NON-CAYLEY-ISOMORPHIC CAYLEY GRAPHS FROM NON-CAYLEY-ISOMORPHIC CAYLEY DIGRAPHS

DAVE WITTE MORRIS AND JOY MORRIS

Abstract. A finite group G is a *non-DCI group* if there exist subsets S_1 and S_2 of G, such that the associated Cayley digraphs $\mathsf{Cay}\overrightarrow{\ }(G;S_1)$ and $\mathsf{Cay}\overrightarrow{\ }(G;S_2)$ are isomorphic, but no automorphism of G carries S_1 to S_2. Furthermore, G is a *non-CI group* if the subsets S_1 and S_2 can be chosen to be closed under inverses, so we have undirected Cayley graphs $\mathrm{Cay}(G;S_1)$ and $\mathrm{Cay}(G;S_2)$.

We show that if p is a prime number, and the elementary abelian p-group $(\mathbb{Z}_p)^r$ is a non-DCI group, then $(\mathbb{Z}_p)^{r+3}$ is a non-CI group. In most cases, we can also show that $(\mathbb{Z}_p)^{r+2}$ is a non-CI group. In particular, from Pablo Spiga's proof that $(\mathbb{Z}_3)^8$ is a non-DCI group, we conclude that $(\mathbb{Z}_3)^{10}$ is a non-CI group. This is the first example of a non-CI elementary abelian 3-group.

0. Preliminaries

We state some basic definitions, in order to establish our conventions.

Definition 0.1 (cf. [7, pp. 302 and 307])**.** Let G be a finite group.

(1) For any subset S of G, the *Cayley digraph* $\mathsf{Cay}\overrightarrow{\ }(G;S)$ is the directed graph with vertex set G, and with a directed edge $g \to h$ if and only if $h \in Sg$.
(2) If S is *symmetric* (i.e., if $S = S^{-1}$), then $\mathsf{Cay}\overrightarrow{\ }(G;S)$ can be viewed as an undirected graph, by replacing each pair of oppositely directed edges ($x \to y$ and $y \to x$) with an undirected edge ($x \text{ — } y$), and replacing each directed loop ($x \to x$) with an undirected loop ($x \text{ — } x$). This undirected graph is called a *Cayley graph*, and is denoted $\mathrm{Cay}(G;S)$.
(3) We often refer to S as the *connection set* of $\mathsf{Cay}\overrightarrow{\ }(G;S)$ or $\mathrm{Cay}(G;S)$.
(4) A Cayley graph $\mathrm{Cay}(G;S)$ is said to be a *CI graph* if, for every symmetric subset S' of G, such that $\mathrm{Cay}(G;S) \cong \mathrm{Cay}(G;S')$, there is an automorphism α of G, such that $\alpha(S) = S'$.
(5) Similarly, a Cayley digraph $\mathsf{Cay}\overrightarrow{\ }(G;S)$ is said to be a *DCI digraph* if, for every subset S' of G, such that $\mathsf{Cay}\overrightarrow{\ }(G;S) \cong \mathsf{Cay}\overrightarrow{\ }(G;S')$, there is an automorphism α of G, such that $\alpha(S) = S'$.
(6) G is a *CI group* if every Cayley graph of G is a CI graph, and
(7) G is a *DCI group* if every Cayley digraph of G is a DCI digraph.

Thus, the difference between "CI" and "DCI" is whether only undirected graphs are considered (so the generating set S is required to be symmetric), or all digraphs are allowed (so S can be any subset of G).

Remark 0.2. The terminology in (6) and (7) is not entirely standard: some authors use "CI" for the concept that we call "DCI," and may use a phrase such as "CI with respect to undirected graphs" for the concept that we call "CI." The letters "CI" are an abbreviation of "Cayley Isomorphism" [7, §3].

1. Introduction

Most finite groups are not CI groups. In particular, it is known that every CI group has a subgroup of index at most 24 that is a direct product of elementary abelian groups [8, Thm. 1.2]. (Recall that a group is *elementary abelian* if it is isomorphic to $(\mathbb{Z}_p)^r$, for some prime number p,

Date: April 18, 2024.

$$S_{0,0,0} = \{v_1, v_3, v_4, v_5\}$$
$$S_{1,0,0} = \{w_1 + av_1 + bv_2 + cv_5 : a, b, c \in \mathbb{Z}_3\}$$
$$S_{0,1,0} = \{w_2 + av_1 + bv_3 + cv_4 + dv_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{0,0,1} = \{w_3 + av_2 + bv_3 + cv_4 + dv_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{1,1,0} = \{w_1 + w_2 + av_1 + bv_2 + cv_3 + bv_4 + dv_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{1,0,1} = \{w_1 + w_3 + av_1 + bv_2 + av_3 + cv_4 + dv_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{0,1,1} = \{w_2 + w_3 + av_1 + bv_2 + cv_3 + dv_4 - (a + b)v_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{1,1,1} = \{w_1 + w_2 + w_3 + av_1 + bv_2 + cv_3 + dv_4 + (-a - b + c + d)v_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{2,1,1} = \{2w_1 + w_2 + w_3 + av_1 + bv_2 + cv_3 + dv_4 - (a + b + c + d)v_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{1,2,1} = \{w_1 + 2w_2 + w_3 + av_1 + bv_2 + cv_3 + dv_4 + (a + b - c + d)v_5 : a, b, c, d \in \mathbb{Z}_3\}$$
$$S_{1,1,2} = \{w_1 + w_2 + 2w_3 + av_1 + bv_2 + cv_3 + dv_4 + (a + b + c - d)v_5 : a, b, c, d \in \mathbb{Z}_3\}$$

FIGURE 1. Eleven sets $S_{i,j,k}$ whose union is the connection set for P. Spiga's non-DCI Cayley digraph of $(\mathbb{Z}_3)^8$.

and some $r \geq 0$.) However, it is not known which groups with this property are indeed CI groups. (See the survey [7].) Therefore, a fundamental problem in the theory of CI groups is to determine which elementary abelian groups are CI groups. Since every subgroup of a CI group is a CI group [2, Lem. 3.2], it suffices to determine, for each prime p, the smallest natural number r, such that $(\mathbb{Z}_p)^r$ is *not* a CI group. This number is 6 for $p = 2$ [3, 13], and it is known that the number is at least 6 for all p [6], but the exact value is unknown for every $p > 2$.

To provide an upper bound, G. Somlai [15, Thm. 2] showed in 2011 that if $p > 3$, then the elementary abelian group of order p^{2p+3} is not a CI group. However, Somlai [15, p. 324] also pointed out that the case $p = 3$ remained open: it was not known whether there is an elementary abelian 3-group that is not a CI group, even though P. Spiga [17, Thm. 2] had proved two years earlier that the elementary abelian group of order 3^8 is not a DCI group (see Theorem 1.3), and larger examples of non-DCI elementary abelian 3-groups had been constructed previously [11, 16]. To fill this gap in the literature, we show that every example of a non-DCI elementary abelian p-group will automatically yield an example of a (slightly larger) non-CI elementary abelian p-group (for the same prime p), even if $p = 3$:

Theorem 1.1. *If $(\mathbb{Z}_p)^r$ is not a DCI group (and p is prime), then $(\mathbb{Z}_p)^{r+3}$ is not a CI group.*

Moreover, the following result shows that we can usually decrease the exponent in our answer by 1. (In fact, it will be explained in Remark 1.5(2) that the exponent $r + 2$ will always suffice, but this improvement relies on a theorem that was proved after the original version of this paper was written.)

Theorem 1.2. *Assume $(\mathbb{Z}_p)^r$ is not a DCI group (and p is prime). If either of the following is true, then $(\mathbb{Z}_p)^{r+2}$ is not a CI group:*

(1) *$p \neq 3$, or*
(2) *there is a non-DCI Cayley digraph $\overrightarrow{\mathsf{Cay}}\big((\mathbb{Z}_p)^r; S\big)$, such that $|S| < p^{r-1}$.*

For the reader's convenience, we recall the detailed statement of the following important example (that was mentioned above).

Theorem 1.3 (Spiga [17, proof of Thm. 2])**.** *Let $\{w_1, w_2, w_3, v_1, v_2, v_3, v_4, v_5\}$ be a generating set of $(\mathbb{Z}_3)^8$, and let S be the union of the sets $S_{i,j,k}$ that are defined in Figure 1. Then $\overrightarrow{\mathsf{Cay}}\big((\mathbb{Z}_3)^8; S\big)$ is a non-DCI digraph.*

We see from Figure 1 that the outvalency of this Cayley digraph (i.e., the cardinality of the connection set S) is $4 + 3^3 + 9 \cdot 3^4 = 760$. Since $760 < 3^7$ $(= 2187)$, we immediately deduce the following from Theorem 1.2(2). It is the first example of a non-CI elementary abelian 3-group.

Corollary 1.4. $(\mathbb{Z}_3)^{10}$ *is not a CI group.*

Remarks 1.5.

(1) By modifying Spiga's example, the second author [9] has shown that $(\mathbb{Z}_3)^8$ is not a CI group. Therefore, Corollary 1.4 may be of limited interest. However, the argument in [9] is longer (and more intricate) than the proofs here (and that paper was completed after this one). (Part of the reason our proof of Corollary 1.4 is short is that we assume it is known that Spiga's example is not a DCI digraph, but [9] also makes this assumption.)

(2) If we assume the above-mentioned fact that $(\mathbb{Z}_3)^8$ is not a CI group, then the conclusion of Theorem 1.2 is true even without assuming (1) or (2):

if $(\mathbb{Z}_p)^r$ *is not a DCI group, then* $(\mathbb{Z}_p)^{r+2}$ *is not a CI group.*

To see this, note that we may assume $p = 3$ (for otherwise Theorem 1.2(1) applies). However, P. Spiga [17, Thm. 1] showed that $(\mathbb{Z}_3)^5$ is a DCI group, so we must have $r \geq 6$. Then $r + 2 \geq 8$. If we assume that $(\mathbb{Z}_3)^8$ is not a CI group, then this implies $(\mathbb{Z}_p)^{r+2}$ is not a CI group, as desired. Note that part (2) of Theorem 1.2 was not used in this argument. In fact, knowing that $(\mathbb{Z}_3)^8$ is not a CI group makes this part of the theorem superfluous.

(3) Theorem 1.2(1) may have a better chance of being useful in the future. For example, if it is ever proved that there is a constant C, such that, for every prime p, the elementary abelian group of order p^C is not a DCI group, then it will immediately follow that there is a constant C', such that the elementary abelian group of order $p^{C'}$ is not a CI group.

(4) Every Cayley graph is a Cayley digraph, so (as is well known) it is clear that every DCI group is a CI group. The reverse is not true. Indeed, the paper [4] provides infinitely many examples of CI groups that are not DCI groups. However, it is not known whether the two properties are equivalent for elementary abelian groups. In some sense, Theorem 1.1 shows, for this class of groups, that the two properties are closely related (even if they are not exactly the same).

(5) The CI property is a Cayley Isomorphism property for graphs, and the DCI property is a Cayley Isomorphism property for digraphs, so comparing CI with DCI is a comparison of the Cayley Isomorphism property for two different relational structures (symmetric binary relations vs. arbitrary binary relations). It is also interesting to consider other relational structures. In particular:
   (a) P. Pálfy [14] showed that the cyclic group $\mathbb{Z}_n$ has the Cayley Isomorphism property for all relational structures if and only if either $n = 4$ or $\gcd\big(n, \phi(n)\big) = 1$ (where ϕ is the the Euler totient function).
   (b) For relational structures with a cyclic, transitive group of automorphisms, M. Muzychuk [10] reduced the isomorphism problem to the case where the number of points is a power of a prime number.
   (c) E. Dobson and P. Spiga [5] (and others) have studied the Cayley Isomorphism problem for ternary relations.
   (d) M. Muzychuk and G. Somlai [12] studied the Cayley Isomorphism property for Cayley maps. Every Cayley map has an associated ternary relational structure, so this is related to (c).

Our construction of a non-CI Cayley graph $\mathrm{Cay}(\widehat{G}; \widehat{S})$ from a non-DCI Cayley digraph $\mathsf{Cay}\overrightarrow{\mathsf{}}(G; S)$ is in Notation 2.3. It is a fairly straightforward adaptation of the well-known observation that if $\widetilde{X}$ is the bipartite double cover of a digraph $\overrightarrow{X}$, i.e., if:

- $V(\widetilde{X}) = V(\overrightarrow{X}) \times \{0,1\}$, and
- $(x,0)$ is adjacent to $(y,1)$ in $\widetilde{X} \iff$ there is a directed edge from x to y in $\overrightarrow{X}$,

and we define a permutation $\widetilde{\pi}$ of $V(\widetilde{X})$ by $\widetilde{\pi}(x,i) = \big(\pi(x), i\big)$, where π is a permutation of $V(\overrightarrow{X})$, then

$\widetilde{\pi}$ is an automorphism of the graph $\widetilde{X} \iff \pi$ is an automorphism of the directed graph $\overrightarrow{X}$.

Acknowledgements. We thank two anonymous referees for their helpful comments that corrected errors and improved the exposition. The second author was partially supported by the Natural Science and Engineering Research Council of Canada (grant RGPIN-2017-04905).

2. Proofs of the main results

This section proves Theorem 2.2, which easily implies the main results that were stated in the Introduction (i.e., Theorems 1.1 and 1.2). Although elementary abelian groups are our primary interest, the result is stated more generally, because assuming that the group G is (elementary) abelian would not simplify the argument to any significant extent.

Notation 2.1. If $\overrightarrow{X}$ is a digraph, then $\overrightarrow{X}^-$ is the digraph that is obtained from $\overrightarrow{X}$ by reversing all of its directed edges.

Theorem 2.2. *Assume*

- *G is a finite group,*
- *$\overrightarrow{X} = \overrightarrow{\mathsf{Cay}}(G; S)$ is a non-DCI Cayley digraph,*
- *$n \geq 3$ and $k = \begin{cases} 2 & \text{if } n > 3; \\ 3 & \text{if } n = 3, \end{cases}$*
- *either $n > 3$ or $|S \cup \{1_G\}| \leq |G|/3$,*
- *$m \geq 3$ and $mk \neq |G|$,*
- *A is a group of order m, and*
- *either $\overrightarrow{X} \ncong \overrightarrow{X}^-$ or there is an automorphism α of G, such that $\alpha(S) = S^{-1}$.*

Then $G \times A \times \mathbb{Z}_n$ is not a CI group.

Before proving this theorem, let us show that it contains Theorem 1.2 as a special case, and then derive Theorem 1.1 from this latter result.

Proof of Theorem 1.2. For $p = 2$, it is well known that $(\mathbb{Z}_2)^r$ is a CI group if and only if it is a DCI group. (Every element of $(\mathbb{Z}_2)^r$ is equal to its inverse, so every generating set is symmetric. Hence, every Cayley digraph of $(\mathbb{Z}_2)^r$ is also a Cayley graph.) Therefore, we may assume $p > 2$.

Let $G = (\mathbb{Z}_p)^r$, $m = n = p$, and $A = \mathbb{Z}_p$, so $G \times A \times \mathbb{Z}_n = G \times (\mathbb{Z}_p)^2$. Since $(\mathbb{Z}_p)^r$ is not a DCI group, there is a non-DCI Cayley digraph $\overrightarrow{X} = \overrightarrow{\mathsf{Cay}}(G; S)$. Also note that, since G is abelian, the function $\alpha(g) = g^{-1}$ is a group automorphism, and it obviously has the property that $\alpha(S) = S^{-1}$.

Assume, for the moment, that $p > 3$. Then $k = 2$ is not a power of p, so it is obvious that $mk \neq p^r = |G|$. Therefore, all of the hypotheses of Theorem 2.2 are satisfied, so $G \times A \times \mathbb{Z}_n$ is not a CI group.

We now assume $p = 3$. In this case, Condition (2) in the statement of Theorem 1.2 must hold, so we may assume $|S| \leq 3^{r-1} - 1$. Then

$$|S \cup \{1_G\}| \leq |S| + 1 \leq (3^{r-1} - 1) + 1 = 3^{r-1} = |G|/3.$$

Also, it is well known that $(\mathbb{Z}_p)^2$ is a DCI group (in fact, even $(\mathbb{Z}_p)^5$ is a DCI group [6]), so $|G| \neq 3^2 = 3 \cdot 3 = mk$. Therefore, all of the hypotheses of Theorem 2.2 are satisfied again, so $G \times A \times \mathbb{Z}_n$ is not a CI group. □

Proof of Theorem 1.1. We may assume $p = 3$, for otherwise Theorem 1.2(1) applies. Then, by assumption, there is a non-DCI, Cayley digraph $\overrightarrow{\mathsf{Cay}}\big((\mathbb{Z}_3)^r; S\big)$. Via the natural embedding of $(\mathbb{Z}_3)^r$ in $(\mathbb{Z}_3)^{r+1}$, we also have the Cayley digraph $\overrightarrow{\mathsf{Cay}}\big((\mathbb{Z}_3)^{r+1}; S\big)$, which is also non-DCI. Since $S \cup \{1\} \subseteq (\mathbb{Z}_3)^r$, we have $|S \cup \{1\}| \leq |(\mathbb{Z}_3)^r| = |(\mathbb{Z}_3)^{r+1}|/3$, so we conclude from Theorem 1.2(2) (with $r+1$ in the place of r) that $(\mathbb{Z}_3)^{(r+1)+2}$ is not a CI group. □

The remainder of this section will prove Theorem 2.2. To get started, we fix some notation.

Notation 2.3. Let

- $\overrightarrow{X} = \overrightarrow{\mathsf{Cay}}(G; S)$ be a Cayley digraph of a nontrivial finite group G, such that $S \neq S^{-1}$ (so $\overrightarrow{X}$ is not an undirected graph),
- $n \geq 3$ and $k = \begin{cases} 2 & \text{if } n > 3; \\ 3 & \text{if } n = 3, \end{cases}$
- A be a group of order $m \geq 3$,
- $B = \langle b \rangle$ be a (multiplicative) cyclic group of order n,
- $\widehat{G} = G \times A \times B$ (so G, A, and B can be naturally identified with subgroups of $\widehat{G}$ that centralize each other),
- $\widehat{S} = G \cup Sb \cup A \cup Ab$, and
- $\widehat{X} = \mathrm{Cay}\big(\widehat{G}, \widehat{S}^{\pm 1}\big)$, where $\widehat{S}^{\pm 1} = \widehat{S} \cup \{\, \hat{s}^{-1} \mid \hat{s} \in \widehat{S} \,\}$.

Note that, since G, A, and B are normal subgroups of $\widehat{G}$, there is no need to specify whether cosets of these subgroups are right cosets or left cosets.

Remark 2.4. In our applications, we will take $G = (\mathbb{Z}_p)^r$ and $A = B = \mathbb{Z}_p$, for some prime p. To prove Theorem 2.2, we will show that if $\overrightarrow{X}$ is not a DCI digraph, and some minor technical conditions are satisfied, then $\widehat{X}$ is not a CI graph.

Notation 2.5 ([1, §2])**.** For any group H, we use H_R to denote the *right regular representation* of H. This consists of all permutations of H that have the form $x \mapsto xh$, for some $h \in H$.

The following well known, fundamental theorem shows that being a CI graph (or CI digraph) is a property of the automorphism group of the graph (or digraph).

Theorem 2.6 (Babai [1, Lem. 3.1], or [7, Thm. 4.1])**.** *A Cayley graph (or Cayley digraph) Y of a group H is a CI graph (or DCI digraph) if and only if the conjugates of H_R are the only subgroups of* $\mathrm{Aut}\, Y$ *that are isomorphic to H and act sharply transitively on $V(Y)$.*

Adding a directed loop at every vertex of a digraph does not affect the automorphism group of the digraph. Therefore, the following causes no loss of generality:

Assumption 2.7. Assume $1_G \in S$, which means that $\overrightarrow{\mathsf{Cay}}(G; S)$ has a directed loop at every vertex.

Remark 2.8. Since $b \in Ab$, we know that $b \in \widehat{S}$, even without Assumption 2.7. Therefore, adding 1_G to S does not change $\widehat{S}$ at all. The reason for making Assumption 2.7 is to ensure that Sb is the set of all outneighbours of $1_{\widehat{G}}$ that are in the coset Gb. This avoids needing to treat the vertex b as a special case when looking at the outneighbours of 1_G.

The following simple result provides a crucial connection between $\mathrm{Aut}\, \overrightarrow{X}$ and $\mathrm{Aut}\, \widehat{X}$.

Proposition 2.9. *Suppose φ is an automorphism of $\widehat{X}$, such that*

(1) $\varphi(1) = 1$,
(2) *φ maps each coset of G to a coset of G, and*
(3) *φ maps each coset of AB to a coset of AB.*

Then the restriction of φ to G is either an automorphism of $\overrightarrow{X}$ or an isomorphism from $\overrightarrow{X}$ to $\overrightarrow{X}^-$.

Proof. By (2), we know that φ maps G to some coset of G. Since $\varphi(1) = 1$, this implies that

$$\varphi(G) = G.$$

So the restriction of φ to G is a permutation of G.

From the definition of $\widehat{S}$, we see that 1 has $|S|$ neighbours in the coset Gb and also has $|S|$ neighbours in the coset Gb^{-1} (and has $|G|$ neighbours in its own coset G) but has at most one neighbour in any other coset of G. Therefore,

$$\varphi(Gb) = Gb^{\epsilon}, \text{ for some } \epsilon \in \{\pm 1\}.$$

Let $\overrightarrow{X}^{\epsilon}$ be $\overrightarrow{X}$ or $\overrightarrow{X}^-$, depending on whether ϵ is 1 or -1, respectively.

We claim that $\varphi(gb) = \varphi(g)b^{\epsilon}$, for every $g \in G$. To see this, note that (3) implies $\varphi(gb) \in \varphi(g)AB$. Also, we see from the above displayed equations that $\varphi(gb) \in Gb^{\epsilon} = \varphi(g)Gb^{\epsilon}$. Since $(AB) \cap G = \{1\}$, this implies the claim.

We can now complete the proof, by showing that the restriction of φ to G is an isomorphism from $\overrightarrow{X}$ to $\overrightarrow{X}^{\epsilon}$. To this end, let $g, h \in G$, such that $g \to h$ in $\overrightarrow{X}$. This means there exists $s \in S$, such that $h = sg$. Since $sb \in Sb$, we have $g \text{ — } (sb)g$ in $\widehat{X}$. Since $\varphi \in \operatorname{Aut} \widehat{X}$, this implies

$$\varphi(g) \text{ — } \varphi\big((sb)g\big) = \varphi\big((sg)b\big) = \varphi(sg)b^{\epsilon}.$$

Since $\varphi(g), \varphi(sg) \in G$, we see from the definition of $\widehat{S}$ that this implies $\varphi(sg) = t^{\epsilon}\varphi(g)$, for some $t \in S$. Hence, there is a directed edge from $\varphi(g)$ to $\varphi(sg)$ in $\overrightarrow{X}^{\epsilon}$.

We have shown that if $g \to h$ in $\overrightarrow{X}$, then $\varphi(g) \to \varphi(h)$ in $\overrightarrow{X}^{\epsilon}$. Since $\overrightarrow{X}$ and $\overrightarrow{X}^{\epsilon}$ are regular digraphs of the same outvalency, this implies that the permutation $\varphi|_G$ is an isomorphism of digraphs. □

Our next series of lemmas culminates in Lemma 2.12, which establishes simple conditions that imply the hypotheses of the above proposition are satisfied. That will complete our preparations for the proof of Theorem 2.2.

Lemma 2.10. *If $n > 3$, then every maximal clique of $\widehat{X}$ is induced by one of the following sets of vertices (for some $x \in \widehat{G}$):*

(a) *Gx (i.e., a coset of the subgroup G),*
(b) *$Ax \cup Abx$, or*
(c) *a subset of $Gx \cup Gbx$ that does not contain any coset of G.*

If $n = 3$, then (b) *and* (c) *are replaced with:*

(b′) *ABx, and*
(c′) *a subset of GBx that does not contain any coset of G.*

Conversely, the subgraph induced by each subset listed in (a) *or* (b/b′) *is a maximal clique.*

Proof. We first prove the "converse" that is stated the final sentence of the lemma. Assume, without loss of generality, that $x = 1$.

(a) Since G is contained in $\widehat{S}$, it is clear that the subgraph induced by G is a clique. So we just need to show that the clique is maximal. Suppose $y \in \widehat{G}$, such that $y \notin G$, but y is adjacent to every vertex in G. After translating by an element of G, we may assume $y \in AB$. Since y is adjacent to 1, we also know that $y \in \widehat{S}^{\pm 1}$. Hence, $y \in A \cup Ab \cup Ab^{-1}$ (and $y \neq 1$). Since $S \neq S^{-1}$ (see Notation 2.3), there is some nontrivial $g \in G$, such that $g^{-1} \notin S$. Now, we see from the definition of $\widehat{S}$ that:

- If $s \in \widehat{S}$, such that $sg \in AB$, and $sg \neq 1$, then $s \in (Sb)^{-1}$. Hence, g is not adjacent to any element of A or Ab. Therefore, $y \notin A \cup Ab$.

- Similarly, if $s \in \widehat{S}$, such that $sg^{-1} \in AB$, and $sg^{-1} \neq 1$, then $s \in Sb$. Hence, g^{-1} is not adjacent to any element of Ab^{-1}. Therefore, $y \notin Ab^{-1}$.

This is a contradiction. So we conclude that the clique induced by G is indeed maximal.

(b) Since A is contained in $\widehat{S}$, it is clear that A and Ab each induce a clique. Also, we know that every vertex in A is adjacent to every vertex in Ab, because Ab is contained in $\widehat{S}$. Therefore, the subgraph induced by $A \cup Ab$ is a clique. So we just need to show that this clique is maximal. Suppose $y \in \widehat{G}$, such that $y \notin A \cup Ab$, but y is adjacent to every vertex in $A \cup Ab$. Since y is adjacent to 1, we know that $y \in \widehat{S}^{\pm 1}$. Since $y \notin A \cup Ab$, we conclude that $y \in G \cup Sb \cup Sb^{-1} \cup Ab^{-1}$. Since $n > 3$, no element of GAb^{-1} is adjacent to any element of Ab. Therefore, we must have $y \in G \cup Sb$ (and $y \neq 1, b$). Then every neighbour of y that is in AB must be in

$$Gy \cup Sby \cup (Sb)^{-1}y \subseteq GBy.$$

Since GBy does not include any nontrivial elements of A, this contradicts the fact that y is adjacent to every vertex in A.

(b′) Since $n = 3$, we have $AB \subseteq \widehat{S}$, so the subgraph induced by AB is a clique. So we just need to show that this clique is maximal. Suppose $y \in \widehat{G}$, such that $y \notin AB$, but y is adjacent to every vertex in AB. We may assume $y \in G$ (after translating by an element of AB). This implies that y is not adjacent to any nontrivial element of A (see the proof of case (b)). This is a contradiction.

Now, let C be any maximal clique in $\widehat{X}$, and assume, without loss of generality, that $1 \in C$. This implies $C \subseteq \widehat{S}^{\pm 1}$. We will prove that C is contained in a clique of type (a), (b), (b′), (c), or (c′).

Case 1. *Assume C is not contained in any coset of GB.* Then C must contain some vertex of the form gab^i where $g \in G$, $i \in \mathbb{Z}$, and a is a nontrivial element of A. Since $gab^i \in C \subseteq \widehat{S}^{\pm 1}$, we must have $g = 1$ and $i \in \{0, \pm 1\}$.

Now, let v be any common neighbour of 1 and ab^i. Since a is nontrivial, these two elements are in different cosets of GB, so we can choose some $c \in \{1, ab^i\}$ that is not in the coset GBv. Then (by the preceding argument) we have $v = a'b^j c$, for some $a' \in A$ and $j \in \{0, \pm 1\}$. Hence, we have $v \in AB$. This shows that C is contained in a maximal clique of type (b′) if $n = 3$.

So we may assume $n > 3$. Then no vertex in Ab is adjacent to any vertex in Ab^{-1}. Thus, C must be contained in either $A \cup Ab$ or $Ab^{-1} \cup A$. Each of these sets is of type (b) (with $x \in \{1, b^{-1}\}$).

Case 2. *Assume C is contained in a coset of GB, and is not of type* (a). Since $1 \in C$, we must have $C \subseteq GB$. We also know that C does not contain any coset of G (since cosets of G induce maximal cliques of type (a)), so we may assume $n > 3$, for otherwise C is of type (c′). Note that

$$C \subseteq GB \cap \widehat{S}^{\pm 1} = G \cup Gb \cup Gb^{-1}.$$

However, no vertex in Gb is adjacent to any vertex in Gb^{-1} (since $n > 3$), so we conclude that C is contained in either $G \cup Gb$ or $Gb^{-1} \cup G$. So C is of type (c) (with $x \in \{1, b^{-1}\}$). □

Without Assumption 2.7 (which tells us that S contains the identity element of G), the conclusion of the following lemma would only be that S is a coset of a subgroup, not that it is a subgroup. It is a variation of the easy (and well known) fact that if x and y are two vertices of $\mathsf{Cay}(G; S)$ that have the same outneighbours, then S is a union of left cosets of the subgroup generated by xy^{-1}.

Lemma 2.11. *Assume D is a set of vertices of $\mathsf{Cay}(G; S)$, such that $|D| \geq \max\big(|S| - 1, 2\big)$, and all of the vertices in D have exactly the same outneighbours. Then S is a subgroup of G.*

Proof. Assume, without loss of generality, that $1 \in D$. Then S is the set of outneighbours of every element of D, so $Sd = S$ for every $d \in D$. This means that S is a union of left cosets of $\langle D \rangle$. Since $1 \in S$ (see Assumption 2.7), this implies that S contains $\langle D \rangle$. If S is not equal to this subgroup, then it is the union of at least 2 cosets, so $|S| \geq 2|\langle D \rangle| \geq 2|D|$. On the other hand, we are also

assuming that $|D| + 1 \geq |S|$. Combining these inequalities implies that $|D| + 1 \geq 2|D|$, which contradicts the assumption that $|D| \geq 2$. □

Lemma 2.12. *Assume*

- *φ is an automorphism of $\widehat{X}$ that fixes the vertex $1_{\widehat{G}}$,*
- *$mk \neq |G|$ (recall that m and k were defined in Notation 2.3), and*
- *$|S| \leq \big(|G| + 1\big)/k$.*

Then the hypotheses of Proposition 2.9 are satisfied.

Proof. 2.9(1): *We have $\varphi(1) = 1$.* This is true by assumption.

2.9(2): *φ maps each coset of G to a coset of G.* The maximal cliques of $\widehat{X}$ are described in Lemma 2.10. It is obvious that every clique of type (a) has cardinality $|G|$, and that every clique of type (b) or (b′) has cardinality mk (since $|A| = m$). Assume, for the moment, that

$$\begin{array}{c}\textit{the cardinality of every maximal clique of type } (\mathrm{c}) \\ (\textit{or of type } (\mathrm{c}') \textit{ if } n = 3) \textit{ is strictly less than } |G|.\end{array} \tag{2.13}$$

(We will show how to complete the proof with this assumption, and we will establish later that the assumption is indeed true.) This assumption implies that the cosets of G are the only maximal cliques whose cardinality is $|G|$. So every automorphism of $\widehat{X}$ (including φ) must map each coset of G to a coset of G.

2.9(3): *φ maps each coset of AB to a coset of AB.* Each maximal clique of type (b) or (b′) contains no more than one vertex of any coset of G. If a maximal clique of type (c) or (c′) has this property, then it cannot have more than k vertices. Since maximal cliques of type (b) or (b′) have mk vertices (and $mk > k$), this implies that no automorphism can carry a maximal clique of type (b) or (b′) to a clique of type (c) or (c′). So φ must preserve the set of cliques of type (b) (or (b′)). This easily implies Hypothesis 2.9(3).

Now, all that remains is to prove Assumption (2.13). To this end, let C be a maximal clique of type (c) (or of type (c′) if $n = 3$), and suppose $|C| \geq |G|$. (This will lead to a contradiction, which completes the proof.) Also assume, without loss of generality, that $1_{\widehat{G}} \in C$. Then

$$C \subseteq GB \cap \widehat{S}^{\pm 1} = G \cup Sb \cup Sb^{-1} \subseteq G \cup Gb \cup Gb^{-1}.$$

Let $C_i = C \cap Gb^i$ for $i \in \{-1, 0, 1\}$. It is clear that $|C_1| \leq |Sb| = |S|$ and $|C_{-1}| \leq |Sb^{-1}| = |S|$.

We claim that also $|C_0| \leq |S|$. Since $C \neq G$ and $|C| \geq |G|$, we know that $C \not\subseteq G$. Hence, $C_{-1} \cup C_1 \neq \emptyset$, so there is some gb^ϵ in C, with $\epsilon \in \{\pm 1\}$. The set of neighbours of this vertex in G is $(Sb)^{-\epsilon} g b^\epsilon$. Since this set of neighbours contains C_0 and has cardinality $|S|$, we conclude that $|C_0| \leq |S|$.

Choose $j \in \{-1, 0, 1\}$, such that $|C_j|$ is maximal. Since at most k of the sets C_{-1}, C_0, C_1 are nonempty, and

$$|C_i| \leq |C_j| \leq |S| \leq \big(|G| + 1\big)/k,$$

then we have

$$|G| \leq |C| = |C_{-1}| + |C_0| + |C_1| \leq k \cdot |C_j| \leq k \cdot |S| \leq k \cdot \big(|G| + 1\big)/k = |G| + 1,$$

so

$$\frac{|G|}{k} \leq |C_j| \leq |S| \leq \frac{|G|}{k} + \frac{1}{k}.$$

Since $1/k < 1$, this implies $|C_j| = |S|$ (because the absolute value of the difference of two distinct integers cannot be less than one). Also, since

$$|C_{-1}| + |C_0| + |C_1| = |C| \geq |G| \geq k \cdot |C_j| - 1,$$

we have $|C_i| \geq |C_j| - 1$ for all $i \neq j$. Assume, for the sake of concreteness, that $j = 1$, so we may let $i = 0$.

Since C is a clique, we know that every element of C_1 is an outneighbour of every element of C_0. From the definition of $\widehat{S}$, we also know, for each $x \in C_0$, that the number of outneighbours of x in Gb is precisely $|S| = |C_1|$. Hence, we conclude that C_1 is the set of all outneighbours of x that are in Gb; so $C_1 = Sbx$. Since x is an arbitrary element of C_0 (and $1_G \in C_0$), we conclude that $Sbx = Sb\,1_G$. Since $Sb = bS$ (recall that b commutes with all elements of G), this implies $Sx = S$, for all $x \in C_0$.

Now Lemma 2.11 tells us that S is a subgroup of G. Therefore S is closed under inverses (i.e., $S = S^{-1}$). This contradicts the first bullet point of Notation 2.3. □

We are now ready to prove Theorem 2.2. For the reader's convenience, we copy the statement here.

Theorem 2.2. *Assume*

- G *is a finite group,*
- $\overrightarrow{X} = \mathsf{Cay}(G; S)$ *is a non-DCI Cayley digraph,*
- $n \geq 3$ *and* $k = \begin{cases} 2 & \text{if } n > 3; \\ 3 & \text{if } n = 3, \end{cases}$
- *either* $n > 3$ *or* $|S \cup \{1_G\}| \leq |G|/3$,
- $m \geq 3$ *and* $mk \neq |G|$,
- A *is a group of order* m, *and*
- *either* $\overrightarrow{X} \ncong \overrightarrow{X}^-$ *or there is an automorphism* α *of* G, *such that* $\alpha(S) = S^{-1}$.

Then $G \times A \times \mathbb{Z}_n$ *is not a CI group.*

Proof. We may assume $S \neq S^{-1}$, for otherwise $\mathrm{Cay}(G; S)$ is a non-CI Cayley graph of G, so G is not a CI group; hence any finite group that contains G is also not a CI group.

Let $B = \mathbb{Z}_n$, and recall that $\widehat{G}$, $\widehat{S}$, and $\widehat{X} = \mathrm{Cay}(\widehat{G}; \widehat{S}^{\pm 1})$ are defined in Notation 2.3. We will show that the Cayley graph $\widehat{X}$ is not a CI graph.

Since $\overrightarrow{X}$ is not DCI, we know from Theorem 2.6 that there is a subgroup M of $\mathrm{Aut}\,\overrightarrow{X}$, such that M is isomorphic to G, and acts sharply transitively on the vertex set $V(\overrightarrow{X}) = G$, but

$$\text{no element of } \mathrm{Aut}\,\overrightarrow{X} \text{ conjugates } M \text{ to } G_R. \tag{2.14}$$

It is easy to see that $\mathrm{Aut}\,\overrightarrow{X} \times A_R \times B_R$ is contained in $\mathrm{Aut}\,\widehat{X}$, so

- $M \times A_R \times B_R \subseteq \mathrm{Aut}\,\widehat{X}$, and it is clear that
- this subgroup is isomorphic to $\widehat{G}$ and acts sharply transitively on $G \times A \times B = \widehat{G} = V(\widehat{X})$.

If $\widehat{X}$ is CI, then Theorem 2.6 tells us that some $\varphi \in \mathrm{Aut}\,\widehat{X}$ conjugates $M \times A_R \times B_R$ to the right regular representation of $\widehat{G}$. We may assume $\varphi(1_{\widehat{G}}) = 1_{\widehat{G}}$ (by composing φ with a translation). Also, there is no loss of generality in assuming that $|S| \leq \big(|G| + 1\big)/2$, because we can replace S with its (almost) complement $(G \smallsetminus S) \cup \{1_G\}$. (Recall that Assumption 2.7 requires us to keep 1_G in S.) Then the hypotheses of Lemma 2.12 are satisfied, so we conclude that the hypotheses of Proposition 2.9 are satisfied. Hence, the restriction of φ to G is either an automorphism of $\overrightarrow{X}$ or an isomorphism from $\overrightarrow{X}$ to $\overrightarrow{X}^-$.

Since φ conjugates $M \times A_R \times B_R$ to $\widehat{G}_R = G_R \times A_R \times B_R$, and we now know that $\varphi(G) = G$, we can conclude that

$$\text{the restriction } \varphi|_G \text{ conjugates } M \text{ to } G_R.$$

This contradicts (2.14) if $\varphi|_G$ is an automorphism of $\overrightarrow{X}$.

Therefore, $\varphi|_G$ must be an isomorphism from $\overrightarrow{X}$ to $\overrightarrow{X}^-$. Then $\overrightarrow{X} \cong \overrightarrow{X}^-$, so, by assumption, there is an automorphism α of G, such that $\alpha(S) = S^{-1}$, so α is an isomorphism from $\overrightarrow{X}$ to $\overrightarrow{X}^-$.

Also, α normalizes G_R (since α is a group automorphism). Then the composition $\alpha \circ \varphi|_G$ is an automorphism of $\overrightarrow{X}$ that conjugates M to G_R. This is again a contradiction to (2.14). □

References

[1] L. Babai: Isomorphism problem for a class of point-symmetric structures. *Acta Math. Acad. Sci. Hungar.* 29 (1977), no. 3-4, 329–336. MR 0485447, doi:10.1007/BF01895854

[2] L. Babai and P. Frankl: Isomorphisms of Cayley graphs I, in A. Hajnal and V. T. Sós, eds.: *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I,* pp. 35–52. North-Holland, New York, 1978. ISBN 0-444-85093-3, MR 0519254

[3] M. Conder and C. H. Li: On isomorphisms of finite Cayley graphs. *European J. Combin.* 19 (1998), no. 8, 911–919. MR 1657923, doi:10.1006/eujc.1998.0243

[4] E. Dobson, J. Morris, and P. Spiga: Groups with elements of order 8 do not have the DCI property. (in preparation).

[5] E. Dobson and P. Spiga: CI-groups with respect to ternary relational structures: new examples. *Ars Math. Contemp.* 6 (2013), no. 2, 351–364. MR 3015643, doi:10.26493/1855-3974.310.59f

[6] Y.-Q. Feng and I. Kovács: Elementary abelian groups of rank 5 are DCI-groups. *J. Combin. Theory A* 157 (2018), 162–204. MR 3780411, doi:10.1016/j.jcta.2018.02.003

[7] C. H. Li: On isomorphisms of finite Cayley graphs—a survey. *Discrete Math.* 256 (2002), no. 1-2, 301–334. MR 1927074, doi:10.1016/S0012-365X(01)00438-1

[8] C. H. Li, Z. P. Lu, and P. P. Pálfy: Further restrictions on the structure of finite CI-groups. *J. Algebraic Combin.* 26 (2007), no. 2, 161–181. MR 2335710, doi:10.1007/s10801-006-0052-1

[9] J. Morris: $\mathbb{Z}_3^8$ is not a CI-group. *Ars Math. Contemp.* (2024) (to appear). doi:10.26493/1855-3974.3087.f36

[10] M. Muzychuk: On the isomorphism problem for cyclic combinatorial objects. *Discrete Math.* 197/198 (1999), 589–606. MR 1674890, doi:10.1016/S0012-365X(99)90119-X

[11] M. Muzychuk: An elementary abelian group of large rank is not a CI-group. *Discrete Math.* 264 (2003), no. 1-3, 167–185. MR 1972028, doi:10.1016/S0012-365X(02)00558-7

[12] M. Muzychuk and G. Somlai: The Cayley isomorphism property for Cayley maps. *Electron. J. Combin.* 25 (2018), no. 1, Paper no. 1.42, 22 pp. MR 3785021, doi:10.37236/5962

[13] L. Nowitz: A non-Cayley-invariant Cayley graph of the elementary abelian group of order 64. *Discrete Math.* 110 (1992), no. 1-3, 223–228. MR 1197456, doi:10.1016/0012-365X(92)90711-N

[14] P. P. Pálfy: Isomorphism problem for relational structures with a cyclic automorphism. *European J. Combin.* 8 (1987), no. 1, 35–43. MR 0884062, doi:10.1016/S0195-6698(87)80018-5

[15] G. Somlai: Elementary abelian p-groups of rank $2p+3$ are not CI-groups. *J. Algebraic Combin.* 34 (2011) 323–335. MR 2836364, doi:10.1007/s10801-011-0273-9

[16] P. Spiga: Elementary abelian p-groups of rank greater than or equal to $4p-2$ are not CI-groups. *J. Algebraic Combin.* 26 (2007), no. 3, 343–355. MR 2348100, doi:10.1007/s10801-007-0059-2

[17] P. Spiga: CI-property of elementary abelian 3-groups. Discrete Math. 309 (2009), no. 10, 3393–3398. MR 2526758, doi:10.1016/j.disc.2008.08.002

Department of Mathematics and Computer Science, University of Lethbridge, 4401 University Drive, Lethbridge, Alberta, T1K 3M4, Canada

Email address: dmorris@deductivepress.ca, https://deductivepress.ca/dmorris

Email address: joy.morris@uleth.ca