RESULTS TOWARDS SHOWING $\mathbb{Z}_p^n$ IS A CI-GROUP

JOY MORRIS

ABSTRACT. It has been shown that $\mathbb{Z}_p^i$ is a CI-group for $1 \leq i \leq 4$, and is not a CI-group for $i \geq 2p-1+\binom{2p-1}{p}$; all other values (except when $p = 2$ and $i = 5$, which is CI) are open. The results presented in this paper are useful in any attempt to prove that $\mathbb{Z}_p^n$ is a CI-group. In fact, they provide complete and elementary proofs that $\mathbb{Z}_p$, $\mathbb{Z}_p^2$ and $\mathbb{Z}_p^3$ are CI-groups.

In 1967, Ádám conjectured [1] that two Cayley graphs of $\mathbb{Z}_n$ are isomorphic if and only if they are isomorphic by a group automorphism of $\mathbb{Z}_n$. Although this conjecture was disproven by Elspas and Turner three years later [8], the problem and its generalizations have subsequently aroused considerable interest. Much of this interest has been focused on the *Cayley Isomorphism Problem*, which asks for necessary and sufficient conditions for two Cayley graphs on the same group to be isomorphic. Particular attention has been paid to determining which groups G have the property that two Cayley graphs of G are isomorphic if and only if they are isomorphic by a group automorphism of G. Such a group is called a CI-group (CI stands for Cayley Isomorphism). One major angle from which the Cayley Isomorphism problem was considered was the question of which cyclic groups are in fact CI-groups. The problem raised by Ádám's conjecture has now been completely solved by Muzychuk [14] and [15]. He proves that a cyclic group of order n is a CI-group if and only if $n = k, 2k$ or $4k$ where k is odd and square-free. The proof uses Schur rings and is very technical. Many special cases were obtained independently along the way to this result.

One other major branch of study of the Cayley Isomorphism problem has focused on elementary abelian groups. In [5], Babai and Frankl asked whether or not all elementary abelian groups are CI-groups. In 1992, Lewis Nowitz constructed a Cayley graph on $\mathbb{Z}_2^6$ that is not a CI-graph, thus showing that not all elementary abelian groups are CI-groups. Alspach provided a simpler proof of the Nowitz result in [2].

From the other side of things, Turner [17] proved that $\mathbb{Z}_p$ is a CI-group; Godsil [9] proved that $\mathbb{Z}_p^2$ is a CI-group, and Dobson [7] provided the first proof that $\mathbb{Z}_p^3$ is a CI-group. A more elementary proof that $\mathbb{Z}_p^3$ is a CI-group is provided by Alspach and Nowitz in [3], and the results presented here extend their techniques. Muzychuk's work was also key to this aspect of

the problem; with Hirasaka, he proved that $\mathbb{Z}_p^4$ is a CI-group [11], a result that was independently proven by the author in her PhD thesis using the techniques presented here [13]. Most recently, Muzychuk has constructed graphs on $\mathbb{Z}_p^{2p-1+\binom{2p-1}{p}}$ that are not CI-graphs. By use of a computer, it has been established that $\mathbb{Z}_2^5$ is a CI-group, but all other values remain open.

We would recommend that those readers interested in a survey of the Cayley Isomorphism Problem see [12].

1. Background Definitions and Theory

The notation used in this paper is something of a hodge-podge from a variety of sources, based sometimes on personal preferences and sometimes on the need for consistency with earlier works. For any graph theory language that is not defined within this paper, the reader is directed to [6]. In the case of language or notation relating to permutation groups, the reader is directed to Wielandt's authoritative work on permutation group theory [18], although not all of the notation used by Wielandt is the same as that employed in this paper. For terminology and notation from abstract group theory that is not explained within this paper, the reader is referred to [10] or [16].

Many results for directed graphs have immediate analogues for graphs, as can be seen by substituting for a graph the directed graph obtained by replacing each edge of the graph with an arc in each direction between the two end vertices of the edge. Consequently, although the results of this paper are proven to be true for all digraphs, the same proofs serve to prove the results for all graphs.

Although for the sake of simplicity we assume in this paper that directed graphs are simple, this assumption is not actually required in any of the proofs that follow. We do allow the digraphs to contain digons.

Notation 1.1. *Let V' be any orbit of G. Then the restriction of the action of $g \in G$ to the set V' is denoted by $g|_{V'}$.*

This ignores what the action of g may be within other orbits of G. For example, $g|_{V'} = 1$ indicates that for every element $v' \in V'$, $g(v') = v'$, but tells us nothing about how g' may act elsewhere.

Sometimes the action of a permutation group G will break down nicely according to its action on certain subsets of the set V. Certainly, this happens when G is intransitive, with the orbits of G being the subsets. However, it can also occur in other situations.

Definition 1.2. *The subset $B \subseteq V$ is a G-**block** if for every $g \in G$, either $g(B) = B$, or $g(B) \cap B = \emptyset$.*

In some cases, the group G is clear from the context and we simply refer to B as a block. It is a simple matter to realise that if B is a G-block, then

for any $g \in G$, $g(B)$ will also be a G-block. Also, intersections of G-blocks are themselves G-blocks.

Definition 1.3. *Let G be a transitive permutation group, and let B be a G-block. Then, as noted above, $\{g(B) : g \in G\}$ is a set of blocks that (since G is transitive) partition the set V. We call this set the* **complete block system** *of G generated by the block B.*

Some of the basic language of blocks will be required in this paper. Notice that any singleton in V, and the entire set V, are always G-blocks. These are called trivial blocks.

Definition 1.4. *The* **stabiliser subgroup** *in G of the set V' is the subgroup of G consisting of all $g \in G$ such that g fixes V' pointwise. This is denoted by $\mathrm{Stab}_G(V')$, or sometimes, particularly if $V' = \{v\}$ contains only one element, simply by $G_{V'}$, or G_v.*

In some cases, we allow the set V' to be a set of subsets of V (where V is the set upon which G acts) rather than a set of elements of V. In this case, the requirement is that every element of $\mathrm{Stab}_G(V')$ fix every set in V' setwise. For example, if $\mathbf{B}$ is a complete block system of G, then $\mathrm{Stab}_G(\mathbf{B})$ is the subgroup of G that consists of all elements of G that fix every block in $\mathbf{B}$ setwise.

Definition 1.5. *Let S be a subset of a group G. The* **Cayley digraph** *$\vec{X} = \vec{X}(G; S)$ is the directed graph given as follows. The vertices of X are the elements of the group G. If $g, h \in G$, there is an arc from the vertex g to the vertex h if and only if $g^{-1}h \in S$. In other words, for every vertex $g \in G$ and element $s \in S$, there is an arc from g to gs.*

Notice that if the identity element $1 \in G$ is in S, then the Cayley digraph will have a directed loop at every vertex, while if $1 \notin S$, the digraph will have no loops. For convenience, we may assume that the latter case holds; it is immaterial to the results. Notice also that since S is a set, it contains no multiple entries and hence there are no multiple arcs. Finally, notice that if the inverse of every element in S is itself in S, then the digraph is equivalent to a graph, since every arc can be paired with an arc going in the opposite direction between the same two vertices.

Definition 1.6. *The* **Cayley colour digraph** *$\vec{X} = \vec{X}(G; S)$ is very similar to a Cayley digraph, except that each entry of S has a colour associated with it, and for any $s \in S$ and any $g \in G$, the arc in $\vec{X}$ from the vertex g to the vertex gs is assigned the colour that has been associated with s.*

All of the results of this paper also hold for Cayley colour digraphs. This is not always made explicit, but is a simple matter to verify without changing any of the proofs used.

Definition 1.7. *The set S of $\vec{X}(G; S)$ is called the* **connection set** *of the Cayley digraph $\vec{X}$.*

Definition 1.8. *The* **automorphism group** *of the digraph $\vec{X}$ is the permutation group that is formed of all possible automorphisms of the digraph. This group is denoted by* $\mathrm{Aut}(\vec{X})$.

We now define some terms that classify the types of problems being studied in this paper.

Definition 1.9. *The digraph $\vec{X}$ is a* **CI-digraph** *on the group G if $\vec{X} = \vec{X}(G;S)$ is a Cayley digraph on the group G and for any isomorphism of $\vec{X}$ to another Cayley digraph $\vec{Y} = \vec{Y}(G;S')$ on the group G, there is a group automorphism ϕ of G that maps $\vec{X}$ to $\vec{Y}$. That is, $\phi(S) = S'$.*

If $\vec{X}$ is a CI-digraph on the group G, we will be able to use that fact together with the known automorphisms of G to determine all Cayley digraphs on G that are isomorphic to $\vec{X}$.

One of the most useful approaches to proving whether or not a given Cayley digraph is a CI-digraph has been the following theorem by Babai. This theorem has been used in the vast majority of results to date on the Cayley Isomorphism problem.

Theorem 1.10. (Babai, see [4]) *Let $\vec{X}$ be a Cayley digraph on the group G. Then $\vec{X}$ is a CI-digraph if and only if all regular subgroups of* $\mathrm{Aut}(\vec{X})$ *isomorphic to G are conjugate to each other in* $\mathrm{Aut}(\vec{X})$.

2. The Results

2.1. **Using the Sylow p-subgroups.** Notice that the Sylow p-subgroups of S_{p^n} have the form $\mathbb{Z}_p \wr \mathbb{Z}_p \ldots \wr \mathbb{Z}_p$ (n copies of $\mathbb{Z}_p$). So every Sylow p-subgroup of S_{p^n} has a unique complete block system of size p^i for any i. Furthermore, any permutation of order p^j that respects these blocks is in this Sylow p-subgroup of S_{p^n}.

Throughout all that follows, all calculations are taken modulo p, and the range of all variable subscripts of vertices and blocks is within $\{0, 1, \ldots, p-1\}$, in addition to any other restrictions given.

Let $\vec{X} = \vec{X}(\mathbf{Z}_p^n; S)$ be a Cayley digraph on the group $\mathbf{Z}_p^n$. Suppose that $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1} \leq \mathrm{Aut}(\vec{X})$ for some $\sigma \in S_{\mathbf{Z}_p^n}$. We want to show that $(\mathbb{Z}_p^n)_L$ and $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ are conjugate in $\mathrm{Aut}(\vec{X})$.

By taking a conjugate of $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ if necessary, we may assume that $(\mathbb{Z}_p^n)_L$ and $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ are in the same Sylow p-subgroup P of Aut $(\vec{X})$. The group P is contained in some Sylow p-subgroup P^* of $S_{\mathbf{Z}_p^n}$, that has unique imprimitive blocks of length p^i for any i. Let the blocks of length 1 be

$$B_{i_1,\ldots,i_n} = \{x_{i_1,\ldots,i_n}\}, 0 \leq i_1, \ldots, i_n \leq p-1.$$

Now, we let the blocks of length p^{n-j} be labelled inductively as follows:

$$B_{i_1,\ldots,i_j} = B_{i_1,\ldots,i_j,0} \cup B_{i_1,\ldots,i_j,1} \cup \ldots \cup B_{i_1,\ldots,i_j,p-1}$$

We use some important properties involving regular permutation groups several times in what follows. First, if a permutation group G is transitive and abelian then it is regular. Second, if G is transitive, abelian and imprimitive, then any permutation in G that fixes some block setwise must fix all blocks setwise. This follows because the action of G on the set of blocks is also transitive and abelian, and consequently regular. This will be used in the next paragraph.

Let the permutation

$$\theta_{i_1,\ldots,i_{n-1}} = (x_{i_1,\ldots,i_{n-1},0}\, x_{i_1,\ldots,i_{n-1},1} \,\ldots\, x_{i_1,\ldots,i_{n-1},p-1})$$

for $0 \leq i_1, \ldots, i_{n-1} \leq p-1$. Since both $(\mathbb{Z}_p^n)_L$ and $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ are abelian and transitive on the sets of blocks of each size, they are regular in their action on these sets of blocks. Without loss of generality, assume that the blocks are coordinatized so that

$$\tau_j(x_{i_1,\ldots,i_j,\ldots,i_n}) = x_{i_1,\ldots,i_j+1,\ldots,i_n} \text{ for all } 0 \leq i_1, \ldots, i_n \leq p-1,$$

are all elements of the group $(\mathbb{Z}_p^n)_L$. Note that $\tau_n = \Pi_{0\leq i_1,\ldots,i_n\leq p-1}\theta_{i_1,\ldots,i_n}$ and $(\mathbb{Z}_p^n)_L = \langle \tau_1, \ldots, \tau_n\rangle$.

Notice also that in any p-group P_1, if $g, g' \in P_1$, $\langle g, g'\rangle$ fixes the block B of length p setwise, and $g|_B \neq 1$, then $g'|_B = g^i|_B$ for some i.

Definition 2.1. *Two sets of vertices V_1 and V_2 are said to be* **wreathed** *if for each possible colour c that an arc can be, the existence of an arc of colour c from some vertex in V_1 to some vertex in V_2 implies the existence of an arc of colour c from each vertex of V_1 to each vertex of V_2, and furthermore if (symmetrically) the existence of an arc of colour c from some vertex in V_2 to some vertex in V_1 implies the existence of an arc of colour c from each vertex of V_2 to each vertex of V_1.*

Sometimes we say (alternatively) that V_1 is wreathed with V_2 if the above conditions hold.

The following lemma is useful in determining whether or not two blocks are wreathed.

Lemma 2.2. *Let G be a transitive subgroup of $\mathrm{Aut}(\vec{X})$, and let B_1 and B_2 be G-blocks in the complete block system $\mathbf{B}$. If $\mathrm{Stab}_G(\mathbf{B})$ is transitive on each block $B \in \mathbf{B}$, $x \in B_1$, and the orbit of $\mathrm{Stab}_G(\mathbf{B})_x$ containing $y \in B_2$ in fact contains all of B_2, then B_1 and B_2 are wreathed.*

Proof. We begin by assuming that there is a red arc from $x' \in B_1$ to $y' \in B_2$, and prove that there must be a red arc from $x'' \in B_1$ to $y'' \in B_2$. This will be sufficient.

Since $\mathrm{Stab}_G(\mathbf{B})$ is transitive on B_1, there exists some $\phi \in \mathrm{Stab}_G(\mathbf{B})$ such that $\phi(x') = x$. Likewise, there exists some $\delta \in \mathrm{Stab}_G(\mathbf{B})$ such that $\delta(x) = x''$. Clearly, $\phi(y') \in B_2$ and $\delta^{-1}(y'') \in B_2$. Since the orbit of $\mathrm{Stab}_G(\mathbf{B})_x$ containing $y \in B_2$ in fact contains all of B_2, there exists some $\psi \in \mathrm{Stab}_G(\mathbf{B})_x$ such that $\psi(\phi(y')) = \delta^{-1}(y'')$.

Thus, $\delta\psi\phi(y') = y''$, and $\delta\psi\phi(x') = x''$. Since δ, ψ and ϕ were all automorphisms of $\vec{X}$, there must be a red arc from x'' to y'', and the proof is complete. □

We use the δ_i function defined by $\delta_i(i) = 1$ and $\delta_i(j) = 0$ for any $j \neq i$.

Proposition 2.3. *Let $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ be any conjugate of $(\mathbb{Z}_p^n)_L$ with the property that $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1} \leq P$, where P is a fixed Sylow p-subgroup of $\mathrm{Aut}(\vec{X})$ that contains $(\mathbb{Z}_p^n)_L$. Let τ_i' be the element of $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ that maps $x_{0,\ldots,0}$ to $x_{0+\delta_i(1),\ldots,0+\delta_i(n)}$. Then τ_i' takes $B_{a_1,\ldots,a_i}$ to $B_{a_1+\delta_i(1),\ldots,a_i+\delta_i(i)}$ for every $a_1, \ldots, a_i$.*

Proof. We know that $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ acts regularly on the vertices and the blocks of $\vec{X}$. By its definition and the definition of a block, the automorphism τ_i' clearly fixes $B_{\delta_i(1),\ldots,\delta_i(i-1)}$ setwise. Consequently, τ_i' must fix every block $B_{a_1,\ldots,a_{i-1}}$ setwise. Let $B = B_{a_1,\ldots,a_{i-1}}$ for some fixed $a_1, \ldots, a_{i-1}$. Since $\tau_i' \in P$, and τ_i' fixes B setwise, the action of τ_i' on the p blocks $B_{a_1,\ldots,a_{i-1},0}, \ldots, B_{a_1,\ldots,a_{i-1},p-1}$ in B must be the same as the action of τ_i^j for some j, and therefore must take $B_{a_1,\ldots,a_{i-1},a_i}$ to $B_{a_1,\ldots,a_{i-1},a_i+j}$ for every a_i (j does not depend on a_i).

Let $x_{a_1,\ldots,a_n} \in B$, and let $\tau' \in \sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ be the element that maps $x_{a_1,\ldots,a_n}$ to $x_{0,\ldots,0}$. Then $\tau_1^{a_1} \ldots \tau_n^{a_n}\tau' \in P$ fixes $x_{a_1,\ldots,a_n}$, so fixes $B_{a_1,\ldots,a_i}$ setwise, and thus fixes $B_{a_1,\ldots,a_{i-1},c}$ setwise for every c. Now, τ_i' and τ' commute, so we have

$$\begin{aligned}\tau_i'(x_{a_1,\ldots,a_n}) &= (\tau')^{-1}\tau_i'\tau'(x_{a_1,\ldots,a_n}) \\ &= (\tau')^{-1}\tau_i'(x_{0,\ldots,0}) \\ &= (\tau')^{-1}(x_{\delta_i(1),\ldots,\delta_i(4)}) \\ &\in \tau_i'(B_{\delta_i(1),\ldots,\delta_i(i)})\end{aligned}$$

and we know that $(\tau')^{-1}(x_{\delta_i(1),\ldots,\delta_i(4)})$ is in the same block of length $n-i$, $\tau_i'(B_{a_1,\ldots,a_i})$, as

$$\tau_1^{a_1} \ldots \tau_n^{a_n}\tau'(\tau')^{-1}(x_{\delta_i(1),\ldots,\delta_i(n)}) = x_{a_1+\delta_i(1),\ldots,a_n+\delta_i(n)},$$

which is in $B_{a_1+\delta_i(1),\ldots,a_i+\delta_i(i)}$. This completes the proof. □

In particular, this has shown that $\tau_n' = \tau_n$.

2.2. **Conjugating τ_1'.** Working from the other end of things, suppose that we have already performed conjugations so that our conjugated group $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ is generated by $\tau_1', \tau_2, \ldots, \tau_n$. We now demonstrate that we can find ψ such that $\psi\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}\psi^{-1} = (\mathbb{Z}_p^n)_L$.

Throughout this section, G is the subgroup of $\langle\tau_1', \tau_1, \tau_2, \ldots, \tau_n\rangle$ that fixes the vertex $x_{0,\ldots,0}$.

Note that every element of $\langle \tau_1', \tau_1, \tau_2, \ldots, \tau_n \rangle$ commutes with $\tau_2, \ldots, \tau_n$ since both $(\mathbb{Z}_p^n)_L$ and $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ are abelian, so if $\phi \in \langle \tau_1', \tau_1, \tau_2, \ldots, \tau_n \rangle$ and $\phi(x_{r_1,\ldots,r_n}) = x_{r_1+a_1, r_2+a_{2,r_1},\ldots,r_n+a_{n,r_1}}$ then

$$\phi(x_{r_1,r_2',\ldots,r_n'}) = x_{r_1+a_1,r_2'+a_{2,r_1},\ldots,r_n'+a_{n,r_1}}.$$

Lemma 2.4. *The orbit of G containing $x_{r_1,\ldots,r_n}$ is the same as the orbit of some subgroup of $\langle \tau_2, \ldots, \tau_n \rangle$ containing $x_{r_1,\ldots,r_n}$.*

Proof. Notice first that G fixes B_0 setwise, and therefore fixes B_{r_1} setwise for any r_1. It therefore suffices to show that if $x_{r_1,\ldots,r_n}$, $x_{r_1,r_2',\ldots,r_n'}$ and $x_{r_1,r_2+a_2,\ldots,r_n+a_n}$ are in the same orbit, then so is $x_{r_1,r_2'+a_2,\ldots,r_n'+a_n}$. Since there is some $g \in G$ such that $g(x_{r_1,\ldots,r_n}) = x_{r_1,r_2+a_2,\ldots,r_n+a_n}$, and g commutes with $\tau_2, \ldots, \tau_n$, it is clear that $g(x_{r_1,r_2',\ldots,r_n'}) = x_{r_1,r_2'+a_2,\ldots,r_n'+a_n}$. □

Lemma 2.5. *Suppose $i \neq 0$, and the orbit of G containing $x_{i,0,\ldots,0}$ is the same as the orbit of the subgroup of $\langle \tau_2, \ldots, \tau_n \rangle$ generated by $\phi_1, \ldots, \phi_k$ containing $x_{i,0,\ldots,0}$. Then the orbit of G containing $x_{ri,0,\ldots,0}$ is also the same as the orbit of $\langle \phi_1, \ldots, \phi_k \rangle$ containing $x_{ri,0,\ldots,0}$.*

Proof. We can assume without loss of generality that no subset of the set $\{\phi_1, \ldots, \phi_k\}$ generates $\langle \phi_1, \ldots, \phi_k \rangle$, so $|\langle \phi_1, \ldots, \phi_k \rangle| = p^k$. Now we prove the result by induction on k.

The base case is given by $k = 0$, so the orbit is a singleton. In this case, we have $G = \tau_1^i G \tau_1^{-i}$, so $G = \tau_1^{ri} G \tau_1^{-ri}$ for any r, and the result is apparent.

We now assume that the lemma holds for any orbit of length p^j where $j \leq k$, and demonstrate that it must hold for orbits of length p^{k+1}. Inside the induction on k, we induct on r. Here the base case is $r = 1$, which is the vacuous statement that the orbit of $x_{i,0,\ldots,0}$ is equal to itself. Assuming that the orbit of $x_{ri,0,\ldots,0}$ is as given (with length p^{k+1}), we proceed to demonstrate that the orbit of $x_{(r+1)i,0,\ldots,0}$ is as given, with length p^{k+1}.

First we show that the orbit of $x_{(r+1)i,0,\ldots,0}$ must be contained in the given set. Let g be any element of G. Then by our induction hypothesis on r, $g(x_{ri,0,\ldots,0}) = \phi(x_{ri,0,\ldots,0})$ for some ϕ in $\langle \phi_1, \ldots, \phi_{k+1} \rangle$. Furthermore, $\phi^{-1}g$ fixes $x_{ri,0,\ldots,0}$ and is therefore an element of the group $\tau_1^{ri} G \tau_1^{-ri}$. Since we know the orbit of G containing $x_{i,0,\ldots,0}$, we also know the orbit of $\tau_1^{ri} G \tau_1^{-ri}$ containing $x_{(r+1)i,0,\ldots,0}$. This tells us that $\phi^{-1}g(x_{(r+1)i,0,\ldots,0}) = \phi'(x_{(r+1)i,0,\ldots,0})$ for some $\phi' \in \langle \phi_1, \ldots, \phi_{k+1} \rangle$. Hence $g(x_{(r+1)i,0,\ldots,0}) = \phi\phi'(x_{(r+1)i,0,\ldots,0})$ for some $\phi\phi' \in \langle \phi_1, \ldots, \phi_{k+1} \rangle$. This has shown the claim that began this paragraph.

Towards a contradiction, suppose that the orbit of $x_{(r+1)i,0,\ldots,0}$ under G were a strict subset of the orbit of $x_{(r+1)i,0,\ldots,0}$ under $\langle \phi_1, \ldots, \phi_{k+1} \rangle$. By Lemma 2.4, the orbit of $x_{(r+1)i,0,\ldots,0}$ under G must therefore be the orbit of $x_{(r+1)i,0,\ldots,0}$ under a strict subgroup of $\langle \phi_1, \ldots, \phi_{k+1} \rangle$, which has order

at most p^k. By the induction hypothesis on k, since $i \equiv s(r+1)i (\text{mod } p)$ for some s, the orbit of $x_{i,0,\ldots,0}$ also has length at most p^k, a contradiction. This completes the proof. □

Corollary 2.6. *The orbit of G containing $x_{i,0,\ldots,0}$ is $\tau_1^{i-j}(O_j)$, where O_j is the orbit of G containing $x_{j,0,\ldots,0}$, if $i, j \neq 0$.*

Proof. Lemma 2.4 tells us that both orbits are orbits of subgroups of the group $\langle \tau_2, \ldots, \tau_n \rangle$, and Lemma 2.5 tells us that both subgroups are the same, since $(i,p) = 1 = (j,p)$. The result follows immediately. □

Proposition 2.7. *Let $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ be any conjugate of $(\mathbb{Z}_p^n)_L$ with the property that $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1} \leq P$, where P is a fixed Sylow p-subgroup of $\text{Aut}(\vec{X})$ that contains $(\mathbb{Z}_p^n)_L$, and $\tau_2, \ldots, \tau_n \in \sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$. Then there exists some $\psi \in P$ such that $\psi\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}\psi^{-1}$ contains $\tau_1, \ldots \tau_{n-1}$ and τ_n.*

Proof. We consider τ_1'. As previously noted, since τ_1' commutes with each of $\tau_2, \ldots, \tau_n$, the action of τ_1' is completely determined by the p triples

$$(a_{2,0}, \ldots, a_{n,0}) = (0, \ldots, 0), (a_{2,1}, \ldots, a_{n,1}) \ldots, (a_{2,p-1}, \ldots, a_{n,p-1}),$$

where $\tau_1'(x_{i_1,0,\ldots,0}) = x_{i_1+1,a_{2,i_1},\ldots,a_{n,i_1}}$.

Define the function ψ as follows:

$$\psi \text{ commutes with } \tau_2, \ldots, \tau_n; \text{ and}$$
$$\psi^{-1}(x_{i,0,\ldots,0}) = (\tau_1')^i(x_{0,\ldots,0})$$

for any i, where $(\tau_1')^0$ is considered to be the identity.

First we show that $\psi\tau_1'\psi^{-1} = \tau_1$. For any $i_1, \ldots, i_n$, we have

$$\begin{aligned}\psi\tau_1'\psi^{-1}(x_{i_1,\ldots,i_n}) &= \psi(\tau_1')^{i_1+1}\tau_1^{-i_1}(x_{i_1,\ldots,i_n}) \\ &= \tau_1^{i_1+1}(\tau_1')^{-i_1-1}(\tau_1')^{i_1+1}\tau_1^{-i_1}(x_{i_1,\ldots,i_n}) \\ &= \tau_1(x_{i_1,\ldots,i_n}),\end{aligned}$$

as required.

There is an alternative and perhaps more intuitive way of showing this. Notice that the disjoint cycle notation for τ_1' consists of p^{n-1} cycles of the form

$$(x_{0,i_2,\ldots,i_n}\ x_{1,i_2,\ldots,i_n}\ x_{2,i_2+a_{2,1},\ldots,i_n+a_{n,1}}\ \cdots \\ x_{p-1,i_2+a_{2,1}+\ldots+a_{2,p-2},\ldots,i_n+a_{n,1}+\ldots+a_{n,p-2}}).$$

Also,

$$\psi(x_{i_1,i_2+a_{2,1}+\ldots+a_{2,i-1},\ldots,i_n+a_{n,1}+\ldots+a_{n,i-1}}) = x_{i_1,\ldots,i_n}$$

for any $i_1 > 1$, while $\psi(x_{1,i_2,\ldots,i_n}) = x_{1,i_2,\ldots,i_n}$ and $\psi(x_{0,i_2,\ldots,i_n}) = x_{0,i_2,\ldots,i_n}$. From this, it is easy to verify that the disjoint cycle notation for $\psi\tau_1'\psi^{-1}$ will consist of p^{n-1} cycles of the form

$$(x_{0,i_2,\ldots,i_n}\ x_{1,i_2,\ldots,i_n}\ \ldots\ x_{p-1,i_2,\ldots,i_n}),$$

which is precisely the form of τ_1.

Now we must show that ψ is an automorphism of $\vec{X}$. Suppose that there is a red arc from the vertex $x_{i_1,\ldots,i_n}$ to the vertex $x_{i'_1,\ldots,i'_n}$. Then showing that there must be a red arc from $\psi^{-1}(x_{i_1,\ldots,i_n})$ to $\psi^{-1}(x_{i'_1,\ldots,i'_n})$ will be sufficient to complete the proof.

If $i_1 = i'_1$, then since ψ commutes with τ_2, τ_3 and τ_4, it is immediately apparent that the appropriate red arc will exist. So we assume $i_1 \neq i'_1$. Now,

$$\begin{aligned}\psi^{-1}(x_{i_1,\ldots,i_n}) &= (\tau'_1)^{i_1}(x_{0,i_2,\ldots,i_n}) \\ &= x_{i_1,i_2+a_{2,0}+\ldots+a_{2,i_1-1},\ldots,i_n+a_{n,0}+\ldots+a_{n,i_1-1}}, \text{ and} \\ \psi^{-1}(x_{i'_1,\ldots,i'_n}) &= (\tau'_1)^{i'_1}(x_{0,i'_2,\ldots,i'_n}) \\ &= x_{i'_1,i'_2+a_{2,0}+\ldots+a_{2,i'_1-1},\ldots,i'_n+a_{n,0}+\ldots+a_{n,i'_1-1}}.\end{aligned}$$

Let B_r be any p^{n-1}-block of $\mathrm{Aut}(\vec{X})$, with $r \neq 0$. We show that the orbit of $x_{r,0,\ldots,0}$ under G contains the set

$$\{x_{r,b_0a_{2,0}+\ldots+b_{p-1}a_{2,p-1},\ldots,b_0a_{n,0}+\ldots+b_{p-1}a_{n,p-1}} : 0 \leq b_0,\ldots,b_{p-1} \leq p-1\}.$$

To show this, we need only show that if $x_{r,c_2,\ldots,c_n}$ is in the orbit, then so is $x_{r,c_2+a_{2,s},\ldots,c_n+a_{n,s}}$ for any s.

If $s = 0$ then $a_{i,s} = 0$ for every i, so the result is trivial. Otherwise, notice that $\tau_1^{-1}\tau'_1(x_{s,0,\ldots,0}) = x_{s,a_{2,s},\ldots,a_{n,s}}$, and $\tau_1^{-1}\tau'_1 \in G$, so by Corollary 2.6, there exists some $g \in G$ such that $g(x_{r,0,\ldots,0}) = x_{r,a_{2,s},\ldots,a_{n,s}}$. Now, since g commutes with $\tau_2,\ldots,\tau_n$, we have $g(x_{r,c_2,\ldots,c_n}) = x_{r,c_2+a_{2,s},\ldots,c_n+a_{n,s}}$.

In particular, we have shown that the orbit of $x_{i'_1-i_1,0,\ldots,0}$ under G contains the vertex $x_{i'_1-i_1,a_{2,i_1}+\ldots+a_{2,i'_1-1},\ldots,a_{n,i_1},\ldots,a_{n,i'_1-1}}$. Since every element of G commutes with $\tau_2,\ldots,\tau_n$, this means that the orbit of the vertex $x_{i'_1-i_1,i'_2-i_2,\ldots,i'_n-i_n}$ under G contains the vertex

$$x_{i'_1-i_1,i'_2-i_2+a_{2,i_1}+\ldots+a_{2,i'_1-1},\ldots,i'_n-i_n+a_{n,i_1},\ldots,a_{n,i'_1-1}}.$$

This has shown that there must be a red arc from the vertex $\psi^{-1}(x_{i_1,\ldots,i_n})$ to the vertex $\psi^{-1}(x_{i'_1,\ldots,i'_n})$, as required. So $\psi \in \mathrm{Aut}(\vec{X})$. Since ψ respects all of the standard blocks, it is clear that $\psi \in P$. □

2.3. **Completing the proof for $\mathbb{Z}_p^3$.** The two propositions have shown that $\tau'_3 = \tau_3$ and that if we can conjugate τ'_2 to τ_2, then we can also conjugate τ'_1 to τ_1, so it only remains to show that we can conjugate τ'_2 to τ_2.

Define the auxiliary graph Y whose vertices are the blocks of size p from the graph X. Two vertices of Y are adjacent precisely if the corresponding blocks of X are *not* wreathed. By Proposition 2.3, we have $\tau'_2(x_{i_1,i_2,i_3}) = x_{i_1,i_2+1,i_3+d_{i_1,i_2}}$ for every i_1, i_2, i_3, for some d_{i_1,i_2} and since τ'_2 and $\tau'_3 = \tau_3$ commute, d_{i_1,i_2} depends only on i_1 and i_2.

Consider the vertices of X that correspond to some connected component of Y. We claim that if x_{i_1,i_2,i_3} and x_{j_1,j_2,j_3} are both in the same component, then $d_{i_1,i_2} = d_{j_1,j_2}$. For suppose this were not the case, and proceed along a path from B_{i_1,i_2} to B_{j_1,j_2} in Y. There is some first block along this path, B_{a_1,a_2}, such that $d_{a_1,a_2} \neq d_{i_1,i_2}$. But the previous block along this path, B_{b_1,b_2} does have $d_{b_1,b_2} = d_{i_1,i_2}$. Since B_{b_1,b_2} and B_{a_1,a_2} are adjacent in Y, these blocks cannot be wreathed, but the action of $\tau_3^{-d_{i_1,i_2}}\tau_2^{-1}\tau_2'$ fixes x_{b_1,b_2,b_3} while moving x_{a_1,a_2,a_3} in an orbit that consists of the full block B_{a_1,a_2}. By Lemma 2.2, these two blocks must be wreathed, a contradiction.

Now, $d_{0,0} = 0$, so $d_{i_1,i_2} = 0$ for any B_{i_1,i_2} in the same connected component of Y as $B_{0,0}$. We may assume that there is some other connected component, C', containing some vertex B_{j_1,j_2}, for which $d_{j_1,j_2} \neq 0$, for otherwise $\tau_2' = \tau_2$ and we are done. Notice that $B_{0,0}$ is wreathed with $B_{0,1}$. For if τ' is the element of $\sigma(\mathbb{Z}_p^n)_L\sigma^{-1}$ that takes $x_{0,0,0}$ to $x_{j_1,j_2,0}$, then $\tau_1^{-j_1}\tau_2^{-j_2}\tau'$ fixes $x_{0,0,0}$ pointwise. However, $\tau_2'\tau'(x_{0,0,k}) = \tau'\tau_2'(x_{0,0,k}) = \tau'(x_{0,1,k}) = \tau_2'(x_{j_1,j_2,k}) = x_{j_1,j_2+1,k+d_{j_1,j_2}}$, so $\tau_1^{-j_1}\tau_2^{-j_2}\tau'(x_{0,1,k}) = x_{0,1,k+d_{j_1,j_2}}$. Now, if $B_{0,k}$ were not wreathed with $B_{0,0}$ for some k, then any automorphism that fixes $x_{0,0,0}$ must fix $x_{0,k,0}$, so must fix $x_{0,sk,0}$ for any s. But since p is prime, there is some s such that $sk \equiv 1 (\text{mod } p)$, which contradicts the fact that $\tau_1^{-j_1}\tau_2^{-j_2}\tau'$ fixes $x_{0,0,0}$ but not $x_{0,1,0}$. So $B_{0,0}$ is wreathed with $B_{0,k}$ for every k, which shows in fact that any two blocks of length p in the same block of length p^2 are wreathed.

The vertices of X that lie in some fixed component of Y must form a block of X, so there must be p, or p^2 such vertices since we have already eliminated the possibility that Y has just one component. What we have just shown demonstrates that each component of Y must meet the blocks of length p^2 in X in at most one block of length p, so τ_2 and τ_2' move every component onto a different component.

Choose one block of length p from each block of length p^2 in such a way that every block in the component of Y that contains $B_{0,0}$ has been chosen. Call these blocks the representative blocks. Define ϕ by $\phi(x_{i,j,k}) = x_{i,j,k}$ if $B_{i,j}$ is a representative block, and $\phi(x_{i,j,k}) = \theta_{i,j,k}^{d_{i,j'}+\ldots+d_{i,j-1}}(x_{i,j,k})$ if the representative block in B_i is $B_{i,j'}$ and $j' \neq j$. Notice that ϕ is some fixed power of τ_3 within any component, and ϕ fixes every block of length p setwise, so ϕ is certainly an automorphism of X. Also, $\phi^{-1}\tau_3\phi = \tau_3$.

Now,

$$\begin{aligned}\phi^{-1}\tau_2'\phi(x_{i,j,k}) &= \phi^{-1}\tau_2'(x_{i,j,k+d_{i,j'}+\ldots+d_{i,j-1}})\\ =&\phi^{-1}(x_{i,j+1,k+d_{i,j'}+\ldots+d_{i,j}}) = x_{i,j+1,k} = \tau_2(x_{i,j,k}),\end{aligned}$$

for any i, j, k, completing the proof.

References

[1] Ádám, A., Research problem 2-10, *J. Combin. be the blocks of length p^2. There are also unique imprimitive blocks of Theory* **2** (1967), 309.

[2] Alspach, B., Isomorphisms of Cayley graphs on Abelian groups, *Graph Symmetry: Algebraic Methods and Applications,* NATO ASI Ser. C **497** (1997), 1-23.

[3] Alspach, B. and L.A. Nowitz, Elementary proofs that $\mathbb{Z}_p^2$ and $\mathbb{Z}_p^3$ are CI-groups, *Europ. J. Combin.* **20** (1999), 607-617.

[4] Babai, L., Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329-336.

[5] Babai, L. and P. Frankl, Isomorphisms of Cayley graphs I, *Colloq. Math. Soc. J. Bolyai* **18** (1976/1978), 35-52.

[6] Bondy, J.A. and U.S.R. Murty, *Graph Theory with Applications*, North-Holland, 1979.

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

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

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

[10] Hall, M., *The Theory of Groups*, Macmillan, New York, 1959.

[11] Hirasaka, M. and M. Muzychuk, The elementary Abelian group of odd order and rank 4 is a CI-group, *J. Combin. Theory Ser. A,* **94** (2001), 339-362.

[12] Li, C.H., On isomorphisms of finite Cayley graphs - a survey, *submitted* (1999).

[13] Morris, J.M., *Isomorphisms of Cayley Graphs*, Ph.D. thesis, Simon Fraser University (1999).

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

[15] Muzychuk, M., On Àdàm's conjecture for circulant graphs, *Disc. Math.* **167/168** (1997), 497-510.

[16] Scott, W.R., *Group Theory*, Dover Press, New York, 1987.

[17] Turner, J., Point-symmetric graphs with a prime number of points, *J. Combin. Theory* **3** (1967), 136-145.

[18] Wielandt, H. (trans. by R. Bercov), *Finite Permutation Groups*, Academic Press, New York, 1964.

Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, AB T1K 3M4, CANADA