Toida's Conjecture is True

Edward Dobson
Department of Mathematics and Statistics
PO Drawer MA
Mississippi State, MS 39762, U.S.A.
dobson@math.msstate.edu

Joy Morris
Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta
Canada T1K 3M4
morris@cs.uleth.ca

Submitted: January 31, 2000; Accepted: March 31, 2002.
MR Subject Classifications: 05C25, 20B25

Abstract

Let S be a subset of the units in $\mathbb{Z}_n$. Let Γ be a circulant graph of order n (a Cayley graph of $\mathbb{Z}_n$) such that if $ij \in E(\Gamma)$, then $i - j \pmod n \in S$. Toida conjectured that if Γ' is another circulant graph of order n, then Γ and Γ' are isomorphic if and only if they are isomorphic by a group automorphism of $\mathbb{Z}_n$. In this paper, we prove that Toida's conjecture is true. We further prove that Toida's conjecture implies Zibin's conjecture, a generalization of Toida's conjecture.

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 disproved by Elspas and Turner three years later [7], 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 [15] and [16]. 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.

In 1977, Toida published a conjecture refining the conjecture that had been proposed by Ádám in 1967 and disproved in 1970. Toida's conjecture [20] suggests that if $\vec{X} = \vec{X}(\mathbb{Z}_n; S)$ and if S is a subset of $\mathbb{Z}_n^*$, then $\vec{X}$ is a CI-digraph. Although this conjecture has aroused some interest, until recently it had only been proven in the special case where n is a prime power. This proof was given by Klin and Pöschel [11], [12] and Golfand, Najmark and Pöschel [8]. In this paper, we will prove Toida's Conjecture. We remark that Muzychuk, Klin and Pöschel [10] have also independently proven Toida's Conjecture. We will prove that Toida's Conjecture implies Zibin's Conjecture [23], a conjecture which includes Toida's Conjecture as a special case (which of course, will imply that Zibin's Conjecture is true), although we make no claim to independently verifying Zibin's Conjecture. We first considered Zibin's Conjecture when asked to revise this paper in light of the previously mentioned paper by Muzychuk, Klin, and Pöschel [10], where Zibin's Conjecture was first proven, although our proof of Toida's Conjecture is independent of the work in [10]. Also, Muzychuk, Klin, and Pöschel's result uses the method of Schur rings, and does not use the Classification of the Finite Simple Groups. The proof presented here makes use of a result that does depend on the Classification of the Finite Simple Groups. We would recommend that those readers interested in a survey of the Cayley Isomorphism Problem see [13]. This work appears as one chapter in the Ph.D. thesis of Joy Morris [14].

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 [4]. In the case of language or notation relating to permutation groups, the reader is directed to Wielandt's authoritative work on permutation group theory [22], 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 [9] or [19].

1.1 Graph Theory

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.

Definition 1.1 The **wreath product** of two digraphs $\vec{X}$ and $\vec{Y}$, denoted by $\vec{X} \wr \vec{Y}$, is given as follows. The vertices of the new digraph are all pairs (x, y) where x is a vertex of $\vec{X}$ and y is a vertex of $\vec{Y}$. The arcs of $\vec{X} \wr \vec{Y}$ are given by the pairs

$$\{((x_1, y_1), (x_1, y_2)) : (y_1, y_2) \text{ is an arc of } \vec{Y}\},$$

together with

$$\{((x_1, y_1), (x_2, y_2)) : (x_1, x_2) \text{ is an arc of } \vec{X}\}.$$

In other words, there is a copy of the digraph $\vec{Y}$ for every vertex of $\vec{X}$, and arcs exist from one copy of $\vec{Y}$ to another if and only if there is an arc in the same direction between the corresponding vertices of $\vec{X}$. If any arcs exist from one copy of $\vec{Y}$ to another, then all arcs exist from that copy of $\vec{Y}$ to the other.

The concept of wreath product of digraphs will be considered in the fully generalized context of digraphs whose arcs have colours associated with them. In the context of digraphs whose arcs are not coloured, simply ignore all references to colour in this discussion.

Definition 1.2 The digraph $\vec{X}$ is said to be **reducible** with respect to $\wr$ if there exists some digraph $\vec{Y}$, such that $\vec{X}$ is isomorphic to $\vec{Y} \wr E_k$ for some $k > 1$. If a digraph is not reducible with respect to $\wr$, then it is said to be irreducible with respect to $\wr$.

1.2 Permutation Group Theory

Notation 1.3 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 1.4 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 realize 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 1.5 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 1.6 The transitive permutation group G is said to be **primitive** if G does not admit nontrivial blocks. If G is transitive but not primitive, then G is said to be **imprimitive**.

Using [22, Proposition 7.1], the following theorem is straightforward to prove. The proof is left to the reader.

Theorem 1.7 *Every complete block system of $\mathbb{Z}_n$ consists of the orbits of some subgroup of $\mathbb{Z}_n$.*

Definition 1.8 The **stabilizer subgroup** in G of the set V' is the subgroup of G consisting of all $g \in G$ such that g fixes V' point-wise. 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' set-wise. 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 $\mathbf{B}$ set-wise.

Definition 1.9 Let U and V be sets, H and K groups of permutations of U and V respectively. The **wreath product** $H \wr K$ is the group of all permutations f of $U \times V$ for which there exist $h \in H$ and an element k_u of K for each $u \in U$ such that

$$f((u,v)) = (h(u), k_{h(u)}(v))$$

for all $(u,v) \in U \times V$.

Theorem 1.10 *Let x be an n-cycle in S_n and $n = mk$. The centralizer in S_n of $\langle x^m \rangle$ is isomorphic to $S_m \wr \mathbb{Z}_k$.*

The proof of this theorem is straightforward, and is left to the reader. Proofs of this and other results whose proofs are omitted in this paper may be found in [14].

Notation 1.11 Let G be a transitive permutation group admitting a complete block system $\mathbf{B}$ of m blocks of size k. For $g \in G$, define $g/\mathbf{B}$ in the permutation group S_m by $g/\mathbf{B}(i) = j$ if and only if $g(B_i) = B_j$, $B_i, B_j \in \mathbf{B}$.

The following classical result of Burnside is quite useful.

Theorem 1.12 ([5], Theorem 3.5B) *A transitive permutation group of prime degree p is either doubly transitive and nonsolvable or has a regular normal Sylow p-subgroup.*

The following result is a combination of Theorems 1.8 and 4.9 of [17]. We remark that this result was proven using the Classification of the Finite Simple Groups.

Theorem 1.13 ([17]) *Let $\langle x\rangle$ and $\langle y\rangle$ be regular cyclic subgroups of degree n. Let $n = p_1^{a_1}\dots p_r^{a_r}$ be the prime power decomposition of n, with $m = \sum_{i=1}^r a_i$. Then there exists $\delta \in \langle x, y\rangle$ such that $\langle x, \delta^{-1}y\delta\rangle$ is solvable. Furthermore, $\langle x, \delta^{-1}y\delta\rangle$ admits complete block systems $\mathbf{B}_0, \dots, \mathbf{B}_{m+1}$ such that if $B_i \in \mathbf{B}_i$, then there exists $B_{i+1} \in \mathbf{B}_{i+1}$ such that $B_i \subset B_{i+1}$ and $|B_{i+1}|/|B_i|$ is prime for every $0 \le i \le m+1$.*

The following result will prove useful and is not difficult to prove. Again, its proof is left to the reader.

Lemma 1.14 *Let $G \le S_n$ such that $\langle x\rangle \le G$. Assume that G admits a complete block system $\mathbf{B}$ of m blocks of size k formed by the orbits of $\langle x^m\rangle$. Furthermore, assume that $\mathrm{Stab}_G(\mathbf{B})|_B$ admits a complete block system of r blocks of size s formed by the orbits of $\langle x^{mr}\rangle|_B$ for some $B \in \mathbf{B}$ ($rs = k$). Then G admits a complete block system $\mathbf{C}$ of mr blocks of size s formed by the orbits of $\langle x^{mr}\rangle$.*

Definition 1.15 The digraph $\vec{X}$ is a **unit circulant** if it is a circulant digraph of order n whose connection set is a subset of $\mathbb{Z}_n^*$.

1.3 Algebraic Graph Theory

Definition 1.16 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 1.17 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 1.18 The set S of $\vec{X}(G; S)$ is called the **connection set** of the Cayley digraph $\vec{X}$.

Definition 1.19 We say that the digraph $\vec{Y}$ **can be represented as a Cayley digraph on the group** G if there is some connection set S such that $\vec{Y} \cong \vec{X}(G; S)$.

Sometimes we say that $\vec{Y}$ is a Cayley digraph on the group G.

Definition 1.20 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 $\mathrm{Aut}(\vec{X})$.

Theorem 1.21 (Sabidussi [18], pg. 694) *Let $\vec{U}$ and $\vec{V}$ be digraphs. Then*

$$\mathrm{Aut}(\vec{U}) \wr \mathrm{Aut}(\vec{V}) \leq \mathrm{Aut}(\vec{U} \wr \vec{V}).$$

This follows immediately from the definition of wreath product of permutation groups, and is mentioned only as an aside in Sabidussi's paper and in the context of graphs. It is equally straightforward for digraphs.

In the case where the digraph $\vec{U}$ is irreducible with respect to $\wr$ and $\vec{V} = E_k$ for some k, the group $\mathrm{Aut}(\vec{U} \wr \vec{V})$ will admit each set of vertices that corresponds to a copy of E_k as a block. Consequently, there is a straightforward partial converse to the above theorem.

Corollary 1.22 *If $\vec{U}$ is a digraph that is irreducible with respect to $\wr$, then*

$$\mathrm{Aut}(\vec{U}) \wr \mathrm{Aut}(E_k) = \mathrm{Aut}(\vec{U}) \wr S_k = \mathrm{Aut}(\vec{U} \wr E_k).$$

Let G be a transitive permutation group that admits a complete block system $\mathbf{B}$ of m blocks of size p, where $\mathbf{B}$ is formed by the orbits of some normal subgroup $N \triangleleft G$. Furthermore, assume that $\mathrm{Stab}_G(\mathbf{B})$ is not faithful. Define an equivalence relation $\equiv$ on $\mathbf{B}$ by $B \equiv B'$ if and only if the subgroups of $\mathrm{Stab}_G(\mathbf{B})$ that fix B and B', pointwise respectively, are equal. We denote these subgroups by $\mathrm{Stab}_G(\mathbf{B})_B$ and $\mathrm{Stab}_G(\mathbf{B})_{B'}$, respectively. Denote the equivalence classes of $\equiv$ by $C_0, \ldots, C_a$ and let $E_i = \cup_{B \in C_i} B$. The following result was proven in [6].

Lemma 1.23 (Dobson, [6]) *Let $\vec{X}$ be a vertex-transitive digraph for which $G \leq \mathrm{Aut}(\vec{X})$ as above. Then $\mathrm{Stab}_G(\mathbf{B})|_{E_i} \leq \mathrm{Aut}(\vec{X})$ for every $0 \leq i \leq a$ (here if $g \in \mathrm{Stab}_G(\mathbf{B})$, then $g|_{E_i}(x) = g(x)$ if $x \in E_i$ and $g|_{E_i}(x) = x$ if $x \notin E_i$). Furthermore, $\{E_i : 0 \leq i \leq a\}$ is a complete block system of G.*

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

Definition 1.24 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 1.25 (Babai, see [3]) *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* $\mathrm{Aut}(\vec{X})$.

The following result was first proven by Turner in 1967.

Theorem 1.26 (Turner, [21]) *The permutation group $\mathbb{Z}_p$ is a CI-group for any prime p.*

2 Main Theorem

Let $x : \mathbb{Z}_n \to \mathbb{Z}_n$ by $x(i) = i + 1$. We use this conceptualization of the n-cycle x at times in what follows. We begin with a sequence of lemmas.

Lemma 2.1 *Let $x, y \in S_n$ be n-cycles such that there exists $a|n$ such that $\langle x^a\rangle = \langle y^a\rangle$. Let $\mathbf{B}$ be the complete block system of $\langle x, y\rangle$ formed by the orbits of $\langle x^a\rangle = \langle y^a\rangle$. Assume that $\langle x, y\rangle/\mathbf{B}$ contains a normal elementary abelian p-subgroup K for some $p|a$ and $\langle x^{a/p}\rangle/\mathbf{B} \leq K$, $\langle y^{a/p}\rangle/\mathbf{B} \leq K$. Then either* $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B}) \neq \langle x^a\rangle$, *$\langle x^{a/p}\rangle = \langle y^{a/p}\rangle$, or $p \not| \frac{n}{a}$ and there exists a normal elementary abelian subgroup K' of $\langle x, y\rangle$ such that $K'/\mathbf{B} = K$ and $|K'| \geq p^2$.*

Proof. For this lemma, it will be convenient notationally to assume that both x, y act on $\mathbb{Z}_{a/p} \times \mathbb{Z}_p \times \mathbb{Z}_b$, where $b = n/a$, in the following fashion:

1. $\mathbf{B} = \{\{(i, j, k) : k \in \mathbb{Z}_b\} : i \in \mathbb{Z}_{a/p}, j \in \mathbb{Z}_p\}$,
2. $x^{a/p}(i, j, k) = (i, j + 1, k + \alpha_j)$, where $\alpha_j = 1$ if $j = p - 1$ and $\alpha_j = 0$ otherwise.

It is straightforward to see that $x^a(i, j, k) = (i, j, k + 1)$ so that $y^a(i, j, k) = (i, j, k + d)$, $d \in \mathbb{Z}_b^*$ and $y^{a/b}(i, j, k) = (i, j + a_i, \omega_{i,j}(k))$, where $a_i \in \mathbb{Z}_p^*$ and $\omega_{i,j} \in S_b$. As $\langle x^a\rangle = \langle y^a\rangle$, y centralizes x^a so by Theorem 1.10, we have that $\omega_{i,j}(k) = k+b_{i,j}$, $b_{i,j} \in \mathbb{Z}_b$ for every $i \in \mathbb{Z}_{a/p}$ and $j \in \mathbb{Z}_p$. As $y^{a/p}(i, j, k) = (i, j+a_i, k+b_{i,j})$, we have that $y^a(i, j, k) = (i, j, k+\sum_{j=0}^{p-1} b_{i,j})$. Hence $\sum_{j=0}^{p-1} b_{i,j} \equiv d \pmod b$ for every $i \in \mathbb{Z}_{a/p}$. Note that $x^{-a/p}(i, j, k) = (i, j-1, k-\alpha_{j-1})$ so that for $s \in \mathbb{Z}_p^*$, $x^{-sa/p}(i, j, k) = (i, j - s, k + \gamma_j)$, where $\gamma_j = -1$ if $p - 1 - s \leq j \leq p - 1$ and $\gamma_j = 0$ otherwise. Thus $y^{a/p}x^{-sa/p}(i, j, k) = (i, j - s + a_i, k + \gamma_j + b_{i,j-s})$ for $s \in \mathbb{Z}_p^*$. If $a_i - s \neq 0$

$$[y^{a/p}x^{-sa/p}]^p(i, j, k) = (i, j, k + \sum_{j=0}^{p} b_{i,j} + \sum_{j=0}^{p-1} \gamma_j) = (i, j, k + d - s).$$

If $a_i - s = 0$, then

$$[y^{a/p}x^{-sa/p}]^p(i, j, k) = (i, j, k + pb_{i,j-s} + p\gamma_j).$$

Now, if $\langle y^{a/p}\rangle/\mathbf{B} = \langle x^{a/p}\rangle/\mathbf{B}$, then $y^{a/p}x^r \in \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})$ for some $r \in \mathbb{Z}_p^*$. Hence either $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B}) \neq \langle x^a\rangle$ or $y^{a/p}x^{ra/p} \in \langle x^a\rangle$, for some $r \in \mathbb{Z}_p^*$. In the latter case, $y^{a/p} \in \langle x^{a/p}\rangle$.

In either case, the result follows. If $\langle y^{a/p}\rangle/\mathbf{B} \neq \langle x^{a/p}\rangle/\mathbf{B}$, then there exists $u, v \in \mathbb{Z}_{a/p}$ such that $a_u \not\equiv a_v \pmod p$, and, of course, $a_u, a_v \not\equiv 0 \pmod p$. If $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B}) = \langle x^a\rangle$, then, as $[y^{a/p}x^{-sa/p}]^p \in \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})$ and $a_u - a_v \not\equiv 0 \pmod p$, we would have that $d - a_u \equiv pb_{u,j-a_u} + p\gamma_j \pmod a$. If $p|b$, we then have that $d - a_u \equiv 0 \pmod p$ so that $d \equiv a_u \pmod p$. Analogous arguments will then show that $d \equiv a_v \pmod p$ so that $a_v \equiv a_u \pmod p$, a contradiction. Thus $p \not| b$.

If $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B}) = \langle x^a\rangle$, $p \not| b$, and there exists $u, v \in \mathbb{Z}_{a/p}$ such that $a_u \neq a_v$, then let K' be a Sylow p-subgroup of $\pi^{-1}(K)$, where $\pi : \langle x, y\rangle \to S_a$ by $\pi(g) = g/\mathbf{B}$. Note that $\mathrm{Ker}(\pi) = \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B}) = \langle x^a\rangle$, and as $a_u \neq a_v$, we have that $|K| \neq p$. Then $\pi^{-1}(K) \triangleleft \langle x, y\rangle$ and, of course, $\langle x^a\rangle \triangleleft \pi^{-1}(K)$. Furthermore, $|\pi^{-1}(K)| = |K| \cdot b$. As $p \not| b$, every Sylow p-subgroup of $\pi^{-1}(K)$ has order $|K|$. We conclude that $\pi^{-1}(K) = K' \cdot \langle x^a\rangle$. Let $k, \kappa \in K'$ and $x^r \in \langle x^a\rangle$. Then $(kx^r)^{-1}\kappa(kx^r) = k^{-1}\kappa k \in K'$ as every element of $\langle x, y\rangle$ centralizes $\langle x^a\rangle$. Whence $K' \triangleleft \pi^{-1}(K)$. As a normal Sylow p-subgroup is characteristic, we have that $K' \triangleleft \langle x, y\rangle$. That K' is elementary abelian follows from the fact that $K'/\mathbf{B} = K$ so that $K' \cong K$. The result then follows. □

The proof of the following result is straightforward and left to the reader.

Lemma 2.2 *Let m, k and s be integers, with $\gcd(m, s) = 1$. Then there exists some integer $i \equiv s \pmod m$ such that $\gcd(i, mk) = 1$.*

Lemma 2.3 *Let $\vec{X}_1$ be an irreducible CI-digraph of $\mathbb{Z}_m$ and $k \geq 2$. Then $\vec{X} = \vec{X}_1 \wr E_k$ and $\vec{X}' = E_k \wr \vec{X}_1$ are CI-digraphs of $\mathbb{Z}_{mk}$.*

PROOF. We will show that $\vec{X}$ is a CI-digraph of $\mathbb{Z}_{mk}$. The proof that $\vec{X}'$ is a CI-digraph of $\mathbb{Z}_{mk}$ is similar, although not exactly analogous. As $\vec{X}_1$ is irreducible, it follows by Corollary 1.22 that

$$\mathrm{Aut}(\vec{X}) = \mathrm{Aut}(\vec{X}_1) \wr S_k.$$

As $\mathbb{Z}_m \wr \mathbb{Z}_k \leq \mathrm{Aut}(\vec{X})$, $\vec{X}$ is a Cayley digraph of $\mathbb{Z}_{mk}$. Furthermore, $\mathrm{Aut}(\vec{X})$ admits a complete block system $\mathbf{B}$ of m blocks of size k, formed by the orbits of $\langle x^m\rangle$. Let $\delta \in S_n$ such that $\delta^{-1}\langle x\rangle\delta \leq \mathrm{Aut}(\vec{X})$ and $y = \delta^{-1}x\delta$. As $\vec{X}_1$ is a CI-digraph of $\mathbb{Z}_m$, any two regular cyclic subgroups of $\mathrm{Aut}(\vec{X}_1)$ are conjugate. Hence there exists $\gamma \in \mathrm{Aut}(\vec{X})$ such that $\gamma^{-1}y\gamma/\mathbf{B} \in \langle x\rangle/\mathbf{B}$. For convenience, we replace $\gamma^{-1}y\gamma$ with y and assume that $y/\mathbf{B} \in \langle x\rangle/\mathbf{B}$. As

$$\mathrm{Stab}_{\mathrm{Aut}(\vec{X})}(\mathbf{B}) = 1_{S_m} \wr S_k,$$

there exists $\gamma \in \mathrm{Stab}_{\mathrm{Aut}(\vec{X})}(\mathbf{B})$ such that $\gamma^{-1}y^m\gamma = x^m$. Again, we replace $\gamma^{-1}y\gamma$ with y and thus assume that $y^m = x^m$.

Fix $v_0 \in B_0$, and define s such that $x(v_0) = y^s(v_0)$. Since $x/\mathbf{B}$ and $y/\mathbf{B}$ are m-cycles and $y/\mathbf{B} \in x/\mathbf{B}$, we must have $\gcd(s, m) = 1$. By Lemma 2.2, there exists some i such that $|\langle y^{s+im}\rangle| = mk$. Furthermore, it is clear that $y^{s+im}/\mathbf{B} = x/\mathbf{B}$. Replace y^{s+im} with y. Observe $\langle x, y\rangle \leq \mathbb{Z}_m \wr \mathbb{Z}_k$, and of course, $\mathbb{Z}_m \wr \mathbb{Z}_k \leq \mathrm{Aut}(\vec{X})$. We identify $\mathbb{Z}_{mk}$ with $\mathbb{Z}_m \times \mathbb{Z}_k$ so that

$$x(i, j) = (i + 1, j + \sigma_i(j)),$$

where $\sigma_i(j) = 0$ if $i \neq m-1$ and $\sigma_{m-1}(j) = 1$. Then

$$y(i,j) = (i+1, j+b_i),$$

where $b_i \in \mathbb{Z}_k$. As $|y| = mk$, we have that $\Sigma_{i=0}^{m-1} b_i \equiv b \pmod k$ and $b \in \mathbb{Z}_k^*$. Let $\beta \in \mathrm{Aut}(\vec{X})$ such that $\beta(i,j) = (i, b^{-1}j)$. We replace y with $\beta y \beta^{-1}$ and thus assume that $\Sigma_{i=0}^{m-1} b_i \equiv 1 \pmod k$. Let $x^m = z_0 z_1 \cdots z_{m-1}$ where each z_i is a k-cycle that contains $(i,0)$. Let

$$\gamma = z_1^{-(\Sigma_{i-1}^{m-1} b_i)} z_2^{-(\Sigma_{i=2}^{m-1} b_i)} \cdots z_{m-1}^{-b_{m-1}}.$$

It is then straightforward to verify that $\gamma^{-1} y \gamma = x$ and $\gamma \in 1_{S_m} \wr \mathbb{Z}_k \leq \mathrm{Aut}(\vec{X})$. □

Lemma 2.4 *Let $\vec{X}$ be a circulant digraph of order n such that if $\langle x\rangle$ and $\langle y\rangle$ are distinct regular cyclic subgroups of $\mathrm{Aut}(\vec{X})$ and $\langle x, y\rangle$ admits a complete block system $\mathbf{C}$, then $\vec{X}[C] = E_{|C|}$ for every $C \in \mathbf{C}$. Assume (inductively) that every such circulant digraph with fewer than n vertices is a CI-digraph. If $\langle x, y\rangle$ admits a complete block system $\mathbf{B}$ of n/p blocks of size p for some prime $p|n$ and $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})$ is not faithful on some block of $\mathbf{B}$, then $\vec{X}$ is a CI-digraph of $\mathbb{Z}_n$.*

Proof. By Lemma 1.23, since the action of $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})$ is not faithful, there are clearly at least two blocks in the block system formed in Lemma 1.23. Denote this block system by $\mathbf{E}$. If vertices of $\vec{X}$ are labelled $0, 1, \ldots, n-1$, according to the action of x, then the vertices in the block E of $\mathbf{E}$ that contains the vertex 0 form the exponents of a proper subgroup of $\langle x\rangle$, by Theorem 1.7. By hypothesis there are no arcs within the block E; and since the action of $\langle x\rangle$ is transitive on the blocks of $\mathbf{E}$, there are no arcs within any block of $\mathbf{E}$. If there is an arc from some vertex in the block B of $\mathbf{B}$ to some vertex in the block B' of $\mathbf{B}$, where B and B' are in different blocks of $\mathbf{E}$, then Lemma 1.23 tells us that all arcs from B to B' exist (take $\langle x^a\rangle|_{E'}$, where $B \in E'$). Thus $\vec{X} = \vec{X}/\mathbf{F} \wr (\vec{X}[B])$ for $B \in \mathbf{B}$. Since $\vec{X}[E]$ contains no arcs for any $E \in \mathbf{E}$, we certainly have $\vec{X}[B]$ contains no arcs for any $B \in \mathbf{B}$. Thus $\vec{X} = \vec{X}/\mathbf{B} \wr E_p$. If $\vec{X}/\mathbf{B}$ is reducible, say $\vec{X}/\mathbf{B} = \vec{X}' \wr E_k$, then $\vec{X} = (\vec{X}' \wr E_k) \wr E_p = \vec{X}' \wr E_{kp}$. We continue this reduction until we reach a digraph $\vec{X}'$ such that $\vec{X}'$ is irreducible and $\vec{X} = \vec{X}' \wr E_{kp}$ for some k. Let $\langle x'\rangle$ and $\langle y'\rangle$ be distinct regular cyclic subgroups of $\mathrm{Aut}(\vec{X}')$ such that $\langle x', y'\rangle$ admits a nontrivial complete block system $\mathbf{C}'$. Let $\mathbf{D}$ be the unique complete block system of $\langle x, y\rangle$ of n/kp blocks of size kp. Then, as $\mathrm{Aut}(\vec{X}) = \mathrm{Aut}(\vec{X}') \wr S_{kp}$, there exist regular cyclic subgroups of $\mathrm{Aut}(\vec{X})$, say $\langle x_1\rangle$ and $\langle y_1\rangle$ such that $\langle x_1\rangle/\mathbf{D} = \langle x'\rangle$ and $\langle y_1\rangle/\mathbf{D} = \langle y'\rangle/\mathbf{D}$. As $\langle x', y'\rangle$ admits $\mathbf{C}'$ as a complete block system of, say, r blocks of size s, we have that $\langle x_1, y_1\rangle$ admits a complete block system $\mathbf{C}$ of r blocks of size kps. Notice that if e is an edge of $\vec{X}'$ between two vertices of $C' \in \mathbf{C}'$, then there is an edge in $\vec{X}$ between two vertices of $C \in \mathbf{C}$, where C is the block of $\mathbf{C}$ that corresponds to the block C'. As there are no edges of $\vec{X}$ between two vertices of $C \in \mathbf{C}$, there are no edges in $\vec{X}'$ between two vertices of $C' \in \mathbf{C}'$. Thus, either $\mathrm{Aut}(\vec{X}')$ contains a unique regular cyclic subgroup (in which case $\vec{X}'$ is a CI-digraph), or by inductive hypothesis $\vec{X}'$ is a CI-digraph. Then by Lemma 2.3, since $p \geq 2$, $\vec{X}$ is a CI-digraph, and we are done. $\square$

Lemma 2.5 *Let x, y be n-cycles acting on a set of n elements. Assume that every element of $\langle x, y\rangle$ commutes with x^a for some $0 < a < n$. Let $ab = n$, so that $\langle x, y\rangle$ admits a complete block system $\mathbf{B}$ of a blocks of size b. Assume that the action of $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})|_B$ is not faithful for some $B \in \mathbf{B}$. Then $\langle x, y\rangle$ admits a complete block system $\mathbf{C}_{b'}$ consisting of ab/b' blocks of size b' for every $b'|b$; furthermore, there is some prime $p|b$ such that the action of $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_p)$ is not faithful.*

Proof. Notice that

$$\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})|_B = \langle x^a\rangle|_B$$

for any $B \in \mathbf{B}$, since x^a commutes with every element of $\langle x, y'\rangle$. Hence $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{B})|_B$ admits blocks of every possible size b' for which $b'|b$. By Lemma 1.14, $\langle x, y'\rangle$ admits a complete block system with blocks of size b' for any $b'|b$.

Suppose that $b = rs$. We choose r, s in such a way that r is as large as possible so that $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_r)|_C$ is faithful for every $C \in \mathbf{C}_r$. (Notice that the transitivity of $\langle x, y\rangle$ means that if $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_r)|_C$ were not faithful for some $C \in \mathbf{C}_r$, then it would not be faithful for any $C \in \mathbf{C}_r$.) We have $1 \leq r < b$, and $2 \leq s \leq b$, since $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})|_B$ is not faithful.

Let $h \in \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{B})$ be such that $h|_B = 1|_B$ but $h \neq 1$. Since $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_r)|_C$ is faithful for every $C \in \mathbf{C}_r$, and for any $C \subset B$ we have $h|_C = 1$, but $h \neq 1$, we must have $h \notin \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_r)$. So if $B' \in \mathbf{B}$ is such that $h|_{B'} \neq 1$, then there exists some $C \subset B'$ such that $h(C) \neq C$. Now, $h|_{B'} = x^{i_{B'}a}|_{B'}$ for some $i_{B'}$. Since there are s blocks of $\mathbf{C}_r$ in B', formed by the orbits of $\langle x^{sa}\rangle$, we have $h^s = 1$, so $x^{i_{B'}as} = 1$. Hence $b|i_{B'}s$, say $k_{B'}b = i_{B'}s$. But $b = rs$, so $k_{B'}rs = i_{B'}s$, meaning that $k_{B'}r = i_{B'}$ for any B'. Thus $h \in \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_s)$. Since $x^{i_{B'}a}|_{B'}$ is nontrivial, this has shown that $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_s)$ is not faithful. Now, suppose that $\gcd(r, s) = t \neq 1$. Let r' be such that $r't = r$ and let s' be such that $s't = s$. Then for any B',

$$i_{B'} = k_{B'}r = k_{B'}tr',$$

and so

$$h^{s'}|'_B = x^{i_{B'}as'}|'_B = x^{k_{B'}ts'r'a} = x^{k_{B'}r'as}.$$

Since $\mathbf{C}_r$ is formed by the orbits of x^{sa}, we have $h^{s'} \in \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_r)$, so $h^{s'} = 1$. It is not difficult to calculate that $i_{B'} = k'_{B'}rt$, and since $\gcd(rt, s/t) = 1$, to see that in fact $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_{rt})$ is faithful, contradicting the choice of r. So we see that $\gcd(r, s) = 1$.

Let p be any prime such that $p|s$. We claim that the action of $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_p)$ is not faithful.

Towards a contradiction, suppose that the action of $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_p)$ were faithful. We will show that this supposition forces the action of $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_{rp})$ to be faithful, contradicting the choice of r.

Let D be a block of $\mathbf{C}_{rp}$ and let $h \in \mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_{rp})$ be such that $h|_D = 1$. If every such h is an element of the group $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_r)$, then every such $h = 1$ and we are done. So we suppose that there is some such h that is not an element of the group $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_r)$. As before, we can calculate that $h|_{B'} = x^{i_{B'}a}$, and that $i_{B'} = k_{B'}r$; and, similarly, $i_{B'} = k'_{B'}p$. Since $\gcd(s,r) = 1$, we have $p \not| r$, so $i_{B'} = k''_{B'}rp$. Now, the intersection of the orbit of h containing the vertex v in B' with the block D' of $\mathbf{C}_{rp}$ that contains the vertex v is clearly the singleton $\{v\}$, since the block D' is an orbit of $x^{as/p}$. This shows that when h fixes the block D' set-wise, it in fact fixes this block point-wise, so that $h \in \mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_{rp})$ with $h|_D = 1$ in fact forces $h = 1$, as required. This proves our claim.

Thus, $\mathbf{C}_p$ is a collection of blocks of prime size of $\langle x, y'\rangle$, formed by the orbits of $x^{n/p}$, upon which $\mathrm{Stab}_{\langle x,y\rangle}(\mathbf{C}_p)$ is not faithful. $\square$

Theorem 2.6 *Let $\vec{X}$ be a circulant digraph such that whenever $\langle x\rangle$ and $\langle y\rangle$ are two distinct regular cyclic subgroups of $\mathrm{Aut}(\vec{X})$ and $\langle x, y\rangle$ admits a nontrivial complete block system $\mathbf{B}$, then $\vec{X}[B] = E_{|B|}$ for every $B \in \mathbf{B}$. Then $\vec{X}$ is a CI-digraph.*

Proof. Let x, y be n-cycles in $\mathrm{Aut}(\vec{X})$. Let

$$Y = \{y' \in \mathrm{Aut}(\vec{X}) : \text{ there exists } \gamma \in \mathrm{Aut}(\vec{X}) \text{ such that } \gamma^{-1}y\gamma = y'\}.$$

By Theorem 1.25, we need only show that $x \in Y$. Note that by Theorem 1.13 there exists $\delta \in \langle x, y\rangle$ such that $\langle x, \delta^{-1}y\delta\rangle$ is solvable and $\langle x, \delta^{-1}y\delta\rangle$ admits complete block systems $\mathbf{B}_0, \ldots, \mathbf{B}_{m+1}$ such that if $B_i \in \mathbf{B}_i$, then there exists $B_{i+1} \in \mathbf{B}_{i+1}$ such that $B_i \subset B_{i+1}$ and $|B_{i+1}|/|B_i|$ is prime for every $0 \le i \le m+1$, where $|\mathbf{B}_0| = n$ and $|\mathbf{B}_{m+1}| = 1$. We thus assume without loss of generality that $\langle x, y\rangle$ has the preceding properties.

In order to enable us to use Lemma 2.3, the proof will proceed by induction on the number of prime factors of n. The base case where n is prime is given by Theorem 1.26, so in what follows, we can assume that any digraphs of strictly smaller order than n that satisfy the hypothesis of this theorem are in fact CI-digraphs.

Choose $y' \in Y$ in such a way that $\langle x^a\rangle = \langle (y')^a\rangle$, where a is as small as possible $(0 < a \le n)$. If $\gcd(a, n) = k$, then $\langle (y')^k\rangle = \langle x^k\rangle$, so by the choice of a, $k = a$. Thus, we must have that $a|n$, say $ab = n$, and by [22, Proposition 7.1], the orbits of x^a are blocks of $\langle x, y'\rangle$, yielding a complete block system $\mathbf{B}$ consisting of a blocks of size b. It follows by the proof of [17, Theorem 4.9] that we may assume $\mathbf{B} = \mathbf{B}_i$ for some $0 \le i \le m+1$.

Let $p = |B_{i+1}|/|B_i|$, $B_{i+1} \in \mathbf{B}_{i+1}$ and $B_i \in \mathbf{B}_i$. As $\langle x, y'\rangle$ admits $\mathbf{B}_{i+1}$ as a complete block system (if not, conjugate it by an element of $\langle x, y'\rangle$ as in Theorem 1.13), $\langle x, y'\rangle/\mathbf{B}$ admits a complete block system $\mathbf{C}$ of a/p blocks of size p induced by $\mathbf{B}_{i+1}$. Hence $\mathbf{C}$ is formed by the orbits of $\langle x^{a/p}\rangle/\mathbf{B}$ and also by the orbits of $\langle (y')^{a/p}\rangle/\mathbf{B}$. As $\langle x, y'\rangle$ is solvable, $\mathrm{Stab}_{\langle x,y'\rangle/\mathbf{B}}(\mathbf{C})|_C$ is solvable of prime degree p for every $C \in \mathbf{C}$, so by Theorem 1.12 $\mathrm{Stab}_{\langle x,y'\rangle/\mathbf{B}}(\mathbf{C})|_C$ has a unique Sylow p-subgroup for every $C \in \mathbf{C}$. Let K be a Sylow p-subgroup of $\mathrm{Stab}_{\langle x,y'\rangle/\mathbf{B}}(\mathbf{C})$. Then $K \triangleleft \mathrm{Stab}_{\langle x,y'\rangle/\mathbf{B}}(\mathbf{C})$ and is elementary abelian. As a Sylow p-subgroup is characteristic, we have that $K \triangleleft \langle x, y'\rangle/\mathbf{B}$. It then follows by Lemma 2.1 and our choice of a that $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{B}) \ne \langle x^a\rangle$ or $p \not| b$ and there exists a normal elementary abelian subgroup K' of $\langle x, y'\rangle$ such that $K'/\mathbf{B} = K$ and $|K'| \ge p^2$.

If $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{B}) \ne \langle x^a\rangle$, then as $\langle x^a\rangle = \langle (y')^a\rangle$, we have that every element of $\langle x, y'\rangle$ centralizes $\langle x^a\rangle$. Hence by Theorem 1.10, $\langle x, y'\rangle \le \langle x, y'\rangle/\mathbf{B} \wr \mathbb{Z}_b$. As $|\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{B})| > b$, we have that $\mathrm{Stab}_{\mathrm{Stab}_{\langle x,y'\rangle}}(w) \neq 1$ for every $w \in \mathbb{Z}_n$. As $\mathbb{Z}_b$ is regular in its action on $\mathbb{Z}_b$, we conclude that $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{B})$ is not faithful on some block of $\mathbf{B}$. By Lemma 2.5, $\langle x, y'\rangle$ admits a complete block system $\mathbf{C}_{b'}$ consisting of ab/b' blocks of size b' for every $b'|b$; furthermore, there is some prime $p|b$ such that the action of $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_p)$ is not faithful. It then follows by Lemma 2.4 that $\vec{X}$ is a CI-digraph of $\mathbb{Z}_n$, so that in this case $a = 1$ and we are done.

If $p \not| b$ and there exists a normal elementary abelian subgroup K' of $\langle x, y'\rangle$ such that $K'/\mathbf{B} = K$ and $|K'| \geq p^2$, then $\langle x, y'\rangle$ admits a complete block system $\mathbf{C}_p$ of n/p blocks of size p, formed by the orbits of K. As p^2 divides $|K|$, p^2 also divides $|\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_p)|$. Then $\mathrm{Stab}_{\langle x,y'\rangle}(\mathbf{C}_p)$ does not act faithfully on some block of $\mathbf{C}_p$ and by Lemma 2.4, $\vec{X}$ is a CI-digraph of $\mathbb{Z}_n$. Thus $a = 1$ and the result follows. □

Corollary 2.7 *Let $\vec{X}$ be a unit circulant digraph on n vertices. Then $\vec{X}$ is a CI-digraph.*

Proof. If $\mathrm{Aut}(\vec{X})$ contains a unique regular cyclic subgroup, then $\vec{X}$ is a CI-digraph as required. We let $\langle x\rangle$ be the regular representation of $\mathbb{Z}_n$ contained in $\mathrm{Aut}(\vec{X})$. If $\langle y\rangle$ is any other regular cyclic subgroup of $\mathrm{Aut}(\vec{X})$ and $\langle x, y\rangle$ admits a complete block system $\mathbf{B}$, then $\mathbf{B}$ is formed by the orbits of a normal subgroup of $\langle x\rangle$, so that $\mathbf{B}$ consists of cosets of a subgroup H of $\mathbb{Z}_n$. As $\vec{X}$ is a unit circulant digraph, $\vec{X}[B] = E_{|B|}$ and the result follows by Theorem 2.6. □

Let d be an arbitrary divisor of the positive integer n. Let $(\mathbb{Z}_n)_d = \{z \in \mathbb{Z}_n : \gcd(z, n) = d\}$. The $d-$th *layer of $S \subseteq \mathbb{Z}_n$* is defined as $(S)_d = S \cap (\mathbb{Z}_n)_d$. In 1975, Zibin' made the following conjecture.

Conjecture 2.8 (Zibin',[23]) *Let X and X' be two isomorphic circulant graphs with connection sets S and T, respectively. Then there exists $m_d \in \mathbb{Z}_n^*$ such that $m_d(S)_d = (T)_d$ for every divisor d of n.*

Note that if $d = 1$, then $(S)_1 \subseteq \mathbb{Z}_n^*$. Hence this special case of Zibin's Conjecture is Toida's Conjecture, so that Zibin's Conjecture implies Toida's Conjecture.

Corollary 2.9 *Toida's Conjecture implies Zibin's Conjecture.*

Proof. We first show that for every $d|n$ and circulant digraphs $\vec{X}(\mathbb{Z}_n, S) \cong \vec{X}(\mathbb{Z}_n, T)$, we have that $\vec{X}(\mathbb{Z}_n, (S)_d) \cong \vec{X}(\mathbb{Z}_n, (T)_d)$. Suppose not, and let $\vec{X}(\mathbb{Z}_n, S)$ be a graph of minimal order and size such that there exists $d|n$ and $T \subset \mathbb{Z}_n$ such that $\vec{X}(\mathbb{Z}_n, S) \cong \vec{X}'(\mathbb{Z}_n, T)$ but $\vec{X}(\mathbb{Z}_n, (S)_d) \not\cong \vec{X}'(\mathbb{Z}_n, (T)_d)$. If $\mathrm{Aut}(\vec{X})$ contains a unique regular cyclic subgroup, then $\vec{X}$ is a CI-digraph, in which case it is easy to verify that $\vec{X}(\mathbb{Z}_n, (S)_d) \cong \vec{X}'(\mathbb{Z}_n, (T)_d)$. Let $\langle x\rangle$ be the canonical regular cyclic subgroup of $\mathrm{Aut}(\vec{X})$, so that $x(i) = i + 1$. Let $\delta : \vec{X} \to \vec{X}'$ be an isomorphism, and $y = \delta^{-1}x\delta$. If $\langle x, y, \rangle$ does not admit a nontrivial complete block system, then [22, Theorem 25.3], then $\langle x, y\rangle$ is doubly transitive, and so $\vec{X}$ the complete graph or it's complement, in which case the result is trivial.

Otherwise, $\langle x, y\rangle$ admits a nontrivial complete block system $\mathbf{B}$ of m blocks of size k, necessarily formed by the orbits of $\langle x^m\rangle$. As there is a unique complete block system of $\langle x\rangle$ with blocks of size k, (and hence of any subgroup of S_n that contains $\langle x\rangle$), we have that $\delta(\mathbf{B}) = \mathbf{B}$. Furthermore, assume that $\vec{X}[B] \neq E_k$ for $B \in \mathbf{B}$. As $\delta(\mathbf{B}) = \mathbf{B}$, we have that $\delta\vec{X}[B] = \vec{X}'[B']$ for some $B' \in \mathbf{B}$. By the minimality of n, it follows that the t-th layers of $\vec{X}[B]$ are isomorphic to the t-th layers of $\vec{X}'[B'] \cong \vec{X}'[B]$, t a divisor of k. Let r be a multiple of m. Then the r-th layer of $\vec{X}$ is a disjoint union of m copies of the t-th layer of $\vec{X}[B]$, and the r-th layer of $\vec{X}'$ is also a disjoint union of m copies of the t-th layer of $\vec{X}'[B]$. We conclude that the r-th layers of $\vec{X}$ and $\vec{X}'$ are isomorphic. Thus d is not a multiple of m. Furthermore, as $\delta(\mathbf{B}) = \mathbf{B}$, δ is also an isomorphism of $\vec{X}(\mathbb{Z}_n, S - \cup\{(S)_r : r \text{ is a multiple of } m\})$ and $\vec{X}'(\mathbb{Z}_n, T - \cup\{(T)_r : r \text{ is a multiple of } m\})$, the d-th layer of $\vec{X}(\mathbb{Z}_n, S - \cup\{(S)_r : r \text{ is a multiple of } m\})$ is the same as the d-th layer of $\vec{X}$, and the d-th layer of $\vec{X}'(\mathbb{Z}_n, T - \cup\{(T)_r : r \text{ is a multiple of } m\})$ is the same as the d-th layer of $\vec{X}'$. By the minimality of the size of $\vec{X}$, we conclude that $\vec{X}[B] = E_k$ for every $B \in \mathbf{B}$. It then follows by Theorem 2.6 that $\vec{X}$ is a CI-graph. This then implies that the d-th layer of $\vec{X}$ is isomorphic to the d-th layer of $\vec{X}'$, a contradiction. Thus the d-th layer of $\vec{X}$ is isomorphic to the d-th layer of $\vec{X}'$ for every $d|n$ and circulant digraph $\vec{X}'$ isomorphic to $\vec{X}$.

Finally, it is straightforward to observe that the d-th layer of $\vec{X}$ is isomorphic to the wreath product of $E_{n/d}$ with a unit circulant graph of order d. As Toida's Conjecture holds, it follows by Lemma 2.3 that the d-th layer of $\vec{X}$ is a CI-digraph. The result then follows. □

The authors would gratefully like to acknowledge the assistance of Dave Witte of Oklahoma State University in proving some of the more technical results in an earlier version of this paper.

References

[1] Ádám, A., Research problem 2-10, *J. Combin. 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] Babai, L., Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329-336.

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

[5] Dixon, J.D., and Mortimer, B., *Permutation Groups*, Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996.

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

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

[8] Golfand, J.J., N.L. Najmark and R. Pöschel, The structure of S-rings over $\mathbb{Z}_{2^m}$, *preprint* (1984).

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

[10] Klin, M.H., M. Muzychuk and R. Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, *Codes and Association Schemes*, American Math. Society, 2001.

[11] Klin, M.H. and R. Pöschel, The Konig problem, the isomorphism problem for cyclic graphs and the method of Schur rings, *Algebraic methods in graph theory, Vol. I, II.*, Szeged, 1978, pp. 405-434.

[12] Klin, M.H. and R. Pöschel, The isomorphism problem for circulant digraphs with p^n vertices, *unpublished manuscript* (1980).

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

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

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

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

[17] Muzychuk, M., On the isomorphism problem for cyclic combinatorial objects, *Disc. Math.* **197/198** (1999), 589-606.

[18] Sabidussi, G., The composition of graphs, *Duke Math J.* **26** (1959), 693-696.

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

[20] Toida, S., A note on Àdàm's conjecture, *J. Combin. Theory B* **23** (1977), 239-246.

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

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

[23] Zibin', D.K., Private communication, August 1975.