8-12-2016

Circulant Digraph Isomorphisms

Elias Cancela

Circulant digraph isomorphisms

By

Elias Cancela

A Thesis
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Master of Science
in Mathematics
in the Department of Mathematics and Statistics

Mississippi State, Mississippi

August 2016

Circulant digraph isomorphisms

By

Elias Cancela

Approved:

Edward T. Dobson
(Major Professor)

Matthew S. McBride
(Committee Member)

Paul Fabel
(Committee Member)

Corlis P. Johnson
(Graduate Coordinator)

Rick Travis
Interim Dean
College of Arts and Sciences

Name: Elias Cancela

Date of Degree: August 12, 2016

Institution: Mississippi State University

Major Field: Mathematics

Major Professor: Dr. Edward Dobson

Director of Thesis: Dr. Edward Dobson

Title of Study: Circulant digraph isomorphisms

Pages of Study: 59

Candidate for Degree of Master of Science

We determine necessary and sufficient conditions for a Cayley digraph of the cyclic group of order n to have the property that any other Cayley digraph of a cyclic group of order n is isomorphic to the first if and only if an isomorphism between the two digraphs is a group automorphism of the cyclic group of order n.

Key words: CI-graph, Cayley graph, isomorphism, circulant graph.

DEDICATION

To Betsabe and Samuel.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Ádám conjectured [1] in 1967 that any two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if there exists $m \in \mathbb{Z}_n^*$ such that $mS = T$. This is equivalent to the two circulant graphs being isomorphic if and only if the automorphism of $\mathbb{Z}_n$ defined by $x \mapsto mx$ is an isomorphism between the two circulant graphs. While the original conjecture was shown to be false in 1970 by Elspas and Turner [12], there has been much interest in determining isomorphisms between circulant digraphs. At first, the focus was on determining for which positive integers any two circulant (di)graphs of order n are isomorphic if an only if they are isomorphic by a group automorphism of $\mathbb{Z}_n$ (such groups $\mathbb{Z}_n$ are called **CI-groups with respect to digraphs**). This line of research was finished by Muzychuk [18], who showed $\mathbb{Z}_n$ is a CI-group with respect to graphs if and only if $n = 9, m, 2m$, or $4m$ and is a CI-group with respect to digraphs if and only if $n = m, 2m$, or $4m$, where m is odd and square-free.

Instead of determining for which n Ádám's conjecture is true, we can ask for a given n, which circulant graphs of order n will the conjecture hold? We can rephrase the question as follows. For which circulant $\mathrm{Cay}(\mathbb{Z}_n, S)$ is it true that any other circulant digraph $\mathrm{Cay}(\mathbb{Z}_n, T)$ is isomorphic to $\mathrm{Cay}(\mathbb{Z}_n, S)$ if and only if $\alpha(S) = T$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$?

Alspach and Parsons in 1979 [2] gave conditions for the case $n = p^2$. In this thesis we will generalize Alspach and Parsons' result and explicitly determine all circulant digraphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ of order n such that if $\mathrm{Cay}(\mathbb{Z}_n, T)$ is another circulant digraph of order n, then $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, T)$ are isomorphic if and only if there exists $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$ such that $\alpha(S) = T$.

CHAPTER 2

GRAPH THEORY AND GROUP THEORY

In this chapter we gather the basic definitions and results concerning Cayley (di)graphs, the main object of study in this thesis.

A digraph is an ordered pair $G = (V, A)$ comprising a set V of vertices together with a set A of arcs, which are ordered pairs of elements of V. A graph is a digraph, whenever $(u, v) \in A(G)$ then $(v, u) \in A(G)$. K_n will denote the **complete graph**, that is the digraph with all possible arcs. In this case, we identify (u, v) and (v, u) and call it an edge.

A **permutation group** is a subgroup of the **symmetric group** on n letters, $\mathcal{S}_n$. Unless otherwise stated, we will take the n letters that $\mathcal{S}_n$ permutes to be the elements of the set $\mathbb{Z}_n$, the integers modulo n. We denote the group of units in $\mathbb{Z}_n$ under multiplication by $\mathbb{Z}_n^*$, and note that $\mathrm{Aut}(\mathbb{Z}_n) = \{x \mapsto ax : a \in \mathbb{Z}_n^*\}$. .

Definition 1

An isomorphism of digraphs G and H is a bijection between the vertex sets of G and H

$f : V(G) \to V(H)$

such that $(u, v) \in A(G)$ if and only if $(f(u), f(v)) \in A(H)$. If an isomorphism exists between two digraphs, then the digraphs are called isomorphic and denoted as $G \cong H$

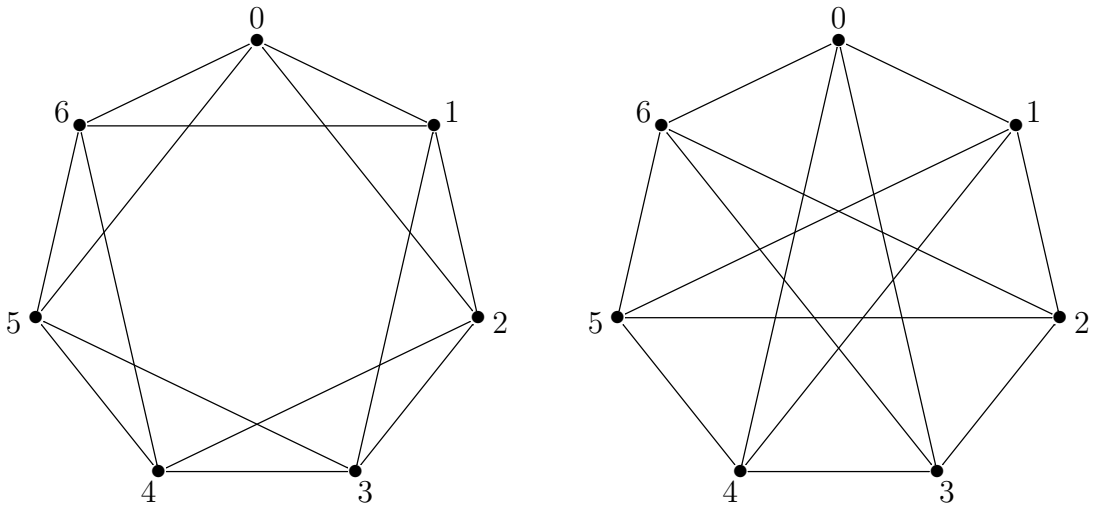

Figure 2.1

Two isomorphic graphs

Definition 2

A (di)graph isomorphism from G to itself is called a automorphism. The set all automorphims of G is denoted $\mathrm{Aut}(G)$.

Definition 3

Let G be a group and $S \subseteq G$. Define a **Cayley digraph of** G, *denoted* $\mathrm{Cay}(G, S)$, *to be the digraph with* $V(\mathrm{Cay}(G, S)) = G$ *and* $A(\mathrm{Cay}(G, S)) = \{(g, gs) : g \in G, s \in S\}$. *We call S the* **connection set of** $\mathrm{Cay}(G, S)$.

If we additionally insist that $S = S^{-1} = \{s^{-1} : s \in S\}$ (or if the group is abelian and the operation is addition, then $S = -S$), then there will be no directed edges in $\mathrm{Cay}(G, S)$, and we obtain a **Cayley graph**. This follows as if $(g, gs) \in A(\mathrm{Cay}(G, S))$ and $s^{-1} \in S$, then $(gs, gs(s^{-1})) = (gs, s) \in A(\mathrm{Cay}(G, S))$.

Perhaps the most common Cayley digraphs that one encounters are Cayley digraphs of the cyclic groups $\mathbb{Z}_n$ of order n, as in Figure 2.2. A Cayley (di)graph of $\mathbb{Z}_n$ is called a **circulant** (di)graph circulant graph of order n. We state this as a definition and we present and example.

Definition 4

A **circulant (di)graph** *is Cayley (di)graph of* $\mathbb{Z}_n$.

The graph in Figure 2.2 is $\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 3, 7, 9\})$. Note that as the binary operation on $\mathbb{Z}_{10}$ is addition, there is an edge between two vertices if and only if the difference of the labels on the vertices is contained in the set $\{1, 3, 7, 9\}$. Observe that a clockwise rotation of 36° leaves the graph unchanged.

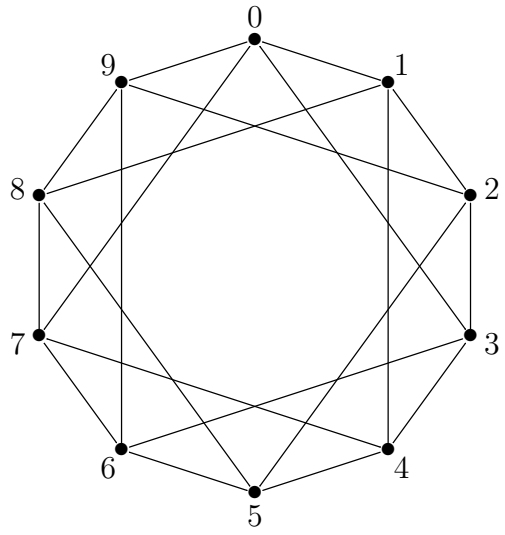

Figure 2.2

The Cayley graph $\mathrm{Cay}(\mathbb{Z}_{10}, \{1, 3, 7, 9\})$.

Definition 5

For a group G, the **left regular representation**, *denoted G_L, is the subgroup of $\mathcal{S}_G$ given by the left translations of G. More specifically, $G_L = \{x \mapsto gx : g \in G\}$. We denote the map $x \mapsto gx$ by g_L. It is straightforward to verify that G_L is a group and that $G_L \cong G$*

Let $x, y \in G$, and $g = yx^{-1}$. Then $g_L(x) = yx^{-1}x = y$ so that G_L is transitive on G.

For example the permutations obtained by clockwise rotation of 36° in the graph of figure 2.2 generates $G_L = (\mathbb{Z}_{10})_L$

In general, for an abelian group G, the group G_L will consist of "translations by g" that is $x \mapsto g + x = x + g$, or $G_L = \{x \mapsto x + g : g \in G\}$. More specifically, the cyclic group $\mathbb{Z}_n$ is generated by the map $x \mapsto x + 1$ (or course instead of 1, one could put any generator of $\mathbb{Z}_n$).

Now we will see some useful results.

Lemma 1

If G is a group and $S \subseteq G$, then $G_L \leq \mathrm{Aut}(\mathrm{Cay}(G, S))$.

Proof: Let $a = (g, gs) \in A(\mathrm{Cay}(G, S))$, where $g \in G$ and $s \in S$. Let $h \in G$. We must show that $h_L(e) \in A(\mathrm{Cay}(G, S))$, or that $h_L(a) = (g', g's')$ for some $g' \in G$ and $s' \in S$. Setting $g' = hg$ and $s' = s$, we have

$$h_L(a) = h_L(g, gs) = (hg, h(gs)) = (hg, (hg)s) = (g', g's').$$

■

Now we turn to the relationship between Cayley digraphs of G and $\mathrm{Aut}(G)$, the **automorphism group of** G.

Lemma 2

Let G be a group, $\alpha \in \mathrm{Aut}(G)$ and $S \subseteq G$. Then $\alpha(\mathrm{Cay}(G, S))$ is a Cayley digraph of G with connection set $\alpha(S)$.

Proof: Clearly $\alpha : G \mapsto G$ so that $V(\alpha(\mathrm{Cay}(G, S))) = G$. Let $a = (g, gs) \in A(\mathrm{Cay}(G, S))$, where $g \in G$ and $s \in S$. Then

$$\alpha(a) = \alpha(g, gs) = (\alpha(g), \alpha(gs)) = (\alpha(g), \alpha(g)\alpha(s)) = (g', g's')$$

where $g' = \alpha(g)$ and $s' = \alpha(s) \in \alpha(S)$. ■

This says that the image under a group automorphism of a Cayley digraph is another Cayley digraph.

CHAPTER 3

ÁDÁM'S CONJECTURE

In 1967, Ádám [1] conjectured that two circulant graphs $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic if and only if there exists $m \in \mathbb{Z}_n^*$ such that $mS = S'$ (where $mS = \{ms : s \in S\}$). If $mS = S'$ it is often said that $\mathrm{Cay}(\mathbb{Z}_n, S)$ and $\mathrm{Cay}(\mathbb{Z}_n, S')$ are isomorphic by a **multiplier**. As for each $m \in \mathbb{Z}_n^*$, the map $x \mapsto mx$ is a group automorphism of $\mathbb{Z}_n$. Ádám conjectured that two circulant graphs of order n are isomorphic if and only if they are isomorphic by a group automorphism of $\mathbb{Z}_n$.

It was quickly shown by Elspas and Turner [12] that Ádám's conjecture is not true, by giving two isomorphic circulant graphs of order 16 that are not isomorphic by a multiplier.

Following Elspas and Turner's example showing that Ádám's original conjecture was false, the conjecture quickly (we remark that one reason that Ádám's conjecture was not abandoned was that already in 1967 Turner [20] had verified Ádám's conjecture for circulant graphs of prime order) turned into a problem and was generalized to Cayley graphs of groups that were non-cyclic. The new question was, which groups G have the property that any two Cayley (di)graphs of G are isomorphic if and only if they are isomorphic by a group automorphism of G? This question motivates the following definition:

Definition 6

A group G which has the property that any two Cayley (di)graphs of G are isomorphic if and only if they are isomorphic by a group automorphism of G is called a **CI-group with respect to (di)graphs**.

One may wonder why we do not just say "CI-group" instead of "CI-group with respect to (di)graphs". This is because it is possible to ask the same question about other classes of "combinatorial objects", e.g. combinatorial designs, once one has a notion of a "Cayley object" or "Cayley design".

One more term is necessary before we proceed.

Definition 7

Suppose that there is a Cayley (di)graph Γ of G such that if Γ' is any Cayley (di)graph of G, then Γ and Γ' are isomorphic if and only if they are are isomorphic by a group automorphism of G. Such a Cayley (di)graph of G is called a **CI-(di)graph of** G.

Evidently, G is a CI-group with respect to (di)graphs if and every Cayley (di)graph of G is a CI-(di)graph.

Theorem 1

Let G be a CI-group with respect to digraphs and $H \leq G$. Then H is a CI-group with respect to digraphs.

Proof: Let $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ be isomorphic Cayley digraphs of H. As the digraph $\mathrm{Cay}(H, S_1)$ is a CI-digraph of H if and only if its complement is a CI-digraph of H we may assume that $\mathrm{Cay}(H, S_1)$ and $\mathrm{Cay}(H, S_2)$ are both connected by replacing them with their complements if necessary. It is not hard to see then that $\langle S_1 \rangle = \langle S_2 \rangle = H$. Then

$\mathrm{Cay}(G, S_1)$ and $\mathrm{Cay}(G, S_2)$ are isomorphic Cayley digraphs of G, so there exists $\alpha \in \mathrm{Aut}(G)$ such that $\mathrm{Cay}(G, S_2) = \alpha(\mathrm{Cay}(G, S_1)) = \mathrm{Cay}(G, \alpha(S_1))$. Hence $\alpha(S_1) = S_2$, and so $H = \langle S_2 \rangle = \alpha(\langle S_1 \rangle) = \alpha(H)$. The restriction of α to H is then an isomorphism from $\mathrm{Cay}(H, S_1)$ to $\mathrm{Cay}(H, S_2)$. ∎

3.1 Counterexamples

As we said it was quickly shown by Elspas and Turner that Ádám's conjecture is not true, that is that there are two isomorphic circulant graphs of order 16 that are not isomorphic by a multiplier.We now give Elspas and Turner's example.

Let $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{16}, \{1, 2, 7, 9, 14, 15\})$ and $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{16}, \{2, 3, 5, 11, 13, 14\})$ be the circulant graphs shown in Figure 3.1. If Γ_1 and Γ_2 are isomorphic by a multiplier, then there exists $m \in \mathbb{Z}_{16}$ such that $m\{1, 2, 7, 9, 14, 15\} = \{2, 3, 5, 11, 13, 14\}$. As both Γ_1 and Γ_2 are graphs, the map $x \mapsto -x$ is an automorphism of both Γ_1 and Γ_2. Thus for graphs, $mS = S'$ if and only if $(-m)S = S'$. We may thus assume without loss of generality that $m \leq 8$, and as $m \in \mathbb{Z}_{16}^*$, $m = 1, 3, 5, 7$. As 1 is in the connection set of Γ_1, m is in the connection set of Γ_2, so $m = 3, 5$. As $3 \cdot 2 = 6 \notin S'$, and $5 \cdot 2 = 10 \notin S'$, where S' is the connection set of Γ_2, we see that Γ_1 and Γ_2 are not isomorphic by a multiplier. Finally, straightforward though tedious computations will show that the map defined by $x \mapsto x$ if x is even and $x \mapsto x + 4$ if x is odd is an isomorphism from Γ_1 to Γ_2.

Elspas and Turner also gave an example of two circulant digraphs of order 8 that are not isomorphic by a multiplier, see[[12].

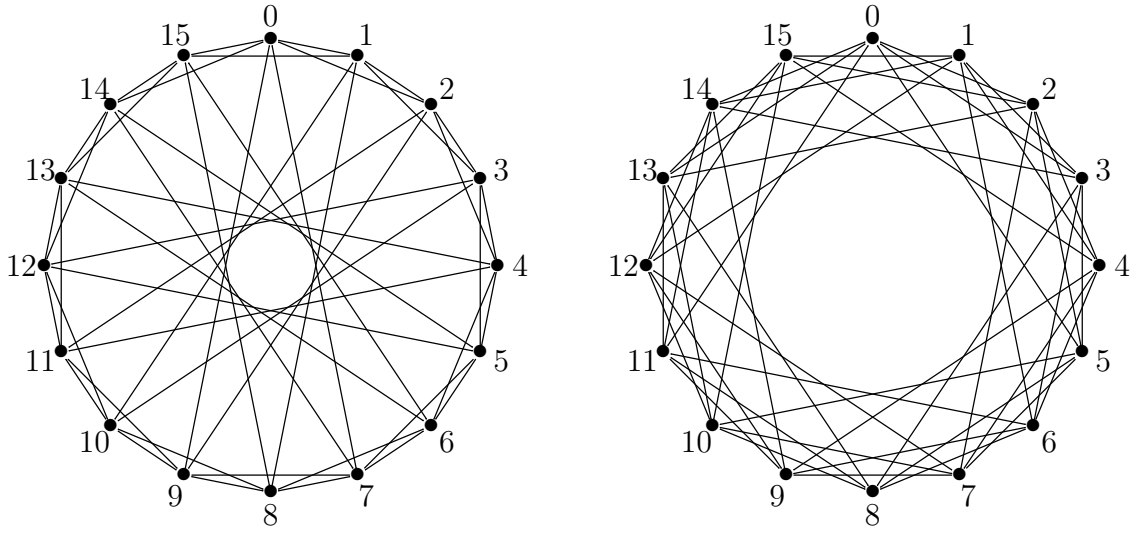

Figure 3.1

Two circulant graphs not isomorphic by a multiplier

Alpach and Parsons also have examples for the case of circulant graphs of order p^2 for p an odd prime. As a simple consequence of Theorem 1 we see that the conjecture is false in most cases when n is divisible by p^2, or n is divisible by 16.

Theorem 2

If $8|n$ and $n > 8$, then $\mathbb{Z}_n$ is not a CI-group with respect to graphs.

Proof: In view of Theorem 1, it suffices to show that $\mathbb{Z}_{8p}$, p a prime, is not a CI-group with respect to graphs. Let $S = \{1, 4p+1, 8p-1, 4p-1, 2, 8p-2\}$, and $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{8p}, S)$. Let $\beta \in \mathbb{Z}_{4p}$ such that $\beta \equiv 3 \pmod 4$ and $\beta \equiv 1 \pmod p$. Let $T = \{1, 4p+1, 8p-1, 4p-1, 2\beta, 8p-2\beta\}$, and $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{8p}, T)$ (here 2β is considered as an element of $\mathbb{Z}_{8p}$ in the natural way). We will show that Γ_1 and Γ_2 are isomorphic but not by an element of $\mathbb{Z}_{8p}^*$.

First observe that as $1 \in S$ if $mS = T$ for any $m \in \mathbb{Z}_{8p}^*$, then $m = 1$, $4p+1$, $8p-1$ or $4p-1$. It is easy to check that for such m, $mS = S$, in which case the map $x \mapsto mx$ is contained in $\mathrm{Aut}(\Gamma_1)$ by Lemma 2. It thus suffices to show that $\Gamma_1 \cong \Gamma_2$.

Define $\phi : \mathbb{Z}_{8p} \mapsto \mathbb{Z}_{8p}$ by $\phi(2k) = 2(\beta k)$ and $\phi(2k+1) = 2(\beta k) + 1$, where $0 \leq k \leq 4p-1$. Let $\alpha = \rho^{-1}\phi^{-1}\rho\phi$. Observe that $\alpha(2k) = 2k$ while $\alpha(2k+1) = 2k+1+2(\beta^{-1}-1)$. Note that $\beta^{-1} - 1 \equiv 0 \pmod{p}$, while $\beta^{-1} - 1 \equiv 2 \pmod{4}$. We conclude that $a = 2(\beta^{-1} - 1) \equiv 4p \pmod{8p}$. Noting α is self-inverse, we see that $\alpha^{-1}\rho\alpha = \rho^{1+a}$. As $\alpha(0) = 0$, we have by Corollary [6, Corollary 4.2B] that $\alpha \in \mathrm{Aut}(\mathbb{Z}_{8p})$. It is easy to see that $\alpha(S) = S$, and so by Lemma 2, $\alpha \in \mathrm{Aut}(\Gamma_1)$. Thus $\phi^{-1}\rho\phi = \rho\alpha \in \mathrm{Aut}(\Gamma_1)$, and $\rho = \phi\rho\alpha\phi^{-1}$. Then $\phi^{-1}\rho\alpha\phi = \rho \in \phi(\Gamma_1)$, and $\phi(\Gamma_1)$ is a circulant graph of order $8p$. Then the neighbors of 0 in $\phi(\Gamma_1)$ are $\phi(S) = T$, and so $\phi(\Gamma_1) = \Gamma_2$. ∎

Theorem 3

The group $\mathbb{Z}_{9n}$ is not a CI-group with respect to graphs for any $n \geq 3$.

Proof: For $i = 0, 1, 2$, let

$$S_i = \{\pm 1, \pm(3n+1), \pm(6n+1), \pm 3(in+1)\}.$$

We first show that if 3 does not divide $in+1$, then $\mathrm{Cay}(9n, S_0) \cong \mathrm{Cay}(9n, S_i)$. For $x \in \mathbb{Z}_{9n}$, let $0 \leq x' \leq 2$ be such that $x' \equiv x \pmod{3}$, and define $\phi : \mathbb{Z}_{9n} \mapsto \mathbb{Z}_{9n}$ by $\phi(x) = x + in(x - x')$. Clearly ϕ is well-defined. Suppose that $\phi(x) \equiv \phi(y) \pmod{9n}$. Observing that $x+in(x-x') \equiv x \pmod{3}$, we see that $\phi(x) \equiv \phi(y) \pmod{3}$. Then $x' = y'$ and so $x + inx \equiv y + iny \pmod{9n}$ or equivalently $x(1+in) \equiv y(1+in) \pmod{9n}$.

As 3 does not divide $in+1$, neither 9 nor n divide $in+1$ and $in+1$ is a unit in $\mathbb{Z}_{9n}$. We conclude that $x \equiv y \pmod{9n}$ and so ϕ is one-to-one and consequently a bijection.

Now consider an edge from x to $x+3n+1$. Notice that $(x+3n+1)' = x'+1$. It is then straightforward to verify that $\phi(x+3n+1) - \phi(x) = 3n(in+1)+1$. If $in+1 \equiv 1 \pmod 3$, then $3n(in+1)+1 \equiv 3n+1 \pmod{9n}$ while if $in+1 \equiv 2 \pmod 3$, then $3n(in+1) \equiv 6n+1 \pmod{9n}$. Similar type computations for the other types of edges of $\mathrm{Cay}(\mathbb{Z}_{9n}, S)$ will show that ϕ is indeed an isomorphism from $\mathrm{Cay}(\mathbb{Z}_{9n}, S)$ to $\mathrm{Cay}(\mathbb{Z}_{9n}, S_i)$.

Finally, we show that $kS_0 \neq S_1$ or S_2. Suppose that $kS_0 = S_i$, where $i = 1$ or 2. As $S_0 \neq S_i$, $\pm 3(in+1)$ is not a unit, and $k \in kS_0$, we see that $k = \pm(3n+1)$ or $\pm(6n+1)$. As the map $x \mapsto -x$ is in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{9n}, S))$, to simplify computations we assume that $k = 3n+1$ or $6n+1$. As the only nonunits in S_i are $\pm 3(in+1)$, $i = 0, 1, 2$, it must be the case that $k(\pm 3) \equiv k(\pm 3(in+1)) \pmod{9n}$. However, $k(\pm 3) \equiv \pm 3 \pmod{9n}$ and $k(\pm 3(in+1)) \equiv \pm 3(in+1) \pmod{9n}$, and so $\pm 3 \equiv 3(in+1) \pmod{9n}$. As $i = 1$ or 2, we have $\pm 3 \equiv 3n+3$ or $6n+3 \pmod{9n}$. The four equations yield that $3n \equiv 0 \pmod{9n}$, $-6 \equiv 3n \pmod{9n}$, $6n \equiv 0 \pmod{9n}$, and $-6 \equiv 6n \pmod{9n}$. The first and third of these equations are not true. The second equation is only true if $n = 1$, while the fourth equation is only true if $n = 2$, a contradiction. This if $im+1 \not\equiv 0 \pmod 3$, then we have isomorphic circulant graphs that are not multiplier equivalent. As only one of $1, n+1$, and $2n+1$ are divisible by 3, some $in+1$, $i = 1, 2$, is not divisible by 3, an $\mathbb{Z}_{9n}$ is not a CI-group with respect to graphs. ∎

Although we saw that the Ádám conjecture is false, Ádám was not totally wrong. In the next section we will see there are integers were Ádáms conjecture is true.

3.2 Examples

In this subsection, we summarize the positive results on Adám's conjecture. The first positive result was obatined by Elspas and Turner in 1967 when they showed the conjecture is true when n is a prime number. As the proof in this case is quite easy, we will state it as a theorem and prove it.

Theorem 4

Let p be a prime. Then $\mathbb{Z}_p$ is a CI-group with respect to digraphs and graphs.

Proof: Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_p, S)$ be a Cayley digraph of $\mathbb{Z}_p$, and $\phi \in \mathcal{S}_p$ such that $\phi^{-1}(\mathbb{Z}_p)_L\phi \leq \mathrm{Aut}(\Gamma)$. Notice that $(\mathbb{Z}_p)_L$ has order p, and that $\mathcal{S}_p$ has order $p!$. Also observe that the highest power of p that divides $p!$ is p. We conclude that $(\mathbb{Z}_p)_L$ and $\phi^{-1}(\mathbb{Z}_p)_L\phi$ are Sylow p-subgroups of $\mathcal{S}_p$, and so are Sylow p-subgroups of $\mathrm{Aut}(\Gamma)$. Consequently, by a Sylow Theorem $(\mathbb{Z}_p)_L$ and $\phi^{-1}(\mathbb{Z}_p)_L\phi$ are conjugate in $\mathrm{Aut}(\Gamma)$. The result then follows by Lemma 3 (this is stated in more generality later). ■

Alpach and Parsons in 1979 [2] showed that $\mathbb{Z}_n$ is a CI-group with respect to digraphs for $n = pq$ where p and q are two different primes numbers. Godsil [13] showed that it is true for $n = 4p$, and Muzychuk [17, 18] showed that $\mathbb{Z}_n$ is a CI-group with respect to graphs if and only if $n = 9, m, 2m$, or $4m$ and is a CI-group with respect to digraphs if and only if $n = m, 2m$, or $4m$, where m is odd and square-free.

Muzychuk [19] gave a polynomial time algorithm to solve the isomorphism problem for circulant digraphs. The algorithm reduces the problem to the prime power case, see Theorem 9.2 at the end of this thesis.

As we said before Alpach and Parsons gave conditions for the case $n = p^2$. In this thesis we will generalize their result. The basic idea is to show that if G is not a CI-digraph of $\mathbb{Z}_n$ then the graph must be a wreath product of very specific digraphs. Before going to the mains results we will need some extra tools and results.

CHAPTER 4

COLOR DIGRAPHS AND WREATH PRODUCTS

Our main results actually hold for a more general object than a digraph, namely a color digraph. In this chapter we define these objects as well as define and give examples of wreath products.

Definition 8

A color digraph Γ *is a set of digraphs* $\{\Gamma_i : 1 \leq i \leq r\}$ *such that* $\cup_{i=1}^{r} A(\Gamma_i) = A(K_n)$, *where each* Γ_i *is of order* n.

Notice that a digraph whose arcs have been colored in some fashion (but perhaps there are some arcs not in the digraph) can always be regarded as a color digraph as any edges which are missing can always be colored with a color not already used. Additionally, it is useful to think of the arcs of Γ_i as being labelled with the color i. In this case, we will refer to Γ_i the subdigraph of Γ colored with the color i.

We will usually work with **color** Cayley digraphs. These are Cayley digraphs in which the arcs have been partitioned into, say r, (color) classes, and each color class is a Cayley digraph of G. Formally,

Definition 9

A **color digraph** *is an unordered set* $\{\Gamma_1, \ldots, \Gamma_r\}$ *where the* Γ_i *are pairwise arc-disjoint digraphs such that* $\cup_{i=1}^{r} A(\Gamma_i) = A(K_n)$. *The automorphism group of a color digraph* Γ

is defined to be the intersection of the automorphism groups of each Γ_i*, so* $\cap_{i=1}^{r}\mathrm{Aut}(\Gamma_i)$*. Two color digraphs* $\Gamma = \{\Gamma_1, \ldots, \Gamma_r\}$ *and* $\Gamma' = \{\Gamma_1, \ldots, \Gamma_s\}$ *are isomorphic if* $r = s$ *and there exists a bijection* $\phi : V(\Gamma) \mapsto V(\Gamma')$ *such that*

$$\begin{aligned}\phi(\{\Gamma_i : 1 \leq i \leq r\}) &= \{\phi(\Gamma_i) : 1 \leq i \leq r\} \\ &= \{\Gamma'_i : 1 \leq i \leq r\}.\end{aligned}$$

If each $\Gamma_i = \mathrm{Cay}(G, S_i)$ *for* $S_i \subset G$*, then* Γ *is a Cayley color digraph, which we denote by* $\mathrm{Cay}(G, S_1, \ldots, S_r)$*. Usually, we will simply denote the set* $\{S_1, \ldots, S_r\}$ *of connection sets of a Cayley color digraph of* G *by* S *.*

Wielandt introduced the notion of a 2-closed group in [22], as well as the 2-closure of a permutation group G, denoted $G^{(2)}$. A **2-closed group** is simply the automorphism group of a color digraph, while the **2-closure of** G is the smallest 2-closed group (in the same symmetric group) that contains G.

The most common way of obtaining a color digraph is via the **orbital digraph** construction. Let $G \leq \mathcal{S}_X$, be a transitive group and let G act on $X \times X$ by $g(x, y) = (g(x), g(y))$. Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the orbits of G under this action, and define digraphs $\Gamma_1, \ldots, \Gamma_r$ by $V(\Gamma_i) = X$ and $A(\Gamma_i) = \mathcal{O}_i$. Then $\{\Gamma_i : 1 \leq i \leq r\}$ is a color digraph, and each Γ_i is an orbital digraph of G.

We shall have need of the wreath product of both digraphs and groups.

Definition 10

Let Γ_1 *and* Γ_2 *be digraphs. The* **wreath product of** Γ_1 **and** Γ_2*, denoted* $\Gamma_1 \wr \Gamma_2$*, is the digraph with vertex set* $V(\Gamma_1) \times V(\Gamma_2)$ *and edges* $(u,v)(u,v')$ *for* $u \in V(\Gamma_1)$ *and* $vv' \in E(\Gamma_2)$ *or* $(u,v)(u',v')$ *where* $uu' \in E(\Gamma_1)$ *and* $v, v' \in V(\Gamma_2)$.

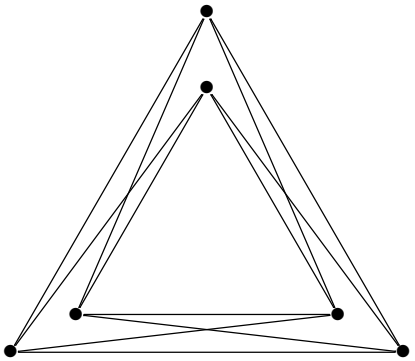

Figure 4.1

The graph $K_3 \wr \bar{K}_2$.

We will also need the wreath product of color digraphs. For such a wreath product to make sense, the two color digraphs Γ_1 and Γ_2 must have the same colors, so we always adopt the convention that if a color is present in Γ_1 but not Γ_2, one color digraph but not in the other, then a digraph with no arcs is added to Γ_2 to represent the missing color. Similarly, if Γ_2 has a color not represented in Γ_1.

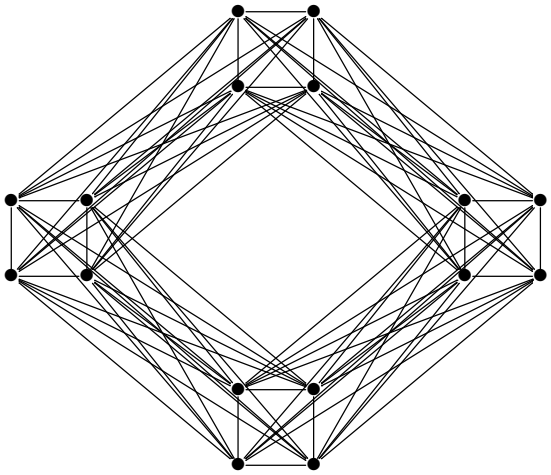

Figure 4.2

The graph $C_4 \wr C_4$.

Definition 11

Let Γ_1 and Γ_2 be color digraphs with the same colors. The **wreath product of Γ_1 and Γ_2,** *denoted $\Gamma_1 \wr \Gamma_2$, IS the color digraph consisting of $\Gamma_{1,i} \wr \Gamma_{2,i}$, where $\Gamma_{j,i}$ is the subdigraph of Γ_j colored with color i, $j = 1, 2$.*

Notice that in this definition, the color digraphs Γ_1 and Γ_2 are necessarily are ordered color digraphs in order for us to know which digraph to wreath with which digraph. That the wreath product cannot be defined for unordered color digraphs will present some additional obstacles in our work. Finally, we mention that the isomorphism problem for unordered circulant digraphs is not the same as the isomorphism problem for ordered circulant digraphs. For example, there are self-complementary circulant graphs Γ and $\bar{\Gamma}$ (where $\bar{\Gamma}$ is the complement of Γ) where the graph and its complement are not isomorphic by a group automorphism of $\mathbb{Z}_n$ [14] or [15]. The unordered color graph $\{\Gamma, \bar{\Gamma}\}$ is obviously

isomorphic to itself by a group automorphism of $\mathbb{Z}_n$, but the two ordered color graphs $(\Gamma, \bar{\Gamma})$ and $(\bar{\Gamma}, \Gamma)$ are not.

Definition 12

Let G be a permutation group acting on the set X and H a permutation group acting on the set Y. Define the **wreath product of G and H**, *denoted $G \wr H$, to be the set of all permutations of $X \times Y$ of the form $(x, y) \mapsto (g(x), h_x(y))$.*

It is easy to see that $\mathrm{Aut}(\Gamma_1) \wr \mathrm{Aut}(\Gamma_2) \leq \mathrm{Aut}(\Gamma_1 \wr \Gamma_2)$. The automorphism groups of the wreath product of two vertex-transitive color digraphs are given in [10, Theorem 5.7]. Based on their automorphism groups, circulant color digraphs can be placed into three classes of digraphs, normal circulant digraphs, deleted wreath types, and generalized wreath products - see [24] for the definition of a normal circulant, and [4] for the definition of a deleted wreath types. Generalized wreath products get their name not from any sort of "product", but because they generalize the notion of the wreath product in Cayley digraphs.

Definition 13

*Let $\Gamma = \mathrm{Cay}(W, S)$ be a color digraph for some abelian group W and $S \subset W$. We say that Γ is a (K, L)-*__generalized wreath product__ *or, more simply a* **generalized wreath product**, *if there exists $1 < L \leq K \leq W$ such that S_i K is a union of cosets of L for each $1 \leq i \leq r$.*

It is not difficult to see that a circulant color digraph is a nontrivial wreath product of two circulants color digraphs of smaller order if and only if it is a (K, K)-generalized wreath product for some $1 < K < A$. In the next section, we will show that every circulant color digraph that is not a CI-digraph is isomorphic to a generalized wreath product. We

then will show a generalized wreath product circulant color digraph is CI-color digraph only if it is a wreath product of circulant color digraphs of smaller order and of a particular and restricted form.

The following result that characterizes CI-color digraphs is due to Babai [3], although a version for cyclic groups was also independently derived by Alspach and Parsons [2].

Lemma 3

Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayley color digraph of G. Then the following are equivalent:

1. *Γ is a CI-color digraph of G,*
2. *whenever $\phi \in \mathcal{S}_G$ such that $\phi^{-1}G_L\phi \leq \mathrm{Aut}(\Gamma)$, then G_L and $\phi^{-1}G_L\phi$ are conjugate in $\mathrm{Aut}(\Gamma)$.*

We finish this section with some terms from permutation group theory that we will need.

Definition 14

Let $G \leq \mathcal{S}_n$ be transitive on $\mathbb{Z}_n$. A subset $B \subseteq \mathbb{Z}_n$ is a **block** *of G if $g(B) = B$ or $g(B) \cap B = \emptyset$ for every $g \in G$. If B is a block, then $g(B)$ is also a block of G, called a* **conjugate block**. *The set of all conjugate blocks of B is classed a G-***invariant partition**, *usually denoted $\mathcal{B}$. Thus $\mathcal{B} = \{g(B) : g \in G\}$. If the group is clear, we will also say that $\mathcal{B}$ is an invariant partition or and invariant partition of G. Any element $g \in G$ also permutes the blocks in $\mathcal{B}$, and so each $g \in G$ induces a permutation $g/\mathcal{B}$ on $\mathcal{B}$ by $g/\mathcal{B}(B) = B'$ if and only if $g(B) = B'$. We let $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\{$, and $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for all } g \in G\}$. Note that there is an induced homomorphism $\phi : G \mapsto S_{\mathcal{B}}$ given by $\phi(g) = g/\mathcal{B}$ and $\mathrm{Ker}(\phi) = \mathrm{fix}_G(\mathcal{B})$. Finally, if $G \leq \mathrm{Aut}(\Gamma)$ for some digraph Γ, we define*

$\Gamma/\mathcal{B}$ *by* $V(\Gamma) = \mathcal{B}$ *and* $(B, B') \in A(\Gamma/\mathcal{B})$ *if and only if* $(b, b') \in A(\Gamma)$ *for some* $b \in B$ *and* $b' \in B'$.

CHAPTER 5

A NON-CI-CIRCULANT IS A GENERALIZED WREATH PRODUCT

We fix some notation that will be used throughout the following chapters. Let p be a prime and define $\beta, \rho : \mathbb{Z}_{p^k} \to \mathbb{Z}_{p^k}$ by $\beta(i) = (1+p)i$ and $\rho(i) = i+1$. It is straightforward to verify that β is an automorphism of $(\mathbb{Z}_{p^k})_L$ of order p^{k-1} if p is odd while $i \to 3i$ has order p^{k-2} if $p = 2$, and that $(\mathbb{Z}_{p^k})_L = \langle\rho\rangle$. If $p = 2$, then define $\iota : \mathbb{Z}_{2^k} \mapsto \mathbb{Z}_{2^k}$ be given by $\iota(i) = -i$.

Lemma 4

Let p be prime, $k \geq 1$, and $P \leq N(p^k) = N_{S_{p^k}}((\mathbb{Z}_{p^k})_L)$ be a p-group that contains $(\mathbb{Z}_{p^k})_L$. Then every circulant color digraph whose automorphism group contains P is a generalized wreath product or

- *if p is odd then $P = (\mathbb{Z}_{p^k})_L$, or*
- *if $p = 2$, then $P = (\mathbb{Z}_{2^k})_L$ or $P = \langle(\mathbb{Z}_{2^k})_L, \iota\beta^{2^{k-3}}\rangle$ or $\langle(\mathbb{Z}_{2^k})_L, \iota\rangle$ is of order 2^{k+1} and has a unique regular cyclic subgroup.*

Proof: If $k = 1$, then the result is trivial as $(\mathbb{Z}_p)_L$ is a Sylow p-subgroup of $\mathcal{S}_p$, so we assume that $k \geq 2$.

As a Sylow p-subgroup of $N(p^k)/\langle\rho\rangle$ is isomorphic to $\mathbb{Z}_{p^{k-1}}$ if p is odd or $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$ if $p = 2$, we see that a Sylow p-subgroup Q of $N(p^k)$ is $\langle\beta, \rho\rangle$ if p is odd and is $\langle\rho, \beta, \iota\rangle$ if $p = 2$.

We now show that if $\beta^\ell \neq 1$ is contained in P, then every circulant color digraph whose automorphism group contains P is a generalized wreath product. Indeed, if such an ℓ exists, then by raising β^ℓ to an appropriate power we may choose $\ell = 2^{k-3}$ if $p = 2$ while if $p \neq 2$, we may choose $\ell = p^{k-2}$. Then $\beta^\ell(a + bp) = a + bp + ap^{k-1}$ and so β^ℓ fixes every element of $H = \langle p \rangle$ and the cycle of β^ℓ that contains $a + bp$, $a \neq 0$ is $(a + bp \;\; a + b + ap^{k-1} \;\; \ldots \;\; a + bp + a(p-1)p^{k-1})$. Thus if $\Gamma = \mathrm{Cay}(\mathbb{Z}_n, S)$ is an orbital digraph of P and 0 is adjacent to any element of the cycle of β^ℓ that contains $a+bp$, then 0 is adjacent in Γ to every element of the cycle that contains $a + bp$. Hence the coset $a + bp + \langle p^{k-1} \rangle \subseteq S$. Setting $K = \langle p^{k-1} \rangle$ we see that $S - H$ is a union of cosets of K and Γ is an (H, K)-generalized wreath product. We may henceforth assume that $p = 2$.

If $k = 2$, Then $\mathbb{Z}_2 \wr \mathbb{Z}_2$ of order 8 is a Sylow 2-subgroup of $\mathcal{S}_4$, $\beta = 1$, and $P = \langle \rho, \iota \rangle$. It is not difficult to verify that $\mathbb{Z}_2 \wr \mathbb{Z}_2$ contains a unique regular cyclic subgroup of order 4. We henceforth assume $k \geq 3$.

Assume that $P \neq \langle \rho \rangle$. Then $N_P(\langle \rho \rangle) \neq \langle \rho \rangle$ by a Sylow Theorem. We may assume that there is no $\beta^\ell \neq 1$ in P as otherwise the result follows by arguments above. Then there exists $u \in \mathbb{Z}$ such that $\iota\beta^u \in P$.

Suppose first that $u \equiv 0 \pmod{2^{k-2}}$, in which case $\iota\beta^u = \iota$. If $|P| > 2^{k+1}$ then there exists $\iota\beta^v \in P$ for some v with $v \not\equiv 0 \pmod{2^{k-2}}$, but then $\beta^v \in P$, a contradiction. Thus if $u \equiv 0 \pmod{2^{k-2}}$, then $|P| = 2^{k+1}$. We claim that $\langle \rho \rangle$ is the unique regular cyclic subgroup of P in this case. Indeed, if $\langle \delta \rangle$ is another regular cyclic subgroup of P, then $\delta = \iota\rho^i$ for some i, but straightforward computations show that $(\iota\rho^i)^2 = 1$, a contradiction. Thus if $u \equiv 0 \pmod{2^{k-2}}$ then the result follows.

Suppose $u \not\equiv 0 \pmod{2^{k-2}}$ or equivalently that $\iota\beta^u \neq \iota$. As $\mathbb{Z}_{2^k}^*$ is abelian, $(\iota\beta^u)^2 = \iota^2\beta^{2u} = \beta^{2u} \in \langle\beta\rangle$. The result then follows by arguments above unless $3^{2u} = 1$, and $|\iota\beta^u| = 2$. This then implies that $|\langle\rho, \iota\beta^u\rangle| = 2^{k+1}$, and that $u \equiv 0 \pmod{2^{k-3}}$ as 3 has multiplicative order 2^{k-2} in $\mathbb{Z}_{2^k}$. If $k = 3$, then we have that $|P| = 2^{k+1}$ as there is now only one choice for $\iota\beta^u$, namely $\iota\beta$. If $k \geq 4$, then $u \equiv 0 \pmod{2^{k-3}}$ and so $u = x2^{k-3}$ for some odd integer x. We may and do assume without loss of generality that $x = 1$.

Now assume that $|P| > 2^{k+1}$ (and so $k \geq 4$). Then there exists $v \in \mathbb{Z}$ such that $\beta^u \neq \beta^v$ and $\iota\beta^v \in P$. Applying arguments analogous to those above to $\iota\beta^v$, we see that $v = y2^{k-3}$ for some odd integer y. But then $\iota\beta^u\iota\beta^v(i) = (1+p)^{(x+y)2^{k-3}}$ and as both x and y are odd, $x + y$ is even. Hence $\iota\beta^u\iota\beta^v = 1$, and $\iota\beta^v = (\iota\beta^u)^{-1} = \iota\beta^u$, a contradiction. Hence if $k \geq 4$ we also have $|P| = 2^{k+1}$, and so if $k \geq 3$ we have $|P| = 2^{k+1}$.

Now let $\delta \in P$ such that $\langle\delta\rangle$ is a regular cyclic subgroup, and assume that $\langle\delta\rangle \neq \langle\rho\rangle$. As $P = \langle\rho, \iota\beta^{2^{k-3}}\rangle$, $\delta = \rho^a\iota\beta^{2^{k-3}}$. Then $\delta^2(i) = i - 3^{2^{k-3}}a + a$. If $k = 3$, then $\delta^2(i) = i + 6a$ which has order 4 if and only if $\gcd(2, a) = 1$. Also, $\delta(i) = 5i + a$, and it is easy to see that the map $i \mapsto 5i$ maps cosets of the unique subgroup K of $\mathbb{Z}_8$ of order 2 to themselves and also maps cosets of the unique subgroup H of $\mathbb{Z}_8$ of order 4 to themselves. This then implies that any generalized orbital digraph of P is an (H, K)-generalized wreath digraph and the result follows. To finish, we will show that if $k \geq 4$, then no such δ exists.

To show δ doesn't exist, we first show that the congruence $3^{2^k} \equiv 1 \pmod{2^{k+2}}$ holds for $k \geq 1$. This is easy to verify if $k = 1$, so inductively assume it is true for $k \geq 1$. Then $3^{2^k} = \ell 2^{k+2} + 1$ for some positive integer ℓ, and $3^{2^{k+1}} = 3^{2^k} \cdot 3^{2^k} = \ell^2 2^{2k+1} + 2\ell 2^{k+3} + 1$ so indeed $3^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$ and the congruence is established by induction. Rewrite

$3^{2^k} \equiv 1 \pmod{2^{k+2}}$ as $3^{2^{k-2}} \equiv 1 \pmod{2^k}$, $k \geq 3$, and observing that $3^{3^{k-2}} = 3^{2^{k-3}} \cdot 3^{2^{k-3}}$, we conclude that $3^{3^{k-3}}$ has multiplicative order 2 in $\mathbb{Z}_{2^k}$. As $\mathbb{Z}_{2^k}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$, there are four elements of $\mathbb{Z}_{2^k}$ whose multiplicative order is divisible by 2, namely, ± 1 and $2^{k-1} \pm 1$. If $k \geq 4$, then we know that $3^{2^{k-3}} \equiv 1 \pmod{2^{k-1}}$ and so $3^{2^{k-3}} \equiv 1$ or $2^{k-1}+1 \pmod{2^k}$. Finally,

$$\begin{aligned} \delta^2(i) &= i - 3^{2^{k-3}}a + a = i - a(3^{2^{k-3}} - 1) \\ &\equiv i \text{ or } i - 2^{k-1} \pmod{2^k}. \end{aligned}$$

This implies that $|\delta| = 1$ or 2, and so $|\delta| = 2$ or 4. This however contradicts $k \geq 4$, establishing the result. ∎

For the next several lemmas we will fix some more notation. Let $\mathcal{B}$ be the invariant partition of $\langle \rho \rangle$ formed by the orbits of $\langle \rho^{p^{k-1}} \rangle$, so that the blocks of $\mathcal{B}$ are of size p. Let $\mathcal{C}$ be the invariant partition of $\langle \rho \rangle$ consisting of $p^{k-\ell}$ blocks of size p^ℓ, where $\ell \geq 2$. Let $G = G_{\mathcal{C}} = \langle \rho, \rho^{p^{k-1}}|_C : C \in \mathcal{C} \rangle$. Then $\mathcal{B}$ and $\mathcal{C}$ are invariant partitions of G, and $G/\mathcal{B} = \langle \rho \rangle / \mathcal{B}$.

Lemma 5

The group G contains at least two different regular cyclic subgroups $R_1 \neq R_2$. Additionally, G is generated by the set of all regular cyclic subgroups.

Proof: For this proof it will be convenient to view ρ as a permutation in $\mathcal{S}_{p^{k-1}} \times \mathcal{S}_p$ given by $\rho(i,j) = (i+1, j+b_i)$, where each $b_i \in \mathbb{Z}_p$. As ρ has order p^k and $\rho^{p^{k-1}} = (i, j + \sum_{m=0}^{p^{k-1}-1} b_i)$, we see that $c = \sum_{m=0}^{p^{k-1}-1} b_i \not\equiv 0 \pmod{p}$. Let $C_n \in \mathcal{C}$ with $(n,0) \in C_i$.

Consider $\rho_n = \rho(\rho^{p^{k-1}}|_{C_n})$, and let $\rho_n(i,j) = (i+1, j+d_i)$, where $d_i \in \mathbb{Z}_p$. For $i \in \mathbb{Z}_{p^{k-1}}$, let $B_i = \{(i,j) : j \in \mathbb{Z}_p\}$, so that $\mathcal{B} = \{B_i : i \in \mathbb{Z}_{p^{k-1}}\}$. Then $d_i = b_i$ if $B_i \not\subset C_n$ and $d_i = b_i + 1$ if $B_i \subset C_n$. Then $(\rho_n)^{p^{k-1}}(i,j) = (i, j + \sum_{m=0}^{p^{k-1}-1} d_i)$, and

$$\sum_{m=0}^{p^{k-1}-1} d_i = p^{\ell-1} + \sum_{m=0}^{p^{k-1}-1} b_i \equiv \sum_{m=0}^{p^{k-1}-1} b_i \not\equiv 0 \pmod{p}.$$

We conclude that $\langle \rho_n \rangle$ has order p^k, and as $\rho_n \notin \langle \rho \rangle$, the first part of the result follows with $R_1 = \langle \rho \rangle$ and $R_2 = \langle \rho_n \rangle$ for some n. The second part follows as $\langle \rho^{-1}\rho_n : n \in \mathbb{Z}_{p^{k-1}} \rangle = \mathrm{fix}_G(\mathcal{B})$. ∎

For the remainder of this section it will be most convenient to view the set $\mathbb{Z}_{p^k}$ as the set $\mathbb{Z}_{p^{k-\ell}} \times \mathbb{Z}_{p^\ell}$ with $\rho(i,j) = (i+1, j+b_i)$, where $b_{p^{k-\ell}-1} = 1$ and $b_i = 0$ if $i \neq p^{k-\ell} - 1$. Also, $\mathcal{C} = \{\{(i,j) : j \in \mathbb{Z}_{p^\ell}\} : i \in \mathbb{Z}_{p^{k-\ell}}\}$. Let $\alpha = (1+p)^{p^{\ell-2}} \in \mathbb{Z}_{p^\ell}^*$, and define $\gamma : \mathbb{Z}_{p^{k-\ell}} \times \mathbb{Z}_{p^\ell} \mapsto \mathbb{Z}_{p^{k-\ell}} \times \mathbb{Z}_{p^\ell}$ be given by $\gamma(i,j) = (i, \alpha j)$.

Lemma 6

If R_1 and R_2 are regular cyclic subgroups of G and $\delta \in \mathcal{S}_{p^k}$ with $\delta^{-1}R_2\delta = R_1$, then $\delta = n\gamma^a g$ normalizes G, where $g \in \mathrm{fix}_G(\mathcal{B})$, $n \in N(p^k)$, and $a \in \mathbb{Z}_p$. Also, $N_{\mathcal{S}_{p^k}}(G) = \langle G, N(p^k), \gamma \rangle$, $\mathrm{fix}_{N_{\mathcal{S}_{p^k}}}(\mathcal{B}) = \langle \mathrm{fix}_G(\mathcal{B}), \gamma \rangle \triangleleft N_{\mathcal{S}_{p^k}}(G)$ and $|N_{\mathcal{S}_{p^k}}(G)| = (p-1)p^{2k-1+p^{k-\ell}}$.

Proof: First, every element of $N(p^k)$ normalizes G. This follows as every subgroup of $\mathbb{Z}_{p^k}$ is characteristic. In particular, if $\omega \in N(p^k)$ then $\omega(\mathcal{B}) = \mathcal{B}$ and $\omega(\mathcal{C}) = \mathcal{C}$. Then $\omega^{-1}\langle \rho^{p^{k-1}} \rangle \omega = \langle \rho^{p^{k-1}} \rangle$, and for any $C \in \mathcal{C}$, $\omega(C) \in \mathcal{C}$. So $\omega^{-1}(\rho^{p^{k-1}}|_C)\omega = \rho^{rp^{k-1}}|_{C'}$ for some $r \in \mathbb{Z}_p$ and $C' \in \mathcal{C}$ and indeed $N(p^k)$ normalizes G.

As G is a p-group, G has nontrivial center, which of course commutes with every element of $\langle \rho \rangle$. As $\langle \rho \rangle$ is a regular abelian subgroup, it is self-centralizing, and hence

$Z(G) \leq \langle\rho\rangle$. We conclude that $\langle\tau^{p^{k-1}}\rangle \leq Z(G)$. Similarly, $\langle\tau^{p^{k-1}}\rangle$ is contained in every regular cyclic subgroup of G.

Let $R_1, R_2 \leq G$ be regular cyclic subgroups with $\delta^{-1}R_2\delta = R_1$. By the immediately preceding paragraph, $\langle\tau^{p^{k-1}}\rangle \leq R_1 \cap R_2$ is characteristic in both R_1 and R_2 as it is the unique subgroup of R_1 and R_2 of order p. We conclude that $\delta(\mathcal{B}) = \mathcal{B}$ as $\mathcal{B}$ is formed by the orbits of $\langle\tau^{p^{k-1}}\rangle$. As $R_1/\mathcal{B} = R_2$, we see that $\delta/\mathcal{B} \in N_{\mathcal{S}_{p^{k-1}}}(\langle\rho/\mathcal{B}\rangle)$. As every element of $\mathrm{Aut}(\mathbb{Z}_{p^{k-1}})$ extends to an automorphism of $\mathbb{Z}_{p^k}$, by [6, Corollary 4.2B] every element of $N_{\mathcal{S}_{p^{k-1}}}(\langle\rho\rangle/\mathcal{B})$ extends to an element of $N_{\mathcal{S}_{p^k}}(\langle\rho\rangle)$. Hence there exists $n \in N_{\mathcal{S}_{p^{k-1}}}(\langle\rho\rangle)$ such that $n/\mathcal{B} = \delta/\mathcal{B}$.

Now, as $\langle\tau^{p^{k-1}}\rangle|_B \cong (\mathbb{Z}_p)_L$ is normal in $\mathrm{fix}_G(\mathcal{B})|_B$ for every $B \in \mathcal{B}$, we conclude that $(n^{-1}\delta)|_B \in \mathrm{AGL}(1,p)$ for every $B \in \mathcal{B}$. Additionally, as $\mathrm{fix}_G(\mathcal{C})|_C \cong \mathbb{Z}_{p^{k-\ell}}$ for every $C \in \mathcal{C}$, $(n^{-1}\delta)|_C$ is contained in $N(p^{k-\ell})$ for every $C \in \mathcal{C}$. As $k - \ell \geq 2$, there is no element of order relatively prime to p that fixes each block of $\mathcal{B}$ set-wise by [9, Lemma 29]. This then implies that $n^{-1}\delta(i,j) = (i, \alpha^{a_i}j + c_i)$ where $a_i \in \mathbb{Z}_p$ and $c_i \in \mathbb{Z}_{p^\ell}$ has additive order p. Note that $\delta^{-1}n(i,j) = (i, \alpha^{-a_i}j - \alpha^{-a_i}c_i)$.

Now, let $\omega = \rho^{-1}n\delta^{-1}\rho n^{-1}\delta$, so that

$$\omega(i,j) = (i, \alpha^{-a_{i+1}+a_i}j + \alpha^{-a_{i+1}}(c_i - c_{i+1}) + b_i(\alpha^{-a_{i+1}} - 1).$$

As $\alpha = (1+p)^{p^{\ell-2}}$, we see that $\alpha^{-a_{i+1}} - 1 \equiv 0 \pmod{p^{\ell-1}}$, and so addition of $b_i(\alpha^{-a_{i+1}} - 1)$ fixes each block of $\mathcal{B}$, as does addition of $\alpha^{-a_{i+1}}(c_i - c_{i+1})$. We conclude that $\omega \in \mathrm{fix}_G(\mathcal{B})$, and as $\mathrm{fix}_G(\mathcal{B})|_C$ is semiregular, it must be that $a_i = a_{i+1}$ for all $i \in \mathbb{Z}_{p^{k-\ell}}$, and $n^{-1}\delta = \gamma^a g$ for some $g \in \mathrm{fix}_G(\mathcal{B})$ and $a = a_i$. Hence $\delta = n\gamma^a g$.

We have already seen that n normalizes G, as does $g \in G$. Similar to the computation for the displayed equation above, we see that $\rho^{-1}\gamma\rho\gamma^{-1}(i,j) = (i, j + b_i(\alpha - 1))$ and again $\alpha - 1 \equiv 0 \pmod{p^{\ell-1}}$. Then $\rho^{-1}\gamma^{-1}\rho\gamma \in \mathrm{fix}_G(\mathcal{B})$ and as γ centralizes $\mathrm{fix}_G(\mathcal{B})$, γ normalizes G as well. Hence $n\gamma^a g$ normalizes G.

To show that $N_{\mathcal{S}_{p^k}}(G) = \langle N(p^k), \gamma, G\rangle$, we observe that conjugation by $\phi \in N_{\mathcal{S}_{p^k}}(G)$ maps the regular cyclic subgroups of G to the regular cyclic subgroups of G. By the immediately preceding argument we see that $\phi = n\gamma^a g$ as above and $\phi \in \langle N(p^k), G, \gamma\rangle$. Finally, let $\delta \in \mathrm{fix}_{N_{\mathcal{S}_{p^k}}}(\mathcal{B})$. As was shown above, $\delta = n\gamma^a g$ for $n \in N(p^k)$, $g \in \mathrm{fix}_G(\mathcal{B})$, and $a \in \mathbb{Z}_p$. As $\delta/\mathcal{B} = 1$, we may choose $n = 1$, in which case $\delta = \gamma^a g$. Hence $\langle \mathrm{fix}_G(\mathcal{B}), \gamma\rangle = \mathrm{fix}_{N_{\mathcal{S}_{p^k}}}(\mathcal{B}) \lhd \langle G, N(p^k), \gamma\rangle$. Finally, as $\mathrm{fix}_G(\mathcal{B}) \lhd \mathrm{fix}_{N_{\mathcal{S}_{p^k}}}(\mathcal{B})$, we see that

$$\begin{aligned}
|N_{\mathcal{S}_{p^k}}(G)| &= |N_{\mathcal{S}_{p^k}}(G)/\mathcal{B}| \cdot |\mathrm{fix}_G(\mathcal{B})| \\
&= p^{k-1} \cdot (p-1)p^{k-1} \cdot |\mathrm{fix}_G(\mathcal{B})| \cdot |\langle\gamma\rangle| \\
&= (p-1)p^{2k-2} \cdot p^{p^{k-\ell}} \cdot p \\
&= (p-1)p^{2k-1+p^{k-\ell}}.
\end{aligned}$$

■

Lemma 7

G contains exactly $p^{p^{k-\ell}}$ regular cyclic subgroups.

Proof: As any regular cyclic subgroup R of G is conjugate in $\mathcal{S}_{p^k}$ to $\langle\rho\rangle$ as R and $\langle\rho\rangle$ are permutation equivalent, and by Lemma 6 any element $\delta \in \mathcal{S}_{p^k}$ with $\delta^{-1}\langle\rho\rangle\delta = R$ is contained in $N_{\mathcal{S}_{p^k}}(G)$, the number of regular cyclic subgroups of G is the number of

regular cyclic subgroups of G conjugate in $N_{\mathcal{S}_{p^k}}(G)$ to $\langle\rho\rangle$. This number is $[N_{\mathcal{S}_{p^k}}(G) : N_{N_{\mathcal{S}_{p^k}}(G)}(\langle\rho\rangle)]$. As $N_{N_{\mathcal{S}_{p^k}}}(\langle\rho\rangle) = N(p^k)$ has order $(p-1)p^{2k-1}$, by Lemma 6 we see the number of regular cyclic subgroups of G is

$$\frac{(p-1)p^{2k-1+p^{k-\ell}}}{(p-1)p^{2k-1}} = p^{p^{k-\ell}}.$$

■

Lemma 8

Let $\Gamma = \mathrm{Cay}(G, S)$ be a Cayey color digraph for some abelian group G, and $1 < H \leq L < G$ such that Γ is a (L, H)-generalized wreath product. Let $\mathcal{B} \preceq \mathcal{C}$ be the invariant partitions of G_L consisting of cosets of H and L, respectively. Let $K \leq \mathrm{Aut}(\Gamma)$ be maximal that admits both $\mathcal{B}$ and $\mathcal{C}$ as invariant partitions. If $\gamma \in K$ such that $\gamma|_C$ fixes each block of $\mathcal{B}$ contained in $\mathcal{C}$, then $\gamma|_C \in K$.

Proof: Let $e = (x, y)$ be an arc of $\Gamma_i = \mathrm{Cay}(G, S_i)$. As G_L is transitive and contained in $\mathrm{Aut}(\Gamma)$, it suffices to only consider the case where $x = 0$. Let $C \in \mathcal{C}$ with $0 \in C$, and $\gamma \in K$ such that $\gamma|_C$ fixes each block of $\mathcal{B}$ contained in C. If $x, y \in C$, then clearly $\gamma|_C(0, y) = \gamma(0, y)$ is an arc of Γ_i. If $x, y \notin C$ then $\gamma|_C(x, y) = (x, y)$ is an arc of Γ_i. If $x \in C$ and $y \notin C$, then as Γ_i is an (L, H)-generalized wreath product, every vertex of $x + H$ is outadjacent in Γ_i to every vertex of $y + H$ and $(y - x) + H \subseteq S$. Also, $\gamma(x + H) = x + H$ and $\gamma|_C(y + H) = y + H$. We conclude that $\gamma|_C(y) - \gamma|_C(0) \in y + H$. The case where $y \in C$ but $x \notin C$ is analogous and $\gamma \in \mathrm{Aut}(\Gamma_i)$. As Γ_i is arbitrary, the result follows. ■

Lemma 9

Let n be an odd positive integer and $G \leq S_n$ contain a regular cyclic subgroup and have an invariant partition $\mathcal{B}$ that is not trivial and is not refined by an nontrivial invariant partition. Then either $|B| = p$ for $B \in \mathcal{B}$ and some prime p or $\mathrm{Stab}_G(B)$ in its action on B is a doubly-transitive group with nonabelian almost simple socle.

Proof: Assume $|B|$ does not have prime order. As $\mathcal{B}$ is not trivial, n is composite. Next, $\mathrm{Stab}_G(B)|_B$ is primitive by [6, Exercise 1.5.10] for every $B \in \mathcal{B}$. As $\mathbb{Z}_n$ is a Burnside group [6, Theorem 3.5A] and $\mathrm{Stab}_G(B)|_B$ contains a regular cyclic subgroup, it is doubly-transitive and has socle a simple group or a regular elementary abelian p-group for some (odd) prime p by [6, Theorem 4.1B]. As a transitive subgroup of S_{p^2} contains a regular subgroup and an elementary abelian subgroup if and only if it has Sylow p-subgroup $\mathcal{S}_p \wr \mathcal{S}_p$ by [11, Lemma 4], it is easy to see that $\mathrm{AGL}(k, p)$ does not contain a regular cyclic subgroup if $k \geq 2$. Thus if $\mathrm{Stab}_G(B)|_B$ has elementary abelian socle then it is a subgroup of $\mathrm{AGL}(1, p)$ and $|B| = p$, and the result follows. ∎

Lemma 10

Let p be prime, $k \geq 2$, and $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ a color digraph that is a nontrivial generalized wreath product that is not isomorphic to a color digraph whose automorphism group has the form $G_1 \wr G_2$ for some 2-closed subgroups $G_1 \leq S_{p^{k-i}}$ and $G_2 \leq S_{p^i}$ is a symmetric group if $i \geq 2$. Then $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ is not a CI-color digraph.

Proof: Let P be a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$ that contains $(\mathbb{Z}_{p^k})_L$. As Γ is a nontrivial generalized wreath product, there exists $1 < L \leq K \leq (\mathbb{Z}_{p^k})_L$ such that $S_j - K$ is a union of cosets of L for every $S_j \in S$. We choose K to be minimal such that $S_j - K$ is a

union of cosets of L for every $S_j \in S$, and suppose that L is not of prime order. Let $\mathcal{C}$ be the invariant partition of $(\mathbb{Z}_{p^k})_L$ formed by the cosets of L. Then $G = G_{\mathcal{C}} \leq \mathrm{Aut}(\Gamma)$ but $G_{\mathcal{D}} \not\leq \mathrm{Aut}(\Gamma)$ for any $\mathcal{D} \prec \mathcal{C}$. We will show that there is a regular cyclic subgroup R in G that is not conjugate in $\mathrm{Aut}(\Gamma)$ to $\langle\rho\rangle$. This will imply our claim by Lemma 3.

By Lemma 6, if R is conjugate to $\langle\rho\rangle$ in $\mathrm{Aut}(\Gamma)$, then there exists $\delta \in N_{\mathcal{S}_{p^k}}(G)$ such that $\delta^{-1}\langle\rho\rangle\delta = R$. Hence the number of regular cyclic subgroups in G conjugate in $\mathrm{Aut}(\Gamma)$ to $\langle\rho\rangle$ is the number of regular cyclic subgroups in G conjugate in $N_{\mathrm{Aut}(\Gamma)}(G)$ to $\langle\rho\rangle$. By Lemma 6, $N_{\mathrm{Aut}(\Gamma)}(G) = \langle G, N(p^k), \gamma\rangle \cap \mathrm{Aut}(\Gamma) = H$ (where γ is defined as above).

Suppose $\gamma \in H$. Let M be the largest subgroup of $\mathrm{Aut}(\Gamma)$ that admits $\mathcal{B}$ (consisting of the cosets of the unique subgroup of $\mathbb{Z}_{p^k}$ of size p). Note that $P \leq M$ and as P is a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$, P is a Sylow p-subgroup of M. Define an equivalence relation $\equiv$ on $\mathcal{B}$ by $B \equiv B'$ if and only if whenever $\omega \in \mathrm{fix}_M(\mathcal{B})$ then $\omega|_B$ is a p-cycle if and only if $\omega|_{B'}$ is a p-cycle. By [7, Lemma 2], the union of the equivalence classes of $\equiv$ is an invariant partition $\mathcal{E}$ of M and $\rho|_E \in \mathrm{Aut}(\Gamma')$ for every $E \in \mathcal{E}$. As ${\rho^{p^{k-1}}}|_C \in \mathrm{Aut}(\Gamma)$ and M, we see that $\mathcal{M} \preceq \mathcal{C}$. As $\gamma|_C$ is of prime order and contains a fixed point for every $C \in \mathcal{C}$, for $C \in \mathcal{C}$ there exists $B, B' \in \mathcal{B}$ with $B, B' \subseteq C$ but $B \not\equiv B'$. This then implies that $\mathcal{E} \prec \mathcal{C}$, and so if $\mathcal{E}$ is formed by the orbits of $A < L \leq \langle\rho\rangle$, then $S_j - A$ is a union of cosets of A for every $S_j \in S$. This contradicts our choice of L, and so $\gamma \notin H$.

Now suppose that $\gamma n \in H$ for some $n \in \mathrm{Aut}(\mathbb{Z}_{p^k})$, and let $|L| = \ell$. Then $\gamma n|_C$ normalizes $\langle {\rho^{p^{k-\ell}}}|_C\rangle$ and fixes 0 so γn is an automorphism of $\mathbb{Z}_{p^\ell}$. As $\mathrm{Aut}(\mathbb{Z}_{p^\ell})$ is abelian, raising γn to an appropriate power relatively prime to p, we may assume without loss of

generality that γn has order a power of p. Then $n|_C = 1$ and by Lemma 8 $\gamma|_C \in \mathrm{Aut}(\Gamma)$. But then $\gamma \in H$, a contradiction. We conclude that $H \leq \langle G, N(p^k)\rangle$.

Let $|H| = |G| \cdot m$. As $H \leq \langle G, N(p^k)\rangle$, we see $G \triangleleft N(p^k)$. As $\langle\rho\rangle \leq G$ and $N(p^k)/\langle\rho\rangle$ is isomorphic to a subgroup of $\mathrm{Aut}(\mathbb{Z}_{p^k})$, there exists $A \leq \mathrm{Aut}(\mathbb{Z}_{p^k})$ such that $H = \langle G, A\rangle = GA$ and

$$|H| = \frac{|G| \cdot |A|}{|G \cap A|} = \frac{p^{k-1+p^{k-\ell}}|A|}{p},$$

and $m = |A|/p^{k+1}$. Then the number of subgroups of H conjugate to $\langle\rho\rangle$ in H is

$$[H : N_H(\langle\rho\rangle)] = \frac{|H|}{|N_H(\langle\rho\rangle)|} = \frac{|H|}{p^k \cdot |A|} = p^{p^{k-\ell}-2}.$$

However, by Lemma 7, G contains exactly $p^{p^{k-\ell}}$ regular cyclic subgroups, so there are indeed regular cyclic subgroups of H that are not conjugate in G. This gives that if Γ is a circulant color digraph that is a CI-digraph of $\mathbb{Z}_{p^k}$, then L is of prime order and so $\mathcal{B} = \mathcal{C}$.

Applying Lemma 8 to M with $\mathcal{C} = \mathcal{B}$, we see that the $\mathrm{Stab}_B(M)|_B \leq \mathrm{Aut}(\Gamma)$, where $\mathrm{Stab}_B(M)$ is the setwise stabilizer of the block $B \in \mathcal{B}$ in M. Applying the Embedding Theorem we see that $M = M/\mathcal{B} \wr (\mathrm{Stab}_M(B)|_B)$. As $M^{(2)} = (M/\mathcal{B})^{(2)} \wr (\mathrm{Stab}_M(B)|_B)^{(2)}$ by [5, Theorem 5.1], the result follows if $M = \mathrm{Aut}(\Gamma)$. Otherwise, $\mathcal{B}$ is not an invariant partition of $\mathrm{Aut}(\Gamma)$. Let $\mathcal{D}$ be the invariant partition of $\mathrm{Aut}(\Gamma)$ with non-singleton blocks of smallest order. As $\mathcal{B} \prec \mathcal{D}$ the blocks of $\mathcal{D}$ are of composite order. By Lemma 9, $\mathrm{Stab}_{\mathrm{Aut}(\Gamma)}(D)|_D$ is a doubly-transitive group with simple nonabelian socle. This implies $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{D}|_D$ is a doubly-transitive group with simple socle for every $D \in \mathcal{D}$. As $\mathcal{B} \prec \mathcal{D}$ and $\rho^{p^{k-1}}|_B \in \mathrm{Aut}(\Gamma)$ for every $B \in \mathcal{B}$, the normal closure N of $\langle \rho^{p^{k-1}}|_B\rangle$ in

$\mathrm{Stab}_{\mathrm{Aut}(\Gamma)}(D)$ is also doubly-transitive with nonabelian socle where $B \subseteq D$. We conclude that any orbital digraph Δ of $\mathrm{Aut}(\Gamma)$ is isomorphic to a wreath $\Delta = \Delta/\mathcal{D} \wr K_{p^{k-i}}$ or $\Delta = \Delta/\mathcal{D} \wr \bar{K}_{p^{k-i}}$ in which case $\mathrm{Aut}(\Gamma)/\mathcal{D} \wr S_{p^{k-i}} = \mathrm{Aut}(\Gamma)^{(2)} = \mathrm{Aut}(\Gamma)$ where the last equality is true as the automorphism group of a color digraph is 2-closed and $|D| = p^{k-i}$.

■

Lemma 11

Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ *be a circulant CI-color digraph, and suppose* $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}, S)) \cong \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1)) \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^i}, S_2))$ *for some circulant color digraphs* $\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1)$ *and* $\mathrm{Cay}(\mathbb{Z}_{p^i}, S_2)$. *Then* $\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1)$ *is a circulant CI-color digraph.*

Proof: Let $\mathcal{B}$ be the invariant partition of $\mathrm{Aut}(\Gamma)$ be formed by the orbits of $1_{S_{p^{k-i}}} \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^i}, S_2))$. Suppose first that for any regular cyclic subgroup R of the color Cayley digraph $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1))$, there exists regular cyclic subgroup T of $\mathrm{Aut}(\Gamma)$ such that $T/\mathcal{B} = R$. Let $\delta \in S_{p^{k-i}}$ such that $R = \delta^{-1}(\mathbb{Z}_{p^{k-i}})_L\delta \leq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1))$. Then there exists a regular cyclic subgroup T such that $T/\mathcal{B} = R$. As any two regular cyclic subgroups are permutation equivalent, there exists $\omega \in \mathcal{S}_{p^k}$ such that $\omega^{-1}(\mathbb{Z}_{p^k})_L\omega = T$. As Γ is a circulant CI-color digraph, by Lemma 3 there exists $\phi \in \mathrm{Aut}(\Gamma)$ such that $\phi^{-1}\omega^{-1}(\mathbb{Z}_{p^k})_L\omega\phi = (\mathbb{Z}_{p^k})_L$. Then $\phi/\mathcal{B} \in \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1))$ and $(\phi/\mathcal{B})^{-1}R\phi/\mathcal{B} = (\mathbb{Z}_{p^{k-i}})_L$ and $\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1)$ is a circulant CI-color digraph. It thus suffices to show that for every regular cyclic subgroup of R of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1))$ there is a regular cyclic subgroup T of $\mathrm{Aut}(\Gamma)$ with $T/\mathcal{B} = R$.

Let $R = \langle\sigma\rangle$ be a regular cyclic subgroup in $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1))$. For $i \in \mathbb{Z}_{p^{k-i}}$, let $b_i = 0$ if $i \neq 0$ and $b_0 = 1$. Then the function $(x, y) \mapsto (\sigma(x), j + b_i)$ is contained in

$\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1)) \wr (\mathbb{Z}_{p^i})_L \leq \mathrm{Aut}(\Gamma)$ and this function has order p^{k-i}. Letting T be the corresponding regular cyclic subgroup of $\mathrm{Aut}(\Gamma)$, we see that $T/\mathcal{B} = R$. ∎

Corollary 1

Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ be a CI-color digraph. Then there exists an integer $0 \leq i \leq k$ and a 2-closed group G_1 that contains $(\mathbb{Z}_{p^{k-i}})_L$, and $G_j \leq S_{p^{a_j}}$ that is 2-closed and contains $(\mathbb{Z}_{p^{a_j}})_L$, $2 \leq j \leq r$ such that $\sum_{j=1}^{r} a_i = k - i$ and if $a_j \geq 2$ then $G_j = S_{p^{a_j}}$ and $\mathrm{Aut}(\Gamma) \cong G_1 \wr G_2 \wr \cdots \wr G_r$. Additionally, the Sylow p-subgroup of G_1 that contains $(\mathbb{Z}_{p^{k-i}})_L$ contains a unique regular cyclic subgroup and is either $(\mathbb{Z}_{p^{k-i}})_L$ or $p = 2$ and is $\langle (\mathbb{Z}_{2^k})_L, \iota \rangle$ or $\langle (\mathbb{Z}_{2^{k-i}})_L, \iota\beta^{2^{k-i-3}} \rangle$ of order 2^{k-i+1}.

Proof: We proceed by induction on k. If $k = 1$, the result is trivial as a Sylow p-subgroup of S_p is a regular cyclic subgroup, so we assume $k \geq 2$ and assume the result is true for all circulant color digraphs of order at most p^{k-1}. Let Γ be a circulant color digraph of order p^k. Let P be a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. By Lemma 4 either the result follows with $\ell = 0$ or Γ is isomorphic to a generalized wreath product. If Γ is isomorphic to a generalized wreath product, then by Lemma 10 $\mathrm{Aut}(\Gamma) = H_1 \wr H_2$ where $H_1 \leq S_{p^{k-i}}$ for some $i \geq 0$ and $H_2 \leq S_{p^i}$ are 2-closed that contain $(\mathbb{Z}_{p^{k-i}})_L$ and $(\mathbb{Z}_{p^i})_L$, respectively, and if $i \geq 2$ then $H_2 = S_{p^i}$. As H_1 is 2-closed, it is the automorphism group of some circulant color digraph $\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S')$. By Lemma 11, we see that $\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S')$ is a circulant CI-color digraph, and the result then follows by induction applied to $\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S')$. ∎

Corollary 2

Let $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ be a circulant color digraph such that there exists $0 \leq i \leq k$ and a 2-closed group G_1 that contains $(\mathbb{Z}_{p^{k-i}})_L$, and $G_j \leq S_p^{a_j}$ that is 2-closed and contains

$(\mathbb{Z}_{p^{a_j}})_L$, $2 \leq j \leq r$ *such that* $\sum_{j=1}^{r} a_i = k - i$ *and if* $a_j \geq 2$ *then* $G_j = S_{p^{a_j}}$ *and* $\mathrm{Aut}(\Gamma) \cong G_1 \wr G_2 \wr \cdots \wr G_r$. *Additionally, the Sylow* p*-subgroup of* G_1 *that contains* $(\mathbb{Z}_{p^{k-i}})_L$ *contains a unique regular cyclic subgroup and is either* $(\mathbb{Z}_{p^{k-i}})_L$ *or* $p = 2$ *and is* $\langle (\mathbb{Z}_{2^k})_L, \iota \rangle$ *or* $\langle (\mathbb{Z}_{2^{k-i}})_L, \iota\beta^{2^{k-i-3}} \rangle$ *of order* 2^{k-i+1}. *Then* $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}, S)) = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}), T)$ *for some circulant digraph* $\mathrm{Aut}(\mathbb{Z}_{p^k}, T)$.

Proof: By [6, Theorem 3.5B] either G_j contains a regular cyclic subgroup or is doubly-transitive and as 2-closed, is a symmetric group. As symmetric groups are automorphism groups of circulant digraphs are automorphism groups of digraphs (either the complete graph or its complement) as are 2-closed groups that contain a normal regular cyclic subgroup by [23], we have that $G_i = \mathrm{Aut}(\Gamma_i)$ for some digraph Γ_i. We need one final condition. Namely, if $\Gamma_i = K_p$, $2 \leq i \leq \ell$, then $\Gamma_{i-1} \neq K_p$ (we choose it to be the complement of K_p if G_{i-1} is doubly-transitive). We then have that

$$\mathrm{Aut}(\Gamma_1 \wr \Gamma_2 \wr \cdots \wr \Gamma_r) = \mathrm{Aut}(\Gamma_1) \wr \mathrm{Aut}(\Gamma_2) \wr \cdots \wr \mathrm{Aut}(\Gamma_\ell) = G_1 \wr G_2 \wr \cdots \wr G_r$$

by [10, Theorem 5.7] and straightforward induction argument. ∎

The preceding result has a more appealing form in the case where Γ is a digraph as then any complete graph or its complement can be written as a wreath product of order p circulants (either all complete or complements of complete graphs, respectively).

Corollary 3

Let $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ *be a CI-digraph. Then*

$$\mathrm{Cay}(\mathbb{Z}_{p^k}, S) = \mathrm{Cay}(\mathbb{Z}_{p^{k-i}}, S_1) \wr \mathrm{Cay}(\mathbb{Z}_p, S_2) \wr \cdots \wr \mathrm{Cay}(\mathbb{Z}_p, S_{k-i+1})$$

for some $S_1 \subseteq \mathbb{Z}_{p^{k-i}}$ *and* $S_j \subseteq \mathbb{Z}_p$, $2 \leq j \leq k-i+1$. *Additionally, the Sylow* p*-subgroup of* $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-i}}), S_1)$ *that contains* $(\mathbb{Z}_{p^{k-i}})_L$ *contains a unique regular cyclic subgroup and is either* $(\mathbb{Z}_{p^{k-i}})_L$ *or* $p = 2$ *and is* $\langle (\mathbb{Z}_{2^k})_L, \iota \rangle$ *or* $\langle (\mathbb{Z}_{2^{k-i}})_L, \iota\beta^{2^{k-i-3}} \rangle$ *of order* 2^{k-i+1}

CHAPTER 6

THE PRIMARY KEY OF A PRIME-POWER CI CIRCULANT

In this chapter we turn towards Muzychuk's solution of the isomorphism problem for circulants. He showed that a necessary (but not sufficient) condition for two circulant digraphs of order n to be isomorphic is that they have the same "key". In this section we will introduce some of the notation that Muzychuk needed for his solution, and compute the "key" of a CI-circulant digraph of prime-power order.

Definition 15

Let p be prime and $n \geq 1$ an integer. Define a **primary key space** $\mathbf{K}_{p^n}$ *to be the set of all integer vectors $(k_1, \ldots, k_n)$ satisfying the following two properties:*

1. $k_i < i$ *for each* $1 \leq i \leq n$, *and*
2. $k_{i-1} \leq k_i$ *for each* $2 \leq i \leq n$.

A vector in $\mathbf{K}_{p^a}$ *is called a* **primary key**.

Definition 16

Let $\mathbf{k}$ *be a primary key. For* $g \in \mathbb{Z}_{p^n} \backslash \{0\}$, *define* $b(g) = k$, *where* $|g| = p^k$, *and let* $C_g = g + \langle p^{n-k_{b(g)}} \rangle$.

Clearly each C_g is a coset of some subgroup of $\mathbb{Z}_{p^n}$. It is easy to verify that all the elements of C_g has the same order as g. Additionally, if $\mathbf{k}$ is a primary key, then $\Sigma(\mathbf{k}) = \{\{0\}, C_g : g \in \mathbb{Z}_{p^n} \backslash \{0\}\}$, then $\Sigma(\mathbf{k})$ is a partition of $\mathbb{Z}_{p^n}$.

Definition 17

The partition $\Sigma(\mathbf{k})$ *is called the* **primary key partition** *corresponding to* $\mathbf{k}$.

We may compare two primary keys by setting $\mathbf{k} = (k_1, \ldots, k_n) \leq (\ell_1, \ldots, \ell_n) = \boldsymbol{\ell}$ if and only if $k_i \leq \ell_i$, $1 \leq i \leq n$. It is not hard to show that if $\mathbf{k} \leq \boldsymbol{\ell}$, then $\Sigma(\mathbf{k}) \preceq \Sigma(\boldsymbol{\ell})$, which means that $\Sigma(\mathbf{k})$ is a refinement of $\Sigma(\boldsymbol{\ell})$.. There is a largest primary key $(0, 1, \ldots, n-1)$, and a smallest primary key $(0, \ldots, 0)$. Corresponding to each primary key there is a set of permutations of $\mathbb{Z}_{p^k}$ defined as follows.

Definition 18

Let p *be prime and* n *a positive integer. Define the set* $\mathbb{Z}_{p^n}^{**}$ *of to be the set of all vectors* $\{(m_1, \ldots, m_n) : m_i \in \mathbb{Z}_{p^i}^{*}\}$. *For each* $\vec{m} \in \mathbb{Z}_{p^n}^{**}$, *define a function* $f_{\vec{m}} : \mathbb{Z}_{p^n} \mapsto \mathbb{Z}_{p^n}$ *by*

$$f_{\vec{m}}(x) = f_{\vec{m}}\left(\sum_{i=0}^{n-1} x_i p^i\right) = \sum_{i=0}^{n-1} m_{n-i} x_i p^i.$$

It is not difficult to show that for $\vec{m} \in \mathbb{Z}_{p^n}^{**}$, the function $f_{\vec{m}}$ is a well-defined bijection of $\mathbb{Z}_{p^n}$.

Definition 19

Let $\mathbf{k} = (k_1, \ldots, k_n) \in \mathbf{K}(p^n)$ *be a primary key. Define the set of all* **primary genuine generalized multipliers corresponding to the key** $\mathbf{k}$, *denoted* $\mathbb{Z}_{p^n}^{**}(\mathbf{k})$, *to be the set of all primary generalized multipliers* $\vec{m}$ *in* $\mathbb{Z}_{p^n}^{**}$ *that satisfy the following two conditions:*

1. $m_\delta \equiv m_{\delta-1} \pmod{p^{\delta - k_\delta - 1}}$, $2 \leq \delta \leq n$, *and*
2. $m_\delta \in \mathbb{Z}_{p^{\delta - k_\delta}}$, $1 \leq \delta \leq n$.

We remark that our notation is slightly different in the previous definition than that of Muzychuk.

Definition 20

For two vectors $\mathbf{u} = (u_1, \ldots, u_n)$ *and* $\mathbf{v} = (v_1, \ldots, v_n)$ *in* $\mathbf{K}_{p^n}$*, define* $\mathbf{u} \wedge \mathbf{v}$ *to be the vector* $(\min\{u_1, v_1\}, \min\{u_2, v_2\}, \ldots, \min\{u_n, v_n\})$*. Now let* P *and* Q *be two partitions of a set* X*. We define the* **join** *of* P *and* Q*, denoted* $P \vee Q$*, to be the smallest partition that refines both* P *and* Q*. join*

Lemma 12

Let $\mathbf{k}$ *and* $\boldsymbol{\ell}$ *be primary keys in* $\mathbf{K}(p^n)$*. Then* $\Sigma(\mathbf{k}) \vee \Sigma(\boldsymbol{\ell}) = \Sigma(\mathbf{k} \wedge \boldsymbol{\ell})$*.*

Definition 21

Let Δ *be a partition of* $\mathbb{Z}_{p^n}$*. The partition for which* $\Sigma(\mathbf{k})$ *is the unique largest (in the sense of refinement) primary key partition that is a refinement of* Δ *is the* **key of** Δ *and denoted* $\mathbf{k}(\Delta)$*. Let* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *be a circulant digraph. The* **key of** $\mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *is defined to be the key of the partition* $\{S, \mathbb{Z}_{p^n} \backslash S\}$*.*

We are now ready to state our final definition, and then give the statement of the Muzychuk's Theorem in the prime-power case.

Definition 22

Let $\mathrm{Cay}(\mathbb{Z}_{p^n}, S_1, \ldots, S_r)$ *have primary key* $\mathbf{k}$*. The* **solving set of** $\mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *is defined to be the set* $P(\mathbf{k}) = \{f_{\vec{m}} : \vec{m} \in \mathbb{Z}_{p^n}^{**}(\mathbf{k})\}$*. That is, the solving set of* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *is the set of all genuine generalized multipliers related to the primary key of* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S)$*.*

Theorem 5

Let p *be prime,* n *a positive integer,* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S_1, \ldots, S_r)$ *and* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S'_1, \ldots, S'_r)$ *circulant color digraphs with primary keys* $\mathbf{k}$ *and* $\mathbf{k}'$*, respectively. Then*

1. *if* $\mathbf{k} \neq \mathbf{k}'$*, then* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S_1, \ldots, S_r)$ *is not isomorphic to* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S'_1, \ldots, S'_r)$*,*
2. *if* $\mathbf{k} = \mathbf{k}'$*, then the following are equivalent:*

(a) $\mathrm{Cay}(\mathbb{Z}_{p^n}, S_1, \ldots, S_r)$ *and* $\mathrm{Cay}(\mathbb{Z}_{p^n}, S'_1, \ldots, S'_r)$ *are isomorphic,*

(b) $f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_{p^n}, S_1, \ldots, S_r)) = \mathrm{Cay}(\mathbb{Z}_{p^n}, S')$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$*, and*

(c) $f_{\vec{m}}(S) = S'$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$*.*

Lemma 13

A circulant digraph $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *is isomorphic to a wreath product of a circulant digraph* $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^{n-i}}, S_1) \wr \mathrm{Cay}(\mathbb{Z}_{p^i}, S_2)$ *if and only if* Γ *has primary key* $\mathbf{k} = (k_1, \ldots, k_n)$ *and* $k_{i+1} = i$*.*

Proof: Let $H = \langle p^{n-i} \rangle$. We first observe that Γ is isomorphic to a wreath product of the given form if and only if $S - H$ is a union of cosets of H. This occurs if and only whenever $g \in \mathbb{Z}_{p^n}$, $|g| \geq p^{i+1}$, either $g + H \subset S$ or $(g + H) \cap S = \emptyset$. This last condition occurs if and only if every cell of the primary key partition $\Sigma(\mathbf{k})$ not contained in H is a union of cosets of H. As the cell of $\Sigma(\mathbf{k})$ that contains g with $|g| = p^j$, $j \geq i + 1$ is $C_g = g + \langle p^{n-k_j} \rangle$, every cell of the primary key partition $\Sigma(\mathbf{k})$ not contained in H is a union of cosets of H if and only if $C_g = g + \langle p^{n-k_j} \rangle$ is a union of cosets of H for every g with $|g| = p^j$, $j \geq i+1$. This occurs if and only if $\langle p^{n-k_j} \rangle \geq \langle p^{n-i} \rangle$, or equivalently, $k_j \geq i$ for every $j \geq i+1$. As $k_j < j$, we see that $k_{i+1} \geq i$ if and only if $k_{i+1} = i$. ∎

Lemma 14

Let $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^i}, S_1)$ *where* $S_1 \subset \mathbb{Z}_{p^i}$*, and* $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{p^j}, S_2)$ *where* $S_2 \subset \mathbb{Z}_{p^j}$*. Let* $\mathbf{k}_1 = (k_1, \ldots, k_i)$ *be the primary key of* Γ_1 *and* $\mathbf{k}_2 = (\ell_1, \ldots, \ell_j)$ *be the primary key of* Γ_2*. Then* $\Gamma_1 \wr \Gamma_2$ *has key* $(\ell_1, \ldots, \ell_j, k_1 + j, \ldots, k_i + j)$*.*

Proof: Let H_m be the unique subgroup of $\mathbb{Z}_{p^{i+j}}$ of order p^m, J_m the unique subgroup of $\mathbb{Z}_{p^j}$ of order p^m, and I_m the unique subgroup of $\mathbb{Z}_{p^i}$ of order p^m. Let $g \in \mathbb{Z}_{p^{i+j}}$ and $|g| = p^m$,

and S the connection set of $\Gamma_1 \wr \Gamma_2$ as a circulant digraph, and $\mathbf{k} = (k'_1, \ldots, k'_{i+j})$ be the key of $\Gamma_1 \wr \Gamma_2$.

If $1 \leq m \leq j$, then $g \in H_m \leq H_j$ and $\Gamma[H_j] \cong \Gamma_2$. Then $g = g'p^i$ where $g' \in \mathbb{Z}_{p^j}$. In $\mathbb{Z}_{p^j}$, $C_{g'}$ is then a coset of the unique subgroup $J_{j-\ell_{g'}}$ of order $p^{j-\ell_{g'}}$, so in $\mathbb{Z}_{p^{i+j}}$, C_g is a coset of the unique subgroup $H_{i+j-\ell_{g'}}$ of $\mathbb{Z}_{p^{i+j}}$ of order $p^{j-\ell'_g}$. Thus C_g is a coset of $H_{i+j-\ell_{g'}}$, and $k' = \ell_{g'}$ as required.

If $i \leq m \leq i+j$, then the connection set $S - H_j$ is a union of cosets of H_j. Additionally, as the primary key partition $\Sigma(\mathbf{k}_1)$ is refinement of $\{S_1, \mathbb{Z}_{p^i} - S_1\}$, either $g \pmod{p^i} + I_{i-k_i}$ is contained in S_1 or disjoint from S_1. As $\Sigma(\mathbf{k})$ is the unique least refinement of $\{S, \mathbb{Z}_{p^{i+j}} - S\}$ that is a key partition, we conclude that either $g + H_{i+j-(j+k_i)}$ is contained in S or disjoint from S. Then, in $\mathbb{Z}_{i+j}$, $C_g = g + H_{i-k_i}$ and so $k'_g = i + j - (i - k_i) = j + k_i$ as required. ∎

Lemma 15

A circulant digraph $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *is a nontrivial generalized wreath product if and only if its primary key* $\mathbf{k} \neq (0, 0, \ldots, 0)$.

Proof: By definition, the key partition $\Sigma(0, \ldots, 0)$ consists of singletons, and every cell of any key partition is a coset of some subgroup of $\mathbb{Z}_n$. It thus suffices to show that the key partition corresponding to a generalized wreath product contains a coset of some nontrivial subgroup. The digraph Γ is a nontrivial generalized wreath product if and only if there exists subgroups $1 < L \leq K \leq \mathbb{Z}_n$ and $S - K$ is a union of cosets of L. Also, $S - K$ is a union of cosets of L if and only if $(\mathbb{Z}_n - S) - K$ is a union of cosets of L. We conclude that Γ is a nontrivial generalized wreath product if and only if the unique key partition that

refines $\{S, \mathbb{Z}_n - S\}$ is bounded below by the partition $\{\{k\}, g + L : k \in K, g \in \mathbb{Z}_n - K\}$ which has key $(0, \ldots, 0, \ell, \ldots, \ell)$ where $|L| = \ell$, and there are k 0's, where $|K| = p^k$. This implies that the key partition of $\{S, \mathbb{Z}_n - S\}$ is not all singletons, and the result follows. ■

Corollary 4

If a circulant digraph $\mathrm{Cay}(\mathbb{Z}_{p^n}, S)$ *is a CI-digraph then it has primary key* $\mathbf{k} = (0, 1, \ldots, i-1, i-1, \ldots, i-1)$.

Proof: By Corollary 1, there exists an integer $0 \leq \ell \leq k$ and Cayley digraph $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^{k-\ell}}, S_1)$, and $\Gamma_i = \mathrm{Cay}(\mathbb{Z}_p, S_i)$, $0 \leq i \leq \ell$ such that $\Gamma \cong \Gamma_1 \wr \Gamma_2 \wr \cdots \wr \Gamma_\ell$. Additionally, the Sylow p-subgroup of $\mathrm{Aut}(\Gamma_1)$ that contains $(\mathbb{Z}_{p^{k-\ell}})_L$ contains a unique regular cyclic subgroup and is either $(\mathbb{Z}_{p^{k-\ell}})_L$ or $p = 2$ and is $\langle (\mathbb{Z}_{2^k})_L, \iota \rangle$ or $\langle (\mathbb{Z}_{2^{k-\ell}})_L, \iota\beta^{2^{k-\ell-3}} \rangle$ of order $2^{k-\ell+1}$. Note that Γ_1 is not isomorphic to a nontrivial generalized wreath product as the automorphism group of a nontrivial generalized wreath product has more than one regular cyclic subgroup by Lemma 5. By 15, we see Γ_1 has key $(0, \ldots, 0)$. By Lemma 13 Γ_2 has key $(0, 1, 2, \ldots, i-1)$ and the result follows by Lemma 14 ■

Muzychuk has shown that two isomorphic circulant digraphs of order p^n have the same primary key, and given a primary key $\mathbf{k}$, they are isomorphic if and only if they are isomorphic by a genuine generalized multiplier. These are straighforward to calculate, and below we record the conditions such a genuine generalized multiplier must satisfy for the primary key $\mathbf{k} = (0, 1, 2, \ldots, i-1, i-1, \ldots, i-1)$.

Lemma 16

The genuine generalized multipliers $(m_1, \ldots m_n)$ *for the primary key* $\mathbf{k} = (0, 1, 2, \ldots, i-1, i-1, \ldots, i-1)$ *satisfy the following conditions:*

- *For* $1 \leq j \leq i$, $m_j \in \{1, \ldots, p-1\}$,
- *For* $1 \leq j \leq n-i$, $m_{i+j} \in \{1, \ldots, p^{j+1}-1\}$, *and*
- *For* $0 \leq j \leq n-i$, $m_{i+j} \equiv m_{i+j-1} \pmod{p^j}$.

CHAPTER 7

CI-DIGRAPHS OF PRIME-POWER ORDER

In this chapter, we will determine a necessary and sufficient condition for a circulant digraph of prime power order to be a CI-digraph.

Lemma 17

Let $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^n}, S_1)$ *be a digraph with primary key*

$$\mathbf{k} = (0, 1, \ldots, i-1, i-1, \ldots, i-1).$$

Suppose that $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{p^n}, S_2)$ *and* $\Gamma_1 \cong \Gamma_2$ *by a genuine generalized multiplier* γ *of the form* $(m_1, \ldots, m_n)$ *where* $m_n \equiv 1 \pmod p$ *and* $m_j \equiv 1 \pmod p$ *for every* $1 \leq j \leq i$. *Then* $\alpha(\Gamma_1) = \Gamma_2$ *for some* $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^n})$ *of order a power of* p.

Proof: As Γ_1 has primary key $\mathbf{k}$, by inductively applying Lemma 13 we see that $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^i}, T_1) \wr \mathrm{Cay}(\mathbb{Z}_p, T_2) \wr \cdots \wr \mathrm{Cay}(\mathbb{Z}_p, T_{n-i+1})$ for $T_1 \subset \mathbb{Z}_{p^i}$ and $T_j \subset \mathbb{Z}_p$, $2 \leq j \leq n-i+1$. Additionally, $\mathrm{Cay}(\mathbb{Z}_{p^i}, T_1)$ is not a generalized wreath product by Lemma 15, and so by Lemma 4 a Sylow p-subgroup of $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^i}, T_1))$ has a unique regular cyclic subgroup. Let P be a Sylow p-subgroup of $\mathrm{Aut}(\Gamma_1)$ that contains $(\mathbb{Z}_{p^n})_L$. It is not hard to see that $\gamma^{-1}(\mathbb{Z}_{p^n})_L\gamma \leq P$. Notice that P admits an invariant partition $\mathcal{B}_j$ consisting of blocks of size p^j for $0 \leq j \leq n$ by [8, Lemma 9], and that $\mathcal{B}_j$ is the unique invariant partition of P by [21, Exercise 6.5]. Then $P/\mathcal{B}_{n-i}$ contains a unique regular cyclic subgroup, and so

every conjugate of $(\mathbb{Z}_{p^n})_L$ contained in P is contained in $P' = \mathbb{Z}_{p^i} \wr \mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p$, where there are $n-i$ factors in this wreath product isomorphic to $\mathbb{Z}_p$.

Now observe that the conditions for the genuine generalized multipliers corresponding to the primary key $\mathbf{k}$ are given in Lemma 16. In particular, $m_{i+1} \equiv m_i \pmod p$. Also, $m_{i+2} \equiv m_{i+1} \pmod{p^2}$, and so $m_{i+2} \equiv m_{i+1} \pmod p$. Arguing inductively, we see that $m_i \equiv m_{i+1} \equiv \ldots \equiv m_n \pmod p$, and as $m_n \equiv 1 \pmod p$, $m_{i+j} \equiv 1 \pmod p$ for every $0 \leq i \leq n-i$. We will show by induction on $n-i$ that there exists $\beta \in P'$ such that $\gamma\beta = \alpha \in \mathrm{Aut}(\mathbb{Z}_{p^n})$.

The base case of induction is $n-i=0$ and as a generalized multiplier fixes 0, we see that in this case $\gamma \in \mathrm{Aut}(\mathbb{Z}_{p^i})$ by Corollary 1. Assume the result is true for $n-i=j \leq n-2$ and suppose $n-i=j+1$. By induction, there exist $\beta_1 \in P'$ such that $\gamma\beta_1/\mathcal{B}_1$ is an automorphism of ${\mathbb{Z}_p}^{n-1}$. Let P'' be the Sylow p-subgroup of S_{p^n} that contains $(\mathbb{Z}_{p^n})_L$, so that $P \leq P''$. Also, a Sylow p-subgroup Π of $\mathrm{Aut}(\mathbb{Z}_{p^n}) \cdot (\mathbb{Z}_{p^n})_L$ is also contained in P''. By the Embedding Theorem [16, Theorem 1.2.6] and the fact that $\Pi/\mathcal{B}_1$ is a Sylow p-subgroup of $\mathrm{Aut}(\mathbb{Z}_{p^{n-1}}) \cdot (\mathbb{Z}_{p^{n-1}})_L$, we see $\mathrm{Aut}(\mathbb{Z}_{p^n}) \cdot (\mathbb{Z}_{p^n})_L \leq (\mathrm{Aut}(\mathbb{Z}_{p^{n-1}}) \cdot (\mathbb{Z}_{p^{n-1}})_L) \wr \mathbb{Z}_p$. Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^n})$ such that $\gamma\beta_1/\mathcal{B}_1 = \alpha/\mathcal{B}_1$. Then $\alpha^{-1}\gamma\beta_1 = \beta_2^{-1} \in \mathrm{fix}_{P''}(\mathcal{B}_1) = \mathbb{Z}_p^n = \mathrm{fix}_P(\mathcal{B})$. Then $\gamma\beta_1\beta_2 = \alpha$ and $\beta_1\beta_2 \in P$. The result follows by induction. ∎

We now consider which digraphs with primary key $\mathbf{k} = (0, 1, \ldots, i-1, i-1, \ldots, i-1)$ are CI-digraphs. For this it will be convenient to write an element of $\mathbb{Z}_{p^n}$ in it p-adic form. That is, each element of $\mathbb{Z}_{p^n}$ can be written uniquely in the form $\sum_{j=0}^{n-1} x_j p^j$, where $j \in \mathbb{Z}_p$. The permutation corresponding to a generalized multiplier $(m_1, \ldots, m_n)$ maps $\sum_{j=0}^{n-1} x_j p^j$ to $\sum_{j=0}^{n-1} m_{n-j} x_j p^j$.

Lemma 18

Let $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^n}, S_1)$ *have primary key* $\mathbf{k} = (0, 1, \ldots, i-1, \ldots, i-1)$ *so that* $\Gamma_1 \cong \mathrm{Cay}(\mathbb{Z}_{p^i}, T_1) \wr \mathrm{Cay}(\mathbb{Z}_p, T_2) \wr \cdots \wr \mathrm{Cay}(\mathbb{Z}_p, T_{n-i+1})$ *for* $T_1 \subset \mathbb{Z}_{p^i}$ *and* $T_j \subset \mathbb{Z}_p$, $2 \leq j \leq n-i+1$. *Suppose that* $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{p^n}, S_2)$ *and* $\Gamma_1 \cong \Gamma_2$ *by a genuine generalized multiplier* γ *of the form* $(m_1, \ldots, m_n)$ *where* $1 \leq m_j \leq p-1$ *for every* $1 \leq j \leq n$. *Then* $\alpha(\Gamma_1) = \Gamma_2$ *for some* $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^n})$ *if and only if there exists* $\ell_1 \in \mathrm{Aut}(\mathbb{Z}_{p^i}, T_1)$ *and* $\ell_j \in \mathrm{Aut}(\mathbb{Z}_p, T_j)$ *such that if* $(t_1, \ldots, t_n) = (\ell_{m-i+1}, \ell_{m-i}, \ldots, \ell_2, \ell_1, \ldots, \ell_1)$ *then for all* $1 \leq r, s \leq n$ *we have* $m_r t_r = m_s t_s$.

Proof: Suppose that there exists $m \in \mathbb{Z}_n^*$ such that the function $\alpha : \mathbb{Z}_{p^n} \mapsto \mathbb{Z}_{p^n}$ given by $\alpha(x) = mx$ is an isomorphism from Γ_1 to Γ_2. As a generalized multiplier, $m = (m, m, \ldots, m)$ and

$$(t_1^{-1}, \ldots, t_n^{-1})(m, \ldots, m) = (t_1^{-1}m, t_2^{-1}m, \ldots, t_n^{-1}m) \in \mathrm{Aut}(\Gamma_1).$$

As

$$\Gamma_1 \cong \mathrm{Cay}(\mathbb{Z}_{p^i}, T_1) \wr \mathrm{Cay}(\mathbb{Z}_p, T_2) \wr \cdots \wr \mathrm{Cay}(\mathbb{Z}_p, T_{n-i+1}),$$

we see

$$\mathrm{Aut}(\Gamma_1) \geq \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^i}, T_1)) \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T_2)) \wr \cdots \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T_{n-i+1})).$$

For $1 \leq j \leq i$, we have that $m_j^{-1}m \in \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T_j))$ and $m_j^{-1}m \cdot m_j = m$ as required.

Conversely, suppose that there exists $\ell_1 \in \mathrm{Aut}(\mathbb{Z}_{p^i}, T_1)$ and $\ell_j \in \mathrm{Aut}(\mathbb{Z}_p, T_j)$ such that if $(t_1, \ldots, t_n) = (\ell_{m-i+1}, \ell_{m-i}, \ldots, \ell_2, \ell_1, \ldots, \ell_1)$ then for all $1 \leq r, s \leq n$ we

have $m_r t_r = m_s t_s$. As $\mathrm{Aut}(\Gamma)$ contains $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^i}, T_1)) \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T_2)) \wr \cdots \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, T_{n-i+1}))$, the permutation in S_{p^n} corresponding to the generalized multiplier $(\ell_{m-i+1}, \ell_{m-i}, \ldots, \ell_2, \ell_1, \ldots, \ell_1)$ is contained in $\mathrm{Aut}(\Gamma)$. Set $m = m_1 t_1$. Then the map

$$x \mapsto \sum_{j=0}^{n-1} m x_j p^j = m \sum_{j=0}^{n-1} x_j p^j = mx$$

is an isomorphism between Γ_1 and Γ_2 as required. ∎

Corollary 5

Let $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}_{p^n}, S_1)$ *have primary key* $\mathbf{k} = (0, 1, \ldots, i-1, \ldots, i-1)$ *so that* $\Gamma_1 \cong \mathrm{Cay}(\mathbb{Z}_{p^i}, T_1) \wr \mathrm{Cay}(\mathbb{Z}_p, T_2) \wr \cdots \wr \mathrm{Cay}(\mathbb{Z}_p, T_{n-i+1})$ *for* $T_1 \subset \mathbb{Z}_{p^i}$ *and* $T_j \subset \mathbb{Z}_p$, $2 \leq j \leq n-i+1$. *Suppose that* $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}_{p^n}, S_2)$ *and* $\Gamma_1 \cong \Gamma_2$ *by a genuine generalized multiplier* $\gamma = (m_1, \ldots, m_n)$. *Then* $\alpha(\Gamma_1) = \Gamma_2$ *for some* $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^n})$ *if and only if there exists* $\ell_1 \in \mathrm{Aut}(\mathbb{Z}_{p^i}, T_1)$ *and* $\ell_j \in \mathrm{Aut}(\mathbb{Z}_p, T_j)$ *such that if* $(t_1, \ldots, t_n) = (\ell_{m-i+1}, \ell_{m-i}, \ldots, \ell_2, \ell_1, \ldots, \ell_1)$ *then for all* $1 \leq r, s \leq n$ *we have* $m_r t_r = m_s t_s$.

Proof: As γ is a genuine generalized multiplier, by Lemma 16

- For $1 \leq j \leq i$, $m_j \in \{1, \ldots, p-1\}$,
- For $1 \leq j \leq n-i$, $m_{i+j} \in \{1, \ldots, p^{j+1}-1\}$, and
- For $0 \leq j \leq n-i$, $m_{i+j} \equiv m_{i+j-1} \pmod{p^j}$.

Then for $1 \leq j \leq n-i$, there exists $u_{i+j} \equiv 1 \pmod{p}$ and $v_{i+j} \in \{1, \ldots, p-1\}$ such that $m_{i+j} = u_{i+j} v_{i+j}$. Let $\nu = (1, \ldots, 1, n_i, v_{i+1}, \ldots, v_n)$. Then ν is a genuine generalized multiplier, so if $v : \mathbb{Z}_p^n \mapsto \mathbb{Z}_{p^n}$ is given by $v(x) = \sum_{j=0}^{n-1} v_{n-j} x_j p^j$, then $v(\Gamma_1)$ is a circulant digraph isomorphic to Γ_1 and Γ_2. By Lemma 17, there exists $\alpha_1 \in \mathrm{Aut}(\mathbb{Z}_{p^n})$ such that $\alpha_1(\Gamma_1) = v(\Gamma)$. Additionally, Γ_1 and Γ_2 are isomorphic by an automorphism of $\mathbb{Z}_{p^n}$ if and

only if $\alpha_1(\Gamma_1)$ and Γ_2 are isomorphic by an automorphism of $\mathbb{Z}_{p^n}$. It thus suffices to verify the result provided that each $m_j \in \{1, \ldots, p-1\}$ and the result follows by Lemma 18. ∎

Definition 23

For a set $S \subseteq \mathbb{Z}_{p^k}$, we let $I(S)$ be the set of all $1 \leq m \leq p-1$ such that $mS = \{ms \pmod{p^k} : s \in S\} = S$, and for $S \subseteq \mathbb{Z}_{p^k}$ and $T \subseteq \mathbb{Z}_{p^j}$, we let $I(S) * I(T) = \langle S, T \rangle$ as a subgroup of $\mathbb{Z}_p^*$.

Theorem 6

Let p be a prime and $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ a circulant digraph. Then $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ is a CI-digraph of $\mathbb{Z}_{p^k}$ if and only if there exist a CI-digraph $\mathrm{Cay}(\mathbb{Z}_{p^i}, S_1)$, $i \leq k$, and $k-i$ circulant digraphs $\mathrm{Cay}(\mathbb{Z}_p, T_2), \ldots, \mathrm{Cay}(\mathbb{Z}_p, T_{k-i+1})$ such that

$$\mathrm{Cay}(\mathbb{Z}_{p^k}, S) \cong \mathrm{Cay}(\mathbb{Z}_{p^i}, S_1) \wr \mathrm{Cay}(\mathbb{Z}_p, T_2) \wr \ldots \wr \mathrm{Cay}(\mathbb{Z}_p, T_{k-i+1}),$$

and $I(T_\ell) * I(T_n) = \mathbb{Z}_p^*$ for every $1 \leq \ell < n \leq k-i+1$.

Proof: Suppose $I(T_\ell) * I(T_n) \neq \mathbb{Z}_p^*$ for $1 \leq \ell < n \leq k-i+1$. Let $r \in \mathbb{Z}_p^* - I(T_\ell) * I(T_n)$. If $\ell = 1$, then let $m_j = r$ for every $j > k-i-1$ and $m_j = 1$ for $1 \leq j \leq k-i+1$, while if $\ell \neq 1$, let $m_\ell = r$ and $m_j = 1$ for $j \neq \ell$. Then $(m_1, ..., m_\ell, ..., m_n)$ defines a genuine generalized multiplier and the image of $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ under $f_{(m_1,...,m_\ell,....,m_n)}$ is a circulant digraph by [19, Theorem 2.4]. By Corollary 5 there must be $t_\ell \in I(T_\ell)$ and $t_n \in I(T_n)$ such that $m_\ell t_\ell = m_n t_n$, in which case $t_\ell t_m^{-1} = r \in I(T_\ell) * I(T_m)$, a contradiction.

Conversely, let Γ_2 be any circulant digraph isomorphic to Γ_1. By Theorem 5 Γ_1 and Γ_2 are isomorphic by $f_{\mathbf{m}}$ for a genuine generalized multiplier $\mathbf{m} = (m_1, \ldots, m_n)$, where m_j is a positive integer. By Corollary 5 we have $\alpha(\Gamma_1) = \Gamma_2$ for some $\alpha \in \mathrm{Aut}(\mathbb{Z}_{p^k})$ if

and only if there exists $\ell_1 \in \mathrm{Aut}(\mathbb{Z}_{p^i}, T_1)$ and $\ell_j \in \mathrm{Aut}(\mathbb{Z}_p, T_j)$ such that if $(t_1, \ldots, t_n) = (\ell_{m-i+1}, \ell_{m-i}, \ldots, \ell_2, \ell_1, \ldots, \ell_1)$ then for all $1 \leq r, s \leq n$ we have $m_r t_r = m_s t_s$.

Let $p - 1 = \Pi_{j=1}^{r} q_j^{a_j}$ be the prime power decomposition of $p - 1$. As $\mathbb{Z}_p^*$ is cyclic and hence nilpotent, $\mathbb{Z}_p^* \cong \prod_{j=1}^{r} Q_j$ where the Q_j are cyclic Sylow q_j-subgroups of $\mathbb{Z}_p^*$, $1 \leq j \leq r$. As $I(T_x) * I(T_y) = \mathbb{Z}_p^*$ for every $1 \leq x < y < k - i$ we must have that $(Q_j \bigcap I(T_x)) * (Q_j \bigcap I(T_y)) = Q_j$ for every $1 \leq j \leq r$. Also, $(Q_j \bigcap I(T_x)) * (Q_j \bigcap I(T_y)) = Q_j$ if and only if $Q_j \bigcap I(T_x) = Q_j$ or $Q_j \bigcap I(T_y) = Q_j$ for each Q_j as Q_j cyclic of prime power order. Consequently, for each $1 \leq j \leq r$ there is at most one $1 \leq z_j \leq k - i + 1$ such that $Q_j \cap \mathrm{Aut}(\mathbb{Z}_p, T_{z_j}) \neq Q_j$.

Let $m_x = \prod_{j=1}^{r} m_{j,x}$, where $m_{j,x} \in Q_j$. Fix $1 \leq j \leq r$. If z_j exists, then let $t_{j,z_j} = m_{j,z_j}$, and otherwise, let $t_{j,z_j} = 1$. If $1 \leq y \leq n - i + 1$ and $y \neq z_j$, then $Q_j \cap \mathrm{Aut}(\mathbb{Z}_p, T_y) = Q_j$, and so there exists $\ell_{j,y} \in \mathrm{Aut}(\mathbb{Z}_p, T_y)$ such that $\ell_{j,y} m_{j,y} = m_{j,z_j}$. Setting $m = \prod_{j=1}^{r} m_{j,z_j}$ and $\ell_j = \prod_{j=1}^{r} \ell_{j,y}$, we have that $\ell_j m_j = m$ for all $1 \leq j \leq r$. ■

CHAPTER 8

CI-COLOR DIGRAPHS OF PRIME-POWER ORDER

A circulant color digraph Γ of order p^k is a CI-color digraph of $\mathbb{Z}_{p^k}$ if and only if there is one conjugacy class of regular cyclic subgroups in its automorphism group by Lemma 3. The preceding result gives conditions, which when appropriately reformulated, will determine which circulant color digraphs of order p^k are CI-color digraphs as $\mathrm{Aut}(\Gamma)$ is the automorphism group of a circulant digraph of order p^k by Corollary 2.

Definition 24

Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ be a circulant color digraph. Let I_j^c be the set of all $1 \leq m_j \leq p-1$ such that there exists a genuine generalized multiplier $m' = (m'_1, m'_2, \ldots, m'_k)$ with $f_{m'} \in \mathrm{Aut}(\Gamma)$ and $m'_j = m_j$.

Lemma 19

Let p be a prime and $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ a circulant color digraph. If Γ has primary key $\mathbf{k} = (0, 1, \ldots, i-1, \ldots, i-1)$ for some $i \leq k$, then there exists a color circulant digraph $\mathrm{Cay}(\mathbb{Z}_{p^k}, T)$, $T \subset \mathbb{Z}_{p^k}$, such that $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}, T))$.

Proof: Let H be the unique subgroup of $\mathbb{Z}_{p^k}$ of prime order p. The primary key $\mathbf{k}_j$ of $\mathrm{Cay}(\mathbb{Z}_{p^k}, S_j)$ is refined by $\mathbf{k}$, and so $S_j - H$ is a union of cosets of H, where $S_j \in S$. This implies that $\mathrm{Cay}(\mathbb{Z}_{p^k}, S_j) = \mathrm{Cay}(\mathbb{Z}_{p^{k-1}}, S_{j,1}) \wr \mathrm{Cay}(\mathbb{Z}_p, S_{j_2})$ for some $S_{j,1} \subseteq \mathbb{Z}_{p^{k-1}}$ and $S_{j,2} \subseteq \mathbb{Z}_p$.

If the cosets of H form an invariant partition of $\mathrm{Aut}(\Gamma)$, then $\mathrm{Aut}(\Gamma) = G_1 \wr G_2$ where $G_1 \leq S_{p^{k-1}}$ is 2-closed and $G_2 \leq S_p$ is 2-closed. Otherwise, let $\mathcal{B}$ be the invariant partition of $\mathrm{Aut}(\Gamma)$ with blocks of smallest size, p^ℓ with $\ell \geq 2$. Note that the cosets of H are a nontrivial refinement of $\mathcal{B}$. Additionally, $\mathrm{Stab}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})|_B$ is a doubly-transitive group with nonabelian simple socle by Lemma 9, $B \in \mathcal{B}$. Also, as $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^{k-1}}, S_{j,1})) \wr \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_p, S_{j_2})) \leq \mathrm{Aut}(\Gamma)$, we see that for each $B \in \mathcal{B}$ there exists $L_B \leq \mathrm{Stab}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})$ such that $L_B/\mathcal{B} = 1$, $L_B|_B$ is a doubly-transitive nonabelian almost simple group with socle T, and $L_B|_{B'} = 1$ if $B' \in \mathcal{B}$ and $B \neq B'$. This then implies that $\mathrm{Cay}(\mathbb{Z}_{p^k}, S_j) = \mathrm{Cay}(\mathbb{Z}_{p^\ell}, S_3) \wr \Delta$, where $S_3 \subseteq \mathbb{Z}_{p^{k-\ell}}$ and $\Delta = K_{p^\ell}$ or $\bar{K}_{p^\ell}$. As $S_j \in S$ was arbitrary, we conclude that $\mathrm{Aut}(\Gamma) = G_1 \wr S_{p^\ell}$ for some 2-closed $G_1 \leq S_{p^{k-\ell}}$. We have thus established that $\mathrm{Aut}(\Gamma) = G_1 \wr G_2$ where $G_1 \leq S_{p^{k-\ell}}$ is 2-closed and $G_2 \leq S_{p^\ell}$ is 2-closed and if $\ell \geq 2$, then $G_2 = S_{p^\ell}$. Also notice that as $\mathbf{k} = (0, 1, \ldots, i-1, i-1, \ldots, i-1)$ we have $\ell \leq i$.

Now let $S = \{S_j : 1 \leq j \leq r\}$ and let $\mathbf{k}_j = (k_{0,j}, k_{1,j}, \ldots, k_{k,j})$ be the primary key of $\mathrm{Cay}(\mathbb{Z}_{p^k}, S_j)$. As the primary key partition of $\mathbf{k}$ is a refinement of each $\mathbf{k}_j$, we see that $k_{x,j} \geq k_\ell$ for every $1 \leq x \leq k$ and $1 \leq j \leq r$. Thus $k_{x,j} = j - 1$ for all $x \leq i$. Also, as $\mathrm{Aut}(\Gamma) = G_1 \wr G_2$, each $\mathrm{Cay}(\mathbb{Z}_{p^k}, S_j)$ can be written as a wreath product $\Gamma_{1,j} \wr \Gamma_{2,j}$, where $\Gamma_{1,j}$ is a circulant digraph of order $p^{k-\ell}$ and $\Gamma_{2,j}$ is a circulant digraph of order p^ℓ. Notice that $\Gamma_{2,j}$ has key partition $(0, 1, \ldots, \ell - 1)$ and so by Lemma 14 it must be that the key partition of $\Gamma_{1,j}$ is $(k_{j,\ell} - \ell, \ldots, k_{j,\ell} - \ell)$ if $\ell < i$ and is $(0, 0, \ldots, 0)$ if $\ell = i$. Then the largest refinement of all of these key partitions is $(0, 1, \ldots, i-1-\ell, i-1-\ell, \ldots, i-1-\ell)$

if $i < \ell$ or $(0, 0, \ldots, 0)$ if $i = \ell$. We conclude that $\Gamma/\mathcal{B}$ has key partition $(0, \ldots, i-1-\ell, i-1-\ell, \ldots, i-1-\ell)$ or $(0, 0, \ldots, 0)$, and the induction hypothesis applies to $\Gamma/\mathcal{B}$.

We now argue inductively and get that there exists a 2-closed group G_1 that contains $(\mathbb{Z}_{p^{k-i}})_L$, and $G_j \leq S_{p^{a_j}}$ that is 2-closed and contains $(\mathbb{Z}_{p^{a_j}})_L$, $2 \leq j \leq r$ such that $\sum_{j=1}^{r} a_i = k - i$ and if $a_j \geq 2$ then $G_j = S_{p^{a_j}}$ and $\mathrm{Aut}(\Gamma) \cong G_1 \wr G_2 \wr \cdots \wr G_r$. By Lemma 2 $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}, S)) = \mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}, T))$ for some $T \subset \mathbb{Z}_{p^k}$. ∎

Corollary 6

Let p be a prime and $\Gamma = \mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ a circulant color digraph. Then Γ is a CI-color digraph of $\mathbb{Z}_{p^k}$ if and only if Γ has primary key $\mathbf{k} = (0, 1, \ldots, i-1, \ldots, i-1)$ for some $1 \leq i \leq k$ and $I_\ell^c * I_n^c = \mathbb{Z}_p^*$ for every $1 \leq \ell < n \leq i+1$.

Proof: Suppose that Γ has primary key $\mathbf{k} = (0, 1, \ldots, i-1, \ldots, i-1)$ for some $1 \leq i \leq k$. By Lemma 19 $\mathrm{Aut}(\Gamma)$ is isomorphic to the automorphism group of a circulant digraph $\mathrm{Cay}(\mathbb{Z}_{p^k}, T)$ for some $T \subset \mathbb{Z}_{p^k}$. Conversely, if Γ is a CI-color digraph then by Corollaries 1 and 2 $\mathrm{Aut}(\Gamma)$ is also isomorphic to the automorphism group of a circulant digraph $\mathrm{Cay}(\mathbb{Z}_{p^k}, T)$. By Lemma 3, we see that Γ is a CI-color digraph of $\mathbb{Z}_{p^k}$ if and only if $\mathrm{Cay}(\mathbb{Z}_{p^k}, T)$ is a CI-digraph of $\mathbb{Z}_{p^k}$. By Theorem 6, $\mathrm{Cay}(\mathbb{Z}_{p^k}, T)$ is a CI-digraph of $\mathbb{Z}_{p^k}$ if and only if there exist a CI-digraph $\mathrm{Cay}(\mathbb{Z}_{p^i}, U_1)$, $i \leq k$, and $k - i$ circulant digraphs $\mathrm{Cay}(\mathbb{Z}_p, U_2), \ldots, \mathrm{Cay}(\mathbb{Z}_p, U_{k-i+1})$ such that

$$\mathrm{Cay}(\mathbb{Z}_{p^k}, T) \cong \mathrm{Cay}(\mathbb{Z}_{p^i}, U_1) \wr \mathrm{Cay}(\mathbb{Z}_p, U_2) \wr \ldots \wr \mathrm{Cay}(\mathbb{Z}_p, U_{k-i+1}),$$

and $I(U_\ell) * I(U_n) = \mathbb{Z}_p^*$ for every $1 \leq \ell < n \leq k - i + 1$. Finally, observe that $y \in I(U_\ell)$, $\ell \leq i$ if and only if the generalized multiplier $m = (m_1, \ldots, m_k)$ with $m_\ell = y$ and $m_j = 1$

otherwise, while if $\ell \geq i+1$, then $m_\ell = y$ if $j \geq i+1$ and $m_\ell = 1$ if $j \leq i$. That is, $I(U_\ell) * I(U_n) = \mathbb{Z}_p^*$ if and only if $I_\ell^c * I_n^c = \mathbb{Z}_p^*$. Thus $\mathrm{Cay}(\mathbb{Z}_{p^k}, T)$ is a CI-digraph of $\mathbb{Z}_{p^k}$, and so $\mathrm{Cay}(\mathbb{Z}_{p^k}, S)$ is a CI-color digraph. This establishes that if Γ has primary key $(0, 1, \ldots, i-1, \ldots, i-1)$ and $I_\ell^c * I_n^c = \mathbb{Z}_p^*$ for every $1 \leq \ell < n \leq i+1$, then Γ is a CI-color digraph of $\mathbb{Z}_{p^k}$, as well as establishing that if Γ is a CI-color digraph of $\mathbb{Z}_{p^k}$ then $I_\ell^c * I_c^n = \mathbb{Z}_p^*$ for every $1 \leq \ell < n \leq i+1$. It only remains to show that if Γ is a CI-color digraph of $\mathbb{Z}_{p^k}$ then Γ has primary key $(0, 1, \ldots, i-1, \ldots, i-1)$. As $\mathrm{Aut}(\Gamma)$ is isomorphic to $\mathrm{Aut}(\mathrm{Cay}(\mathbb{Z}_{p^k}, T))$ as above, this follows by Lemma 4. ∎

Definition 25

Henceforth a primary key of the form $(0, 1, \ldots, i-1, i-1, \ldots, i-1)$ *for some* i *will be called a* **CI primary key with top** i.

CHAPTER 9

CIRCULANT CI-COLOR DIGRAPHS

We are now ready for the final terminology that will be needed for our solution to which circulant color digraphs are CI-color digraphs.

As $\mathbb{Z}_n$ may be written as a direct product $\Pi_{i=1}^{s}\mathbb{Z}_{p_i^{a_i}}$, where n has prime-power decomposition $n = p_1^{a_1}\cdots p_s^{k_s}$, there are **keys**, **key partitions**, and **generalized multipliers**, each of which is a direct product of primary keys, primary key partitions, and primary generalized multipliers corresponding to the prime-power decomposition of n. All such definitions are stated in the following definition.

Definition 26

Let n be a positive integer with prime-power decomposition $n = p_1^{a_1}\cdot p_2^{a_2}\cdots p_s^{a_s}$. Define the **key space** $\mathbf{K}_n$ *to be $\Pi_{i=1}^{s}\mathbf{K}(p_i^{a_i})$. That is, $\mathbf{K}_n$ is the direct product of primary keys. Similarly, if $\Sigma(\mathbf{k}_i)$ is a primary key partition of $\mathbb{Z}_{p_i^{a_i}}$, then a* **key partition of** $\mathbb{Z}_n$ *is $\Pi_{i=1}^{s}\Sigma(\mathbf{k}_i)$. Define a set of* **generalized multipliers**, *denoted $\mathbb{Z}_n^{**}$, as $\Pi_{i=1}^{s}\mathbb{Z}_{p_i^{a_i}}^{**}$. For each $\vec{m} = (\vec{m}_1, \vec{m}_2, \ldots, \vec{m}_s) \in \mathbb{Z}_n^{**}$, where each $\vec{m}_i \in \mathbb{Z}_{p_i^{a_i}}^{**}$, define a function $f_{\vec{m}} : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ by*

$$f_{\vec{m}}(x_1, \ldots, x_s) = (f_{\vec{m}_1}(x_1), f_{\vec{m}_2}(x_2), \ldots, f_{\vec{m}_s}(x_s)).$$

For a key $\mathbf{k} = (\mathbf{k}_1, \mathbf{k}_2, \ldots, \mathbf{k}_s)$ *where* $\mathbf{k}_i \in \mathbf{K}_{p_i^{a_i}}$ *is a primary key, define the set of all* **genuine generalized multipliers related to the key** $\mathbf{k}$, *denoted* $\mathbb{Z}_n^{**}(\mathbf{k})$, *to be* $\Pi_{i=1}^{s}\mathbb{Z}_{p_i^{a_i}}^{**}(\mathbf{k}_i)$. *Now let* Δ *be a partition of* $\mathbb{Z}_n$. *The partition for which* $\Sigma(\mathbf{k})$ *is the unique largest (in the sense of refinement) primary key partition that is a refinement of* Δ *is the* **key of** Δ *and denoted* $\mathbf{k}(\Delta)$. *Let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *be a circulant color digraph. The* **key of** $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is defined to be the key of the partition* $\{S_j \in S : 1 \leq j \leq r\}$. *Finally, let* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *have key* $\mathbf{k}$. *The* **solving set of** $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is defined to be the set* $P(\mathbf{k}) = \{f_{\vec{m}} : \vec{m} \in \mathbb{Z}_n^{**}(\mathbf{k})\}$.

The following result is Muzychuk's solution to the isomorphism problem for circulant color digraphs.

Theorem 7

Let n *be a positive integer,* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *circulant color digraphs with keys* $\mathbf{k}$ *and* $\mathbf{k}'$, *respectively. Then*

1. *if* $\mathbf{k} \neq \mathbf{k}'$, *then* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *is not isomorphic to* $\mathrm{Cay}(\mathbb{Z}_n, S')$,
2. *if* $\mathbf{k} = \mathbf{k}'$, *then the following are equivalent:*
   - *(a)* $\mathrm{Cay}(\mathbb{Z}_n, S)$ *and* $\mathrm{Cay}(\mathbb{Z}_n, S')$ *are isomorphic,*
   - *(b)* $f_{\vec{m}}(\mathrm{Cay}(\mathbb{Z}_n, S) = \mathrm{Cay}(\mathbb{Z}_n, S')$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$, *and*
   - *(c)* $f_{\vec{m}}(S) = S'$ *for some* $f_{\vec{m}} \in P(\mathbf{k})$.

Definition 27

Let $\Gamma = \mathrm{Cay}(\mathbb{Z}_n, S)$ *be a circulant color digraph and* $n = p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$ *the prime-power decomposition of* n. *Let* $m = (m_1, \ldots, m_s)$ *be a genuine generalized multiplier with* $m_i = (m_{i,1}, m_{i,2}, \ldots, m_{i,a_i})$. *For* $1 \leq i \leq s$ *and* $1 \leq j \leq a_i$, *let* $I_{i,j}^c$ *be the set of all* $1 \leq m'_{i,j} \leq p_i - 1$ *such that* $f_m \in \mathrm{Aut}(\Gamma)$ *with* $m_{i,j} = m'_{i,j}$.

Combining Theorem 7 with Corollary 6 we have the following characterization of circulant color digraphs that are CI-color digraphs.

Theorem 8

Let n be an integer with prime-power decompostion $n = p_1^{a_1} \cdots p_s^{a_s}$. A circulant color digraph $\mathrm{Cay}(\mathbb{Z}_n, S)$ with key $\mathbf{k} = (\mathbf{k}_1, \ldots, \mathbf{k}_s)$ is a CI-color digraph of $\mathbb{Z}_n$ if and only if each $\mathbf{k}_i$ is a CI-primary key with top j_i and for every $1 \leq i \leq s$ and $1 \leq j, \ell \leq j_i$ we have $I^c_{i,j} * I^c_{i,\ell} = \mathbb{Z}^*_{p_i}$.

REFERENCES

[1] A. Ádám, "Research Problem 2-10," *J. Combin. Theory*, vol. 2, 1967, p. 393.

[2] B. Alspach and T. D. Parsons, "Isomorphism of circulant graphs and digraphs," *Discrete Math.*, vol. 25, no. 2, 1979, pp. 97–108.

[3] L. Babai, "Isomorphism problem for a class of point-symmetric structures," *Acta Math. Acad. Sci. Hungar.*, vol. 29, no. 3-4, 1977, pp. 329–336.

[4] S. Bhoumik, E. Dobson, and J. Morris, "On the automorphism groups of almost all circulant graphs and digraphs," *Ars Math. Contemp.*, vol. 7, no. 2, 2014, pp. 487–506.

[5] P. J. Cameron, M. Giudici, G. A. Jones, W. M. Kantor, M. H. Klin, D. Marušič, and L. A. Nowitz, "Transitive permutation groups without semiregular subgroups," *J. London Math. Soc. (2)*, vol. 66, no. 2, 2002, pp. 325–333.

[6] J. D. Dixon and B. Mortimer, *Permutation groups*, vol. 163 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1996.

[7] E. Dobson, "Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$," *Discrete Math.*, vol. 147, no. 1-3, 1995, pp. 87–94.

[8] E. Dobson, "On isomorphisms of abelian Cayley objects of certain orders," *Discrete Math.*, vol. 266, no. 1-3, 2003, pp. 203–215, The 18th British Combinatorial Conference (Brighton, 2001).

[9] E. Dobson, "On groups of odd prime-power degree that contain a full cycle," *Discrete Math.*, vol. 299, no. 1-3, 2005, pp. 65–78.

[10] E. Dobson and J. Morris, "Automorphism groups of wreath product digraphs," *Electron. J. Combin.*, vol. 16, no. 1, 2009, pp. Research Paper 17, 30.

[11] E. Dobson and D. Witte, "Transitive permutation groups of prime-squared degree," *J. Algebraic Combin.*, vol. 16, no. 1, 2002, pp. 43–69.

[12] B. Elspas and J. Turner, "Graphs with circulant adjacency matrices," *J. Combinatorial Theory*, vol. 9, 1970, pp. 297–307.

[13] C. D. Godsil, "On Cayley graph isomorphisms," *Ars Combin.*, vol. 15, 1983, pp. 231–246.

[14] R. Jajcay and C. H. Li, "Constructions of self-complementary circulants with no multiplicative isomorphisms," *European J. Combin.*, vol. 22, no. 8, 2001, pp. 1093–1100.

[15] V. Liskovets and R. Pöschel, "Non-Cayley-isomorphic self-complementary circulant graphs," *J. Graph Theory*, vol. 34, no. 2, 2000, pp. 128–141.

[16] J. D. P. Meldrum, *Wreath products of groups and semigroups*, vol. 74 of *Pitman Monographs and Surveys in Pure and Applied Mathematics*, Longman, Harlow, 1995.

[17] M. Muzychuk, "Ádám's conjecture is true in the square-free case," *J. Combin. Theory Ser. A*, vol. 72, no. 1, 1995, pp. 118–134.

[18] M. Muzychuk, "On Ádám's conjecture for circulant graphs," *Discrete Math.*, vol. 176, no. 1-3, 1997, pp. 285–298.

[19] M. Muzychuk, "A solution of the isomorphism problem for circulant graphs," *Proc. London Math. Soc. (3)*, vol. 88, no. 1, 2004, pp. 1–41.

[20] J. Turner, "Point-symmetric graphs with a prime number of points," *J. Combinatorial Theory*, vol. 3, 1967, pp. 136–145.

[21] H. Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov. Academic Press, New York, 1964.

[22] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, lectures given at The Ohio State University, Columbus, Ohio, 1969.

[23] J. Xu, "Digraph representations of 2-closed permutation groups with a normal regular cyclic subgroup," *Electron. J. Combin.*, vol. 22, 2015.

[24] M.-Y. Xu, "Automorphism groups and isomorphisms of Cayley digraphs," *Discrete Math.*, vol. 182, no. 1-3, 1998, pp. 309–319, Graph theory (Lake Bled, 1995).