Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 7 (2014) 499–518

On the automorphism groups of almost all circulant graphs and digraphs*

Soumya Bhoumik
Department of Mathematics, Fort Hays State University
Hays, KS 67601, USA

Edward Dobson †
Department of Mathematics and Statisitics, Mississippi State University
Mississippi State, MS 39762 USA
and
UP IAM, University of Primorska
Muzejeski trg 2, 6000 Koper, Slovenia

Joy Morris
Department of Mathematics and Computer Science, University of Lethbridge
Lethbridge, AB T1K 3M4 Canada

Received 4 March 2012, accepted 18 June 2013, published online 6 October 2014

Abstract

We attempt to determine the structure of the automorphism group of a generic circulant graph. We first show that almost all circulant graphs have automorphism groups as small as possible. The second author has conjectured that almost all of the remaining circulant (di)graphs (those whose automorphism group is not as small as possible) are normal circulant (di)graphs. We show this conjecture is not true in general, but is true if we consider only those circulant (di)graphs whose order is in a "large" subset of integers. We note that all non-normal circulant (di)graphs can be classified into two natural classes (generalized wreath products, and deleted wreath type), and show that neither of these classes contains almost every non-normal circulant digraph.

Keywords: Circulant graph, automorphism group, Cayley graph, DRR, GRR.

Math. Subj. Class.: 05C25, 05E18

*This paper is a part of Bled'11 Special Issue.

†Project sponsored by the National Security Agency under Grant Number H98230-11-1-0179

E-mail addresses: s_bhoumik@fhsu.edu (Soumya Bhoumik), dobson@math.msstate.edu (Edward Dobson), joy.morris@uleth.ca (Joy Morris)

1 Introduction

We must begin by introducing Cayley (di)graphs and circulant (di)graphs.

Definition 1.1. Let G be a group and $S \subset G$ such that $1_G \notin S$. Define a digraph $\Gamma = \Gamma(G, S)$ by $V(\Gamma) = G$ and $E(\Gamma) = \{(u, v) : v^{-1}u \in S\}$. Such a digraph is a **Cayley digraph of G with connection set S**. A Cayley graph of G is defined analogously though we insist that $S = S^{-1} = \{s^{-1} : s \in S\}$. If $G = \mathbb{Z}_n$, then a Cayley (di)graph of G is a **circulant (di)graph of order n.**

It is straightforward to verify that for $g \in G$, the map $g_L : G \to G$ by $g_L(x) = gx$ is an automorphism of Γ. Thus $G_L = \{g_L : g \in G\}$, the left regular representation of G, is a subgroup of the automorphism group of Γ, $\mathrm{Aut}(\Gamma)$.

Determining the full automorphism group of a Cayley (di)graph is one of the most fundamental questions one can ask about a Cayley (di)graph. While it is usually quite difficult to determine the automorphism group of a Cayley (di)graph, characterizing almost all Cayley graphs of a group G, based on the structure of G, has been of consistent interest in the last few decades. Babai, Godsil, Imrich, and Lovász (see [2, Conjecture 2.1]) conjectured that almost all Cayley graphs of any group G that is not generalized dicyclic or abelian with exponent greater than 2 are GRRs (graphs that have automorphism group G_L). A similar conjecture (with no exceptions) was made for digraphs being DRRs (digraphs that have automorphism group G_L) by Babai and Godsil [2]. Babai and Godsil [2, Theorem 2.2] proved these two conjectures for nilpotent (and nonabelian in the case of undirected graphs) groups of odd order.

Definition 1.2 (Xu [15])**.** A **normal** Cayley (di)graph of the group G is a Cayley (di)graph $\Gamma = \Gamma(G, S)$ such that $G_L \lhd \mathrm{Aut}(\Gamma)$.

Xu also conjectured [15, Conjecture 1] that almost every Cayley (di)graph is normal. The precise formulation of Xu's conjecture is:

Conjecture 1.3 (Conjecture 1, [15])**.** *For any positive integer n, we let $\mathcal{F}_n$ denote the class of all groups of order n, and let*

$$f(n) = \min_{G \in \mathcal{F}_n} \frac{\#\text{ of normal Cayley digraphs of } G}{\#\text{ of Cayley digraphs of } G}.$$

Then $\lim_{n\to\infty} f(n) = 1$.

In 2010, the second author showed that almost all Cayley graphs of an abelian group G of odd prime-power order are normal [4].

Before proceeding farther, we specify what we will mean in this paper when we say something about "almost all" graphs in a particular family:

Definition 1.4. Let $F_2 \subseteq F_1$ be two families of circulant (di)graphs, and $F_i(n)$ $(i = 1, 2)$ be the graphs of order $n \in \mathbb{N}$ in F_i. Then by **almost all** circulant (di)graphs in F_1 are in F_2, we mean that

$$\lim_{n\in\mathbb{N}, n\to\infty} \frac{|F_2(n)|}{|F_1(n)|} = 1.$$

If in the above we replace $\mathbb{N}$ by some set I of infinitely many integers, we say that "almost all" circulant (di)graphs in F_1 **of order n, where $n \in I$**, are in F_2.

Our object in this paper is to determine as far as we can what the automorphism group of a generic circulant (di)graph should look like, by recursively classifying (or attempting to classify) the automorphism groups of almost all circulant (di)graphs that do not fall within a previous step's classification.

The following maps will be used in a number of places in this paper:

Definition 1.5. Let $\iota_G : G \to G$ be defined by $\iota_G(g) = g^{-1}$ for every $g \in G$. If $G \cong \mathbb{Z}_n$, we use ι_n instead of $\iota_{\mathbb{Z}_n}$.

Let $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\rho(i) = i + 1 \pmod n$. Thus $\langle \rho \rangle = (\mathbb{Z}_n)_L$.

Notice that if G is abelian then ι_G is an automorphism of every Cayley graph $\Gamma(G, S)$ since $S = S^{-1}$. Thus it is not possible for a Cayley graph on an abelian group G to be a GRR unless $G = \mathbb{Z}_2^k$, $k \geq 1$, while Imrich [7, Theorem] has shown that $\mathbb{Z}_2^k$ has a GRR if and only if $k \neq 2, 3, 4$. Nowitz showed [11] during the classification of GRRs that a Cayley graph on a generalized dicyclic group cannot be a GRR.

Definition 1.6. We say that a Cayley (di)graph $\Gamma = \Gamma(G, S)$ has automorphism group **as small as possible** if one of the following holds:

- Γ is a GRR or a DRR; or
- G is either abelian or generalized dicyclic, and $|\mathrm{Aut}(\Gamma)| = 2|G|$.

When $G = \mathbb{Z}_n$, we let $\mathrm{Small}(n)$ denote the set of all circulant graphs whose automorphism group is as small as possible, and $\mathrm{Small} = \cup_{n \in \mathbb{N}} \mathrm{Small}(n)$.

When G is abelian and $\mathrm{Aut}(\Gamma(G, S))$ is as small as possible, we have that $\mathrm{Aut}(\Gamma(G, S)) = \langle G_L, \iota_G \rangle$. Clearly ι_n normalizes $(\mathbb{Z}_n)_L$, so every member of Small will be a normal circulant graph. The first theorem in this paper, Theorem 3.2, shows that almost all circulant graphs are in Small, and thus are normal. This represents some progress towards the proof of Xu's conjecture, and is the first step in our determination of the structure of the automorphism group of a generic circulant graph. It is a natural extension of the work of Babai and Godsil, mentioned above [2, Theorem 2.2].

From there, we proceed to consider classifying the automorphism groups of circulant (di)graphs that are not DRRs. In [4, Conjecture 4.1], the second author conjectured that almost every Cayley (di)graph whose automorphism group is not as small as possible is a normal Cayley (di)graph. We show that this conjecture fails for circulant digraphs of order n, where $n \equiv 2 \pmod 4$ has a fixed number of distinct prime factors (Theorem 3.5), and point out some "gaps" in the proof of [4, Theorem 3.5], which lead to additional counterexamples to [4, Conjecture 4.1] for graphs in the case where $n = p$ or p^2 and p is a **safe prime**, i.e. $p = 2q + 1$ where q is prime, or when n is a power of 3 (Theorem 3.6). Finally, we prove that the conjecture holds for digraphs of order n where n is odd and not divisible by 9 (Theorem 3.7) and for graphs of order n, where n is odd, not a safe prime or the square of a safe prime and not divisible by 9 (Theorem 3.8).

In Section 4, we focus on non-normal circulant (di)graphs. A variety of authors (see [5, 6, 8, 9]) have shown that non-normal Cayley (di)graphs are either generalized wreath products (see Definition 2.5) or have the same automorphism group as a deleted wreath product (see Definition 2.14). We show in general, neither of these classes dominate.

In the next section, we will focus on background results and terminology, as well as developing the counting tools needed in Sections 3 and 4.

2 Preliminaries and tools

We start by stating basic definitions, and then proceed to known results in the literature that we will need. We will finish with results that will be the main tools throughout the rest of the paper.

Definition 2.1. Let G be a transitive permutation group with block system $\mathcal{B}$. By $G/\mathcal{B}$, we mean the subgroup of $S_{\mathcal{B}}$ induced by the action of G on $\mathcal{B}$, and by $\mathrm{fix}_G(\mathcal{B})$ the kernel of this action. Thus $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$ where $g/\mathcal{B}(B_1) = B_2$ if and only if $g(B_1) = B_2$, $B_1, B_2 \in \mathcal{B}$, and $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g(B) = B \text{ for all } B \in \mathcal{B}\}$.

Let G be a transitive permutation group, $\mathcal{B}$ a block system of G, and $\langle\rho\rangle \leq G$. Since $\langle\rho\rangle$ is transitive and abelian, it is regular [13, Proposition 4.4], and so there is a subgroup of $\langle\rho\rangle$ (namely $\mathrm{fix}_{\langle\rho\rangle}(\mathcal{B})$) whose orbits are precisely the blocks of $\mathcal{B}$. It is therefore not difficult to show that $\mathcal{B}$ consists of the cosets of some (cyclic) subgroup of $\mathbb{Z}_n$.

A **vertex-transitive (di)graph** is a (di)graph whose automorphism group acts transitively on the vertices of the (di)graph.

Definition 2.2. The **wreath (or lexicographic) product** of Γ_1 and Γ_2, denoted $\Gamma_1 \wr \Gamma_2$, is the digraph such that $V(\Gamma_1 \wr \Gamma_2) = V(\Gamma_1) \times V(\Gamma_2)$ and edge set

$$\{((x,x'),(y,y')) : xy \in E(\Gamma_1), x', y' \in V(\Gamma_2) \text{ or } x = y \text{ and } x'y' \in E(\Gamma_2)\}.$$

We remark that the wreath product of a circulant digraph of order m and a circulant digraph of order n is circulant. Note that what we have just defined as $\Gamma_1 \wr \Gamma_2$ is sometimes defined as $\Gamma_2 \wr \Gamma_1$, particularly in the work of Praeger, Li, and others from the University of Western Australia.

Definition 2.3. Let Ω be a set and $G \leq S_\Omega$ be transitive. Let G act on $\Omega \times \Omega$ by $g(\omega_1, \omega_2) = (g(\omega_1), g(\omega_2))$ for every $g \in G$ and $\omega_1, \omega_2 \in \Omega$. We define the **2-closure of G**, denoted $G^{(2)}$, to be the largest subgroup of S_Ω whose orbits on $\Omega \times \Omega$ are the same as G's. Let $\mathcal{O}_1, \ldots, \mathcal{O}_r$ be the orbits of G acting on $\Omega \times \Omega$. Define digraphs $\Gamma_1, \ldots, \Gamma_r$ by $V(\Gamma_i) = \Omega$ and $E(\Gamma_i) = \mathcal{O}_i$. Each Γ_i, $1 \leq i \leq r$, is an **orbital digraph of G**, and it is straightforward to show that $G^{(2)} = \cap_{i=1}^{r} \mathrm{Aut}(\Gamma_i)$. A **generalized orbital digraph of** G is an arc-disjoint union of orbital digraphs of G. We say G is **2-closed** if $G^{(2)} = G$.

Clearly the automorphism group of a graph or digraph is 2-closed.

The following theorem appears in [10] and is a translation of results that were proven in [6, 8, 9] using Schur rings, into group theoretic language. We have re-worded part (1) slightly to clarify the meaning. In the special case of circulant digraphs of square-free order n, an equivalent result was proven independently in [5].

Theorem 2.4. *Let $G \leq S_n$ contain $\langle\rho\rangle$. Then one of the following statements holds:*

1. *There exist $G_1, \ldots, G_r$ such that $G^{(2)} = G_1 \times \ldots \times G_r$, and for each G_i, either $G_i \cong S_{n_i}$, or G_i contains a normal regular cyclic group of order n_i. Furthermore, $r \geq 1$, $\gcd(n_i, n_j) = 1$ for $i \neq j$, and $n = n_1 n_2 \cdots n_r$.*
2. *G has a normal subgroup M whose orbits form the block system $\mathcal{B}$ of G such that each connected generalized orbital digraph contains a subdigraph Γ which is an orbital digraph of G and has the form $\Gamma = (\Gamma/\mathcal{B}) \wr \bar{K}_b$, where $b = |M \cap \langle\rho\rangle|$.*

Definition 2.5. A circulant digraph $\Gamma(\mathbb{Z}_n, S)$ is said to be a **(K, H)-generalized wreath circulant digraph** (or just a **generalized wreath circulant digraph**) if there exist groups H, K with $1 < K \leq H \leq \mathbb{Z}_n$ such that $S \setminus H$ is a union of cosets of K.

The name generalized wreath is chosen for these digraphs as if $K = H$, then Γ is in fact a wreath product. We now wish to investigate the relationship between generalized wreath circulant digraphs and the preceding result. We shall have need of the following lemma.

Lemma 2.6. *Let Γ be a disconnected generalized orbital digraph of a transitive group G. Then the components of Γ form a block system $\mathcal{B}$ of G.*

Proof. As the blocks of $G^{(2)}$ are identical to the blocks of G [12, Theorem 4.11] ([12] is contained in the more accessible [14]), we need to show that the set of components $\mathcal{B}$ of Γ is a block system of $G^{(2)}$. This is almost immediate as $G^{(2)} = \cap_{i=1}^{r}\mathrm{Aut}(\Gamma_i)$, where $\Gamma_1, \cdots, \Gamma_r$ are all of the orbital digraphs of G. Assume that $\Gamma = \cup_{i=1}^{s}\Gamma_i$, for some $s \leq r$. Then $\cap_{i=1}^{s}\mathrm{Aut}(\Gamma_i) \leq \mathrm{Aut}(\Gamma)$, so that $\mathcal{B}$ is a block system of $\cap_{i=1}^{s}\mathrm{Aut}(\Gamma_i)$. Also, $G \leq G^{(2)} = \cap_{i=1}^{r}\mathrm{Aut}(\Gamma_i) \leq \cap_{i=1}^{s}\mathrm{Aut}(\Gamma_i)$. Thus $\mathcal{B}$ is a block system of $G^{(2)}$ as $\mathcal{B}$ is a block system of $\cap_{i=1}^{s}\mathrm{Aut}(\Gamma_i)$. □

We will require the following partial order on block systems.

Definition 2.7. We say that $\mathcal{B} \preceq \mathcal{C}$ if for every $B \in \mathcal{B}$ there exists $C \in \mathcal{C}$ with $B \subseteq C$. That is, each block of $\mathcal{C}$ is a union of blocks of $\mathcal{B}$. For $g \in \mathrm{Stab}_G(C)$, $C \in \mathcal{C}$, we denote by $g|_C$ the permutation defined by $g|_C(x) = g(x)$ if $x \in C$ and $g|_C(x) = x$ otherwise. For $H \leq \mathrm{Stab}_G(C)$, we write $H|_C = \{g|_C : C \in \mathcal{C}\}$.

Our main tool in examining generalized wreath circulants will be the following result.

Lemma 2.8. *Let G be 2-closed with a normal subgroup M and a regular subgroup $\langle\rho\rangle$. Let $\mathcal{B}$ be the block system of G formed by the orbits of M, and suppose that each connected generalized orbital digraph contains a subdigraph Γ which is an orbital digraph of G and has the form $\Gamma = (\Gamma/\mathcal{B}) \wr \bar{K}_b$, where $b = |M \cap \langle\rho\rangle|$. Then there exists a block system $\mathcal{C} \succeq \mathcal{B}$ of G such that $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$.*

Proof. Observe that we may choose $M = \mathrm{fix}_G(\mathcal{B})$, in which case $|M \cap \langle\rho\rangle| = |B|$, where $B \in \mathcal{B}$, so that b is the size of a block of $\mathcal{B}$. First suppose that if $B, B' \in \mathcal{B}$, $B \neq B'$, then any orbital digraph Γ' that contains some edge of the form $x\vec{y}$ with $x \in B$, $y \in B'$ has every edge of the form $x\vec{y}$, with $x \in B$, $y \in B'$. It is then easy to see that every orbital digraph Γ of G can be written as a wreath product $\Gamma' = \Gamma_1 \wr \Gamma_2$, where Γ_1 is a circulant digraph of order n/b and Γ_2 is a circulant digraph of order b. Then $G/\mathcal{B} \wr \mathrm{fix}_G(\mathcal{B})|_B \leq \mathrm{Aut}(\Gamma')$ for every orbital digraph Γ', and so $G/\mathcal{B} \wr (\mathrm{fix}_G(\mathcal{B})|_B) \leq G^{(2)}$. Then result then follows with $\mathcal{C} = \mathcal{B}$. (Note that G is 2-closed, so $G^{(2)} = G$.)

Denote the orbital digraph that contains the edge $x\vec{y}$ by Γ_{xy}. We may now assume that there exists some $B, B' \in \mathcal{B}$, $B \neq B'$, and $x \in B$, $y \in B'$ such that Γ_{xy} does not have every edge of the form $x'\vec{y'}$, with $x' \in B$ and $y' \in B'$. Note then that no $\Gamma_{x'y'}$ with $x' \in B$ and $y' \in B'$ has every directed edge from B to B'. Let $\mathcal{X}$ be the set of all Γ_{xy} such that if $x \in B_1 \in \mathcal{B}$ and $y \in B_2 \in \mathcal{B}$, $B_1 \neq B_2$, then Γ_{xy} does not have every edge from B_1 to B_2. Let $\hat{\Gamma}$ be the generalized orbital digraph whose edges consist of all edges from every orbital digraph in $\mathcal{X}$, as well as every directed edge contained within a block of $\mathcal{B}$. Then no

orbital digraph that is a subgraph of $\hat{\Gamma}$ can be written as a connected wreath product $\Gamma' \wr \bar{K}_b$ for some Γ', and so by hypothesis, $\hat{\Gamma}$ must be disconnected.

By Lemma 2.6, the components of $\hat{\Gamma}$ form a block system $\mathcal{C} \succeq \mathcal{B}$ of G. (To see that $\mathcal{C} \succeq \mathcal{B}$, note that $\hat{\Gamma}$ contains every edge from B to B', so B is in a connected component of $\hat{\Gamma}$. Since G is transitive, $\mathcal{C} \succeq \mathcal{B}$.) Let $\Gamma_1, \Gamma_2, \ldots, \Gamma_r$ be the orbital digraphs of G, and assume that $\cup_{i=1}^{s} \Gamma_i = \hat{\Gamma}$. If $1 \leq i \leq s$, then $(G^{(2)}/\mathcal{C}) \wr (\mathrm{fix}_{G^{(2)}}(\mathcal{C})|_C) \leq \mathrm{Aut}(\Gamma_i)$; this is because $G^{(2)} \leq \mathrm{Aut}(\Gamma_i)$, Γ_i is disconnected, and each component is contained in a block of $\mathcal{C}$. Thus $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq \mathrm{Aut}(\Gamma_i)$ for every $1 \leq i \leq s$. If $s+1 \leq i \leq r$, then if $B, B' \in \mathcal{B}$, $B \neq B'$ and $\vec{xy} \in E(\Gamma_i)$ for some $x \in B$, $y \in B'$, then $\vec{xy} \in E(\Gamma_i)$ for every $x \in B$ and $y \in B'$. Also observe that as the subgraph of $\hat{\Gamma}$ induced by B is K_b, the subgraph of Γ_i induced by G is $\bar{K}_b$. We conclude that $\Gamma_i = \Gamma_i/\mathcal{B} \wr \bar{K}_b$, and so $\mathrm{Aut}(\Gamma_i/\mathcal{B}) \wr S_b \leq \mathrm{Aut}(\Gamma_i)$. Then $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_B \leq \mathrm{Aut}(\Gamma_i)$ for every $B \in \mathcal{B}$. As $\mathcal{B} \preceq \mathcal{C}$, $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq \mathrm{Aut}(\Gamma_i)$ for every $1 \leq i \leq r$ and as $G^{(2)} = \cap_{i=1}^{r} \mathrm{Aut}(\Gamma_i)$, $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$. □

Lemma 2.9. *Let Γ be a circulant digraph of order n. Then Γ is a (K, H)-generalized wreath circulant digraph if and only if there exists $G \leq \mathrm{Aut}(\Gamma)$ such that G contains a regular cyclic subgroup, and $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$, where $\mathcal{B} \preceq \mathcal{C}$ are formed by the orbits of K and H, respectively.*

Proof. Suppose first that $G \leq \mathrm{Aut}(\Gamma)$ with $\rho \in G$, and there exist block systems $\mathcal{B} \preceq \mathcal{C}$ of G such that $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq G^{(2)} \leq \mathrm{Aut}(\Gamma)$ for every $C \in \mathcal{C}$. Since $\rho \in G$, the action of $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C$ is transitive on every $B \subseteq C$, so between any two blocks $B_1, B_2 \in \mathcal{B}$ that are not contained in a block of $\mathcal{C}$, we have that there is either every edge from B_1 to B_2 or no edges from B_1 to B_2. Let $\mathcal{B}$ be formed by the orbits of $K \leq \langle \rho \rangle$. Then for every edge $\vec{xy}$ whose endpoints are not both contained within a block of $\mathcal{C}$, $(y - x) + K \subset S$. Let $\mathcal{C}$ be formed by the orbits of $H \leq \langle \rho \rangle$. Then $S \setminus H$ is a union of cosets of K as required.

Conversely, suppose that Γ is a (K, H)-generalized wreath circulant digraph. Then $\rho^m|_C \in \mathrm{Aut}(\Gamma)$ for every $C \in \mathcal{C}$, where $m = [\mathbb{Z}_n : K]$. Let $G \leq \mathrm{Aut}(\Gamma)$ be the maximal subgroup of $\mathrm{Aut}(\Gamma)$ that admits both $\mathcal{B}$ and $\mathcal{C}$ as block systems; clearly $\rho \in G$. Also, since $G^{(2)}$ has the same block systems as G and $G^{(2)} \leq \mathrm{Aut}(\Gamma)$, $G^{(2)} = G$. Now, if $g \in \mathrm{fix}_G(\mathcal{B})$, then $g|_C \in \mathrm{Aut}(\Gamma)$ as well. But this implies that $g|_C \in G$. □

Combining Lemma 2.8 and Lemma 2.9, and recalling that the full automorphism group of a (di)graph is always 2-closed, we have the following result.

Corollary 2.10. *Let Γ be a circulant digraph whose automorphism group $G = \mathrm{Aut}(\Gamma)$ satisfies Theorem 2.4(2). Then Γ is a generalized wreath circulant digraph.*

We now wish to count the number of generalized wreath circulant digraphs.

Lemma 2.11. *The total number of generalized wreath circulant digraphs of order n is at most*

$$\sum_{p|n} 2^{n/p-1} \left(\sum_{q|(n/p)} 2^{(n-n/p)/q} \right),$$

where p and q are prime.

Proof. Let Γ be a (K, H)-generalized wreath circulant digraph of order n. By Lemma 2.9, there exists $G \leq \mathrm{Aut}(\Gamma)$ that admits $\mathcal{B}$ and $\mathcal{C}$ such that $\rho \in G$, and $\mathrm{fix}_{G^{(2)}}(\mathcal{B})|_C \leq \mathrm{Aut}(\Gamma)$

for every $C \in \mathcal{C}$, where $\mathcal{B}$ is formed by the orbits of K and $\mathcal{C}$ is formed by the orbits of H. Let $\mathcal{B}$ consist of m blocks of size k. Then $\rho^m|_C \in \mathrm{Aut}(\Gamma)$ for every $C \in \mathcal{C}$. Choose $q|k$ to be prime, and let $G' \leq \mathrm{Aut}(\Gamma)$ be the largest subgroup of $\mathrm{Aut}(\Gamma)$ that admits a block system $\mathcal{D}$ consisting of n/q blocks of size q. Note then that $\rho^{n/q}|_C \in G'$ for every $C \in \mathcal{C}$. Let p be a prime divisor of the number of blocks of $\mathcal{C}$, and $\mathcal{E}$ the block system of $\langle\rho\rangle$ consisting of p blocks of size n/p. Then $\mathcal{C} \preceq \mathcal{E}$ and $\rho^{n/q}|_E \in G'$ for every $E \in \mathcal{E}$. Thus every (K, H)-generalized wreath circulant digraph is a (L_q, M_p)-generalized wreath circulant digraph, where L_q has prime order q where q divides $|K|$ and M_p has order n/p where p divides $n/|H|$. Note that there is a unique subgroup of $\mathbb{Z}_n$ of prime order q for each $q|n$, and that M_p is also the unique subgroup of $\mathbb{Z}_n$ of order n/p.

As $|L_q| = q$, we use the definition of an (L_q, M_p)-generalized wreath circulant digraph to conclude that $S \setminus M_p$ is a union of some subset of the $(n - n/p)/q$ cosets of L_q that are not in M_p. Thus there are $2^{(n-n/p)/q}$ possible choices for the elements of S not in M_p. As there are at most $2^{n/p-1}$ choices for the elements of S contained in M_p, there are at most $2^{n/p-1} \cdot 2^{(n-n/p)/q} = 2^{n/p+n/q-n/(pq)-1}$ choices for S. Summing over every possible choice of q and then p, we see that the number of generalized wreath digraphs is bounded above by

$$\sum_{p|n} 2^{n/p-1} \left(\sum_{q|(n/p)} 2^{(n-n/p)/q} \right).$$

□

We will denote the set of all circulant digraphs of order n whose automorphism groups are of generalized wreath type by $\mathrm{GW}(n)$. The corresponding set of all circulant graphs will be denoted by $\mathrm{GWG}(n)$. Note that no term in the previous summation given in Lemma 2.11 is larger than $2^{n/p+n/q-n/(pq)-1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of n/q. As the number of prime divisors of n is at most $\log_2 n$, we have the following result.

Corollary 2.12. *Let q be the smallest prime dividing n, and p the smallest prime prime dividing n/q. Then*

$$|\mathrm{GW}(n)| \leq (\log_2^2 n) 2^{n/p+n/q-n/pq-1}.$$

Using the fact that there are at most two elements that are self-inverse in $\mathbb{Z}_n$ (namely 0 and $n/2$ if n is even, and $0 \notin S$), and at most one coset of $\mathbb{Z}_n/L_q$ that is self-inverse and not in M_p (as $\mathbb{Z}_n/L_q$ is cyclic), and the fact that $(p+q-1)/pq \leq 3/4$, a similar argument shows that:

Corollary 2.13. *Let q be the smallest prime dividing n, and p the smallest prime prime dividing n/q. Then*

$$|\mathrm{GWG}(n)| \leq (\log_2^2 n) 2^{n(p+q-1)/(2pq)+1/2} \leq (\log_2^2 n) 2^{3n/8+1/2}.$$

We now consider circulant (di)graphs Γ for which $\mathrm{Aut}(\Gamma)$ satisfies Theorem 2.4 (1), and use the notation of that result. If no $G_i \cong S_{n_i}$ with $n_i \geq 4$, then $\mathrm{Aut}(\Gamma)$ contains a normal regular cyclic group and Γ is a normal circulant digraph. Otherwise, we have the following definition.

Definition 2.14. A circulant (di)graph $\Gamma(\mathbb{Z}_n, S)$ is of **deleted wreath type** if there exists some $m > 1$ such that:

- $m \mid n$;
- $\gcd(m, n/m) = 1$; and
- if $H = \langle n/m \rangle$ is the unique subgroup of order m in G, then $S \cap H \in \{\emptyset, H \setminus \{0\}\}$, and for every $g \in \langle m \rangle \setminus \{0\}$, $S \cap (g+H) \in \{\emptyset, \{g\}, (g+H) \setminus \{g\}, g+H\}$. (Notice that because $\gcd(m, n/m) = 1$, the group $\langle m \rangle$ contains precisely one representative of each coset of H in G.)

A circulant digraph is said to be of **strictly deleted wreath type** if it is of deleted wreath type and is not a generalized wreath circulant.

There are deleted wreath type circulants which are not of strictly deleted wreath type. For an example of this, consider a circulant digraph on pqm vertices where $m \geq 4$ and p, q and m are relatively prime, whose connection set is $S = (\langle pq \rangle \setminus \{0\}) \cup (m + \langle mq \rangle)$. This digraph is an (H, K)-generalized wreath circulant for $H = \langle q \rangle$ and $K = \langle mq \rangle$. It is also of deleted wreath type with $H = \langle pq \rangle$, since $S \cap H = H \setminus \{0\}$, while for $g \in \langle m \rangle \setminus \{0\}$, we have $S \cap (g + H) = \{g\}$ if $g \in m + \langle mq \rangle$ and $S \cap (g + H) = \emptyset$ otherwise.

Definition 2.15. For a positive integer m, and a digraph Γ, we denote by $m\Gamma$ the digraph consisting of m vertex-disjoint copies of Γ. The digraph $\Gamma \wr \bar{K}_m - m\Gamma$ is a **deleted wreath product**. Thus this digraph is the digraph whose vertex set is the vertex set of $\Gamma \wr \bar{K}_m$ and whose edge set is the edge set of $\Gamma \wr \bar{K}_m$ with the edges of $m\Gamma$ removed.

The name deleted wreath type is chosen as these digraphs have automorphism groups that are isomorphic to the automorphism groups of deleted wreath products.

Lemma 2.16. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$, and let $m \geq 4$ be a divisor of n such that $\gcd(m, n/m) = 1$. Then Γ is of deleted wreath type with m being the divisor of n that satisfies the conditions of that definition, if and only if $\mathrm{Aut}(\Gamma)$ contains a subgroup isomorphic to $H \times S_m$ with the canonical action, for some 2-closed group H with $\mathbb{Z}_{n/m} \leq H \leq S_{n/m}$.*

Proof. In this proof for a given m satisfying $n = km$ and $\gcd(m, k) = 1$, it will be convenient to consider $\mathbb{Z}_n = \mathbb{Z}_k \times \mathbb{Z}_m$ in the obvious fashion. For $i \in \mathbb{Z}_k$, set $B_i = \{(i, j) : j \in \mathbb{Z}_m\}$.

First, suppose Γ is of deleted wreath type with $m \geq 4$ being the divisor of n that satisfies the conditions of that definition, and $n = mk$. Using $\mathbb{Z}_n = \mathbb{Z}_k \times \mathbb{Z}_m$, we see that for every $i \in \mathbb{Z}_k \setminus \{0\}$, we have $S \cap B_i \in \{\emptyset, \{(i, 0)\}, B_i \setminus \{(i, 0)\}, B_i\}$. Also, $S \cap B_0 \in \{\emptyset, B_0 \setminus \{(0, 0)\}\}$. Let $\mathcal{B} = \{B_i : i \in \mathbb{Z}_k\}$ and let $G \leq \mathrm{Aut}(\Gamma)$ be maximal such that G admits $\mathcal{B}$ as a block system. Let $H \leq S_k$ be the projection of G onto the first coordinate. Since $\mathbb{Z}_k \times \mathbb{Z}_m \cong \langle \rho \rangle \leq G$, clearly $\mathbb{Z}_k \leq H$.

We claim that $H \times S_m \leq \mathrm{Aut}(\Gamma)$. Let $((i_1, j_1), (i_2, j_2)) \in E(\Gamma)$, and $(h, g) \in H \times S_m$. Suppose first that $i_1 = i_2$. We have $S \cap B_0 \in \{\emptyset, B_0 \setminus \{(0, 0)\}\}$, and $i_1 = i_2$ forces $S \cap B_0 \neq \emptyset$. Hence $\Gamma[B_i]$ is complete, so clearly $((h(i_1), g(j_1)), (h(i_2), g(j_2))) \in E(\Gamma)$, as $h(i_2) = h(i_1)$. Now suppose $i_1 \neq i_2$. So $h(i_1) \neq h(i_2)$. Let $i = i_2 - i_1$ and let $i' = h(i_2) - h(i_1)$, with $1 \leq i, i' \leq k - 1$. By the definition of H, there is some $g \in G$ that takes B_{i_1} to $B_{h(i_1)}$ and B_{i_2} to $B_{h(i_2)}$. Hence the number of arcs in Γ from B_{i_1} to B_{i_2}, which is $|S \cap B_i|$, must be the same as the number of arcs from $B_{h(i_1)}$ to $B_{h(i_2)}$, which is $|S \cap B_{i'}|$. Since $1 \leq i, i' \leq k - 1$ and $(i_1, j_1), (i_2, j_2) \in E(\Gamma)$, $|S \cap B_i| = |S \cap B_{i'}|$ must be $1, m - 1$ or m. Since $m \geq 4 > 2$, the integers $1, m - 1$ and m are all distinct, so $S \cap B_i$ and $S \cap B_{i'}$ are uniquely determined by their cardinality. If $|S \cap B_i| = 1$, then

$S \cap B_i = \{(i,0)\}$ and $j_2 = j_1$. Hence $g(j_1) = g(j_2)$, and since $S \cap B_{i'} = \{(i',0)\}$, the arc $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is in Γ. Similarly, if the cardinality is $m-1$, then $S \cap B_i = \{B_i \setminus \{(i,0)\}\}$ so $j_2 \neq j_1$. Hence $g(j_1) \neq g(j_2)$, and since $S \cap B_{i'} = \{B_{i'} \setminus \{(i',0)\}\}$, the arc $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is in Γ. Finally, if the cardinality is m, then $S \cap B_i = B_i$, and $S \cap B_{i'} = B_{i'}$, so the arc $((h(i_1), g(j_1)), (h(i_2), g(j_2)))$ is in Γ. Thus $H \times S_m \leq \mathrm{Aut}(\Gamma)$.

By [12, Theorem 4.11], we have that $(H \times S_m)^{(2)}$ admits $\mathcal{B}$ as $H \times S_m \leq \mathrm{Aut}(\Gamma)$ does. Finally, by [3, Theorem 5.1], $\mathrm{Aut}(\Gamma) \geq (H \times S_m)^{(2)} \geq H^{(2)} \times S_m$. As H is the projection of G onto the first coordinate, we conclude that $H^{(2)} = H$ and H is 2-closed.

Conversely, assume that $\mathrm{Aut}(\Gamma)$ contains a subgroup isomorphic to $H \times S_m$ with the canonical action, for some 2-closed group H with $\mathbb{Z}_{n/m} \leq H \leq S_{n/m}$. Clearly $\mathrm{Stab}_{1\times S_m}(0,0)$ is transitive on $B_i \setminus \{(i,0)\}$, and so the orbits of $\mathrm{Stab}_{1\times S_m}(0,0)$ on B_i are $\{(i,0)\}$ and $B_i \setminus \{(i,0)\}$. Also $1 \times S_m \leq H \times S_m \leq \mathrm{Aut}(\Gamma)$ implies $\mathrm{Stab}_{1\times S_m}(0,0) \leq \mathrm{Stab}_{H\times S_m}(0,0) \leq \mathrm{Stab}_{\mathrm{Aut}(\Gamma)}(0,0)$. Thus each $S \cap B_i$ is a union of some (possibly none) of these two orbits. Hence the only possibilities for each $S \cap B_i$ are $\emptyset, \{(i,0)\}, B_i \setminus \{(i,0)\}$ and B_i if $1 \leq i \leq k-1$; and since $0 \notin S$, $S \cap B_0$ is either $\emptyset$ or $B_0 \setminus \{(0,0)\}$. □

We remark that the above lemma shows that a deleted wreath product type circulant digraph is not a normal circulant digraph when $m \geq 4$.

The following result is an easy consequence of Lemma 2.16 together with the fact that the 2-closure of a direct product is the direct product of the 2-closures of the factors [3, Theorem 5.1].

Corollary 2.17. *A non-normal circulant (di)graph whose automorphism group satisfies the conclusion of Theorem 2.4(1) is of deleted wreath type with $m \geq 4$.*

Corollary 2.18. *There are at most $2^{n/m+1}$ graphs Γ and at most $2^{2n/m}$ digraphs Γ that contain $K \times S_m$ for any choice of K that is 2-closed and has $\mathbb{Z}_{n/m} \leq K \leq S_{n/m}$, where $m \geq 4$. Equivalently, there are at most $2^{2n/m}$ digraphs of deleted wreath type, and at most $2^{n/m+1}$ graphs of deleted wreath type, for any fixed $m \geq 4$ with $m \mid n$ and $\gcd(m, n/m) = 1$.*

Proof. A consequence of Lemma 2.16 is that there are $2 \cdot 4^{n/m-1} < 4^{n/m} = 2^{2n/m}$ digraphs Γ of order n such that $K \times S_m \leq \mathrm{Aut}(\Gamma)$ for $m \geq 4$. Note that a digraph Γ with $\mathrm{Aut}(\Gamma) = K \times S_m$, $m \geq 3$, is a graph if and only if K contains the map $\iota_{n/m}$. Then $\iota_{n/m}(g + H) = (-g) + H$ where $H = \langle n/m \rangle$, and so if n/m is odd, there are at most $4^{n/(2m)} = 2^{n/m}$ graphs Γ that contain $K \times S_m$ for any choice of K that is 2-closed and has $\mathbb{Z}_{n/m} \leq K \leq S_{n/m}$. Even if n/m is even, only one nontrivial coset of $\langle n/m \rangle$ is fixed by $\iota_{n/m}$, so there are at most $2 \cdot 4 \cdot 4^{(n/m-2)/2} = 2^{n/m+1}$ graphs Γ that contain $K \times S_m$ for any choice of K that is 2-closed and has $\mathbb{Z}_{n/m} \leq K \leq S_{n/m}$. □

3 Normal circulants

In this section our main focus is on determining whether or not almost all circulants that do not have automorphism groups as small as possible are normal circulants, as conjectured by the second author [4, Conjecture 1]. We begin by showing that almost every circulant graph of order n has automorphism group as small as possible. We remark that Babai and Godsil [2, Theorem 5.3] have shown this to be true for Cayley graphs on abelian groups of order n, where $n \equiv 3 \pmod 4$.

We require some additional notation that will be used through the remainder of this paper.

Definition 3.1. Let $\mathrm{ACG}(n)$ be the set of all circulant graphs of order n.

Throughout this paper $\mathbb{Z}_n^*$ denotes the group of units (invertible elements) of $\mathbb{Z}_n$. For $a \in \mathbb{Z}_n^*$, we define $\bar{a} : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\bar{a}(i) = ai$. As previously defined, if $a = -1$ then we denote $\bar{a}$ by ι_n. Finally, by $|g|$ we denote the order of any element g in any group G.

Theorem 3.2. *For almost every circulant graph* Γ, $\mathrm{Aut}(\Gamma)$ *is as small as possible. More precisely,*

$$\lim_{n\to\infty} \frac{|\mathrm{Small}(n)|}{|\mathrm{ACG}(n)|} = 1.$$

Proof. We first count the number of circulant graphs of order n not in $\mathrm{Small}(n)$. By Corollary 2.13, there are at most $\log_2^2 n \cdot 2^{3n/8+1/2}$ generalized wreath circulant graphs of order n.

Now assume $\Gamma \notin \mathrm{GWG}(n) \cup \mathrm{Small}(n)$. By Corollary 2.10, $\mathrm{Aut}(\Gamma)$ satisfies Theorem 2.4(1). Either $\mathrm{Aut}(\Gamma)$ normalizes $\langle\rho\rangle$ or $G_i = S_{n_i}$ for some $n_i \geq 4$ (using the notation of Theorem 2.4(1)). We will find an automorphism α of $\mathbb{Z}_n$ such that $\alpha \in \mathrm{Aut}(\Gamma) \setminus \langle\iota_n\rangle$. Obviously, if $\langle\rho\rangle \triangleleft \mathrm{Aut}(\Gamma)$, then since $\Gamma \notin \mathrm{Small}(n)$, such an α exists. If $G_i = S_{n_i}$ and $n_i \geq 4$, then G_i contains a nontrivial automorphism $\bar{b}$ of $\mathbb{Z}_{n_i}$. Regard $\mathbb{Z}_n$ as $\mathbb{Z}_{n/n_i} \times \mathbb{Z}_{n_i}$ in the usual way. If $n_i \geq 7$ then we may choose $b \neq \pm 1$, and $\alpha = \overline{(1, b)}$. We may assume n is arbitrarily large, so if $4 \leq n_i < 7$ we may assume $n/n_i \geq 3$, and let $\alpha = \overline{(-1, 1)}$. Thus there exists $\alpha \in \mathrm{Aut}(\mathbb{Z}_n) \cap \mathrm{Aut}(\Gamma)$ but not in $\langle\iota_n\rangle$.

Now observe that ι_n has at most two fixed points, and so has at most $(n-2)/2 + 2$ orbits. Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$ be such that $\alpha \notin \langle\iota_n\rangle$. Observe that we may divide the orbits of $\langle\iota_n, \alpha\rangle$ into three types: singleton orbits, orbits of length 2, and orbits of length greater than 2. As $\langle\iota_n\rangle$ has at most 2 singleton orbits, $\langle\iota_n, \alpha\rangle$ has at most two singleton orbits, namely 0 and $n/2$. If $x \neq 0, n/2$, then x is contained in an orbit of $\langle\iota_n\rangle$ of length 2. If such an x is contained in an orbit of $\langle\iota_n, \alpha\rangle$ of length 2, then setting $\alpha = \bar{a}$, $a \in \mathbb{Z}_n^*$, we have that $\{x, -x\} = \{ax, -ax\}$, in which case either $x = ax$ and x is a fixed point of α, or $x = -ax$ and x is a fixed point of $\iota_n\alpha$. If $x = ax$ set $\beta = \alpha$ and if $x = -ax$, set $\beta = \iota_n\alpha$. Then $\langle\iota_n, \alpha\rangle = \langle\iota_n, \beta\rangle$, and x is a fixed point of β. It is easy to see that the set of fixed points of β, say $H(\beta)$, forms a subgroup of $\mathbb{Z}_n$, and so $|H(\beta)| \leq n/2$. Thus $\langle\iota_n, \alpha\rangle$ has at at most $(n/2-1)/2$ orbits of length two, and so at most $(n/2-1)/2+2$ orbits of length one or two. Every remaining orbit of $\langle\iota_n, \alpha\rangle$ is a union of orbits of $\langle\iota_n\rangle$ of size 2, and so every remaining orbit of $\langle\iota_n, \alpha\rangle$ has length at least 4. Clearly, the number of orbits of $\langle\iota_n, \alpha\rangle$ is maximized if it has 2 orbits of length 1, $(n/2-1)/2$ orbits of length 2, and the remainder have length greater than 2. In this case, there will be at most $(n/2-1)/4 = n/8 - 1/4$ orbits of length greater than 2. We conclude that there are at most $3n/8 + 5/4$ orbits of $\langle\iota_n, \alpha\rangle$, and as S must be a union of orbits of $\langle\iota_n, \alpha\rangle$ not including $\{0\}$, there are at most $2^{3n/8+1/4}$ such circulant graphs for each $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, $\alpha \notin \langle\iota_n\rangle$. As there are at most n (actually $\varphi(n)$ of course) automorphisms of $\mathbb{Z}_n$, there are at most $n \cdot 2^{3n/8+1/4}$ circulant graphs that contain an automorphism of $\mathbb{Z}_n$ other than ι_n.

We have shown that there are at most $n \cdot 2^{3n/8+1/4} + \log_2^2 n \cdot 2^{3n/8+1/2} < \sqrt{2}(n + \log_2^2 n)2^{3n/8}$ circulant graphs of order n that are not in $\mathrm{Small}(n)$. As there are $2^{(n-2)/2+1} = 2^{n/2}$ circulant graphs of order n if n is even and $2^{(n-1)/2}$ circulant graphs

of order n if n is odd,

$$\lim_{n\to\infty} \frac{|\mathrm{Small}(n)|}{|\mathrm{ACG}(n)|} \geq 1 - \lim_{n\to\infty} \frac{\sqrt{2}(n+\log_2^2 n)2^{3n/8}}{2^{(n-1)/2}} = 1.$$

□

The above theorem clearly shows that almost all circulant graphs are normal. In 2010, the second author made the following conjecture for Cayley (di)graphs (not necessarily circulant) whose automorphism group is not as small as possible [4, Conjecture 1].

Conjecture 3.3. *Almost every Cayley (di)graph whose automorphism group is not as small as possible is a normal Cayley (di)graph.*

It is difficult to determine the automorphism group of a (di)graph, so the main way to obtain examples of vertex-transitive graphs is to construct them. An obvious construction is that of a Cayley (di)graph, and the conjecture of Imrich, Lovász, Babai, and Godsil says that when performing this construction, additional automorphisms are almost never obtained. The obvious way of constructing a Cayley (di)graph of G that does not have automorphism group as small as possible is to choose an automorphism α of G and make the connection set a union of orbits of α. The above conjecture in some sense says that this construction almost never yields additional automorphisms other than the ones given by the construction.

Throughout the remainder of this paper, all circulant digraphs of order n whose automorphism groups are of deleted wreath, and strictly deleted wreath types will be denoted by $\mathrm{DW}(n)$, and $\mathrm{SDW}(n)$ respectively. The corresponding set of all graphs whose automorphism groups are of deleted wreath type will be denoted by $\mathrm{DWG}(n)$. If we wish to consider a subset of one of these sets with a restriction on m, we indicate this in a subscript, as for example $\mathrm{DW}(n)_{m\geq 4}$. Also, the sets of all digraphs that are circulants, DRR circulants, normal circulants, and non-normal circulants of order n will be denoted as $\mathrm{ACD}(n), \mathrm{DRR}(n), \mathrm{Nor}(n)$ and $\mathrm{NonNor}(n)$, respectively. The corresponding sets of all graphs that are circulants, normal circulants, and nonnormal circulants, will be denoted by $\mathrm{ACG}(n)$, $\mathrm{NorG}(n)$, and $\mathrm{NonNorG}(n)$, respectively.

The following lemma will prove useful in determining how many circulant (di)graphs are not normal.

Lemma 3.4. *If a circulant digraph Γ of composite order n that is a (K, H)-generalized wreath circulant digraph is normal, then $4 \mid n$.*

Proof. Without loss of generality we may assume that K is of prime order p. Let $\mathcal{B}$ be the block system of $\langle\rho\rangle$ formed by the orbits of $\langle\rho^m\rangle$, where $|H| = n/m$. Then $\rho^{n/p}|_B \in \mathrm{Aut}(\Gamma)$ for every $B \in \mathcal{B}$. Set $G = \langle\rho, \rho^{n/p}|_B : B \in \mathcal{B}\rangle$, and let $\mathcal{C}$ be the block system of G formed by the orbits of $\langle\rho^{n/p}\rangle$, so that $\mathrm{fix}_G(\mathcal{C}) = \langle\rho^{n/p}|_B : B \in \mathcal{B}\rangle$, and has order $p^{n/m}$. Then $\mathcal{C}$ is also a block system of $N(n)$, where $N(n) = \{x \to ax + b : a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$. Let $n = p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}$ be the prime power decomposition of n. As $N(n) = \Pi_{i=1}^r N(p_i^{a_i})$, we see that a Sylow p-subgroup of $\mathrm{fix}_{N(n)}(\mathcal{C})$ is a Sylow p-subgroup of $1_{S_{n/p^a}} \times N(p^a)$, where $p = p_j$ and $a = a_j$ for some j. Let $\mathcal{E}$ be the block system of $N(p^a)$ consisting of blocks of size p. Then a Sylow p-subgroup of $\mathrm{fix}_{N(p^a)}(\mathcal{E})$ has order at most p^2 as a Sylow p-subgroup of $N(p^a)$ is metacyclic. If $\Gamma \in \mathrm{Nor}(n)$, then $\langle\rho\rangle \triangleleft G$ since $G \leq \mathrm{Aut}(\Gamma)$, so $G \leq N(n)$. This implies that a Sylow p-subgroup of $\mathrm{fix}_G(\mathcal{C})$ has order at most p^2, and

so $p^{n/m} \leq p^2$. Since $H > 1$ we have $n > m$, so this forces $n = 2m$, and $\mathcal{B}$ consists of 2 blocks. Finally, let $\delta = \rho^{n/p}|_B$, where $B \in \mathcal{B}$ with $0 \in B$. If $\Gamma \in \mathrm{Nor}(n)$, then $\gamma = \rho^{-1}\delta^{-1}\rho\delta \in \langle\rho\rangle$, and straightforward computations will show that $\gamma(i) = i + n/p$ if i is even, while $\gamma(i) = i - n/p$ if i is odd. As $\gamma \in \langle\rho\rangle$, we must have that $n/p \equiv -n/p \pmod{n}$, and so $2n/p \equiv 0 \pmod{n}$. This then implies that $p = 2$ and so $4|n$ as required. □

We first show that Conjecture 3.3 is false for circulant digraphs of order n, where $n \equiv 2 \pmod 4$ has a fixed number of distinct prime factors.

Theorem 3.5. *Let $n = 2p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, where the p_i are distinct odd primes and r is fixed. Then*

$$\lim_{n\to\infty, r \text{ fixed}} \frac{|\mathrm{NonNor}(n)|}{|\mathrm{Nor}(n)\backslash\mathrm{DRR}(n)|} \geq \frac{1}{2(2^r-1)}.$$

Proof. By Lemma 3.4, we have that $|\mathrm{NonNor}(n)| \geq |\mathrm{GW}(n)|$. We claim that $|\mathrm{GW}(n)| \geq 2^{n/2+n/(2p)-1}$, where $1 \neq p$ is the smallest divisor of $n/2$. To see this, we construct this number of distinct generalized wreath circulant digraphs of order n, as follows: $\mathcal{B}$ will be the block system formed by the orbits (cosets) of $\langle n/2\rangle$, and $\mathcal{C}$ the block system formed by the orbits (cosets) of $\langle p\rangle$. Since there are n/p elements in each block of $\mathcal{C}$, there are $2^{n/p-1}$ choices for $S \cap C_0$, where C_0 is the block of $\mathcal{C}$ that contains 0. Since there are $n/2 - n/(2p)$ orbits (cosets) of $\langle n/2\rangle$ that are not in C_0, there are $2^{n/2-n/(2p)}$ choices for $S - C_0$ that create a generalized circulant digraph with this choice of $\mathcal{B}$ and $\mathcal{C}$. These $2^{n/p+n/2-n/(2p)-1} = 2^{n/2+n/(2p)-1}$ generalized circulant digraphs are all distinct (though not necessarily nonisomorphic), so $|\mathrm{GW}(n)| \geq 2^{n/2+n/(2p)-1}$ as claimed.

Let $S(n)$ be the set of all circulant digraphs of order n whose automorphism group contains a nontrivial automorphism of $\mathbb{Z}_n$. Clearly then $|S(n)| \geq |\mathrm{Nor}(n)\backslash\mathrm{DRR}(n)|$. We now seek an upper bound on $|S(n)|$. Observe that for any circulant digraph Γ, if there exists an nontrivial automorphism $\alpha \in \mathrm{Aut}(\Gamma) \cap \mathrm{Aut}(\mathbb{Z}_n)$, then we may choose such an α of prime order.

Let $1 \neq a \in \mathbb{Z}_n^*$ have prime order ℓ. We first consider the case that $\bar{a}$ has a fixed point $i \neq 0$. Then $ai \equiv i \pmod n$, so $(a-1)i \equiv 0 \pmod n$. Since $a \neq 1$, we must have $\gcd(i, n) = m > 1$, which clearly implies $i \in \langle m\rangle$. Since $a \in \mathbb{Z}_n^*$, $a = sn/m + 1$ for some $0 < s < m$ must be a unit, i.e., $\gcd(n, sn/m + 1) = 1$. Note that $m > 2$, since if $m = 2$ then $s = 1$, but $\gcd(n, n/2 + 1) \geq 2$ since $n/2$ is odd. Now, $\bar{a}$ fixes n/m points $\{0, m, \cdots, (n/m - 1)m\}$, and since $|\bar{a}| = \ell$ is prime, every non-singleton orbit of $\bar{a}$ has length ℓ. So $\bar{a}$ has $n(1 - 1/m)/\ell$ orbits of length ℓ, and $n/m + n/\ell - n/(m\ell)$ orbits in total. We will separate the cases $\ell = 2$ and $\ell = 3$ to make the proof easier. If $\ell = 2$ then $1/m + 1/\ell - 1/(m\ell) = 1/2 + 1/(2m) \leq (p + 1)/(2p)$ since $m \geq p$ (p is still the smallest nontrivial divisor of $n/2$), so if $|\bar{a}| = 2$, then α has at most $(p+1)n/(2p)$ orbits. If $\ell = 3$ then $1/m + 1/\ell - 1/(m\ell) = 1/3 + 2/(3m) \leq (p + 2)/(3p)$ since $m \geq p$, so if $|\bar{a}| = 3$, then $\bar{a}$ has at most $(p + 2)n/(3p)$ orbits. Finally, if $\ell \geq 5$ then $1/m + 1/\ell - 1/(m\ell) \leq (m + 4)/(5m) \leq 7/15$ since $m \geq 3$, so if $|\bar{a}| \geq 5$ then $\bar{a}$ has at most $7n/15$ orbits.

Finally, notice that if $\bar{a}$ fixes only 0, it will have 1 fixed point and $n - 1$ points that are not fixed. If $|\bar{a}| = 2$ then its orbits are all of length 1 or 2, and since $n - 1$ is odd, it cannot be partitioned into orbits of length 2. So an element of order 2 must have some fixed point other than 0. Hence if $\bar{a}$ fixes only 0, it must have order at least 3, so each non-singleton

orbit must have length at least 3. Hence $\bar{a}$ has at most $\lfloor (n-1)/3 \rfloor < n/3$ orbits other than $\{0\}$.

We now split the set of all elements of $\mathbb{Z}_n^*$ that have prime order into disjoint subsets: U (consisting of all elements of order 2 that have fixed points); V (consisting of all elements of order 3 that have fixed points); W (consisting of all elements of order 5 or greater that have fixed points) and X (consisting of all elements that have no fixed points other than 0). Notice that $\mathbb{Z}_n^* = \mathbb{Z}_{p_1^{e_1}}^* \times \ldots \times \mathbb{Z}_{p_r^{e_r}}^*$ and each $\mathbb{Z}_{p_i^{e_i}}^*$ is cyclic, so contains a unique element of order 2. Any element of order 2 in $\mathbb{Z}_n^*$ must be a product of elements of order 1 or 2 from the $\mathbb{Z}_{p_i}^*$, at least one of which must have order 2. So there are $2^r - 1$ elements of order 2 in $\mathbb{Z}_n^*$. Also, there are at most n elements of any other order in $\mathbb{Z}_n^*$. Thus,

$$\begin{aligned} |S(n)| &\leq \sum_{\bar{a}\in U} 2^{(p+1)n/(2p)} + \sum_{\bar{a}\in V} 2^{(p+2)n/(3p)} + \sum_{\bar{a}\in W} 2^{7n/15} + \sum_{\bar{a}\in X} 2^{n/3} \\ &\leq (2^r - 1)2^{(p+1)n/(2p)} + n(2^{(p+2)n/(3p)} + 2^{7n/15} + 2^{n/3}). \end{aligned}$$

Now,

$$\lim_{n\to\infty, r \text{ fixed}} \frac{|\mathrm{NonNor}(n)|}{|\mathrm{Nor}(n)\backslash \mathrm{DRR}(n)|} \geq \lim_{n\to\infty, r \text{ fixed}} \frac{2^{n/2+n/(2p)-1}}{|S(n)|} = \frac{1}{2(2^r-1)}.$$

□

A **safe prime** is a prime number $p = 2q + 1$, where q is also prime.

We now show that it is not true that almost all circulant graphs of order p or p^2, where p is a safe prime, or of order 3^k, are normal. This shows that [4, Theorem 3.5] is not correct. We provide a correct statement of [4, Theorem 3.5] as well as point out explicitly where "gaps" occur in the proof. As a consequence, much of the following result is essentially the same as the proof of [4, Theorem 3.5]. The entire argument is included for completeness.

Theorem 3.6. *Let $X = \{p, p^2 : p \text{ is a safe prime}\} \cup \{3^k : k \in \mathbb{N}\}$, T the set of all powers of odd primes, and $R = T \setminus X$. Then*

$$\lim_{n\in R, n\to\infty} \frac{|\mathrm{NonNorG}(n)|}{|\mathrm{ACG}(n) \setminus \mathrm{Small}(n)|} = 0.$$

Additionally, if $n \in X$, then more than one fifth of all elements of $\mathrm{ACG}(n) \setminus \mathrm{Small}(n)$ are in $\mathrm{NonNorG}(n)$.

Proof. Let $n = p^k \in T$, where p is an odd prime, $\Gamma = \Gamma(\mathbb{Z}_n, S)$.

First suppose that $k = 1$. The statement about X is vacuously true for $p = 3$ and easy to verify for $p = 5$, so we assume $p > 5$. If $p = 2q + 1$ is a safe prime, then $\mathbb{Z}_p^*$ is cyclic of order $2q \geq 6$, so every element of $\mathbb{Z}_p^*$ has order 2, q, or $2q$. Since $\iota_p \in \mathrm{Aut}(\Gamma)$, if $\Gamma \notin \mathrm{Small}(p)$ is normal then $\bar{a} \in \mathrm{Aut}(\Gamma)$ for $a \in \mathbb{Z}_p^*$ of order q or $2q$. Since $q > 2$, the orbit of length q that contains 1 in $\mathbb{Z}_p^*$ does not contain -1, so the orbits of $\langle \alpha, \iota_p \rangle$ have length 1 (the orbit of 0) and $2q = p - 1$ (everything else). So $\Gamma = K_p$ or $\bar{K_p}$ and $\mathrm{Aut}(\Gamma) = S_p$ contradicting Γ being normal. Hence $\mathrm{ACG}(p) \setminus \mathrm{Small}(p) \subseteq \mathrm{NonNorG}(p)$. (The proof of [4, Theorem 3.5] overlooks this case.)

Now if p is not a safe prime, then we can write $(p-1)/2 = rs$ where $1 < r \leq s < (p-1)/2$. As $\mathbb{Z}_p^*$ is cyclic of order $p - 1$, there is $a \in \mathbb{Z}_p^*$ with $|a| = 2r$. Then $\bar{a}$ has $s + 1$ orbits

(the cosets of $\langle a\rangle$ in $\mathbb{Z}_p^*$, together with 0). Since $|a|$ is even, $-1 \in \langle a\rangle$. If S is a union of these orbits, Γ is a graph, and since $|a| > 2$, $\Gamma \notin \mathrm{Small}(p)$. Hence $|\mathrm{ACG}(p) \setminus \mathrm{Small}(p)| \geq 2^s \geq 2^{\sqrt{(p-1)/2}}$. Meanwhile, if $\mathrm{Aut}(\Gamma) \not< \mathrm{AGL}(1,p)$ then $\mathrm{Aut}(\Gamma) = S_p$ by [1], and $\Gamma = K_p$ or $\bar{K}_p$. So $|\mathrm{NonNor}(p)| = 2$ and clearly $2/(2^{\sqrt{(p-1)/2}}) \to 0$ as $p \to \infty$.

Now let $k \geq 2$. Through the rest of this proof, let $a = p^{k-1} + 1$. We show that $\bar{a} \in \mathrm{Aut}(\Gamma)$ if and only if $\Gamma \in \mathrm{NonNor}(n)$. Using the binomial theorem, it is easy to see that $|\bar{a}| = p$. Furthermore, $\bar{a}$ fixes every element of $\langle p\rangle$, and fixes setwise every coset of $\langle p^{k-1}\rangle$. Since $|\bar{a}| = p$ and $\bar{a}$ does not fix any element of any coset of $\langle p^{k-1}\rangle$ that is not in $\langle p\rangle$, the orbits of $\bar{a}$ on each coset of $\langle p^{k-1}\rangle$ that is not in $\langle p\rangle$ have length p. Thus if $\bar{a} \in \mathrm{Aut}(\Gamma)$, then Γ is a $(\langle p^{k-1}\rangle, \langle p\rangle)$-generalized wreath circulant digraph, and in fact by Lemma 3.4, $\Gamma \in \mathrm{NonNor}(n)$. Conversely, if $\Gamma \in \mathrm{NonNor}(n)$, then by Theorem 2.4, $\mathrm{Aut}(\Gamma)$ either falls into category (1) with a single factor in the direct product (since $n = p^k$ does not permit coprime factors) and since $\Gamma \in \mathrm{NonNor}(n)$, Γ is complete (or empty), or category (2) so by Corollary 2.10, $\Gamma \in \mathrm{GW}(n)$. Since $K_n, \bar{K}_n \in \mathrm{GW}(n)$, $\Gamma \in \mathrm{GW}(n)$. It is straightforward to verify using the definition of a generalized wreath circulant, that $\bar{a} \in \mathrm{Aut}(\Gamma)$.

Now suppose $p = 3$. We have $\mathbb{Z}_{3^k}^*$ is cyclic of order $2 \cdot 3^{k-1}$. For $\Gamma \in \mathrm{Nor}(3^k) \setminus \mathrm{Small}(3^k)$, there exists $-1 \neq b \in \mathbb{Z}_{3^k}^*$ with $\bar{b} \in \mathrm{Aut}(\Gamma)$. If $|b|$ is divisible by 3, then since $\mathbb{Z}_{3^k}^*$ is cyclic and a generates the unique subgroup of order 3, we have $\bar{a} \in \langle \bar{b}\rangle$, so $\bar{a} \in \mathrm{Aut}(\Gamma)$. Hence $\Gamma \in \mathrm{NonNor}(3^k)$. But the only divisor of $2 \cdot 3^{k-1}$ not divisible by 3 is 2, and so $b = -1$. This shows that if $\Gamma \in \mathrm{NorG}(3^k)$ then $\Gamma \in \mathrm{Small}(3^k)$. Thus $\mathrm{ACG}(3^k) \setminus \mathrm{Small}(3^k) \subseteq \mathrm{NonNorG}(3^k)$.

Now we calculate $|\mathrm{NonNorG}(n)|$. As noted above, if $\Gamma \in \mathrm{NonNorG}(n)$ then $\bar{a} \in \mathrm{Aut}(\Gamma)$, and the orbits of $\bar{a}$ all have length 1 or length p. Now since multiplication is commutative, ι_{p^k} permutes the orbits of $\langle \bar{a}\rangle$, and since $|\bar{a}| = p$ is odd, $\iota_{p^k} \notin \langle \bar{a}\rangle$, so ι_{p^k} will exchange pairs of orbits of $\langle \bar{a}\rangle$, except the orbit $\{0\}$. Consequently, $\langle \bar{a}, \iota_{p^k}\rangle$ will have one orbit of length 1 ($\{0\}$); $(p^{k-1}-1)/2$ orbits of length 2 (whose union is $\langle p\rangle \setminus \{0\}$); and $(p^k - p^{k-1})/(2p)$ orbits of length $2p$ (everything else). So $\langle \bar{a}, \iota_{p^k}\rangle$ has exactly $p^{k-1} - (1 + p^{k-2})/2$ orbits other than $\{0\}$. Since we have shown that $\Gamma \in \mathrm{NonNor}(p^k)$ if and only if $\langle \bar{a}, \iota_{p^k}\rangle \leq \mathrm{Aut}(\Gamma)$, $|\mathrm{NonNor}(p^k)| = 2^{p^{k-1} - (1+p^{k-2})/2}$.

Now we find a lower bound for $|\mathrm{ACG}(n) \setminus \mathrm{Small}(n)|$ when $n \in R$ and $k > 2$. Since p is an odd prime, $\mathbb{Z}_{p^k}^*$ is cyclic of order $(p-1)p^{k-1}$. Let $b \in \mathbb{Z}_{p^k}^*$ have order $p-1$. Note that $\iota_{p^k} \in \langle \bar{b}\rangle$ since b has even order, and $\bar{b} \neq \iota_{p^k}$ since $p > 3$ (the proof of [4, Theorem 3.5] overlooks the fact that $\bar{b} = \iota_{p^k}$ when $p = 3$). Clearly, $\bar{b}$ fixes 0, and since the order of $\bar{b}$ is $p-1$, every other orbit of $\bar{b}$ has length at most $p-1$, so $\bar{b}$ has at least $(p^k-1)/(p-1)$ orbits other than $\{0\}$. Thus there are at least $2^{(p^k-1)/(p-1)}$ circulant graphs of order p^k whose automorphism group contains $\bar{b}$, and $|\mathrm{ACG}(p^k) \setminus \mathrm{Small}(p^k)| \geq 2^{1+(p^k-1)/(p-1)}$, $p > 3$. Note that as $k \geq 2$, $(p^k-1)/(p-1) \neq 1$. Then

$$\begin{aligned}\lim_{p^k\to\infty} \frac{|\mathrm{NonNorG}(p^k)|}{|\mathrm{ACG}(p^k) \setminus \mathrm{Small}(p^k)|} &\leq \lim_{p^k\to\infty} \frac{2^{p^{k-1}-(1+p^{k-2})/2}}{2^{(p^k-1)/(p-1)}} \\ &= \lim_{p^k\to\infty} \frac{1}{2^{(3p^{k-2}+1)/2+\sum_{i=0}^{k-3} p^i}}.\end{aligned}$$

Thus as $k \geq 3$, the result follows. (The proof of [4, Theorem 3.5] concludes the above limit is 1 in all cases – hence the gap in that theorem when $k = 2$.)

For the remainder of the proof we suppose that $k = 2$ and $p > 3$. Substituting $k = 2$ into our formula for $|\mathrm{NonNorG}(n)|$, we conclude that $|\mathrm{NonNorG}(p^2)| = 2^{p-1}$.

If $p = 2q + 1$ is a safe prime, q prime, then $\langle \bar{a} \rangle$ is the unique subgroup of order p in $\mathbb{Z}_{p^2}^*$, so any subgroup of $\mathbb{Z}_{p^2}^*$ that contains -1 but does not contain $a = p + 1$, must have even order not a multiple of p. Since $\mathbb{Z}_{p^2}^*$ is cyclic of order $p(p-1) = 2pq$, the group C of order $2q$ is the only such subgroup. Then if $\Gamma \in \mathrm{Nor}(p^2) \setminus \mathrm{Small}(p^2)$, then $\mathrm{Aut}(\Gamma) = C \cdot (\mathbb{Z}_{p^2})_L$. Now, C fixes 0 and since C has order $2q$ and is cyclic, the other orbits of C all have length precisely $2q$ (it is not hard to show that the only elements of $\mathbb{Z}_{p^2}^*$ that fix anything but 0 are 1 and the elements of order p; this forces the orbit lengths of C to be the order of C), so there are $(p^2 - 1)/2q = 1 + p$ orbits of C other than $\{0\}$, and hence fewer than 2^{1+p} graphs in $\mathrm{Nor}(p^2)$ are not in $\mathrm{Small}(p^2)$ (the "fewer than" is due to the fact that some of these graphs are not normal, for example K_{p^2}). Hence $\mathrm{NonNor}(p^2)/(\mathrm{ACG}(p^2) \setminus \mathrm{Small}(p^2)) \geq 2^{p-1}/(2^{p-1} + 2^{p+1}) = 1/5$.

Suppose now that p is not a safe prime. Then there exists $b \in \mathbb{Z}_{p^2}^*$ of order $p - 1$. Since p is not a safe prime, there exists $1 < r \leq s < (p-1)/2$ such that $rs = (p-1)/2$. As every non-singleton orbit of $\langle \bar{b} \rangle$ has length $p - 1$ (as shown for the orbits of C in the preceding paragraph), every nonsingleton orbit of $\langle \bar{b}^s \rangle$ has length $(p-1)/s$. Then $\bar{b}^s$ has $s(p+1)$ orbits not including $\{0\}$ and since $|b^s| = 2r > 2$, $\bar{b}^s \neq \iota_{p^2}$. We conclude that there are at least $2^{s(p+1)}$ graphs of order p^2 in $\mathrm{ACG}(p^2) \setminus \mathrm{Small}(p^2)$. As there are 2^{p-1} non-normal circulant graphs of order p^2 and $s \geq \sqrt{(p-1)/2}$,

$$\lim_{p^2 \to \infty} \frac{|\mathrm{NonNorG}(p^2)|}{|\mathrm{ACG}(p^2) \setminus \mathrm{Small}(p^2)|} \leq \lim_{p \to \infty} \frac{2^{p-1}}{2^{s(p+1)}} = 0.$$

□

We now verify that Conjecture 3.3 does hold for circulant digraphs of order n, and also for circulant graphs of order n, for large families of integers. Note that, using Corollaries 2.10 and 2.17, we have for any n, $|\mathrm{NonNor}(n)| \leq |\mathrm{DW}(n)_{m \geq 4}| + |\mathrm{GW}(n)|$.

Theorem 3.7. *Let n be any odd integer such that $9 \nmid n$. Then almost all circulant digraphs of order n that are not DRRs are normal circulant digraphs.*

Proof. A lower bound for $|\mathrm{ACD}(n) \setminus \mathrm{DRR}(n)|$ is the number of circulant graphs of order n, which is $2^{(n-1)/2}$. We first find an upper bound for $|\mathrm{DW}(n)_{m \geq 4}|$. As n is odd, we have $2n/m \leq 2n/5$. Also, n is an upper bound on the number of nontrivial divisors of n. By Corollary 2.18, $|\mathrm{DW}(n)_{m \geq 4}| \leq \sum_{m | n, m \geq 4} 2^{2n/m} \leq n \cdot 2^{2n/5}$.

By Corollary 2.12, we have $|\mathrm{GW}(n)| \leq \log_2^2 n \cdot 2^{n/p + n/q - n/(pq) - 1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of n/q. Since n is odd we have $q \geq 3$, and since $9 \nmid n$ we have $p \geq 5$. If $q \geq 5$ then $1/p + 1/q - 1/(pq) < 1/p + 1/q \leq 2/5$, while if $q = 3$ then $1/p + 1/q - 1/(pq) = 2/(3p) + 1/3 \leq 7/15$, so we always have $1/p + 1/q - 1/(pq) \leq 7/15$. Note that if $9 | n$ then $p = q = 3$, and this inequality is not true. Then

$$\lim_{n \to \infty} \frac{|\mathrm{NonNor}(n)|}{|\mathrm{ACD}(n) \setminus \mathrm{DRR}(n)|} \leq \lim_{n \to \infty} \frac{n \cdot 2^{2n/5} + \log_2^2 n \cdot 2^{7n/15}}{2^{(n-1)/2}} = 0.$$

□

Theorem 3.8. *Let n be any odd integer such that $9 \nmid n$, and n is not a safe prime or the square of a safe prime. Then almost all circulant graphs of order n that do not have automorphism group as small as possible are normal circulant graphs.*

Proof. We need to show that

$$\lim_{n\to\infty, n\notin T} \frac{|\mathrm{NonNorG}(n)|}{|\mathrm{ACG}(n) \setminus \mathrm{Small}(n)|} = 0,$$

where $T = \{p, p^2 : p \text{ is a safe prime}\} \cup \{n : 9 \mid n\} \cup \{n : 2 \mid n\}$. This is true if n is a prime power by Theorem 3.6, so we assume there is a proper divisor m of n such that $\gcd(m, n/m) = 1$. We also assume that $n/m > m$, and regard $\mathbb{Z}_n$ as $\mathbb{Z}_{n/m} \times \mathbb{Z}_m$ in the natural way.

We begin by finding a lower bound for $|\mathrm{ACG}(n) \setminus \mathrm{Small}(n)|$. Let $\Gamma \in \mathrm{ACG}(n)$ such that $\bar{a} \in \mathrm{Aut}(\Gamma)$ where $a = (1, -1)$. Obviously $\bar{a} \notin \langle \rho, \iota_n \rangle$, so $\Gamma \notin \mathrm{Small}(n)$. Straightforward computations will show that the orbits of $\langle \bar{a}, \iota_n \rangle \leq \mathrm{Aut}(\Gamma)$ are the sets $\{(0,0)\}$, $\{(i,0),(-i,0)\}$, $\{(0,j),(0,-j)\}$, and $\{(i,j),(-i,j),(i,-j),(-i,-j)\}$, where $i \in \mathbb{Z}_{n/m} \setminus \{0\}$ and $j \in \mathbb{Z}_m \setminus \{0\}$. We conclude that $\langle \bar{a}, \iota_n \rangle$ has

$$1 + \frac{n/m - 1}{2} + \frac{m-1}{2} + \frac{n - n/m - m + 1}{4} = \frac{n + n/m + m + 1}{4} > \frac{n}{4}$$

orbits. Hence $|\mathrm{ACG}(n) \setminus \mathrm{Small}(n)| \geq 2^{n/4}$. Recall (by Corollaries 2.10 and 2.17) $|\mathrm{NonNorG}(n)| \leq |\mathrm{DWG}(n)_{m\geq 4}| + |\mathrm{GWG}(n)|$. By Corollary 2.18, we have that $|\mathrm{DWG}(n)_{m\geq 4}| \leq \sum_{m|n, m\geq 4} 2^{n/m+1}$. Since n is odd, m is odd, so $m \geq 5$, so $n/m \leq n/5$, and $\sum_{m|n,m\geq 4} 2^{n/m+1} \leq n2^{n/5+1}$. By Corollary 2.13, we have that $|\mathrm{GWG}(n)| \leq (\log_2^2 n)2^{n(p+q-1)/(2pq)+1/2}$, where p is the smallest divisor of n and q is the smallest divisor of n/p. As in the proof of Theorem 3.7, it is straightforward to show that since n is odd and not divisible by 9, $(p+q-1)/(pq) \leq 7/15$. Hence

$$\begin{aligned} \lim_{n\to\infty, n\notin S} \frac{|\mathrm{NonNorG}(n)|}{|\mathrm{ACG}(n) \setminus \mathrm{Small}(n)|} &\leq \lim_{n\to\infty, n\notin S} \frac{n2^{n/5+1} + (\log_2^2 n)2^{7n/30+1/2}}{2^{n/4}} \\ &= 0. \end{aligned}$$

□

4 Non-normal circulants

By Theorem 2.4, a circulant (di)graph that is not normal is generalized wreath or deleted wreath type. For each of these classes, we will now consider whether or not almost all non-normal circulant (di)graphs lie within this class. The short answer is "No" and is given by the following result.

Theorem 4.1. *Let Γ be a circulant digraph of order pq, where p and q are primes and $p, q \geq 5$. Then*

1. *if $q \neq p$ then*

$$\frac{|\mathrm{GW}(pq)|}{|\mathrm{SDW}(pq)|} = \frac{2^{p+q-1} - 2}{2^{2p-1} + 2^{2q-1} - 2^p - 2^q - 2},$$

2. *if p is fixed, then* $\lim_{q\to\infty} |\mathrm{GW}(pq)|/|\mathrm{SDW}(pq)| = 0$,
3. *if $q = p + c$ for some constant $c \geq 2$, then*

$$\lim_{p\to\infty} \frac{|\mathrm{GW}(pq)|}{|\mathrm{SDW}(pq)|} = \frac{2^c}{(1 + 2^{2c})},$$

4. *if $q = p$ then all non-normal circulants are generalized wreath products.*

Proof. Note that for $\Gamma \in \mathrm{SDW}(pq)$ we have $m \in \{p, q\}$ so $m \geq 5$ and $\Gamma \in \mathrm{NonNor}(n)$.

(1): We require exact counts of $|\mathrm{GW}(pq)|$ and of $|\mathrm{SDW}(pq)|$. First, when $n = pq$ a generalized wreath product will actually be a wreath product. For a wreath product digraph with p blocks of size q, there are $q - 1$ possible elements of $S \cap \langle p\rangle$, and $p - 1$ choices for the cosets of $\langle p\rangle$ to be in S. Hence there are 2^{p+q-2} wreath product circulant digraphs with p blocks of size q. Similarly, there are 2^{q+p-2} wreath product circulant digraphs with q blocks of size p. The only digraphs that have both of these properties are K_{pq} and its complement, each of which has been counted twice, so $|\mathrm{GW}(pq)| = 2 \cdot 2^{p+q-2} - 2 = 2^{p+q-1} - 2$.

Now we count strictly deleted wreath products. As mentioned in the first sentence of the proof of Corollary 2.18, there are precisely $2 \cdot 4^{p-1}$ digraphs whose automorphism group contains $K \times S_q$, and $2 \cdot 4^{q-1}$ digraphs whose automorphism group contains $K' \times S_p$. Of the first set, $2 \cdot 2^{p-1}$ are wreath products (those in which $S \cap (rq + \langle p\rangle)$ is chosen from $\{\emptyset, rq + \langle p\rangle\}$, for every $1 \leq r \leq p - 1$). Similarly, of the second set, $2 \cdot 2^{q-1}$ are wreath products (those in which $S \cap (rp + \langle q\rangle)$ is chosen from $\{\emptyset, rp + \langle q\rangle\}$, for every $1 \leq r \leq q - 1$). Finally, notice that if a digraph is counted in both the first and second sets then its automorphism group must contain $S_q \times S_p$. Consequently, the number of elements in $S \cap (rp + \langle q\rangle)$ is constant over r, as is the number of elements in $S \cap (rq + \langle p\rangle)$. Since we have already eliminated wreath products from our count, the first number must be 1 or $p - 1$, and the second must be 1 or $q - 1$. Furthermore, if the first number is 1 then we have $p \in S$ but $p + q \notin S$, so the second cannot be $q - 1$ (and the same holds if we exchange p and q), so there are only 2 choices for such digraphs: that in which all of the values are 1, which is $K_p \Box K_q$ (where $\Box$ denotes the cartesian product), and its complement, in which all of the values are $p - 1$ or $q - 1$. Summing up, we see that $|\mathrm{SDW}(pq)| = 2 \cdot 4^{p-1} + 2 \cdot 4^{q-1} - 2 \cdot 2^{p-1} - 2 \cdot 2^{q-1} - 2$. The result follows.

(2): This follows from (1) by letting q tend to infinity.

(3): Substituting $q = p + c$ into (1) and letting p tend to infinity, we have

$$\lim_{p\to\infty} \frac{|\mathrm{GW}(pq)|}{|\mathrm{SDW}(pq)|} = \lim_{p\to\infty} \frac{2^{c-1} - 2^{1-2p}}{2^{-1} + 2^{2c-1} - 2^{-p} - 2^{c-p} - 2^{1-2p}}.$$

Deleting the terms that tend to zero, we are left with

$$\lim_{p\to\infty} \frac{2^{c-1}}{2^{-1} + 2^{2c-1}} = \frac{2^c}{1 + 2^{2c}},$$

as claimed.

(4): By Theorem 2.4, if $\Gamma \in \mathrm{NonNor}(p^2)$, then $\mathrm{Aut}(\Gamma)$ must either fall into category (1) or category (2). If it falls into category (1) then, since $n = p^2$ and the n_i are coprime, there can only be a single factor in the direct product, and since $\Gamma \in \mathrm{NonNor}(n)$, the factor must be S_{p^2}, so $\Gamma \in \{K_{p^2}, \bar{K}_{p^2}\} \subseteq \mathrm{GW}(p^2)$. If it falls into category (2) then by Corollary 2.10, $\Gamma \in \mathrm{GW}(p^2)$. □

Notice that if we choose a constant $c \geq 2$ and define $T_c = \{pq : q = p+c\}$ where p and q are prime, then as a consequence of Theorem 4.1(3), since $0 < 2^c/(1+2^{2c}) < \infty$, neither generalized wreath circulant digraphs nor strictly deleted circulant digraphs dominates in T_c. The recent breakthrough by Zhang [16] shows that the union of the first 70 million T_cs is infinite, and therefore that at least one of these sets is infinite. Essentially, we have shown that if $n = pq$ is a product of two primes, then generalized wreath products dominate amongst circulant digraphs of order n if $p = q$ (in fact there are no others); neither family dominates if p and q are "close" to each other, and strictly deleted wreath products dominate if one prime is much larger than the other.

We now give two infinite sets N_1 and N_2 of integers, each integer in both sets being divisible by three distinct primes. In N_1, almost all non-normal circulant digraphs are of strictly deleted wreath type (and N_1 includes all of the square-free integers that are not divisible by 2 or 3). Meanwhile in N_2, almost all non-normal circulant digraphs are generalized wreath circulant digraphs.

Theorem 4.2. *Let* $N_1 = \{n \in \mathbb{N} |\ n$ is the product of at least three primes and $q^2 \nmid n$ where $q \geq 5$ is the smallest prime divisor of $n\}$. *Then,*

$$\lim_{n \in N_1, n \to \infty} \frac{|\mathrm{SDW}(n)|}{|\mathrm{NonNor}(n)|} = 1$$

Proof. By Corollaries 2.10 and 2.17, $\mathrm{NonNor}(n) \subseteq \mathrm{GW}(n) \cup \mathrm{SDW}(n)_{m \geq 4}$, and by the definition of $\mathrm{SDW}(n)$, these sets are disjoint. Since $q \geq 5$ we also have $m \geq 5$ for any proper divisor m of n, so $\mathrm{SDW}(n) = \mathrm{SDW}(n)_{m \geq 4}$. Hence $|\mathrm{NonNor}(n)| = |\mathrm{GW}(n)| + |\mathrm{SDW}(n)|$. We show that $\lim_{n \to \infty} \frac{|\mathrm{GW}(n)|}{|\mathrm{NonNor}(n)|} = 0$, which implies the result.

The first sentence of the proof of Corollary 2.18 notes that for a proper divisor m of n, the number of digraphs Γ with $H \times S_m \leq \mathrm{Aut}(\Gamma)$ for some 2-closed group $H \leq S_{n/m}$ is precisely $2 \cdot 4^{n/m-1}$. The maximum number of times that a specific circulant digraph Γ can be counted in $\sum_{m|n} 2 \cdot 4^{n/m-1}$, is the number of divisors of n, $d(n) \leq n$. Thus $|\mathrm{DW}(n)| \geq \sum_{m|n} 2 \cdot 4^{n/m-1}/n$, and so by Lemma 2.16, $|\mathrm{NonNor}(n)| \geq \sum_{m|n} 2 \cdot 4^{n/m-1}/n$. By Corollary 2.12, we have that $|\mathrm{GW}(n)| \leq (\log_2^2 n) 2^{n/p+n/q-n/(pq)-1}$, where q is the smallest prime divisor of n and p is the smallest prime divisor of n/q. Then

$$\begin{aligned}
\lim_{n \to \infty} \frac{|\mathrm{GW}(n)|}{|\mathrm{NonNor}(n)|} &\leq \lim_{n \to \infty} \frac{(\log_2^2 n) 2^{n/p+n/q-n/(pq)-1}}{\sum_{m|n} 2 \cdot 4^{n/m-1}/n} \\
&< \lim_{n \to \infty} \frac{(\log_2^2 n) 2^{n/(q+2)+n/q}}{4 \cdot 4^{n/q-1}/n} \\
&= \lim_{n \to \infty} \frac{n \log_2^2 n}{2^{2n/(q(q+2))}}.
\end{aligned}$$

Since $q(q+2) < n^{2/3}$ as q is the smallest prime factor of n, $q^2 \nmid n$, and n has at least 3 prime factors, we have $n/(q(q+2)) > n^{1/3}$, so $\lim_{n \to \infty} \frac{|\mathrm{GW}(n)|}{|\mathrm{NonNor}(n)|} = 0$. □

Theorem 4.3. *For any natural number n, let p_n be the smallest prime divisor of n, and q_n the smallest prime divisor of n such that $q_n \neq p_n$ and $q_n^2 \nmid n$. Let* $N_2 = \{n \in \mathbb{N} : p_n \geq$

$5, p_n^2 \mid n$, n has at least 3 distinct prime divisors, and $q_n > 2p_n\}$. *Then*

$$\lim_{n\in N_2, n\to\infty} \frac{|\mathrm{GW}(n)|}{|\mathrm{NonNor}(n)|} = 1.$$

Proof. Let $p = p_n$. First notice that there are $2^{p-1+n/p-1}$ circulant digraphs that are wreath products $\Gamma_1 \wr \Gamma_2$ where Γ_1 has order n/p and Γ_2 has order p: 2^{p-1} choices for $S \cap \langle n/p\rangle$ and $2^{n/p-1}$ choices for which cosets of $\langle n/p\rangle$ are in S. All of these digraphs are distinct, so since by Lemma 3.4 these are all non-normal, we have $|\mathrm{NonNor}(n)| \geq 2^{p+n/p-2}$.

By Corollary 2.18, for a proper divisor $m \geq p_n > 4$ of n, the number of digraphs of deleted wreath type is at most $4^{n/m}$. Thus

$$|\mathrm{DW}(n)| \leq \sum_{m\mid n, \gcd(m,n/m=1)} 4^{n/m}.$$

Let $\prod_{i=1}^{t} p_i^{a_i}$ be the prime decomposition of n, and let $p_k^{a_k} = \min\limits_{1\leq i\leq t}\{p_i^{a_i}\}$. Clearly $4^{n/(p_k^{a_k})}$ is the largest term in this sum, and there are at most $d(n)$ (the number of divisors of n) terms in this sum. Thus $|\mathrm{DW}(n)| \leq d(n)\cdot 4^{n/(p_k^{a_k})}$.

Observe that if $a_k \geq 2$, then $p_k^{a_k} \geq 5p > 2p$ since $p \geq 5$ is the smallest divisor of n. Also, if $a_k = 1$, then by hypothesis $p_k \geq q_n > 2p$. Hence $p_k^{a_k} - 2p \geq 1$ since both are integers. Now,

$$\begin{aligned}
\lim_{n\to\infty} \frac{|\mathrm{DW}(n)|}{|\mathrm{NonNor}(n)|} &\leq \lim_{n\to\infty} \frac{d(n)\cdot 4^{n/({p_k}^{a_k})}}{2^{p+n/p-2}} \\
&< \lim_{n\to\infty} \frac{4n}{2^{p+n\cdot(p_k^{a_k}-2p)/(pp_k^{a_k})}} \\
&\leq \lim_{n\to\infty} \frac{4n}{2^{p+n/(pp_k^{a_k})}}.
\end{aligned}$$

Since n has at least 3 distinct prime divisors, there is some j such that $p_j \neq p, p_k$. Now $p_j^{a_j} > p_k^{a_k}$ by our choice of k, and $p_j^{a_j} \geq p_j > p$, so since $n/(pp_k^{a_k}) \geq p_j^{a_j}$, we have $(n/(pp_k^{a_k}))^2 \geq pp_k^{a_k}$. Hence $pp_k^{a_k} \leq n^{2/3}$, so $n/(pp_k^{a_k}) \geq n^{1/3}$. So the above limit is at most

$$\lim_{n\to\infty} \frac{4n}{2^{p+n^{1/3}}} = 0.$$

□

Acknowledgement: The authors are indebted to the anonymous referees whose suggestions improved the clarity of the proofs as well as the exposition in this manuscript.

References

[1] B. Alspach, Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree, *J. Combinatorial Theory Ser. B* **15** (1973), 12–17.

[2] L. Babai and C. D. Godsil, On the automorphism groups of almost all Cayley graphs, *European J. Combin.* **3** (1982), 9–15.

[3] P. J. Cameron, Michael Giudici, Gareth A. Jones, William M. Kantor, Mikhail H. Klin, Dragan Marušič and Lewis A. Nowitz, Transitive permutation groups without semiregular subgroups, *J. London Math. Soc.* **66** (2002), 325–333.

[4] E. Dobson, Asymptotic automorphism groups of Cayley digraphs and graphs of abelian groups of prime-power order, *Ars Math. Contemp.* **3** (2010), 200–213.

[5] E. Dobson and J. Morris, On automorphism groups of circulant digraphs of square-free order, *Discrete Math.* **299** (2005), 79–98.

[6] S. A. Evdokimov and I. N. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, *Algebra i Analiz* **14** (2002), 11–55.

[7] W. Imrich, Graphs with transitive abelian automorphism group, in *Combinatorial theory and its applications*, Coll. Math. Soc. János Bolyai 4, Balatonfüred, Hungary (1969), 651-656.

[8] K. H. Leung and S. H. Man, On Schur rings over cyclic groups. II, *J. Algebra* **183** (1996), 273–285.

[9] K. H. Leung and S. H. Man, On Schur rings over cyclic groups, *Israel J. Math.* **106** (1998), 251–267.

[10] C. H. Li, Permutation groups with a cyclic regular subgroup and arc transitive circulants, *J. Algebraic Combin.* **21** (2005), 131–136.

[11] L. A. Nowitz, On the non-existence of graphs with transitive generalized dicyclic groups, *J. Combinatorial Theory* **4** (1968), 49–51.

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

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

[14] H. Wielandt, *Mathematische Werke/Mathematical works. Vol. 1*, Walter de Gruyter & Co., Berlin, 1994, Group theory, With essays on some of Wielandt's works by G. Betsch, B. Hartley, I. M. Isaacs, O. H. Kegel and P. M. Neumann, Edited and with a preface by Bertram Huppert and Hans Schneider.

[15] M.-Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319, Graph theory (Lake Bled, 1995).

[16] Y. Zhang, Bounded gaps between primes, *Annals of Math.* **179** (2014), 1121–1174.