another interesting property from the isomorphism problem point of view. Observe that each element of S is an involution contained in $R \setminus A$. This implies that Γ is a bipartite graph, in which case Γ is isomorphic to a Haar graph, also called a bi-coset graph. In our example above, as every element of the connection set is an involution, it is a Haar graph of $\mathbb{Z}_3^3$ but as it is not a CI-graph of $\mathrm{Dih}(\mathbb{Z}_3^3)$, $\mathbb{Z}_3^3$ is not a BCI-group. This is the first example the authors are aware of where a group is an abelian DCI-group but not a BCI-group, as $\mathbb{Z}_p^3$ is a DCI-group [3]. Our next result shows $\mathbb{Z}_3^k$ is not a BCI-group for any $k \geq 3$.

Lemma 2.3. *Let R be an abelian group and let $H \leq R$. If R is BCI-group, then R/H is BCI-group.*

Proof. For this result, it is most convenient to have the vertex sets of Haar graphs and Cayley graphs of dihedral groups be the same. So, for an abelian group R, we will have $\mathrm{Dih}(R)$ permuting the set $R \times \mathbb{Z}_2$ (the vertex set of a Haar graph of R), where an element $s \in R$ is identified with the map $s_t\colon R \times \mathbb{Z}_2 \to R \times \mathbb{Z}_2$ given by $s_t(r, i) \mapsto (r + s, i)$. Define $\iota\colon R \times \mathbb{Z}_2 \to R \times \mathbb{Z}_2$ by $\iota(r, i) = (-r, i + 1)$. Then $\mathrm{Dih}(R)$ is canonically isomorphic to $G = \langle \iota, s_t : s \in R\rangle$. It is straightforward to show that $\iota \in \mathsf{Aut}(\mathrm{Haar}(R, S))$, and so we have $G \leq \mathsf{Aut}(\mathrm{Haar}(R, S))$ for every $S \subseteq R$. By [28, Theorem 2], we have $\mathrm{Haar}(R, S) \cong \mathrm{Cay}(\mathrm{Dih}(R), T)$, for some $T \subseteq G$, by the map ϕ which identifies (r, i) with the unique element of G which maps $(0, 0)$ to (r, i), $r \in R$, $i \in \mathbb{Z}_2$. Hence $\phi(r, i) = r_t\iota^i$, and $T = \{s\iota : s \in S\} = S \cdot \iota$.

If R is a BCI-group, then $\mathrm{Haar}(R, S)$ is a BCI graph. Let $\mathcal{C} = \{R \times \{0\}, R \times \{1\}\}$, $\mathcal{B}$ be the set of right cosets of H in $\mathrm{Dih}(R)$, and $U = \{sH : s \in S\}$. Then, as partitions of $R \times \mathbb{Z}_2$, $\mathcal{B}$ refines $\mathcal{C}$. As $\mathcal{C}$ is a bipartition of $\mathrm{Cay}(\mathrm{Dih}(R), S \cdot \iota)$, $\mathrm{Cay}(\mathrm{Dih}(R/H), U \cdot \iota)$ is bipartite with bipartition $\{\{(rH, i) : r \in R\} : i \in \mathbb{Z}_2\}$ and so $\mathrm{Cay}(\mathrm{Dih}(R/H), U \cdot \iota) = \mathrm{Haar}(R/H, U)$.

As $\mathrm{Cay}(\mathrm{Dih}(R), S \cdot \iota)$ is a CI-graph of $\mathrm{Dih}(R)$, by the proof of [6, Theorem 8], we see $\mathrm{Cay}(\mathrm{Dih}(R/H), U \cdot \iota)$ is a CI-graph of $\mathrm{Dih}(R/H)$ and any Cayley graph of $\mathrm{Dih}(R/H)$ isomorphic to $\mathrm{Cay}(\mathrm{Dih}(R/H), U \cdot \iota)$ is isomorphic by a group automorphism of $\mathrm{Dih}(R/H)$. But this means any two Haar graphs of R/H are isomorphic by a group automorphism of $\mathrm{Dih}(R/H)$, and so R/H is a BCI-group. □

Finally, Γ, as well as the graphs constructed in the next section, have the property that the Sylow p-subgroups of their automorphism groups are not isomorphic to Sylow p-subgroups of any 2-closed group of degree 3^3 or p^2 (in the next section). For the example above, the Sylow p-subgroups of the automorphism groups of Cayley digraphs of $\mathbb{Z}_p^3$ can be obtained from [5, Theorem 1.1], and none have order 3^6 as a Sylow p-subgroup of $\mathrm{AGL}(3,3)$ is not 2-closed (for p^2 in the next section, the Sylow p-subgroup has order p^3, but Sylow p-subgroups of the automorphism groups of Cayley digraphs of $\mathbb{Z}_p^2$ have order p^2 or p^{p+1} [10, Theorem 14]).

3 The permutation group G is 2-closed

In this section we prove the following.

Proposition 3.1. *The group G in its action on H is 2-closed.*

We start with some preliminary observations.

Lemma 3.2. *The orbits of G_e on H have one of the following forms:*

(1) $S_t := \{[1,(t,0)]\}$, *for every* $t \in \mathbb{F}$*;*

(2) $C_t \cup C_{-t}$*, where* $C_t := \{[1,(z,t)] \mid z \in \mathbb{F}\}$ *and* $t \in \mathbb{F} \setminus \{0\}$*;*

(3) $P_t := \big\{[-1,(t+z^2,2z)] \mid z \in \mathbb{F}\big\}$ *with* $t \in \mathbb{F}$.

Proof. Let $g := [a,(x,y)] \in H$. If $a = 1$ and $y = 0$, then (2.2) yields

$$g^{[b,z]} = [1,(x,0)] = g$$

and hence the G_e-orbit containing g is simply $\{g\}$. Therefore we obtain the orbits in Case (1).

Suppose then $a = 1$ and $y \neq 0$. Now, 2.2 yields

$$g^{[1,z]} = [1,(-yz+x,y)],$$
$$g^{[-1,z]} = [1,(yz+x,-y)].$$

In particular, $C_y = \{g^{[1,z]} \mid z \in \mathbb{F}\}$ and $C_{-y} = \{g^{[-1,z]} \mid z \in \mathbb{F}\}$ and we obtain the orbits in Case (2).

Finally suppose $a = -1$. Now, (2.2) yields

$$g^{[b,z]} = [1,(z^2 - byz + x, -2z + by)].$$

In particular, if we choose $z := by/2$ and $t = -y^2/4 + x$, then g and $[-1,(t,0)]$ are in the same G_e-orbit. Therefore $[-1,(x,y)]^{G_e} = [-1,(t,0)]^{G_e}$. Using again (2.2), we get

$$[-1,(t,0)]^{[b,-z]} = [-1,(t+z^2,2z)].$$

In particular, $P_t = \{g^{[b,z]} \mid [b,z] \in G_e\}$ and we obtain the orbits in Case (3). □

We call the G_e-orbits in (1) *singleton orbits*, the G_e-orbits in (2) *coset orbits* and the G_e-orbits in (3) *parabolic orbits*. Clearly, singleton orbits have cardinality 1, coset orbits have cardinality $2q$ and parabolic orbits have cardinality q. Also, it follows from Lemma 3.2 that there are q singleton orbits, $\frac{q-1}{2}$ coset orbits and q parabolic orbits. Indeed,

$$q \cdot 1 + \frac{q-1}{2} \cdot 2q + q \cdot q = 2q^2 = |H|.$$

It is also clear from Lemma 3.2 that all non-singleton orbits are self-paired and the only self-paired singleton orbit is S_0.

Before continuing, we recall [14, Definitions 2.5.3 and 2.5.4] tailored to our needs.

Definition 3.3. We say that $h \in H$ ***separates*** the pair $(h_1, h_2) \in H \times H$, if (h, h_1) and (h, h_2) belong to distinct G-orbitals, that is, hh_1^{-1} and hh_2^{-1} are in distinct G_e-orbits.

We also say that a subset $S \subseteq H$ ***separates*** G-orbitals if, for any two distinct elements $h_1, h_2 \in H \setminus S$, there exists $s \in S$ separating the pair (h_1, h_2).

Proposition 3.4. *If $q \geq 5$, then $\{e\} \cup P_0$ separates G-orbitals.*

Proof. Set $S := \{e\} \cup P_0$. Let $h_1, h_2 \in H \setminus S$ be two distinct elements. If h_1 and h_2 belong to distinct G_e-orbits, then $e \in S$ separates (h_1, h_2). Therefore, we assume that h_1 and h_2 belong to the same G_e-orbit, say, O. Since $h_1 \neq h_2$, O is not a singleton orbit and hence O is either a coset or a parabolic orbit.

Assume first that O is a parabolic orbit, that is, $O = P_t$, for some $t \in \mathbb{F}$. By Lemma 3.2, for each $i \in \{1, 2\}$, there exists $x_i \in \mathbb{F}$ with $h_i = [-1, (t + x_i^2, 2x_i)]$. As $q = |\mathbb{F}| \geq 5$, it is easy to verify that there exists $x \in \mathbb{F}$ with $x \notin \{x_1, x_2\}$ and with $x - x_1 \neq -(x - x_2)$. Now, let $s := [-1, (x^2, 2x)] \in P_0 \subseteq S$. From (2.1), we deduce

$$sh_i^{-1} = [1, (t + x_i^2 - x^2, 2x_i - 2x)].$$

As $2x_i - 2x \neq 0$, from Lemma 3.2, we obtain $sh_i^{-1} \in C_{2(x-x_i)} \cup C_{-2(x-x_i)}$. As $x - x_1 \neq -(x - x_2)$, we deduce that sh_1^{-1} and sh_2^{-1} are in distinct G_e-orbits and hence s separates (h_1, h_2).

Assume now that O is a coset orbit, that is, $O = C_t \cup C_{-t}$, for some $t \in \mathbb{F} \setminus \{0\}$. In this case, for each $i \in \{1, 2\}$, there exist $x_i \in \mathbb{F}$ and $a_i \in \{\pm 1\}$ with $h_i = [1, (x_i, a_i t)]$. Let $x \in \mathbb{F}$ with

$$xt(a_2 - a_1) \neq x_2 - x_1.$$

(The existence of x is clear when $a_1 \neq a_2$ and it follows from the fact that $h_1 \neq h_2$ when $a_1 = a_2$.) Set $s := [-1, (x^2, 2x)] \in P_0 \subseteq S$. From (2.1), we have

$$sh_i^{-1} \in [-1, (x^2 - x_i, 2x - a_i t)].$$

In particular, from Lemma 3.2, we have $sh_i^{-1} \in P_{t_i}$, for some $t_i \in \mathbb{F}$. Thus, $(x^2 - x_i, 2x - a_i t) = (t_i + y^2, 2y)$, for some $y \in \mathbb{F}$. From this it follows that

$$t_i = x^2 - x_i - \frac{(2x - a_i t)^2}{4}.$$

As $xt(a_2 - a_1) \neq x_2 - x_1$, a simple computation yields $t_1 \neq t_2$ and hence sh_1^{-1} and sh_2^{-1} are in distinct G_e-orbits. Therefore, s separates (h_1, h_2). □

Proof of Proposition 3.1. When $q = 3$, the proof follows with a computation with the computer algebra system Magma. Therefore, for the rest of the proof we suppose $q \geq 5$. Let T be the 2-closure of G. As $\{e\} \cup P_0$ separates the G-orbitals, it follows from [14, Theorem 2.5.7] that the action of T_e on P_0 is faithful, and hence so is the action of G_e on P_0. We denote by $G_e^{P_0}$ (respectively, $T_e^{P_0}$) the permutation group induced by G_e (respectively, T_e) on P_0. In particular, $G_e \cong G_e^{P_0}$ and $T_e \cong T_e^{P_0}$.

We claim that

$$(T_e)^{P_0} = (G_e)^{P_0}. \tag{3.1}$$

Observe that from (3.1) the proof of Proposition 3.1 immediately follows. Indeed, $T_e \cong T_e^{P_0} = G_e^{P_0} \cong G_e$ and hence $T_e = G_e$. As H is a transitive subgroup of G, we deduce that

$G = G_eH = T_eH = T$ and hence G is 2-closed. Therefore, to complete the proof, we need only establish (3.1).

From Lemma 3.2, $|P_0| = q$. Hence $(G_e)^{P_0}$ is a dihedral group of order $2q$ in its natural action on q points.

For each $t \in \mathbb{F}^*$ let Φ_t be the subgraph of $\mathsf{Cay}(H, C_t \cup C_{-t})$ induced by P_0. Let (h_1, h_2) be an arc of Φ_t. As $h_1, h_2 \in P_0$, there exist $x_1, x_2 \in \mathbb{F}$ with $h_1 = [-1, (x_1^2, 2x_1)]$ and $h_2 = [-1, (x_2^2, 2x_2)]$. Moreover, $h_2h_1^{-1} \in C_t \cup C_{-t}$ and hence, by (2.1), we obtain

$$h_2h_1^{-1} = [1, (x_2^2 - x_1^2, 2x_2 - 2x_1)] \in C_t \cup C_{-t},$$

that is, $2x_2 - 2x_1 \in \{-t, t\}$. This shows that the mapping

$$\begin{aligned} P_0 &\to \mathbb{F}^+ \\ (x^2, 2x) &\mapsto 2x \end{aligned}$$

is an isomorphism between the graphs Φ_t and $\mathsf{Cay}(\mathbb{F}^+, \{-t, t\})$. Therefore

$$(G_e)^{P_0} \le (T_e)^{P_0} \le \bigcap_{t \in \mathbb{F}^*} \mathrm{Aut}(\Phi_t) \cong \bigcap_{t \in \mathbb{F}^*} \mathrm{Aut}(\mathsf{Cay}(\mathbb{F}^+, \{-t, t\})) \cong \mathrm{Dih}(\mathbb{F}^+).$$

Since $(G_e)^{P_0}$ and $\mathrm{Dih}(\mathbb{F}^+)$ are dihedral groups of order $2q$, we conclude that $(G_e)^{P_0} = (T_e)^{P_0} = \bigcap_{t \in \mathbb{F}^*} \mathrm{Aut}(\Phi_t)$, proving 3.1. □

4 Generating graph

Combining Proposition 3.1, Proposition 2.2, and Lemma 1.6, we have proven that $\mathrm{Dih}(\mathbb{Z}_p^2)$ is not a CI-group with respect to colour Cayley digraphs for odd primes p. In this section we strengthen that result to Cayley graphs.

4.1 Schur rings

Let R be a finite group with identity element e. We denote the group algebra of R over the field $\mathbb{Q}$ by $\mathbb{Q}R$. For $Y \subseteq R$, we define

$$\underline{Y} := \sum_{y \in Y} y \in \mathbb{Q}R.$$

Elements of $\mathbb{Q}R$ of this form will be called *simple quantities*, see [33]. A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{Q}R$ is called a *Schur ring* over R if the following conditions are satisfied:

(1) there exists a basis of $\mathcal{A}$ as a $\mathbb{Q}$-vector space consisting of simple quantities $\underline{T}_0, \ldots, \underline{T}_r$;

(2) $T_0 = \{e\}$, $R = \bigcup_{i=0}^r T_i$ and, for every $i, j \in \{0, \ldots, r\}$ with $i \neq j$, $T_i \cap T_j = \emptyset$;

(3) for each $i \in \{0, \ldots, r\}$, there exists i' such that $T_{i'} = \{t^{-1} \mid t \in T_i\}$.

Now, $\underline{T}_0, \ldots, \underline{T}_r$ are called the *basic quantities* of $\mathcal{A}$. A subset S of R is said to be an $\mathcal{A}$- *subset* if $\underline{S} \in \mathcal{A}$, which is equivalent to $S = \bigcup_{j \in J} T_j$, for some $J \subseteq \{0, \ldots, r\}$.

Given two elements $a := \sum_{x \in R} a_x x$ and $b := \sum_{y \in R} b_y y$ in $\mathbb{Q}R$, the *Schur-Hadamard* product $a \circ b$ is defined by

$$a \circ b := \sum_{z \in R} a_z b_z z.$$

It is an elementary exercise to observe that, if $\mathcal{A}$ is a Schur ring over R, then $\mathcal{A}$ is closed by the Schur-Hadamard product.

The following statement is known as the *Schur-Wielandt principle*, see [33, Proposition 22.1].

Proposition 4.1. *Let $\mathcal{A}$ be a Schur ring over R, let $q \in \mathbb{Q}$ and let $x := \sum_{r\in R} a_r r \in \mathcal{A}$. Then*

$$x_q := \sum_{\substack{r\in R\\ a_r=q}} r \in \mathcal{A}.$$

Let X be a permutation group containing a regular subgroup R. As in Section 2.1, we may identify the domain of X with R. Let $T_0, \dots, T_r$ be the orbits of X_e with $T_0 = \{e\}$. A fundamental result of Schur [33, Theorem 24.1] shows that the $\mathbb{Q}$-vector space spanned by $\underline{T}_0, \underline{T}_1, \dots, \underline{T}_r$ in $\mathbb{Q}R$ is a Schur ring over R, which is called the *transitivity module* of the permutation group X and is usually denoted by $V(R, G_e)$. In particular, the $V(R, G_e)$-subsets of the Schur ring $V(R, G_e)$ are unions of G_e-orbits.

Let $\mathcal{A} := \langle \underline{T}_0, \dots, \underline{T}_r \rangle$ be a Schur ring over R (where $T_0, \dots, T_r$ are the basic quantities spanning $\mathcal{A}$). The *automorphism group* of $\mathcal{A}$ is defined by

$$\mathrm{Aut}(\mathcal{A}) := \bigcap_{i=0}^{r} \mathrm{Aut}(\mathsf{Cay}(R, T_i)). \tag{4.1}$$

Given a subset S of R, we denote by

$$\langle\langle \underline{S} \rangle\rangle,$$

the smallest (with respect to inclusion) Schur ring containing $\underline{S}$. Now, $\langle\langle \underline{S} \rangle\rangle$ is called the *Schur ring generated* by $\underline{S}$.

We conclude this brief introduction to Schur rings recalling [25, Theorem 2.4].

Proposition 4.2. *Let S be a subset of R. Then* $\mathrm{Aut}(\langle\langle \underline{S} \rangle\rangle) = \mathrm{Aut}(\mathsf{Cay}(R, S))$.

4.2 The group G is the automorphism group of a single (di)graph

It was shown above that the group G is 2-closed, i.e. it is the automorphism of a coloured digraph. In this section we give a Cayley digraph $\mathsf{Cay}(H, T)$ having automorphism group G. To build such a digraph it is sufficient to find a subset $T \subseteq H$ such that $\langle\langle \underline{T} \rangle\rangle = V(H, G_e)$ (Proposition 4.2). Such a set is constructed in Proposition 4.3. Note that T is symmetric for $q \geq 7$, so the digraph $\mathsf{Cay}(H, T)$ is undirected. The cases of $q = 3, 5$ are exceptional, because in those cases no inverse-closed subset of H has the required property.

Proposition 4.3. *Let q be prime, and*

$$T := \begin{cases} P_0 \cup P_1 \cup P_x \cup C_1 \cup C_{-1} & \text{where } x \in \mathbb{F} \text{ with } x \notin \{0, \pm 1, \pm 2, \frac{1}{2}\} \text{ and } x^6 \neq 1, \\ & \text{when } q > 7, \\ P_0 \cup P_1 \cup P_3 \cup C_1 \cup C_{-1} & \text{when } q = 7, \\ S_1 \cup P_0 & \text{when } q = 5, \\ S_1 \cup P_0 & \text{when } q = 3. \end{cases}$$

Then $\langle\langle \underline{T} \rangle\rangle = V(H, G_e)$. In particular, T is not a (D)CI-subset of H.

Proof. When $q \leq 7$, the result follows by computations with the computer algebra system Magma. Therefore for the rest of the proof we suppose $q > 7$.

According to Proposition 3.2 the basic sets of $V(H, G_e)$ are of three types: $S_a, C_b \cup C_{-b}, P_c$ with $a, b, c \in \mathbb{F}$ and $b \neq 0$. Thus we have three types of basic quantities $\underline{S_a}$, $\underline{C_b} + \underline{C_{-b}}, \underline{P_c}$ and

$$V(H, G_e) = \langle \underline{S_a}, \underline{C_b} + \underline{C_{-b}}, \underline{P_c} | a, b, c \in \mathbb{F}, b \neq 0 \rangle.$$

Set

$$H_1 := \{[1, \vec{v}] \mid \vec{v} \in \mathbb{F}^2\},$$
$$H_2 := \{[1, (t, 0)] \mid t \in \mathbb{F}\}.$$

By (2.1), H_1 and H_2 are subgroups of H with $|H_2| = q$, $|H_1| = q^2$ and, by Lemma 3.2, $H_2 = \cup_{t \in \mathbb{F}} S_t$. In Table 4.2 we have reported the multiplication table among the basic quantities of $V(H, G_e)$: this will serve us well.

	$\underline{S_r}$	$\underline{C_s}$	$\underline{P_t}$
$\underline{S_a}$	$\underline{S_{a+r}}$	$\underline{C_s}$	$\underline{P_{t-a}}$
$\underline{C_b}$	$\underline{C_b}$	$\begin{cases} q\underline{C_{b+s}} & \text{if } b+s \neq 0 \\ q\underline{H_2} & \text{if } b+s = 0 \end{cases}$	$\underline{H \setminus H_1}$
$\underline{P_c}$	$\underline{P_{c+r}}$	$\underline{H \setminus H_1}$	$q\underline{S_{-c+t}} + \underline{H_1 \setminus H_2}$

Table 1: Multiplication table for the basic quantities of $V(H, G_e)$.

Fix $a, b, c \in \mathbb{F}$ with $b, c \neq 0$ and let $\mathcal{A}$ be the smallest Schur ring of the group algebra $\mathbb{Q}H$ containing $\underline{P_a}, \underline{C_b} + \underline{C_{-b}}, \underline{S_c}$. We claim that

$$\mathcal{A} = V(H, G_e). \tag{4.2}$$

Clearly, $\mathcal{A} \leq V(H, G_e)$. From Table 4.2, for every $k \in \{0, \dots, q-1\}$, we have $\underline{S_c}^k = \underline{S_{ck}}$ and hence $\underline{S_{ck}} \in \mathcal{A}$. As $c \neq 0$, $\underline{S_i} \in \mathcal{A}$, for each $i \in \{0, \dots, q-1\}$. Now, as $\underline{P_a} \in \mathcal{A}$, from Table 4.2, we have $\underline{P_a} \cdot \underline{S_i} = \underline{P_{a+i}} \in \mathcal{A}$ for any $i \in \{0, \dots, q-1\}$. The equality $(\underline{C_b} + \underline{C_{-b}})^2 = 2q\underline{H_2} + q\underline{C_{2b}} + q\underline{C_{-2b}}$ implies $\underline{C_{2b}} + \underline{C_{-2b}} \in \mathcal{A}$. Now arguing inductively we deduce $\underline{C_k} + \underline{C_{-k}} \in \mathcal{A}$, for all $k \in \{1, \dots, q-1\}$. Thus (4.2) follows.

Let $x \in \mathbb{F}$ with $x \notin \{0, \pm 1, \pm 2, \frac{1}{2}\}$ and $x^6 \neq 1$, let $T := P_0 \cup P_1 \cup P_x \cup C_1 \cup C_{-1}$ and let $\mathcal{T} := \langle\langle \underline{T} \rangle\rangle$ (the existence of x is guaranteed by the fact that $q > 7$). We claim that

$$\underline{H_2},\ \underline{H_1},\ \underline{C_2} + \underline{C_{-2}},\ \underline{S_1} + \underline{S_{-1}} + \underline{S_x} + \underline{S_{-x}} + \underline{S_{1-x}} + \underline{S_{x-1}} \in \mathcal{T}. \tag{4.3}$$

Using Table 4.2 for squaring $\underline{T}$, we obtain (after rearranging the terms):

$$\begin{aligned} \underline{T}^2 =& 3q\underline{S_0} + q\underline{S_1} + q\underline{S_{-1}} + q\underline{S_x} + q\underline{S_{-x}} + q\underline{S_{1-x}} + q\underline{S_{x-1}} \\ &+ 9\underline{H_1 \setminus H_2} + 12\underline{H \setminus H_1} + q\underline{C_2} + q\underline{C_{-2}} + 2q\underline{H_2}. \end{aligned}$$

From the assumptions on x, the elements $-1, 1, -x, x, -(x-1), x-1$ are pairwise distinct. Therefore

$$\underline{T}^2 \circ \underline{S_b} = \begin{cases} 5q\underline{S_0}, & b = 0, \\ 3q\underline{S_b}, & \text{if } b \in \{\pm 1, \pm x, \pm(x-1)\}, \\ 2q\underline{S_b}, & \text{if } b \notin \{0, \pm 1, \pm x, \pm(x-1)\}, \end{cases}$$

$$\underline{T}^2 \circ \underline{C_b} = \begin{cases} (q+9)\underline{C_b}, & \text{if } b \in \{\pm 2\}, \\ 9\underline{C_b}, & \text{if } b \notin \{0, \pm 2\}, \end{cases}$$

$$\underline{T}^2 \circ \underline{P_b} = 12\underline{P_b}, \quad \text{if } b \in \mathbb{F}.$$

Since the numbers $6, 9, q+9, 2q, 3q, 5q$ are also pairwise distinct (because $q \neq 3$), an application of the Schur-Wielandt principle yields

$$\begin{aligned} (\underline{T}^2)_{3q} &= \underline{S_1} + \underline{S_{-1}} + \underline{S_x} + \underline{S_{-x}} + \underline{S_{1-x}} + \underline{S_{x-1}} \in \mathcal{T}, \\ (\underline{T}^2)_{12} &= \underline{H \setminus H_1} \in \mathcal{T}, \\ (\underline{T}^2)_{2q} &= \underline{H_2} - (\underline{S_0} + \underline{S_1} + \underline{S_{-1}} + \underline{S_x} + \underline{S_{-x}} + \underline{S_{1-x}} + \underline{S_{x-1}}) \in \mathcal{T}, \\ (\underline{T}^2)_{q+9} &= \underline{C_2} + \underline{C_{-2}} \in \mathcal{T}. \end{aligned}$$

From this, (4.3) immediately follows.

We claim that

$$\underline{S_1} + \underline{S_{-1}} \in \mathcal{T}. \tag{4.4}$$

Let

$$\mathcal{T}_{H_2} := \mathcal{T} \cap \mathbb{Q}H_2$$

and observe that $\mathcal{T}_{H_2}$ is a Schur ring over the cyclic group $H_2 \cong \mathbb{Z}_q$ of prime order q. It is well known that every Schur ring over $\mathbb{Z}_q$ is determined by a subgroup $M \leq \mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_q^*$ such that, every basic set of the corresponding Schur ring is an M-orbit. Let M be such a subgroup for $\mathcal{T}_{H_2}$. From (4.3), the simple quantity $\underline{S_1} + \underline{S_{-1}} + \underline{S_x} + \underline{S_{-x}} + \underline{S_{1-x}} + \underline{S_{x-1}}$ belongs to $\mathcal{T}_{H_2}$ and hence $\{\pm 1, \pm x, \pm(1-x)\}$ is a $\mathcal{T}_{H_2}$-subset of cardinality 6. It follows that $|M|$ divides six and $M \subseteq \{\pm 1, \pm x, \pm(1-x)\}$. If $|M| \in \{3, 6\}$, then $\{\pm 1, \pm x, \pm(1-x)\}$ is a subgroup of $\mathbb{Z}_q^*$, contrary to the assumption $x^6 \neq 1$. Therefore

$$\text{either } M = \{1\} \text{ or } |M| = \{\pm 1\}. \tag{4.5}$$

In both cases, $\{-1, 1\}$ is a union of M-orbits. Therefore, $\underline{S_1} + \underline{S_{-1}} \in \mathcal{T}_{H_2}$. From this, (4.4) follows immediately.

We are now ready to conclude the proof. Clearly, $\underline{T} \in V(H, G_e)$ and hence $\mathcal{T} \subseteq V(H, G_e)$. From (4.3), $\underline{H_1} \in \mathcal{T}$ and, from (4.4), $\underline{S_1} + \underline{S_{-1}} \in \mathcal{T}$. Therefore $\underline{H_1} \circ \underline{T} = \underline{C_1} + \underline{C_{-1}} \in \mathcal{T}$ and $(\underline{T} - \underline{H_1}) \circ \underline{T} = \underline{P_0} + \underline{P_1} + \underline{P_x} \in \mathcal{T}$. Therefore

$$\Big((\underline{P_0} + \underline{P_1} + \underline{P_x})(\underline{S_1} + \underline{S_{-1}})\Big) \circ (\underline{P_0} + \underline{P_1} + \underline{P_x}) \in \mathcal{T}.$$

As $(\underline{P_0} + \underline{P_1} + \underline{P_x})(\underline{S_1} + \underline{S_{-1}}) = \underline{P_1} + \underline{P_2} + \underline{P_{x+1}} + \underline{P_{-1}} + \underline{P_0} + \underline{P_{x-1}}$, we deduce

$$\Big((\underline{P_0} + \underline{P_1} + \underline{P_x})(\underline{S_1} + \underline{S_{-1}})\Big) \circ (\underline{P_0} + \underline{P_1} + \underline{P_x}) = \underline{P_0} + \underline{P_1}$$

and hence $\underline{P_0} + \underline{P_1} \in \mathcal{T}$. Therefore, $\underline{P_x} = (\underline{P_0} + \underline{P_1} + \underline{P_x}) - (\underline{P_0} + \underline{P_1}) \in \mathcal{T}$. As

$$(\underline{P_0} + \underline{P_1})\underline{P_x} = q\underline{S_x} + q\underline{S_{x-1}} + 2(\underline{H \setminus H_1}),$$

from the Schur-Wielandt principle, we obtain $\underline{S_x} + \underline{S_{x-1}} \in \mathcal{T}$. Therefore $\underline{S_x} + \underline{S_{x-1}} \in \mathcal{T}_{H_2}$ and hence $\{x, x-1\}$ is a $\mathcal{T}_{H_2}$-subset. Thus $\{x, x-1\}$ is an M-orbit. Recall (4.5). If $M = \{-1, 1\}$, then $x - 1 = -1 \cdot x = -x$, contrary to the assumption $x \neq 1/2$. Therefore $M = \{1\}$ and $\mathcal{T}_{H_2} = \mathbb{Q}H_2$. Thus $\underline{S_i} \in \mathcal{T}$, for each $i \in \mathbb{Z}_q$. Thus $\underline{S_1}, \underline{P_x}, \underline{C_1} + \underline{C_{-1}} \in \mathcal{T}$ and (4.2) implies $V(H, G_e) \subseteq \mathcal{T}$. □

5 Proof of Theorem 1.2

Proof of Theorem 1.2. The list of candidate CI-groups is on page 323 in [20]. From here, we see that, if R is in this list and if $R = \mathrm{Dih}(A)$ is generalised dihedral, then for every odd prime p the Sylow p-subgroup of R is either elementary abelian or cyclic of order 9.

Assume that the Sylow p-subgroup (p is an odd prime) of A is elementary abelian of rank at least 2. Let $P \leq A$ be a subgroup isomorphic to $\mathbb{Z}_p^2$ and let $x \in R \setminus A$. Then $\langle P, x\rangle \cong \mathrm{Dih}(\mathbb{Z}_p^2)$. By Proposition 4.3, $\mathrm{Dih}(\mathbb{Z}_p^2)$ contains a non-DCI subset. Therefore $\mathrm{Dih}(\mathbb{Z}_p^2)$ is a non-DCI-group. Since subgroups of a (D)CI-group are also (D)CI, we conclude that R is a not a DCI-group as well. The non-DCI set T constructed in Proposition 4.3 is symmetric for $p \geq 7$. Hence $\mathrm{Dih}(\mathbb{Z}_p^2)$ and, therefore, R are non-CI groups when $p \geq 7$. If $p = 5$, then the group $\mathrm{Dih}(\mathbb{Z}_p^2)$ contains a non-CI subset, namely: $P_0 \cup S_1 \cup S_{-1}$ (this was checked by Magma[1]). Combining these arguments we conclude that if $\mathrm{Dih}(A)$ is a CI-group, then its Sylow p-subgroup is cyclic if $p \geq 5$. If $p = 3$, then the Sylow 3-subgroup is either cyclic of order 9 or elementary abelian. The example in Section 2.2 shows that the rank of an elementary abelian group is bounded by 2. □

We now give the updated list of CI-groups. It is a combination of the list in [20], together with our results here and [12, Corollary 13] (note [12, Corollary 13] contains an error, and should list Q_8 on line (1c), not on line (1b)). We need to define one more group:

Definition 5.1. Let M be a group of order relatively prime to 3, and $\exp(M)$ be the largest order of any element of M. Set $E(M, 3) = M \rtimes_\phi \mathbb{Z}_3$, where $\phi(g) = g^\ell$, and ℓ is an integer satisfying $\ell^3 \equiv 1 \pmod{\exp(M)}$ and $\gcd(\ell(\ell-1), \exp(M)) = 1$.

Theorem 5.2. *Let G, M, and K be* CI-*groups with respect to graphs such that M and K are abelian, all Sylow subgroups of M are elementary abelian, and all Sylow subgroups of K are elementary abelian of order* 9 *or cyclic of prime order.*

(1) *If G does not contain elements of order* 8 *or* 9*, then $G = H_1 \times H_2 \times H_3$, where the orders of H_1, H_2, and H_3 are pairwise relatively prime, and*

  (a) *H_1 is an abelian group, and each Sylow p-subgroup of H_1 is isomorphic to $\mathbb{Z}_p^k$ for $k < 2p + 3$ or $\mathbb{Z}_4$;*

  (b) *H_2 is isomorphic to one of the groups $E(K, 2)$, $E(M, 3)$, $E(K, 4)$, A_4, or* 1*;*

  (c) *H_3 is isomorphic to one of the groups D_{10}, Q_8, or* 1.

[1]The automorphism group of the corresponding Cayley graph is 4 times bigger than G but the subgroups H and K are non-conjugate inside it.

(2) *If G contains elements of order* 8*, then* $G \cong E(K,8)$ *or* $\mathbb{Z}_8$*.*

(3) *If G contains elements of order* 9*, then G is one of the groups* $\mathbb{Z}_9 \rtimes \mathbb{Z}_2$*,* $\mathbb{Z}_9 \rtimes \mathbb{Z}_4$*,* $\mathbb{Z}_2^2 \rtimes \mathbb{Z}_9$*, or* $\mathbb{Z}_2^n \times \mathbb{Z}_9$*, with* $n \leq 5$*.*

Remark 5.3. The rank bound of an elementary abelian group used in part (1)(a) is due to [29].

Other than positive results already mentioned, the abelian groups known to be CI-groups are $\mathbb{Z}_{2n}$ [22], $\mathbb{Z}_{4n}$ [23] with n an odd square-free integer, $\mathbb{Z}_q \times \mathbb{Z}_p^2$ [18], $\mathbb{Z}_q \times \mathbb{Z}_p^3$ [31], and $\mathbb{Z}_q \times \mathbb{Z}_p^4$ [19] with q and p and distinct primes, and $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ [9]. Additional results are given in [4, Theorem 16] and [11] with technical restrictions on the orders of the groups. A similar result with technical restrictions on M is given in [4, Theorem 22] for some $E(M,3)$. Also, $E(\mathbb{Z}_p,4)$ and $E(\mathbb{Z}_p,8)$ were shown to be CI-groups in [21], and $Q_8 \times \mathbb{Z}_p$ in [30]. Finally, Holt and Royle have determined all CI-groups of order at most 47 [16]. Applying Theorem 5.2 to determine possible CI-groups, and then checking the positive results above to see that all possible CI-groups are known to be CI-groups, we extend the census of CI-groups up to groups of order at most 59. The isomorphism problem for circulant digraphs was independently solved in [13] and [26] (in both cases a polynomial time algorithm for solving the isomorphism problem was given). A polynomial time algorithm for finding the automorphism group of circulant digraph was provided in [27]. Finally, we remark that the groups $E(M,3)$ and $E(M,8)$ are *not* DCI-groups.

Appendix A An alternative approach

In this section we give an alternative approach to the proof of Theorem 1.2. We do not give all of the details - just the basic idea. In principle, this section is independent from the previous sections, but for convenience we deduce the main result from our previous work.

For each $g \in \mathsf{GL}_3(\mathbb{F})$, let $g^\top$ denote the transpose of the matrix g and let $g^\iota := (g^{-1})^\top$. It is easy to verify that $\iota : \mathsf{GL}_3(\mathbb{F}) \to \mathsf{GL}_3(\mathbb{F})$ is an automorphism. Let

$$s = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

and let α be the automorphism of $\mathsf{GL}_3(\mathbb{F})$ defined by

$$g^\alpha := s^{-1} g^\iota s = s^{-1}(g^{-1})^\top s, \tag{A.1}$$

for every $g \in \mathsf{GL}_3(\mathbb{F})$.

We now define $\hat{\alpha} \in \mathrm{Sym}(H)$ by

$$[a,(x,y)]^{\hat{\alpha}} = [a,(y^2/2 - x, ay)], \tag{A.2}$$

for every $[a,(x,y)] \in H$.

Lemma A.1. *Let α and $\hat{\alpha}$ be as in* (A.1) *and* (A.2)*. We have*

(1) $G^\alpha = G$ *and* $D^\alpha = D$*;*

(2) $K = H^\alpha$ *and* $H = K^\alpha$*;*

(3) *for every* $h \in H$, $(Dh)^\alpha = Dh^{\hat{\alpha}}$*;*

(4) *for every* $x \in \mathbb{F}$ *and for every* $t \in \mathbb{F}^*$, $S_x^{\hat{\alpha}} = S_{-x}, C_t^{\hat{\alpha}} = C_t, P_x^{\hat{\alpha}} = P_{-x}$.

Proof. The proof follows from straightforward computations. For every $a \in \{-1, 1\}$ and $x \in \mathbb{F}$, we have

$$\begin{aligned}
\begin{pmatrix} a & ax & ax^2/2 \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix}^\alpha &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \left(\begin{pmatrix} a & ax & ax^2/2 \\ 0 & 1 & x \\ 0 & 0 & a \end{pmatrix}^{-1} \right)^\top \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & -x & a(-x)^2/2 \\ 0 & 1 & a(-x) \\ 0 & 0 & a \end{pmatrix}^\top \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 & 0 \\ -x & 1 & 0 \\ a(-x)^2/2 & a(-x) & a \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \\
&= \begin{pmatrix} a & a(-x) & a(-x)^2/2 \\ 0 & 1 & -x \\ 0 & 0 & a \end{pmatrix} \in D.
\end{aligned}$$

This shows $D^\alpha = D$. The computations for proving $G = G^\alpha$, $K = H^\alpha$ and $H = K^\alpha$ are similar.

Let $h := [a, (x, y)] \in H$. A direct computation shows that

$$h^\alpha = \begin{pmatrix} a & 0 & x \\ 0 & a & y \\ 0 & 0 & 1 \end{pmatrix}^\alpha = \begin{pmatrix} 1 & -ay & -ax \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix}$$

and hence

$$\begin{aligned}
h^\alpha (h^{\hat{\alpha}})^{-1} &= \begin{pmatrix} 1 & -ay & -ax \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \left(\begin{pmatrix} a & 0 & y^2/2 - x \\ 0 & a & ay \\ 0 & 0 & 1 \end{pmatrix} \right)^{-1} \\
&= \begin{pmatrix} 1 & -ay & -ax \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \begin{pmatrix} a & 0 & -ay^2/2 + ax \\ 0 & a & -y \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} a & -y & ay^2/2 \\ 0 & 1 & -ay \\ 0 & 0 & a \end{pmatrix} \in D.
\end{aligned}$$

Therefore

$$(Dh)^\alpha = D^\alpha h^\alpha = Dh^\alpha = Dh^{\hat{\alpha}}$$

and part (3) follows. Now, part (4) follows immediately from Lemma 3.2 and part (3). □

Lemma A.2. *Let* $x \in \mathbb{F}$ *with* $x \notin \{0, \pm 1, \pm 2, \frac{1}{2}\}$ *and* $x^6 \neq 1$*, and let*

$$\begin{aligned}
T &:= P_0 \cup P_1 \cup P_x \cup C_1 \cup C_{-1}, \\
T' &:= P_0 \cup P_{-1} \cup P_{-x} \cup C_1 \cup C_{-1}.
\end{aligned}$$

Then $\mathsf{Cay}(H,T)$ *and* $\mathsf{Cay}(H,T')$ *are isomorphic but not Cayley isomorphic. In particular,* H *is not a* CI*-group.*

Proof. We view G as a permutation group on $D\backslash G$, which we may identify with H via the Schur notation.

It follows from Lemma A.1(1) and (3) that $\hat{\alpha}$ normalizes G. Therefore, $\hat{\alpha}$ permutes the orbitals of G. Since $\hat{\alpha}$ fixes $e = [1,(0,0)]$, $\hat{\alpha}$ permutes the suborbits of G and, from Lemma A.1(4), we have $\mathsf{Cay}(H,T^{\hat{\alpha}}) = \mathsf{Cay}(H,T')$. Hence $\mathsf{Cay}(H,T)^{\hat{\alpha}} = \mathsf{Cay}(H,T')$ and $\mathsf{Cay}(H,T) \cong \mathsf{Cay}(H,T')$.

Assume that there exists $\beta \in \mathsf{Aut}(H)$ with $\mathsf{Cay}(H,T)^{\beta} = \mathsf{Cay}(H,T')$. Then $\hat{\alpha}\beta^{-1}$ is an automorphism of $\mathsf{Cay}(H,T)$. It follows from Propositions 4.2 and 4.3 that $\hat{\alpha}\beta^{-1} \in \mathrm{Aut}(\mathsf{Cay}(H,T)) = G$. Therefore $\hat{\alpha} \in G\beta$. Since G and β normalize H, so does α. However, this contradicts Lemma A.1(2). □

On the previous proof, one could prove directly that there exists no automorphism β of H with $T^{\beta} = T'$; however, this requires some detailed computations, in the same spirit as the computations in Section 4.2.

ORCID iDs

Mikhail Muzychuk https://orcid.org/0000-0002-6346-8976
Pablo Spiga https://orcid.org/0000-0002-0157-7405
Ted Dobson https://orcid.org/0000-0003-2013-4594

References

[1] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336, doi:10.1007/BF01895854.

[2] L. Babai and P. Frankl, Isomorphisms of Cayley graphs. I, in: *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I*, North-Holland, Amsterdam, volume 18 of *Colloq. Math. Soc. János Bolyai*, pp. 35–52, 1978.

[3] E. Dobson, Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$, *Discrete Math.* **147** (1995), 87–94, doi:10.1016/0012-365X(95)00099-I.

[4] E. Dobson, On the Cayley isomorphism problem, *Discrete Math.* **247** (2002), 107–116, doi:10.1016/S0012-365X(01)00164-9.

[5] E. Dobson and I. Kovács, Automorphism groups of Cayley digraphs of $\mathbb{Z}_p^3$, *Electron. J. Comb.* **16** (2009), Research Paper 149, 20, doi:10.37236/238.

[6] E. Dobson and A. Malnič, Groups that are transitive on all partitions of a given shape, *J. Algebraic Combin.* **42** (2015), 605–617, doi:10.1007/s10801-015-0593-2.

[7] E. Dobson and J. Morris, Quotients of CI-groups are CI-groups, *Graphs Comb.* **31** (2015), 547–550, doi:10.1007/s00373-013-1400-2.

[8] E. Dobson, J. Morris and P. Spiga, Further restrictions on the structure of finite DCI-groups: an addendum, *J. Algebraic Combin.* **42** (2015), 959–969, doi:10.1007/s10801-015-0612-3.

[9] E. Dobson and P. Spiga, CI-groups with respect to ternary relational structures: new examples, *Ars Math. Contemp.* **6** (2013), 351–364, doi:10.26493/1855-3974.310.59f.

[10] E. Dobson and D. Witte, Transitive permutation groups of prime-squared degree, *J. Algebr. Comb.* **16** (2002), 43–69, doi:10.1023/A:1020882414534.

[11] T. Dobson, On the isomorphism problem for Cayley graphs of abelian groups whose Sylow subgroups are elementary abelian cyclic, *Electron. J. Comb.* **25** (2018), Paper No. 2.49, doi: 10.37236/4983.

[12] T. Dobson, Some new groups which are not CI-groups with respect to graphs, *Electron. J. Comb.* **25** (2018), Paper No. 1.12, doi:10.37236/6541.

[13] S. A. Evdokimov and I. N. Ponomarenko, Recognition and verification of an isomorphism of circulant graphs in polynomial time, *Algebra i Analiz* **15** (2003), 1–34, doi:10.1090/s1061-0022-04-00833-7.

[14] I. A. Faradžev, M. H. Klin and M. E. Muzichuk, Cellular rings and groups of automorphisms of graphs, in: *Investigations in algebraic theory of combinatorial objects*, Kluwer Acad. Publ., Dordrecht, volume 84 of *Math. Appl. (Soviet Ser.)*, pp. 1–152, 1994, doi: 10.1007/978-94-017-1972-8_1.

[15] Y.-Q. Feng and I. Kovács, Elementary abelian groups of rank 5 are DCI-groups, *J. Comb. Theory Ser. A* **157** (2018), 162–204, doi:10.1016/j.jcta.2018.02.003.

[16] D. Holt and G. Royle, A census of small transitive groups and vertex-transitive graphs, *J. Symb. Comput.* **101** (2020), 51–60, doi:10.1016/j.jsc.2019.06.006.

[17] H. Koike and I. Kovács, A classification of nilpotent 3-BCI graphs, *Int. J. Group Theory* **8** (2019), 11–24, doi:10.22108/ijgt.2017.100795.1404.

[18] I. Kovács and M. Muzychuk, The group $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ is a CI-group, *Comm. Algebra* **37** (2009), 3500–3515, doi:10.1080/00927870802504957.

[19] I. Kovács and G. Ryabov, The group $C_p^4 \times C_q$ is a DCI-group, *Discrete Mathematics* **345** (2022), 112705, doi:10.1016/j.disc.2021.112705.

[20] 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.

[21] C. H. Li, Z. P. Lu and P. P. Pálfy, Further restrictions on the structure of finite CI-groups, *J. Algebr. Comb.* **26** (2007), 161–181, doi:10.1007/s10801-006-0052-1.

[22] M. Muzychuk, Ádám's conjecture is true in the square-free case, *J. Comb. Theory Ser. A* **72** (1995), 118–134, doi:10.1016/0097-3165(95)90031-4.

[23] M. Muzychuk, On Ádám's conjecture for circulant graphs, *Discrete Math.* **167-168** (1997), 497–510, doi:10.1016/s0012-365x(96)00251-8.

[24] M. Muzychuk, On the isomorphism problem for cyclic combinatorial objects, *Discrete Math.* **197/198** (1999), 589–606, doi:10.1016/S0012-365X(99)90119-X.

[25] M. Muzychuk, An elementary abelian group of large rank is not a CI-group, *Discrete Math.* **264** (2003), 167–185, doi:10.1016/s0012-365x(02)00558-7.

[26] M. Muzychuk, A solution of the isomorphism problem for circulant graphs, *Proc. Lond. Math. Soc. (3)* **88** (2004), 1–41, doi:10.1112/s0024611503014412.

[27] I. N. Ponomarenko, Determination of the automorphism group of a circulant association scheme in polynomial time, *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)* **321** (2005), 251–267, 301, doi:10.1007/s10958-006-0217-4.

[28] G. Sabidussi, On a class of fixed-point-free graphs, *Proc. Am. Math. Soc.* **9** (1958), 800–804, doi:10.2307/2033090.

[29] G. Somlai, Elementary abelian p-groups of rank $2p + 3$ are not CI-groups, *J. Algebr. Comb.* **34** (2011), 323–335, doi:10.1007/s10801-011-0273-9.

[30] G. Somlai, The Cayley isomorphism property for groups of order $8p$, *Ars Math. Contemp.* **8** (2015), 433–444, doi:10.26493/1855-3974.593.12f.

[31] G. Somlai and M. Muzychuk, The Cayley isomorphism property for $\mathbb{Z}_p^3 \times \mathbb{Z}_q$, *Algebr. Comb.* **4** (2021), 289–299, doi:10.5802/alco.154.

[32] P. Spiga, CI-property of elementary abelian 3-groups, *Discrete Math.* **309** (2009), 3393–3398, doi:10.1016/j.disc.2008.08.002.

[33] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.