AUTOMORPHISM GROUPS OF CIRCULANT DIGRAPHS WITH APPLICATIONS TO SEMIGROUP THEORY

JOÃO ARAÚJO, WOLFRAM BENTZ, EDWARD DOBSON, JANUSZ KONIECZNY, AND JOY MORRIS

Abstract. We characterize the automorphism groups of circulant digraphs whose connection sets are relatively small, and of unit circulant digraphs. For each class, we either explicitly determine the automorphism group or we show that the graph is a "normal" circulant, so the automorphism group is contained in the normalizer of a cycle. Then we use these characterizations to prove results on the automorphisms of the endomorphism monoids of those digraphs. The paper ends with a list of open problems on graphs, number theory, groups and semigroups.

1. Introduction

The description of automorphisms has a long tradition in mathematics. Regarding automorphisms of semigroups, the pioneering work of Schreier [36] and Mal'cev [32] – proving that the group of automorphisms of the full transformation monoid T_n is isomorphic to the symmetric group S_n – was followed by a long sequence of similar descriptions (see [1, 4, 5, 6, 8, 9, 7, 10, 11, 12, 22, 25, 26, 27, 30, 31, 33, 37, 38, 39, 45] and the references therein). The effort to find the automorphisms of transformation semigroups containing all constants culminated in 1972 with the description, provided by Važenin [41], of the automorphisms of the endomorphism monoid $\mathrm{End}(\Gamma)$, where Γ is a reflexive digraph containing an edge that is not contained in a cycle (of length at least 2). This result contained as particular cases many older theorems and, in some sense, was the best possible at the time since a full treatment of the cases left open (the digraphs in which every edge is contained in a cycle) is probably impossible without the classification of finite simple groups, not available in 1972.

Circulant digraphs have been intensively studied (with more than 400 papers written on them since 1979) and they are obvious examples of digraphs in which every edge is contained in a cycle. In this paper we use the classification to prove some results on automorphisms of circulant digraphs Γ and then use those results to describe the automorphisms of the endomorphism monoid of Γ.

The automorphisms of a digraph Γ and the automorphisms of the endomorphism monoid of Γ are linked by the following general procedure. Suppose we have a semigroup S and want to calculate its automorphisms; then we should try to find a subsemigroup $T \leq S$ such that:

(1) T is characteristic in S; that is, the restriction to T of an automorphism of S is an automorphism of T;
(2) we can describe the automorphisms of T;
(3) we can find the extensions of the automorphisms of T to automorphisms of S.

Now suppose Γ is a circulant digraph and $\mathrm{End}(\Gamma)$ is its endomorphism monoid. Then a natural characteristic subsemigroup of $\mathrm{End}(\Gamma)$ is its group $\mathrm{Aut}(\Gamma)$ of units. To realize (2) and (3) above, we need to:

(a) have a handy description of the automorphisms of $\mathrm{Aut}(\Gamma)$;
(b) find the extensions of the automorphisms of $\mathrm{Aut}(\Gamma)$ to automorphisms of $\mathrm{End}(\Gamma)$.

Recently, there has been significant progress on determining the automorphism group of a circulant digraph Γ (see Theorem 3.1), which has been used to produce a polynomial time algorithm that finds generators of $\mathrm{Aut}(\Gamma)$. In general, however, it seems difficult to give a "closed form" description of $\mathrm{Aut}(\Gamma)$, although this may be possible for certain families of circulant digraphs. We give such a description for two families of circulant digraphs that have received considerable attention in the literature, namely circulant digraphs of small valency (Theorem 4.2) and unit circulant digraphs (Theorem 5.2).

Considering the case of small valency is a standard approach to take when studying vertex-transitive graphs (graphs whose automorphism group is transitive on the vertex set), with the first results obtained in a celebrated paper of Tutte [40]. The precise meaning of "small valency" that we will adopt was first introduced by Babai [13, Theorem 3.6] with regard to the Cayley isomorphism problem. This problem asks for necessary and sufficient condition to determine if two Cayley digraphs of the same group G are isomorphic. The most common results here state that for a given group G, two Cayley digraphs of G are isomorphic if and only if they are isomorphic by a group automorphism of G.

A *CI-digraph* is a Cayley digraph of a group such that every isomorphic Cayley digraph of the same group is isomorphic via a group automorphism. A group G is a *CI-group* if every Cayley digraph of G is a CI-digraph of G. Babai showed that Cayley graphs of G of small valency are CI-digraphs of G. The property of a Cayley digraph Γ being a CI-digraph is known to be related to properties of $\mathrm{Aut}(\Gamma)$ (see [3, Theorem 1] or more generally [13, Lemma 3.1]). Therefore, it is reasonable to suspect that circulant digraphs of small valency have "nice" automorphism groups.

Unit circulant digraphs are also known to be CI-digraphs [17, 35] as was conjectured by Toida, so again one would expect them to have "nice" automorphism groups. Also, in recent years the *unitary Cayley graphs* (the unit circulant digraphs for which the connection set is all of $\mathbb{Z}_n^*$) have been studied, and the problem of finding the automorphism groups of these graphs was posed [21, Problem 1]. This problem was solved in [2, Theorem 4.2], and our result greatly generalizes this solution.

In Section 2, we introduce definitions and basic facts about circulant digraphs. The results of this paper rely on some deep recent results, proved in a different setting. In Section 3, we translate these results into the language of groups and circulant digraphs. Sections 4 and 5 contain descriptions of the automorphism groups of circulant digraphs of small valency (Theorem 4.2) and of unit circulant digraphs (Theorem 5.2). In Section 6, we extract the corollary (from the two theorems mentioned above) that gives the normalizer of $\mathrm{Aut}(\Gamma)$ for these two types of circulant graphs Γ (Corollary 6.2). We then use this corollary to describe the automorphism groups of the endomorphism monoids of the corresponding reflexive circulant digraphs (Theorem 6.4 and Corollaries 6.10 and 6.5). Finally, Section 7 contains some open problems.

2. Preliminaries

This section contains definitions and notation that will be needed to describe the automorphism groups of the circulant digraphs under discussion.

Definition 2.1. Let n be a positive integer and $S \subseteq \mathbb{Z}_n$. A *circulant digraph* of order n with *connection set* S, denoted $\Gamma(\mathbb{Z}_n, S)$, is the digraph with vertex set $\mathbb{Z}_n$ and edge set $\{ij : i - j \in S\}$. Each vertex of $\Gamma(\mathbb{Z}_n, S)$ has in-valency and out-valency $|S|$. So $\Gamma(\mathbb{Z}_n, S)$ is $2|S|$-regular and we will say that the *valency* of $\Gamma(\mathbb{Z}_n, S)$ is $2|S|$.

Recent deep results about Schur rings have provided us with considerable information about the automorphism groups of circulant (di)graphs. Using these results we will determine the automorphism groups of circulant digraphs of small valency (circulant digraphs whose valency is at most twice the smallest prime divisor of their order), and unit circulant digraphs (circulant digraphs whose connection sets consist entirely of units). In each case, we will show that every such digraph lies in one of a few classes. Furthermore, we will either explicitly give the automorphism group of the digraph (in some cases in terms of the automorphism groups of strictly smaller digraphs in the same family), or show that a regular cyclic subgroup of the automorphism group is normal in the full automorphism group, so that the full automorphism group is contained in the normalizer of a cycle and can be efficiently computed.

Before we can classify the digraphs in these families, we need some definitions. The Schur ring results (as we present them, in a form that has been translated into the language of algebraic graph theory) involve 2-closed groups, and generalized orbital digraphs. For a set X, we denote by S_X the symmetric group of permutations on X.

Definition 2.2. 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 the orbits of G. If $G = G^{(2)}$, we say that G is 2-*closed*. 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 $G^{(2)} = \cap_{i=1}^{r} \mathrm{Aut}(\Gamma_i)$. A *generalized orbital digraph* of G is the edge-disjoint union of orbital digraphs of G. A *vertex-transitive digraph* is a digraph whose automorphism group acts transitively on the vertices of the digraph. Clearly the automorphism group of a vertex-transitive digraph is 2-closed. As every circulant digraph is vertex-transitive, the automorphism group of every circulant digraph is 2-closed.

One of the basic structures that arises in circulant digraphs and impacts directly on the automorphism group, is the wreath product.

Definition 2.3. Let Γ_1 and Γ_2 be vertex-transitive digraphs. Let

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

Define the *wreath product* of Γ_1 and Γ_2, denoted $\Gamma_1 \wr \Gamma_2$, to be the digraph such that $V(\Gamma_1 \wr \Gamma_2) = V(\Gamma_1) \times V(\Gamma_2)$ and $E(\Gamma_1 \wr \Gamma_2) = E$. We remark that the wreath product of a circulant digraph of order m and a circulant digraph of order n is circulant.

The name "wreath product" for these digraphs comes from the fact that their automorphism groups are often wreath products.

Definition 2.4. Let G be a group of permutations on a set X and let H be a group. Denote by H^X the set of all functions $\alpha : X \to H$ and note that H^X with multiplication defined by

$$(\alpha_1\alpha_2)(x) = \alpha_1(x)\alpha_2(x) \quad (\alpha_1, \alpha_2 \in H^X, x \in X)$$

is a group. Define multiplication on the set $G \times H^X$ by

$$(g_1, \alpha_1)(g_2, \alpha_2) = (g_1g_2, \alpha_1^{g_2}\alpha_2), \tag{2.1}$$

where $\alpha_1^{g_2} \in H^X$ is defined by $\alpha_1^{g_2}(x) = \alpha_1(g_2(x))$, so for every $x \in X$,

$$(\alpha_1^{g_2}\alpha_2)(x) = \alpha_1(g_2(x))\alpha_2(x).$$

It is straightforward to verify that $G \times H^X$ with multiplication (2.1) is a group. It is called the *wreath product* of G and H (with respect to the set X), and denoted by $G \wr H$.

If H is a group of permutations on a set Y, then the wreath product $G \wr H$ acts on the set $X \times Y$ by $(g, \alpha)(x, y) = (g(x), (\alpha(x))(y))$, so it is a group of permutations on $X \times Y$.

Remark 2.5. The wreath product $S_m \wr S_k$ is a permutation group that has a unique nontrivial block system, consisting of m blocks of size k, the orbits of $1_{S_m} \wr S_k$. The reason we use $G \wr H$, rather than the more standard $H \wr G$, for the wreath product is that in Definition 2.4, G acts on H^X by $(g, \alpha) \to \alpha^g$, where $\alpha^g(x) = \alpha(g(x))$. On the other hand, in the more traditional definition of $H \wr G$, G acts on H^X by $(g, \alpha) \to \alpha^g$, where $\alpha^g(x) = \alpha(g^{-1}(x))$. We find the former action more suitable for our purposes.

A basic method for analyzing the structure of vertex-transitive digraphs, is to consider subsets of the vertices on which the automorphism group continues to act nicely.

Definition 2.6. Let G be a permutation group with a block system $\mathcal{B}$ [16, page 12]. Each $g \in G$ induces a permutation in $S_{\mathcal{B}}$, denoted by $g/\mathcal{B}$. Set $G/\mathcal{B} = \{g/\mathcal{B} : g \in G\}$. Denote the kernel of this action by $\mathrm{fix}_G(\mathcal{B})$, so $\mathrm{fix}_G(\mathcal{B}) = \{g \in G : g/\mathcal{B} = 1/\mathcal{B}\}$. That is, $\mathrm{fix}_G(\mathcal{B})$ is the set-wise stabilizer of each block $B \in \mathcal{B}$. For a digraph Γ such that $G \leq \mathrm{Aut}(\Gamma)$, denote by $\Gamma/\mathcal{B}$ the digraph with vertex set $\mathcal{B}$ and $BB' \in E(\Gamma/\mathcal{B})$ if and only if $bb' \in E(\Gamma)$ for some $b \in B$, $b' \in B'$. If G acts on Ω and $S \subseteq \Omega$, define $S/\mathcal{B} = \{B \in \mathcal{B} : s \in B \text{ for some } s \in S\}$.

Finally, we introduce a piece of notation that we will use throughout this paper.

Definition 2.7. Throughout this paper, define $\rho : \mathbb{Z}_n \to \mathbb{Z}_n$ by $\rho(i) = i + 1$. Thus $\langle\rho\rangle = (\mathbb{Z}_n)_L$ is the left and right regular representation of $\mathbb{Z}_n$. For $H \leq \mathbb{Z}_n$, we denote by H_L the subgroup of $(\mathbb{Z}_n)_L$ consisting of all maps $x \to x + h$, where $h \in H$. *Note that* $\langle\rho\rangle \leq \mathrm{Aut}(\Gamma)$ *for any circulant digraph of order* n. *All permutation groups of degree* n *in this paper will contain* ρ.

3. The Main Tools

The following result [29, Theorem 2.3] is a translation into a group theoretic language of results contained in [20, 23, 24], which have been proved using Schur rings. We have modified part (1) slightly to clarify the meaning. In the special case of circulant digraphs of square-free order n, a result equivalent to this result was proved independently in [18]. This will be our main tool for analyzing the automorphism group of a circulant digraph.

Theorem 3.1. *Let $G \leq S_n$ contain a regular cyclic subgroup $\langle\rho\rangle$. Then one of the following statements holds:*

(1) *there exist integers $n_1, \ldots, n_r$ such that $n = n_1 n_2 \cdots n_r$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$, and there exist groups $G_1, \ldots, G_r$ such that $G_i \leq S_{n_i}$, G_i is either S_{n_i} or it contains a normal regular cyclic group of order n_i, and $G^{(2)} = G_1 \times \cdots \times G_r$;*

(2) *G has a normal subgroup M whose orbits form a nontrivial 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 $b = |M \cap \langle\rho\rangle|$, and $\bar{K}_b$ is the complement of a complete graph of order b.*

It will be shown below that if the automorphism group of a digraph has form (2) from this theorem, it satisfies the definition of a generalized wreath circulant digraph.

Definition 3.2. A circulant digraph Γ with connection set 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 $1 < K \leq H < \mathbb{Z}_n$ such that $S \setminus H$ is a union of cosets of K.

There are actually many alternative ways of looking at the automorphism group of a generalized wreath circulant digraph. Although we do not require all of these in this paper, various characterizations have been used by different authors in the literature, so we believe that it is useful to show that they are all equivalent. We require one definition before stating the result.

Definition 3.3. Let B be a block of G. The action of G on B is *faithful* if for every $g \in G$ that fixes B, $g|_B = 1|_B$ implies $g = 1$. For block systems $\mathcal{B}$ and $\mathcal{C}$, we write $\mathcal{B} \preceq \mathcal{C}$ if every block of $\mathcal{C}$ is a union of blocks of $\mathcal{B}$.

Lemma 3.4. *Suppose that $G \leq S_n$ contains a regular cyclic subgroup $\langle\rho\rangle$. Then the following are equivalent:*

(1) *G is the automorphism group of a generalized wreath circulant digraph;*

(2) *G has a normal subgroup M whose orbits form a nontrivial 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 is of the form $\Gamma = (\Gamma/\mathcal{B}) \wr \bar{K}_b$, where $b = |M \cap \langle\rho\rangle|$, and $\bar{K}_b$ is the complement of a complete graph of order b;*

(3) *there exist nontrivial block systems $\mathcal{B} \preceq \mathcal{C}$ of $\langle\rho\rangle \leq H \leq G$ such that $\mathrm{fix}_{H^{(2)}}(\mathcal{B})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$;*

(4) *G has a nontrivial block system $\mathcal{D}$ such that $\mathrm{fix}_{G^{(2)}}(\mathcal{D})$ does not act faithfully on $D \in \mathcal{D}$, and $\mathrm{fix}_G(\mathcal{D})|_D$ is primitive; and*

(5) *$G^{(2)} = G_1 \cap G_2$, where $G_1 = S_r \wr H_1$ and $G_2 = H_2 \wr S_k$, H_1 and H_2 are 2-closed groups, $r \mid (n/k)$, and $1 < r, k < n$.*

Proof. (1)⇔(3): This is [14, Lemma 2.9].

(2)⇒(3): This is [14, Lemma 2.8].

(3)⇒(4): Choose $\mathcal{D} \preceq \mathcal{B}$ to be nontrivial such that there exists no nontrivial $\mathcal{E} \prec \mathcal{D}$. Let $D \in \mathcal{D}$. By [17, Lemma 1.14], $\mathrm{fix}_{G^{(2)}}(\mathcal{D})|_D$ is primitive. If $\mathrm{Stab}_G(\mathcal{D})|_D$ is imprimitive with nontrivial block system $\mathcal{E}'$, then by [16, Exercise 1.5.10] G admits a nontrivial block system $\mathcal{E} \prec \mathcal{D}$ with the blocks of $\mathcal{E}'$ also being blocks of $\mathcal{E}$. Then $\mathcal{E}$ is a block system of $G^{(2)}$ by [42, Theorem 4.11]. So $\mathrm{Stab}_G(D)|_D$ is primitive. If $\mathrm{fix}_G(\mathcal{D})|_D$ is imprimitive, then as $\mathrm{fix}_G(\mathcal{D}) \triangleleft \mathrm{Stab}_G(D)$ we have $g(\mathcal{E}')$ is also a block system of $\mathrm{fix}_G(\mathcal{D})|_D$. However, as $\mathrm{fix}_G(\mathcal{D})|_D$ contains a regular cyclic subgroup, $\mathrm{fix}_G(\mathcal{D})|_D$ has a unique block system with blocks of a given size. Then $g(\mathcal{E}') = \mathcal{E}'$ for every $g \in \mathrm{Stab}_G(D)$ and so $\mathcal{E}'$ is a block system of $\mathrm{Stab}_G(D)|_D$, a contradiction. Thus $\mathrm{fix}_G(\mathcal{D})|_D$ is primitive. As $\mathcal{D} \preceq \mathcal{B} \preceq \mathcal{C}$ and (3) holds, we have $\mathrm{fix}_{G^{(2)}}(\mathcal{D})|_C \leq G^{(2)}$ for every $C \in \mathcal{C}$, so $\mathrm{fix}_{G^{(2)}}(\mathcal{D})$ does not act faithfully on $D \in \mathcal{D}$.

(4)⇒(5): This is [18, Lemma 28] (and we remark that it is not necessary that n be square-free in the hypothesis of Lemma 28).

(5)⇒(2): Let $\bar{H}_1$ be the largest subgroup of H_1 that has a block system of $n/(rk)$ blocks of size k (so $S_r \wr \bar{H}_1$ has a block system of n/k blocks of size k), and $\bar{H}_2$ the largest subgroup of H_2 that has a block system of r blocks of size $n/(rk)$ (so $\bar{H}_2 \wr S_k$ has a block system consisting of r blocks of size n/r). As any block system of either $S_r \wr H_1$ or $H_2 \wr S_k$ is also a block system of $G^{(2)}$, $G^{(2)}$ has a block system $\mathcal{B}$ of n/k blocks of size k and a block system $\mathcal{C}$ of r blocks of size n/r. Note that as $G^{(2)}$ contains a regular cyclic subgroup $\langle\rho\rangle$, there is exactly one block system with blocks of a given size t formed by the orbits of the unique subgroup of $\langle\rho\rangle$ of order t. We conclude that $\mathcal{B} \preceq \mathcal{C}$ and that $\mathcal{B}$ and $\mathcal{C}$ are the block systems that we have determined of both $S_r \wr \bar{H}_1$ and $\bar{H}_2 \wr S_k$. We also have $G^{(2)} = (S_r \wr \bar{H}_1) \cap (\bar{H}_2 \wr S_k)$ since $G^{(2)}$ cannot contain any elements that do not preserve $\mathcal{B}$ and $\mathcal{C}$.

Now, $\langle \rho^{n/k} \rangle \leq \mathrm{fix}_G(\mathcal{B})$, and we claim that $\rho^{n/k}|_C \in G^{(2)}$ for every $C \in \mathcal{C}$. This follows as $\rho^{n/k}|_C$ is certainly in $S_r \wr \bar{H}_1$, and $\rho^{n/k}|_C$ is in $\bar{H}_2 \wr S_k$ as $\rho^{n/k}|_B$ is in $\bar{H}_2 \wr S_k$ and $B \in \mathcal{B} \preceq \mathcal{C}$. As every block system of $G^{(2)}$ is also a block system of G [42, Theorem 4.11] ([42] is included in the more accessible [43]), both $\mathcal{B}$ and $\mathcal{C}$ are also block systems of G. Set $M = \mathrm{fix}_G(\mathcal{B}) \triangleleft G$. As G contains a regular cyclic subgroup, the orbits of M form $\mathcal{B}$. Now let Γ be a connected generalized orbital digraph. As Γ is connected, there exist distinct blocks $B, B' \in \mathcal{B}$ such that $\vec{xy} \in E(\Gamma)$ for some $x \in B$, $y \in B'$ and $B \subset C$, $B' \subset C'$, $C, C' \in \mathcal{C}$ and $C \neq C'$. Let Γ_{xy} be the orbital digraph of G such that $\vec{xy} \in E(\Gamma_{xy})$. Then $G^{(2)} \leq \mathrm{Aut}(\Gamma_{xy})$ so that $\rho^{n/k}|_C, \rho^{n/k}|_{C'} \in \mathrm{Aut}(\Gamma_{xy})$. We conclude that $\vec{x'y'} \in E(\Gamma_{xy})$ for every $x' \in B$, $y' \in B'$. Furthermore, as $\mathcal{B}$ is a block system of G, Γ_{xy} contains no edges whose endpoints are within a block of $\mathcal{B}$. Then $\Gamma_{xy} = \Gamma_{xy}/\mathcal{B} \wr \bar{K}_k$, and the result follows with $b = k$. □

The next lemma will prove useful in analyzing the structure of a circulant digraph, if (1) of Theorem 3.1 applies to its automorphism group. It is essentially a special case of a lemma that appears in [14].

Lemma 3.5. *Suppose that n is a positive integer with $m|n$, $m \geq 4$, and $\gcd(m, n/m) = 1$, and that $\Gamma = \Gamma(\mathbb{Z}_n, S)$ where $\mathrm{Aut}(\Gamma) = S_m \times K$. Let $\mathcal{B}$ be the block system formed by the orbits of $S_m \times 1_K$. Then $S \cap B \in \{\emptyset, \{h\}, B - \{h\}, B\}$ for every $B \in \mathcal{B}$, where h is the unique element of $\langle m \rangle \cap B$ (recall that $V(\Gamma) = \mathbb{Z}_n$, $\langle m \rangle \leq \mathbb{Z}_n$ is the unique subgroup of order n/m, and B is a coset of the unique subgroup $\langle n/m \rangle \leq \mathbb{Z}_n$ of order n/m).*

Proof. For this to be immediate from [14, Lemma 2.16], we need only show that K is 2-closed. Now, by [15, Theorem 5.1], $(S_m \times K)^{(2)} = S_m^{(2)} \times K^{(2)} = S_m \times K^{(2)}$, so since $G = \mathrm{Aut}(\Gamma)$ is a 2-closed group, we have

$$S_m \times K = G = G^{(2)} = (S_m \times K)^{(2)} = S_m \times K^{(2)},$$

giving $K = K^{(2)}$. □

The following theorem gives the automorphism group of a wreath product digraph.

Theorem 3.6. [19, Theorem 5.7] *For any finite vertex-transitive digraph $\Gamma \cong \Gamma_1 \wr \Gamma_2$, if $\mathrm{Aut}(\Gamma) \neq \mathrm{Aut}(\Gamma_1) \wr \mathrm{Aut}(\Gamma_2)$ then there are some natural numbers $r > 1$ and $s > 1$ and vertex-transitive digraphs Γ_1' and Γ_2' for which either*

- *$\Gamma_1 \cong \Gamma_1' \wr K_r$ and $\Gamma_2 \cong K_s \wr \Gamma_2'$; or*
- *$\Gamma_1 \cong \Gamma_1' \wr \bar{K}_r$ and $\Gamma_2 \cong \bar{K}_s \wr \Gamma_2'$,*

and $\mathrm{Aut}(\Gamma) \cong \mathrm{Aut}(\Gamma_1') \wr (S_{rs} \wr \mathrm{Aut}(\Gamma_2'))$.

With these tools in hand, we are ready to examine the circulant digraphs of small valency.

4. Circulant digraphs of small valency

In this section, we will analyze the structure and the automorphism groups of circulant digraphs of order n whose valency is no greater than $2p$, where p is the smallest prime divisor of n.

We require some additional definitions to perform our analysis.

Definition 4.1. A circulant digraph Γ of order n is called a *normal circulant digraph* if $(\mathbb{Z}_n)_L \triangleleft \mathrm{Aut}(\Gamma)$.

Normal circulant digraphs have been introduced in the more general context of normal Cayley graphs of a group G by M. Y. Xu [44]. By $\mathbb{Z}_n^*$ we denote the group of units of $\mathbb{Z}_n$.

Theorem 4.2. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be a circulant digraph of order n such that Γ has valency $d \leq 2p$, where p is the smallest prime divisor of n. Then one of the following is true:*

(1) *Γ is connected and one of the following is true:*
   (a) *Γ is a normal circulant digraph of $\mathbb{Z}_n$;*
   (b) *$d = 2p-2$, $S = (u + \langle n/p \rangle) - \{h\}$ for some $u \in \mathbb{Z}_n^*$, and $h \in (u + \langle n/p \rangle) \cap \langle p \rangle$. Furthermore, p^2 does not divide n. In this case, $\mathrm{Aut}(\Gamma) = \mathbb{Z}_{n/p} \times S_p$;*
   (c) *$d = 2p$ and $S = \{n/p, 2n/p, \ldots, (p-1)n/p, w\}$, where $w \equiv 0 \pmod{p}$ and $w \pmod{n/p}$ is a unit. In this case, $\mathrm{Aut}(\Gamma) = \mathbb{Z}_{n/p} \times S_p$;*

(d) $d = 2p$ *and* $S = [(u + \langle n/p \rangle) - \{h\}] \cup \{w\}$, *where* $u \in \mathbb{Z}_n^*$, $h \in (u + \langle n/p \rangle)$, $w \equiv 0 \pmod p$, *and* $\langle u \pmod{n/p}, w \pmod{n/p} \rangle = \mathbb{Z}_{n/p}$. *In this case,* $\mathrm{Aut}(\Gamma) = \mathbb{Z}_{n/p} \times S_p$;

(e) $d = 2p$, $\Gamma = C_{n/p} \wr \bar{K}_p$, *where* $C_{n/p}$ *is a directed cycle of length* n/p. *In this case,* $\mathrm{Aut}(\Gamma) = \mathbb{Z}_{n/p} \wr S_p$.

(2) Γ *is disconnected and*

(a) Γ *has no edges. In this case,* $\mathrm{Aut}(\Gamma) = S_n$; *or*

(b) $\Gamma \cong \bar{K}_m \wr \Gamma'$, *where* Γ' *is a connected circulant digraph of order* k, $mk = n$ *(and so* Γ' *is one of the digraphs listed in part (1)). In this case,* $\mathrm{Aut}(\Gamma) = S_m \wr \mathrm{Aut}(\Gamma')$.

Proof. Let $G = \mathrm{Aut}(\Gamma)$, so $G = G^{(2)}$.

If Γ is disconnected, then the components of Γ form a block system $\mathcal{C}$. Since any disconnected vertex-transitive digraph can be written as a wreath product of a graph with no edges and any connected component of the digraph, we have $\Gamma \cong \bar{K_m} \wr \Gamma[C]$ where $C \in \mathcal{C}$ has order k, $mk = n$, and $\Gamma[B]$ denotes the subgraph of Γ induced by B. The hypotheses of this theorem hold with respect to $\Gamma[C]$, and $\Gamma[C]$ is connected. As $G = S_m \wr \mathrm{Aut}(\Gamma[C])$ by Theorem 3.6, the proof is complete in this case.

We now assume that Γ is connected. By Theorem 3.1 and Lemma 3.4, one of the following is true:

(i) there exist nontrivial block systems $\mathcal{B} \preceq \mathcal{C}$ of G such that $\mathrm{fix}_G(\mathcal{B})|_C \leq G$ for every $C \in \mathcal{C}$, or

(ii) there exist integers $n_1, \ldots, n_r$ such that $n = n_1 n_2 \cdots n_r$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$, and there exist groups $G_1, \ldots, G_r$ such that $G_i \leq S_{n_i}$, G_i is either S_{n_i} or it contains a normal regular cyclic group of order n_i, and $G^{(2)} = G_1 \times \cdots \times G_r$.

Suppose (i) occurs and some vertex $v \in B \in \mathcal{B}$ is out-adjacent to some vertex of $B' \subset C'$, where $B \not\subset C'$, $C' \in \mathcal{C}$. Since $\mathrm{fix}_G(\mathcal{B})|_{C'} \leq G$ fixes v and is transitive on B', we see that v has out-valency (and in-valency) at least $|B| \geq p$, and so valency at least $2p$. Consequently every vertex has valency exactly $2p$, and so $\mathcal{B}$ consists of n/p blocks of size p. As Γ is connected, so is $\Gamma/\mathcal{B}$, and the only edge directed from B is to B', so B has outdegree (and indegree) 1 in $\Gamma/\mathcal{B}$. We conclude that $\Gamma/\mathcal{B}$ is a directed cycle, $\Gamma = C_{n/p} \wr \bar{K}_p$, and (1e) follows.

If (ii) occurs and $n = p$, then either G is doubly-transitive or $G < \mathrm{AGL}(1, p)$ by Burnside's Theorem [16, Theorem 3.5B] (and the fact that $\mathrm{AGL}(1, p)$ is itself doubly-transitive). If $G < \mathrm{AGL}(1, p)$ then Γ is a normal circulant digraph, so (1a) follows. Otherwise, Γ is complete, $G = S_p$, and (1b) occurs.

If (ii) occurs and $n > p$, then since $p \mid n$, we have $n \geq p + 2$. We conclude that $\Gamma \neq K_n$. This follows since K_n has valency $2n - 2 \geq 2p + 2 > 2p$, a contradiction. Also, if Γ is a normal circulant then (1a) follows, so the only remaining possibility is that some $G_i = S_{n_i}$ and S_{n_i} does not have a normal cyclic subgroup. Hence $n_i \neq 2$ or 3.

If some $G_i = S_{n_i}$, with $n_i \neq p$, then G has a block system $\mathcal{C}$ with n_i blocks of size n/n_i formed by the orbits of $G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_r$. The action of $G/\mathcal{C} = S_{n_i}$ is doubly-transitive and so if a vertex $v \in C \in \mathcal{C}$ is out-adjacent to a vertex in $C' \in \mathcal{C}$ with $C' \neq C$, then v is out-adjacent to at least $n_i - 1$ vertices of Γ. So v has valency at least $2(n_i - 1) \leq 2p$ and $n_i - 1 \leq p$. Since $n_i - 1 \geq p - 1$ and $n_i \neq p$, we conclude that $n_i - 1 = p$. As p is the smallest prime divisor of n, n_i is prime, and so both p and $p + 1$ are prime. This implies that $p = 2$ and $n_i = 3$, a contradiction. Hence $n_i = p \geq 5$.

Since $n_i = p \geq 5$ and $\gcd(n_i, n_k) = 1$ if $i \neq k$, we see that $\gcd(p, n/p) = 1$. Let $\mathcal{B}$ be the block system of G formed by the orbits of $1_{S_{n/p}} \times S_p$. By Lemma 3.5, $S \cap B \in \{\emptyset, \{h\}, B - \{h\}, B\}$ for every $B \in \mathcal{B}$, where h is the unique element of $\langle p \rangle \cap B$. As $1_{S_{n/p}} \times S_p \leq G$, we see $\Gamma[B] = K_p$ or $\bar{K}_p$ for every $B \in \mathcal{B}$.

If $\Gamma[B] = K_p$, then as Γ is connected Γ has valency at least $2p$, and so has valency exactly $2p$. As $\Gamma[B]$ has valency $2p-2$, $\Gamma/\mathcal{B}$ has valency 2 and so is a directed cycle. Let $B_0 \in \mathcal{B}$ with $0 \in B_0$, so that $B_0 = \{0, n/p, 2n/p, \ldots, (p-1)n/p\}$ and $\{n/p, 2n/p, \ldots, (p-1)n/p\} \subset S$. Then 0 is outadjacent to exactly one vertex w outside of B_0, and as $1_{S_{n/p}} \times S_p \leq G$, it follows that $\mathrm{Stab}_{1_{S_{n/p}}}(0) = \mathrm{Stab}_{1_{S_{n/P}}}(\ell p)$ for every integer ℓ. Then $w \equiv 0 \pmod{p}$. As 0 is outadjacent to exactly one vertex w outside of B_0 and Γ is connected, we see Γ/B is a directed cycle and therefore $w \pmod{n/p}$ is a unit. Finally, $\mathbb{Z}_{n/p} = \mathrm{Aut}(\Gamma/\mathcal{B}) \geq \mathrm{Aut}(\Gamma)/\mathcal{B} \geq \mathbb{Z}_{n/p}$, and so $G/\mathcal{B} = \mathbb{Z}_{n/p}$. Then $G = \mathbb{Z}_{n/p} \times S_p$ and (1c) follows.

As Γ is connected, there exists $u \in S$ such that $u \not\equiv 0 \pmod{p}$. Let $B \in \mathcal{B}$ such that $u \in B$. As $\gcd(n/p, p) = 1$ and each block of $\mathcal{B}$ is a coset of the unique subgroup of $\mathbb{Z}_n$ of order p, we see that each block $B' \in \mathcal{B}$ contains exactly one element $v_{B'} \in \mathbb{Z}_n$ that is 0 modulo p. Since $1_{S_{n/p}} \times S_p \leq G$, each $B' \in \mathcal{B}$ is the union of two orbits of $1_{S_{n/p}} \times S_p$, namely $\{v_{B'}\}$ and $B' - \{v_{B'}\}$. Then $S \cap B = B - \{h\}$, where $h = v_B$ is the unique element of $\langle p \rangle \cap B$, or the upper bound on the valency would force Γ to be a wreath product, and G would not satisfy (ii).

If $|S| = p - 1$, then $S = B - \{h\} = (u + H) - \{h\}$. Since $p \geq 5$ is the smallest prime divisor of n, n/p is odd. Hence, $u \pmod{n/p} \not\equiv -u \pmod{n/p}$, and $\Gamma/\mathcal{B}$ is a directed cycle whose automorphism group is $\mathbb{Z}_{n/p}$. Thus $G/\mathcal{B} = \mathbb{Z}_{n/p}$ and $G = \mathbb{Z}_{n/p} \times S_p$. Finally, as $\Gamma/\mathcal{B}$ is a directed cycle, we see that $u \pmod{n/p}$ is a unit, and as $u \not\equiv 0 \pmod{p}$ and $\gcd(p, n/p) = 1$, $u \in \mathbb{Z}_n^*$. Thus (1b) occurs.

If $|S| = p$, then there exists $w \in S$ such that $w \notin (u + H) - \{h\}$ and $w \notin \langle n/p \rangle$. As Γ is connected, $\Gamma/\mathcal{B}$ is connected, and so $\langle u, w \pmod{n/p} \rangle = \mathbb{Z}_{n/p}$. Additionally, as $d = 2p$, we see $w \equiv 0 \pmod{p}$ by Lemma 3.5. Now suppose that $G/\mathcal{B} \neq \mathbb{Z}_{n/p}$. As (ii) holds, $G/\mathcal{B}$ contains a nontrivial automorphism of $\mathbb{Z}_{n/p}$. As $\gcd(n/p, p) = 1$, we see that G contains a nontrivial automorphism α of $\mathbb{Z}_n$ such that $\alpha/\mathcal{B} \neq 1$. Now, α cannot fix both u and w, as otherwise α fixes every element of $\langle u, w \rangle = \mathbb{Z}_n$. Let $w \in B' \in \mathcal{B}$ (and recall that $u \in B \in \mathcal{B}$). As $p \neq 2$, $|S \cap B| \neq |S \cap B'|$, and so α cannot map B to B' or vice versa. We conclude $|S| \geq p + 1$, a contradiction. Hence $G/\mathcal{B} = \mathbb{Z}_{n/p}$ and $G = \mathbb{Z}_{n/p} \times S_p$, and (1d) follows. □

5. Unit circulant digraphs

In this section, we examine the full automorphism group of circulant digraphs of order n whose connection set S is contained in $\mathbb{Z}_n^*$. We will need a definition before we can state the main result.

Definition 5.1. 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.

Theorem 5.2. *Let Γ be a nonempty unit circulant digraph of order n. Then one of the following is true:*

(1) *Γ is a normal circulant digraph;*

(2) $\Gamma \cong \Gamma_1 \wr \bar{K}_\ell$, *where* $\ell | n$ *and* Γ_1 *is a unit circulant digraph of order* n/ℓ *that cannot be written as a nontrivial wreath product. Thus* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \wr S_\ell$. *Furthermore, if* $p \mid \ell$ *is prime, then* $p \mid (n/\ell)$ *as well;*

(3) $\Gamma \cong \Gamma_1 \wr \bar{K}_p - p\Gamma_1$, *where* p *is prime,* $\gcd(n/p, p) = 1$, *and* Γ_1 *is a unit circulant digraph of order* n/p *that cannot be written as a nontrivial wreath product. Thus* Γ *is a deleted wreath product, and* $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \times S_p$.

Proof. Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$, where $S \subseteq \mathbb{Z}_n^*$, and let $G = \mathrm{Aut}(\Gamma)$. By Theorem 3.1, one of the following is true:

(a) there exist integers $n_1, \ldots, n_r$ such that $n = n_1 n_2 \cdots n_r$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$, and there exist groups $G_1, \ldots, G_r$ such that $G_i \leq S_{n_i}$, G_i is either S_{n_i} or it contains a normal regular cyclic group of order n_i, and $G^{(2)} = G_1 \times \cdots \times G_r$, or

(b) $\mathrm{Aut}(\Gamma)$ has a normal subgroup M whose orbits form a block system $\mathcal{B}$ of $\mathrm{Aut}(\Gamma)$ such that each connected generalized orbital digraph contains a subdigraph Γ' which is an orbital digraph of $\mathrm{Aut}(\Gamma)$ and is of the form $\Gamma' \cong (\Gamma'/\mathcal{B}) \wr \bar{K}_b$, where $b = |M \cap \langle \rho \rangle|$.

We consider the cases above separately.

If (b) occurs, then by Lemma 3.4 (3) (with $G = \mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma)^{(2)}$) there exists a nontrivial block system $\mathcal{B} \preceq \mathcal{C}$ of $\mathrm{Aut}(\Gamma)$ such that $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})|_C \leq \mathrm{Aut}(\Gamma)$ for every $C \in \mathcal{C}$. So if G has blocks of size i, then since $\langle n/i \rangle \cap S = \emptyset$, the induced subgraph of Γ on any block is $\bar{K}_i$. In particular, if $\Gamma = \Gamma_1 \wr \Gamma_2$ then Γ_2 is an empty digraph. Observe that since $\mathcal{B} \preceq \mathcal{C}$, and $\mathcal{B}$ is formed by the orbits of $K_L \leq \langle \rho \rangle$ while $\mathcal{C}$ is formed by the orbits of $H_L \leq \langle \rho \rangle$, we have $K \leq H$. As $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{B})|_C \leq \mathrm{Aut}(\Gamma)$ and the induced subgraph on C is empty for any $C \in \mathcal{C}$, between blocks of $\mathcal{B}$ there must either be no edges, all directed edges, or all edges in one direction and none in the other. Clearly then $\Gamma = \Gamma' \wr \bar{K}_k$, for some circulant digraph Γ' of order m, where $mk = n$ and $k = |B|$. Also, if $\Gamma = \Gamma'' \wr \bar{K}_{k'}$ for some Γ'' and k', and Γ is a unit circulant, it is easy to see Γ'' is also a unit circulant. Choose t maximal such that $\Gamma = \Gamma_1 \wr \bar{K}_t$. As noted earlier, if $\Gamma_1 = \Gamma_1' \wr \Gamma_2$ then Γ_2 is empty, contradicting the maximality of t. Then Γ_1 is a unit circulant digraph that cannot be written as a nontrivial wreath product, and $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \wr S_\ell$ by Theorem 3.6.

It now only remains to show that if $p \mid \ell$ is prime, then $p \mid (n/\ell)$ as well. Suppose otherwise, and let k be the largest positive integer such that $p^k \mid \ell$. Then $\Gamma = (\Gamma_1 \wr \bar{K}_{\ell/p^k}) \wr \bar{K}_{p^k}$. Let $L \leq \mathbb{Z}_n$ be the unique subgroup of $\mathbb{Z}_n$ of order p^k, so that S is a union of cosets of L. Observe that if $u \in \mathbb{Z}_n^*$, then $u + L$ contains a nonunit of $\mathbb{Z}_n$. The result then follows.

If (a) occurs, then $\mathrm{Aut}(\Gamma)$ has block systems $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_r$ formed by the orbits of G_i (viewed as an internal direct product), and block systems $\mathcal{C}_1, \ldots, \mathcal{C}_r$, where $\mathcal{C}_j$ is formed by the orbits of $\Pi_{i=1, i\neq j}^r G_i$. Also, Γ cannot be written as a nontrivial wreath product (since its automorphism group is not a wreath product, by Theorem 3.6), and so Γ is connected. If Γ is normal, then we have (1) and are done, so we assume that Γ is not normal. Hence some $G_i = S_{n_i}$ with $n_i \geq 4$. By Lemma 3.5, $S \cap B \in \{\emptyset, \{h\}, B - \{h\}, B\}$ for every $B \in \mathcal{B}_i$, where h is the unique element of $\langle m \rangle \cap B$. Since $h \in \langle m \rangle$ and Γ is a unit circulant, $h \notin S$, so in fact we can conclude that $S \cap B \in \{\emptyset, B - \{h\}\}$ for every $B \in \mathcal{B}_i$.

Note that for some $B \in \mathcal{B}_i$, we have $S \cap B = B - \{h\}$, since Γ is nonempty. If n_i is composite, then observe that every coset of $\langle n/n_i \rangle$ contains at least two nonunits as $\gcd(n/n_i, n_i) = 1$ and $\mathbb{Z}_{n_i}$ contains at least two nonunits. So B contains at least two nonunits, at least one of which much be in S, a contradiction that shows that n_i is prime. This shows $\Gamma \cong \Gamma_1 \wr \bar{K}_{n_i} - n_i\Gamma_1$. Clearly, since Γ is a unit circulant, Γ_1 is also a unit circulant.

Note that $\mathrm{Aut}(\Gamma)/\mathcal{B}_i \leq \mathrm{Aut}(\Gamma_1)$, so $\mathrm{Aut}(\Gamma) \leq \mathrm{Aut}(\Gamma_1) \times S_{n_i}$. Conversely, let $g \in \mathrm{Aut}(\Gamma_1)$. Viewing $\mathbb{Z}_n$ as $\mathbb{Z}_{n/n_i} \times \mathbb{Z}_{n_i}$, we certainly have $(g, \sigma) \in \mathrm{Aut}(\Gamma_1 \wr \bar{K}_{n_i})$ for every $\sigma \in S_{n_i}$. Also, $n_i\Gamma_1 = \bar{K}_{n_i} \wr \Gamma_1$ so $\mathrm{Aut}(n_i\Gamma_1) = S_{n_i} \wr \mathrm{Aut}(\Gamma_1)$. We conclude that $(g, \sigma) \in \mathrm{Aut}(n_i\Gamma_1)$, for every $\sigma \in S_{n_i}$, so $(g, \sigma) \in \mathrm{Aut}(\Gamma)$. Thus $\mathrm{Aut}(\Gamma_1) \times S_{n_i} \leq \mathrm{Aut}(\Gamma)$ and so $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \times S_{n_i}$. It now only remains to show that Γ_1 cannot be written as a nontrivial wreath product.

If $\Gamma_1 = \Gamma_2 \wr \Gamma_3$, where Γ_2 and Γ_3 are circulant digraphs of orders s and t, respectively, then since Γ_1 is a unit circulant, by arguments above $\Gamma_3 = \bar{K}_t$ with t chosen to be maximal. Then $\mathrm{Aut}(\Gamma_1) = \mathrm{Aut}(\Gamma_2) \wr S_t$ and so $\mathrm{Aut}(\Gamma) = (\mathrm{Aut}(\Gamma_2) \wr S_t) \times S_p$. Hence $(1_{S_s} \wr S_t) \times 1_{S_p} \triangleleft \mathrm{Aut}(\Gamma)$, and so the orbits of $(1_{S_s} \wr S_t) \times 1_{S_p}$ form a block system $\mathcal{C}$ consisting of sp blocks of size t, and $(1_{S_s} \wr S_t) \times 1_{S_p} \leq \mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{C})$. Then $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{C})$ does not act faithfully on $C \in \mathcal{C}$, and $\mathrm{fix}_{\mathrm{Aut}(\Gamma)}(\mathcal{C})|_C$ is primitive for every $C \in \mathcal{C}$. By Lemma 3.4, Γ is generalized wreath circulant and satisfies (b), a contradiction. □

6. Endomorphism monoids of reflexive circulant digraphs

In this section, we use a technique described in [4] to determine the automorphism groups of the endomorphism monoids of reflexive circulant digraphs of two types. These types correspond to the families discussed in the previous sections. (Note that $\Gamma(\mathbb{Z}_n, S)$ is reflexive if and only if $0 \in S$.) This technique uses the notion of the normalizer of a monoid of transformations on $\mathbb{Z}_n$.

Definition 6.1. Let T be a semigroup of transformations on the set $\mathbb{Z}_n$. Then

$$N_{S_n}(T) = \{g \in S_n : gTg^{-1} = T\}$$

is called the *normalizer* of T in S_n. It is clear that $N_{S_n}(T)$ is a subgroup of S_n.

Theorems 4.2 and 5.2 enable us to describe the normalizer of $\mathrm{Aut}(\Gamma)$, where Γ is a circulant graph from one of the two families under discussion.

Corollary 6.2. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be either a circulant digraph of valency at most $2p$, where p is the smallest prime divisor of n, or a unit circulant digraph. Then $N_{S_n}(\mathrm{Aut}(\Gamma)) = \mathrm{Aut}(\Gamma) \cdot \mathrm{Aut}(\mathbb{Z}_n)$.*

Proof. By [4, Theorem 4.4] and the fact that all such graphs are CI-graphs (see [28, Theorem 1.1 (1)], and [17] or [35]), we have $N_{S_n}(\mathrm{Aut}(\Gamma)) \leq \mathrm{Aut}(\Gamma) \cdot \mathrm{Aut}(\mathbb{Z}_n)$. We need only show that $\mathrm{Aut}(\mathbb{Z}_n)$ normalizes $\mathrm{Aut}(\Gamma)$. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ and $m = \sum_{i=1}^{r} a_i$. Observe first that if $(\mathbb{Z}_n)_L \triangleleft \mathrm{Aut}(\Gamma)$, then the result is true. This follows as $\mathrm{Aut}(\mathbb{Z}_n) \cdot (\mathbb{Z}_n)_L/(\mathbb{Z}_n)_L = \mathrm{Aut}(\mathbb{Z}_n)$ is abelian, and so every subgroup of $\mathrm{Aut}(\mathbb{Z}_n) \cdot (\mathbb{Z}_n)_L/(\mathbb{Z}_n)_L$ is normal. This implies that every subgroup of $\mathrm{Aut}(\mathbb{Z}_n) \cdot (\mathbb{Z}_n)_L$ that contains $(\mathbb{Z}_n)_L$ is normal in $\mathrm{Aut}(\mathbb{Z}_n) \cdot (\mathbb{Z}_n)_L$, and so $\mathrm{Aut}(\Gamma) \triangleleft \mathrm{Aut}(\mathbb{Z}_n) \cdot (\mathbb{Z}_n)_L$. We proceed by induction on m.

If $m = 1$, then either $\mathrm{Aut}(\Gamma) < \mathrm{AGL}(1,n)$ or $\mathrm{Aut}(\Gamma) = S_n$. The latter case is trivial, while in the former case $(\mathbb{Z}_n)_L \triangleleft \mathrm{Aut}(\Gamma)$. So we assume the result is true for all such circulant digraphs with $\sum_{i=1}^{r} a_i = m$, and let Γ be an appropriate circulant digraph with $\sum_{i=1}^{r} a_i = m+1$. By arguments above, we may assume that Γ is not a normal circulant digraph. By Theorems 4.2 and 5.2 there are three possibilities for $\mathrm{Aut}(\Gamma)$, which we now consider in turn.

If $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \times S_p$ where p is prime and Γ_1 is a circulant digraph of order n/p relatively prime to p, and either $\mathrm{Aut}(\Gamma_1) = \mathbb{Z}_{n/p}$ or Γ_1 is a unit circulant digraph, then by induction, $\mathrm{Aut}(\mathbb{Z}_{n/p})$ normalizes $\mathrm{Aut}(\Gamma_1)$. As $\gcd(n/p, p) = 1$,

$$\mathrm{Aut}(\mathbb{Z}_n) = \mathrm{Aut}(\mathbb{Z}_{n/p}) \times \mathrm{Aut}(\mathbb{Z}_p) \leq \mathrm{Aut}(\mathbb{Z}_{n/p}) \times S_p$$

and $\mathrm{Aut}(\mathbb{Z}_{n/p}) \times S_p$ normalizes $\mathrm{Aut}(\Gamma_1) \times S_p$. Hence $\mathrm{Aut}(\mathbb{Z}_n)$ normalizes $\mathrm{Aut}(\Gamma)$ as required.

If $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \wr S_\ell$ where Γ_1 is a unit circulant digraph of order n/ℓ, then by the induction hypothesis $\mathrm{Aut}(\mathbb{Z}_{n/\ell})$ normalizes $\mathrm{Aut}(\Gamma_1)$ and by [4, Lemma 4.10] we see that $\mathrm{Aut}(\mathbb{Z}_{n/\ell}) \times S_\ell$ normalizes $\mathrm{Aut}(\Gamma)$. As $\mathrm{Aut}(\Gamma) = \mathrm{Aut}(\Gamma_1) \wr S_\ell$ normalizes $\mathrm{Aut}(\Gamma)$, we have $\mathrm{Aut}(\mathbb{Z}_{n/\ell}) \wr S_\ell$ normalizes $\mathrm{Aut}(\Gamma)$. Clearly $\mathrm{Aut}(\mathbb{Z}_n) \leq \mathrm{Aut}(\mathbb{Z}_{n/\ell}) \wr S_\ell$, and so $\mathrm{Aut}(\mathbb{Z}_n)$ normalizes $\mathrm{Aut}(\Gamma)$.

If $\mathrm{Aut}(\Gamma) = S_m \wr \mathrm{Aut}(\Gamma')$ where Γ' is a connected circulant of order n/m whose valency is at most $2p$ where p is the smallest prime divisor of n, then both $\mathrm{Aut}(\Gamma)$ and $(\mathbb{Z}_n)_L \cdot \mathrm{Aut}(\mathbb{Z}_n)$ have a block system $\mathcal{C}$ formed by the connected components of Γ. Hence $\mathrm{Aut}(\mathbb{Z}_n)/\mathcal{C} \leq S_m = \mathrm{Aut}(\Gamma)/\mathcal{C}$. Let $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$. Now there exists $\gamma \in S_m \times 1_{S_{n/m}} \leq \mathrm{Aut}(\Gamma)$ such that $\gamma\alpha/\mathcal{C} = 1$. Let H be the unique subgroup of $(\mathbb{Z}_n)_L$ of order n/m, so both γ and α normalize H. Applying [16, Corollary 4.2B] we obtain $\gamma\alpha|_C \leq (\mathbb{Z}_{n/m})_L \cdot \mathrm{Aut}(\mathbb{Z}_{n/m})$. Now observe that every element of $\mathbb{Z}_n$ may be written uniquely as $i + jm$ where $0 \leq i \leq m-1$ and $0 \leq j \leq n/m - 1$. As $\gamma\alpha/\mathcal{C} = 1$, we see that $\gamma\alpha(i+jm) = i + \delta_i(j)m$, where $\delta_i \in S_{n/m}$. Since $\gamma\alpha|_C \leq (\mathbb{Z}_{n/m})_L \cdot \mathrm{Aut}(\mathbb{Z}_{n/m})$, it follows that $\delta_i(j) = \alpha_i j + b_i$, where $\alpha_i \in \mathbb{Z}_{n/m}^*$ and $b_i \in \mathbb{Z}_{n/m}$. As $1_{S_m} \wr (\mathbb{Z}_{n/m})_L \leq \mathrm{Aut}(\Gamma)$, the map δ which maps $i + jm$ to $i + (j - b_i)m$ is in $\mathrm{Aut}(\Gamma)$ and normalizes H. Hence $\delta\gamma\alpha(i+jm) = i + \alpha_i jm$. Define $\rho : \mathbb{Z}_n \mapsto \mathbb{Z}_n$ by $\rho(i+jm) = i + (j+1)m$ so that $H = \langle\rho\rangle$. Then $(\delta\gamma\alpha)\rho(\delta\gamma\alpha)^{-1}(i+jm) = i + (j+\alpha_i)m$, and $(\delta\gamma\alpha)\rho(\delta\gamma\alpha)^{-1} \in H$. We conclude that $\alpha_i = \alpha_{i'}$ for all $0 \leq i, i' \leq n/m - 1$. As $\mathrm{Aut}(\mathbb{Z}_{n/m})$ normalizes $\mathrm{Aut}(\Gamma')$ by induction, we see that $\delta\gamma\alpha$ normalizes $\mathrm{Aut}(\Gamma)$, and since $\delta, \gamma \in \mathrm{Aut}(\Gamma)$, we have α normalizes $\mathrm{Aut}(\Gamma)$, so $\mathrm{Aut}(\mathbb{Z}_n)$ normalizes $\mathrm{Aut}(\Gamma)$. □

Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be a reflexive circulant digraph, so $0 \in S$. We will say that Γ is a 0-*unit* circulant graph if every element of S except 0 is a unit of $\mathbb{Z}_n$. It is clear that $\mathrm{Aut}(\Gamma(\mathbb{Z}_n, S)) = \mathrm{Aut}(\Gamma(\mathbb{Z}_n, S - \{0\}))$. Thus Corollary 6.2 extends to 0-unit circulant graphs. Moreover, $\Gamma(\mathbb{Z}_n, S - \{0\})$ has valency at most $2p$ if and only if $|S| \leq p+1$, so Corollary 6.2 also extends to reflexive circulant graphs with $|S| \leq p+1$. Finally, by [4, Theorem 4.11], $N_{S_n}(\mathrm{Aut}(\Gamma)) = \mathrm{Aut}(\Gamma) \cdot \mathrm{Aut}(\mathbb{Z}_n)$ holds whenever n is square free. We summarize these observations in the following proposition.

Proposition 6.3. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be a reflexive circulant digraph of order $n \geq 2$ and let p be the smallest prime that divides n. If n is square free, or $|S| \leq p+1$, or Γ is a 0-unit circulant digraph, then $N_{S_n}(\mathrm{Aut}(\Gamma)) = \mathrm{Aut}(\Gamma) \cdot \mathrm{Aut}(\mathbb{Z}_n)$.*

An *endomorphism* of a circulant digraph Γ is any mapping $\beta : \mathbb{Z}_n \to \mathbb{Z}_n$ that preserves edges. That is, whenever ij is an edge in Γ then $\beta(i)\beta(j)$ is also an edge in Γ. The set $\mathrm{End}(\Gamma)$ of all endomorphisms of Γ is a monoid under composition of mappings, called the *endomorphism monoid* of Γ. The group $\mathrm{Aut}(\Gamma)$ is then the group of units of $\mathrm{End}(\Gamma)$. For any monoid M, we have the group of automorphisms of M:

$$\mathrm{Aut}(M) = \{\phi : M \to M : \phi \text{ is a bijection and for all } x, y \in M,\ \phi(xy) = \phi(x)\phi(y)\}.$$

Suppose that Γ is reflexive. To describe $\mathrm{Aut}(\mathrm{End}(\Gamma))$, we follow the technique presented in [4, Section 4.2]. First, by [4, Theorem 1.1],

$$\mathrm{Aut}(\mathrm{End}(\Gamma)) \cong N_{S_n}(\mathrm{End}(\Gamma)). \tag{6.1}$$

Therefore, the description of $\mathrm{Aut}(\mathrm{End}(\Gamma))$ reduces to that of $N_{S_n}(\mathrm{End}(\Gamma))$. Let $\delta \in N_{S_n}(\mathrm{End}(\Gamma))$. Then clearly $\delta \in N_{S_n}(\mathrm{Aut}(\Gamma))$.

Suppose that Γ is as in Proposition 6.3. Then $\delta = \omega\alpha$ for some $\omega \in \mathrm{Aut}(\Gamma)$ and $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$. Since $\mathrm{Aut}(\Gamma)$ is a subgroup of $N_{S_n}(\mathrm{End}(\Gamma))$, $\omega\,\mathrm{End}(\Gamma)\omega^{-1} = \mathrm{End}(\Gamma)$. Thus

$$\begin{aligned}
\delta\,\mathrm{End}(\Gamma)\delta^{-1} = \mathrm{End}(\Gamma) &\Leftrightarrow (\omega\alpha)\,\mathrm{End}(\Gamma)(\omega\alpha)^{-1} = \mathrm{End}(\Gamma)\\
&\Leftrightarrow \omega(\alpha\,\mathrm{End}(\Gamma)\alpha^{-1})\omega = \mathrm{End}(\Gamma)\\
&\Leftrightarrow \alpha\,\mathrm{End}(\Gamma)\alpha^{-1} = \omega^{-1}\,\mathrm{End}(\Gamma)\omega\\
&\Leftrightarrow \alpha\,\mathrm{End}(\Gamma)\alpha^{-1} = \omega^{-1}(\omega\,\mathrm{End}(\Gamma)\omega^{-1})\omega\\
&\Leftrightarrow \alpha\,\mathrm{End}(\Gamma)\alpha^{-1} = \mathrm{End}(\Gamma).
\end{aligned}$$

It follows that

$$\delta \in N_{S_n}(\mathrm{End}(\Gamma)) \Leftrightarrow \alpha \in N_{S_n}(\mathrm{End}(\Gamma)). \tag{6.2}$$

It is well known that for every $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$, there is a unit $k \in \mathbb{Z}_n$ such that $x\alpha = xk$ for every $x \in \mathbb{Z}_n$. Consequently, $\mathrm{Aut}(\mathbb{Z}_n)$ is isomorphic to the group of units $\mathbb{Z}_n^*$ of $\mathbb{Z}_n$ via the isomorphism $\alpha \to k$, where α and k are as above. We will identify $\alpha \in \mathrm{Aut}(\mathbb{Z}_n)$ with the corresponding unit k. As in [4, Section 4.2], we consider

$$U_{\mathrm{S}}(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n^* : k\,\mathrm{End}(\Gamma)k^{-1} = \mathrm{End}(\Gamma)\},$$

which is a subgroup of $\mathbb{Z}_n^*$. Now, by Proposition 6.3, (6.1), and (6.2), we obtain the following result, which extends [4, Theorem 4.12].

Theorem 6.4. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be a reflexive circulant digraph of order $n \geq 2$ and let p be the smallest prime that divides n. If n is square free, or $|S| \leq p + 1$, or Γ is a 0-unit circulant digraph, then*

$$\mathrm{Aut}(\mathrm{End}(\Gamma)) \cong \mathrm{Aut}(\Gamma) \cdot U_S(\mathbb{Z}_n).$$

To obtain a complete description of $\mathrm{Aut}(\mathrm{End}(\Gamma))$, we need to determine $U_{\mathrm{S}}(\mathbb{Z}_n)$ for a given $S \subseteq \mathbb{Z}_n$. Some progress in the description of $U_{\mathrm{S}}(\mathbb{Z}_n)$ was made in [4] for circulant digraphs with 2-cycles and for certain 3-circulant digraphs.

Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be a circulant digraph. For $x, y \in \mathbb{Z}_n$ and $u \in S$, we will write $x \xrightarrow{u} y$ if $y = x + u$, that is, if there is an edge from x to y labeled u. We will write $x \to y$ if $y = x + u$ for some $u \in S$. Let $x_0, x_1, \ldots, x_k, y_0, y_1, \ldots, y_{k-1}$ ($k \geq 1$) be elements of $\mathbb{Z}_n$ (not necessarily distinct) such that $x_i \to x_{i+1}$, for every $i \in \{0, 1, \ldots, k-1\}$, $y_i \to y_{i+1}$, for every $i \in \{0, 1, \ldots, k-2\}$, and $y_{k-1} \to y_0$. The subgraphs $x_0 \to x_1 \to \cdots \to x_k$ and $y_0 \to y_1 \to \cdots \to y_{k-1} \to y_0$ of Γ will be called a *path* (of length k) and a *cycle* (of length k), respectively. We will say that $y_0 \to y_1 \to \cdots \to y_{k-1} \to y_0$ is a *minimal cycle* containing y_0 if $k \geq 2$, $y_0, y_1, \ldots, y_{k-1}$ are pairwise distinct, and there is no shorter cycle of length ≥ 2 with distinct vertices that contains y_0. For example, if $\Gamma = \Gamma(\mathbb{Z}_{10}, S)$ with $S = \{0, 2, 3\}$, then $0 \to 3 \to 6 \to 8 \to 0$ is a minimal cycle (of length 4) containing 0.

6.1. **Circulant digraphs with 2-cycles.** Suppose that $0 \in S$ and there is a nonzero $s \in \mathbb{Z}_n$ such that $s, -s \in S$. This happens if and only if $\Gamma = \Gamma(\mathbb{Z}_n, S)$ is reflexive and every vertex lies on a 2-cycle $x \to x' \to x$ with $x \neq x'$. Following [4, Section 4.3], we consider the following sets:

$$\begin{aligned} -S &= \{-x : x \in S\}, \\ W(S) &= \{(x, y) \in (S \cap (-S)) \times (S \cap (-S)) : x + y \notin S\}, \\ U_{\mathrm{S}}^{\pm}(\mathbb{Z}_n) &= \{k \in \mathbb{Z}_n^* : kS = S \text{ or } kS = -S\}. \end{aligned}$$

It was proved in [4, Section 4.3] that if there exists $(x, y) \in W(S)$ such that $x + y \in -S$, then $U_{\mathrm{S}}(\mathbb{Z}_n) = U_{\mathrm{S}}^{\pm}(\mathbb{Z}_n)$. This gives us the following corollary of Theorem 6.4, which extends [4, Theorem 4.18].

Corollary 6.5. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$ be a reflexive circulant digraph such that $s, -s \in S$ for some nonzero $s \in \mathbb{Z}_n$. Let p be the smallest prime that divides n. Suppose that there is $(x, y) \in W(S)$ such that $x + y \in -S$. If n is square free, or $|S| \leq p + 1$, or Γ is a 0-unit circulant digraph, then* $\mathrm{Aut}(\mathrm{End}(\Gamma)) \cong \mathrm{Aut}(\Gamma) \cdot U_S^{\pm}(\mathbb{Z}_n)$.

The group $U_{\mathrm{S}}^{\pm}(\mathbb{Z}_n)$ can be easily calculated. For example, consider $\Gamma(\mathbb{Z}_9, S)$, where $S = \{0, 2, 4, 5, 7, 8\}$. Note that $\Gamma(\mathbb{Z}_9, S)$ is a reflexive 0-unit circulant digraph with $2, -2 \in S$. We have:

$$\begin{aligned} -S &= \{0, 1, 2, 4, 5, 7\}, \\ S \cap (-S) &= \{0, 2, 4, 5, 7\}, \\ W(S) &= \{(2, 4), (4, 2), (5, 5), (5, 7), (7, 5)\}. \end{aligned}$$

Now, $(5, 5) \in W(S)$ and $5 + 5 = 1 \in -S$, so the hypothesis of Corollary 6.5 is satisfied. Thus to determine $\mathrm{Aut}(\mathrm{End}(\Gamma(\mathbb{Z}_9, S)))$, it is enough to find all $k \in \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ such that $kS = S$ or $kS = -S$. The set of all such k contains 1 and is closed under negatives, so it is enough to check $k = 2, 4$. We have $2S = \{0, 4, 8, 1, 5, 7\} \neq S$ or $-S$ and $4S = \{0, 8, 7, 2, 1, 5\} \neq S$ or $-S$. Hence $U_{\mathrm{S}}^{\pm}(\mathbb{Z}_9) = \{1, -1\}$, and so $\mathrm{Aut}(\mathrm{End}(\Gamma(\mathbb{Z}_9, S))) \cong \mathrm{Aut}(\Gamma(\mathbb{Z}_9, S)) \cdot \{1, -1\}$.

6.2. **3-circulant digraphs.** If $|S| = k$, we say that $\Gamma = \Gamma(\mathbb{Z}_n, S)$ is *k-circulant*. Suppose that $S = \{0, s, -s\}$, where $s \in \mathbb{Z}_n^*$. It was proved in [4, Section 4.4] that if $S = \{0, s, -s\}$, then $U_{\mathrm{S}}(\mathbb{Z}_n) = \{1, -1\}$ for every n. Thus, since Γ is a 0-unit circulant digraph, we have another corollary of Theorem 6.4, which extends [4, Corollary 4.19] (where it is assumed that n is square free).

Corollary 6.6. *Let* $\Gamma = \Gamma(\mathbb{Z}_n, S)$*, where* $S = \{0, s, -s\}$ *with* $s \in \mathbb{Z}_n^*$*. Then* $\mathrm{Aut}(\mathrm{End}(\Gamma)) \cong \mathrm{Aut}(\Gamma) \cdot \{1, -1\}$.

Suppose that $S = \{0, s, t\}$ with $s, t \in \mathbb{Z}_n^*$ and $s \neq t, -t$. [4, Theorem 4.21] states that for such an S,

$$\mathrm{End}(\Gamma) = \mathrm{Aut}(\Gamma) \cup \{\beta : \mathbb{Z}_n \to \mathbb{Z}_n : |\operatorname{im}(\beta)| = 1\}.$$

However, there is a gap in the proof of [4, Theorem 4.21]. In the two paragraphs following equation (4.6) in [4], we have the following implications in $\mathbb{Z}_n$:

$$m_2(k-1) = (1-k) \Rightarrow m_2 = -1,$$
$$m_2(k-1) = 0 \Rightarrow m_2 = 0,$$

where $k = s^{-1}t$ and m_2 is an integer such that $0 \leq m_2 \leq k$. These implications hold when n is prime, and this hypothesis should be added to the statement of the theorem.

For a composite n, [4, Theorem 4.21] does not hold. Let m be any number of the form $m = lq + 1$ with $l \geq 1$ and $q \geq 3$, and set $n = (q-1)m + 1$. Let $S = \{0, 1, m\}$, and consider $\Gamma = \Gamma(\mathbb{Z}_n, S)$. Now let β be the function that maps each $k \in \mathbb{Z}_n$ to rm, where $0 \leq r \leq q-1$ is given by $r \equiv k \pmod{q}$. The image of β is $\{0, m, 2m, \ldots, (q-1)m\}$, which forms a cycle of Γ. It is now straightforward to confirm that β is an endomorphism of Γ that is neither an automorphism nor a constant.

We will prove a weaker version of [4, Theorem 4.21], which will be true for a general n (see Theorem 6.9). First, we need some lemmas.

Lemma 6.7. *Let* $\Gamma = \Gamma(\mathbb{Z}_n, S)$*, where* $S = \{0, s, t\}$ *with* $s, t \in \mathbb{Z}_n^*$ *and* $t \neq s, -s$*. Then* $\beta \in \mathrm{End}(\Gamma)$ *is a constant if and only if there exist* $x \in \mathbb{Z}_n$ *and* $u \in \{s, t\}$ *such that* $\beta(x + u) = \beta(x)$.

Proof. Let $\beta \in \mathrm{End}(\Gamma)$. If β is a constant, then the desired x and u clearly exist. Conversely, suppose that there exist $x \in \mathbb{Z}_n$ and $u \in \{s, t\}$ such that $\beta(x + u) = \beta(x)$. We may assume that $u = s$, so $\beta(x + s) = \beta(x)$. We wish to prove that β is a constant.

Consider the following cycle in Γ:

$$0 = x_0 \xrightarrow{s} x_1 \xrightarrow{s} \cdots \xrightarrow{s} x_{n-1} \xrightarrow{s} x_0. \tag{6.3}$$

Since s is a unit in $\mathbb{Z}_n$, $x_0, x_1, \ldots, x_{n-1}$ are pairwise distinct, that is, (6.3) is a cycle containing all vertices of Γ. Since $\beta \in \mathrm{End}(\Gamma)$, we obtain the corresponding cycle of images:

$$\beta(x_0) \to \beta(x_1) \to \cdots \to \beta(x_{n-1}) \to \beta(x_0).$$

Since $\{x_0, x_1, \ldots, x_{n-1}\} = \mathbb{Z}_n$, $x = x_i$ for some i. Thus $\beta(x_{i+1}) = \beta(x_i + s) = \beta(x + s) = \beta(x) = \beta(x_i)$.

Suppose there exists a minimal cycle containing $x = x_i$ with at least two edges labeled s. Since any permutation of labels of edges in a cycle also gives a cycle, we have a minimal cycle containing x_i that begins with two edges labeled s:

$$x_i \xrightarrow{s} x_{i+1} \xrightarrow{s} x_{i+2} \to z_3 \to \cdots \to z_{l-1} \to x_i.$$

Since $\beta(x_{i+1}) = \beta(x_i)$, we have the corresponding cycle of images:

$$\beta(x_i) \to \beta(x_i) \to \beta(x_{i+2}) \to \beta(z_3) \to \cdots \to \beta(z_{l-1}) \to \beta(x_i). \tag{6.4}$$

By [4, Lemma 4.20], either $\beta(\{x_i, x_{i+1}, x_{i+2}, z_3, \ldots, z_{l-1}\}) = \{\beta(x_i)\}$ or (6.4) is a minimal cycle containing $\beta(x_i)$. The latter is impossible because of the initial repetition, and so $\beta(x_i) = \beta(x_{i+2})$. There exists a minimal cycle containing x_{i+1} with at least two edges labeled s. (If $y \overset{u_1}{\to} y_1 \overset{u_2}{\to} \cdots \overset{u_{l-1}}{\to} y_{l-1} \overset{u_l}{\to} y$ is a minimal cycle containing y, then the cycle $z \overset{u_1}{\to} z_1 \overset{u_2}{\to} \cdots \overset{u_{l-1}}{\to} z_{l-1} \overset{u_l}{\to} z$ is a minimal cycle containing z.) Hence we may repeat the previous argument to show that β is a constant.

Suppose there is no minimal cycle containing $x = x_i$ with at least two edges labeled s. Then every minimal cycle containing $x = x_i$ must have at least two edges labeled t. (Since $t \neq -s$, any minimal cycle has length at least 3.) Hence, every minimal cycle containing any $z \in \mathbb{Z}_n$ must have at least two edges labeled t.

Suppose $\beta(z + t) = \beta(z)$ for some $z \in \mathbb{Z}_n$. Then, by the foregoing argument with s replaced by t, β is a constant.

Suppose $\beta(z + t) \neq \beta(z)$ for every $z \in \mathbb{Z}_n$. Consider any minimal cycle containing x:

$$x \overset{u_1}{\to} y_1 \overset{u_2}{\to} y_2 \overset{u_3}{\to} \cdots \overset{u_{l-1}}{\to} y_{l-1} \overset{u_l}{\to} x, \tag{6.5}$$

and the corresponding cycle of images:

$$\beta(x) \to \beta(y_1) \to \beta(y_2) \to \cdots \to \beta(y_{l-1}) \to \beta(x). \tag{6.6}$$

We know that at least two edges in (6.5) are labeled t. Since the cycle (6.5) is minimal, it must have an edge labeled s. (Otherwise, (6.5) would have length n. Then the cycle (6.3) would be minimal, which would contradict our assumption that there is no minimal cycle containing x with at least two edges labeled s.) We may assume that $u_1 = s$ and $u_2 = t$. Then $y_1 = x + s$, and so $\beta(y_1) = \beta(x + s) = \beta(x)$. Hence (6.6) is not a minimal cycle, and so $\beta(\{x, y_1, y_2, \ldots, y_{l-1}\}) = \{\beta(x)\}$ by [4, Lemma 4.20]. Then $\beta(y_1 + t) = \beta(y_2) = \beta(y_1)$, which contradicts the assumption that $\beta(z + t) \neq \beta(z)$ for every $z \in \mathbb{Z}_n$. Therefore, the latter is impossible, which concludes the proof. □

Lemma 6.8. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$, where $S = \{0, s, t\}$ with $s, t \in \mathbb{Z}_n^*$ and $t \neq s, -s$. Let $k = s^{-1}t$ and $d = \frac{n}{\gcd(n,k-1)}$. Suppose that either* (i) *$k - 1$ is a unit in $\mathbb{Z}_n$ or* (ii) *$d > k + 1$. Let $\beta \in \mathrm{End}(\Gamma)$ be such that β is not a constant. Consider the path $z_0 \overset{s}{\to} z_1 \overset{s}{\to} \cdots \overset{s}{\to} z_k$. Then all edges in the corresponding path*

$$\beta(z_0) \to \beta(z_1) \to \cdots \to \beta(z_k) \tag{6.7}$$

are labeled s.

Proof. In this proof all calculations and equalities are modulo n unless otherwise indicated. First note that, since $t \neq \pm s$, $2 \leq k \leq n - 2$. Let m_1 be the number of edges in (6.7) labeled s, and m_2 the number of edges in (6.7) labeled t. Then $m_1 + m_2 = k$ in $\mathbb{Z}$ since, by Lemma 6.7, $\beta(x + s) \neq \beta(x)$ for every $x \in \mathbb{Z}_n$, and so no edge in (6.7) can have label 0. Since $z_0 \overset{ks}{\to} z_k$ and $ks = t$, we have $\beta(z_0) \overset{u}{\to} \beta(z_k)$ with $u = s$ or $u = t = ks$. (Note that u cannot be 0 since $\beta(z_k) = \beta(z_0 + t) \neq \beta(z_0)$ by Lemma 6.7.)

Suppose $u = s$. Then, by (6.7), $m_1 s + m_2 ks = s$, and so $m_1 + m_2 k = 1$. Since $m_1 + m_2 = k$ (in $\mathbb{Z}$ and hence in $\mathbb{Z}_n$), it easily follows that $(m_2 + 1)(k - 1) = 0$. If $k - 1$ is a unit in $\mathbb{Z}_n$, then $m_2 + 1 = 0$, and so $m_2 = n - 1$ in $\mathbb{Z}$ (since $m_2 \geq 0$), which is a contradiction since $k = m_1 + m_2$ in $\mathbb{Z}$ and $2 \leq k \leq n - 2$.

Thus $k-1$ is not a unit, which implies $d > k+1$. Let $e = \gcd(n, k-1)$. Then in $\mathbb{Z}$: $n = de$, $k-1 = qe$ for some $q \in \mathbb{Z}$, and d and q are relatively prime. Since $(m_2+1)(k-1) = 0$, we have $(m_2+1)(k-1) = jn$ in $\mathbb{Z}$, for some $j \in \mathbb{Z}$. Thus in $\mathbb{Z}$: $(m_2+1)qe = jne$, and so $(m_2+1)q = jd$. Since d and q are relatively prime, it follows that d divides m_2+1 in $\mathbb{Z}$. This is a contradiction since $d > k+1 \geq m_2+1$.

Thus we must have $u = t = ks$. Then, by (6.7), $m_1 s + m_2 ks = ks$, and so $m_1 + m_2 k = k$. Since $m_1 + m_2 = k$, it follows that $m_2(k-1) = 0$. If $k-1$ is a unit in $\mathbb{Z}_n$, then $m_2 = 0$, and so $m_2 = 0$ in $\mathbb{Z}$ (since $0 \leq m_2 \leq k \leq n-2$). Suppose that $d > k+1$. Then, by the foregoing argument applied to $m_2(k-1) = 0$ instead of $(m_2+1)(k-1) = 0$, we obtain d divides m_2 in $\mathbb{Z}$. As $d > k+1 > m_2 \geq 0$, we also get that $m_2 = 0$ in $\mathbb{Z}$.

We have proved that $m_2 = 0$ in $\mathbb{Z}$. Thus $m_1 = k$ in $\mathbb{Z}$, that is, all edges in (6.7) are labeled s. □

Theorem 6.9. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$, where $S = \{0, s, t\}$ with $s, t \in \mathbb{Z}_n^*$ and $t \neq s, -s$. Let $k = s^{-1}t$ and $d = \frac{n}{\gcd(n,k-1)}$. If either* (i) *$k-1$ is a unit in $\mathbb{Z}_n$ or* (ii) *$d > k+1$, then*

$$\operatorname{End}(\Gamma) = \operatorname{Aut}(\Gamma) \cup \{\beta : \mathbb{Z}_n \to \mathbb{Z}_n : |\operatorname{im}(\beta)| = 1\}.$$

Proof. Suppose that either (i) or (ii) holds. Let $\beta \in \operatorname{End}(\Gamma)$ such that β is not a constant. We want to show that β is an automorphism. As in the proof of Lemma 6.7, consider the cycle

$$0 = x_0 \xrightarrow{s} x_1 \xrightarrow{s} \cdots \xrightarrow{s} x_{n-1} \xrightarrow{s} x_0, \tag{6.8}$$

which contains all vertices of Γ, and the corresponding cycle of images:

$$\beta(x_0) \to \beta(x_1) \to \cdots \to \beta(x_{n-1}) \to \beta(x_0). \tag{6.9}$$

As β is not a constant and $1 < k < n$, we may apply Lemma 6.8 to every subpath of (6.8) of length k. It follows that all edges in (6.9) are labeled s. As s is a unit, $\beta(z_0), \beta(z_1), \ldots, \beta(z_{n-1})$ are pairwise distinct, and so β is a bijection.

We have proved that every $\beta \in \operatorname{End}(\Gamma)$ is either a constant or a bijection, which gives $\operatorname{End}(\Gamma) \subseteq \operatorname{Aut}(\Gamma) \cup \{a : \mathbb{Z}_n \to \mathbb{Z}_n : |\operatorname{im}(a)| = 1\}$. This concludes the proof since the reverse inclusion is obvious. □

Let Γ be as in Theorem 6.9. Then for every $\alpha \in \operatorname{Aut}(\mathbb{Z}_n)$,

$$\alpha \operatorname{End}(\Gamma)\alpha^{-1} = \operatorname{End}(\Gamma) \Leftrightarrow \alpha \operatorname{Aut}(\Gamma)\alpha^{-1} = \operatorname{Aut}(\Gamma).$$

By Proposition 6.3, $\alpha \operatorname{Aut}(\Gamma)\alpha^{-1} = \operatorname{Aut}(\Gamma)$ for every $\alpha \in \operatorname{Aut}(\mathbb{Z}_n)$, which implies that $U_S(\mathbb{Z}_n) = \mathbb{Z}_n^*$. Thus, by Theorem 6.4, we obtain the following corollary, which is a correct version of [4, Corollary 4.22]. The latter depends on [4, Theorem 4.21], and so the hypothesis that n is prime must be added to its statement.

Corollary 6.10. *Let $\Gamma = \Gamma(\mathbb{Z}_n, S)$, where $S = \{0, s, t\}$ with $s, t \in \mathbb{Z}_n^*$ and $t \neq s, -s$. Let $k = s^{-1}t$ and $d = \frac{n}{\gcd(n,k-1)}$. If either* (i) *$k-1$ is a unit in $\mathbb{Z}_n$ or* (ii) *$d > k+1$, then* $\operatorname{Aut}(\operatorname{End}(\Gamma)) \cong \operatorname{Aut}(\Gamma) \cdot \mathbb{Z}_n^*$.

For example, let $n = 2m$, where $m > 1$ and m is not divisible by 2 or 3. Let $S = \{0, 1, 3\}$, so 1 and 3 are units in $\mathbb{Z}_n$ and $3 \neq -1$. We have $k = 1^{-1} \cdot 3 = 3$, $\gcd(k-1, n) = \gcd(2, n) = 2$, and $d = \frac{n}{\gcd(n,2)} = m$. Thus $k-1 = 2 \notin \mathbb{Z}_n^*$, but $d > k+1$ (since $k+1 = 4$ and $d = m \geq 5$). Thus (ii) of Corollary 6.10 is satisfied, and so $\operatorname{Aut}(\operatorname{End}(\Gamma)) \cong \operatorname{Aut}(\Gamma) \cdot \mathbb{Z}_n^*$.

Let $S = \{0, s, t\}$, where $s, t \in \mathbb{Z}_n^*$ and $s \neq t, -t$. Note that in Corollary 6.10, we can switch s and t. Let $k_1 = s^{-1}t$, $k_2 = t^{-1}s$, $d_1 = \frac{n}{\gcd(n,k_1-1)}$, and $d_2 = \frac{n}{\gcd(n,k_2-1)}$. We note that $k_2 = k_1^{-1}$, and it is easy to check that $d_1 = d_2 =: d$, and if $k_1 - 1 \in \mathbb{Z}_n^*$, then $k_2 - 1 \in \mathbb{Z}_n^*$. By Corollary 6.10, if $k_1 - 1 \in \mathbb{Z}_n^*$ or $d > k_1 + 1$ or $d > k_2 + 1$, then $U_{\mathrm{S}}(\mathbb{Z}_n) = \mathbb{Z}_n^*$. On the other hand, if $k_1 - 1 \notin \mathbb{Z}_n^*$, $d \leq k_1 + 1$, and $d \leq k_2 + 1$, then we do not know what $U_{\mathrm{S}}(\mathbb{Z}_n)$ is. However, the calculation of $U_{\mathrm{S}}(\mathbb{Z}_n)$ can be facilitated by Corollary 6.12. The corollary follows from Lemma 6.11, which states that multiplying S by units of a certain form does not preserve endomorphisms of Γ that are not automorphisms or constants.

Lemma 6.11. *Let $S = \{0, s, t\}$, where $s, t \in \mathbb{Z}_n^*$ and $s \neq t, -t$. Let $k = s^{-1}t$, $d = \frac{n}{\gcd(n,k-1)}$, and $k - 1 \notin \mathbb{Z}_n^*$. Then for all $\beta \in \mathrm{End}(\Gamma(\mathbb{Z}_n, S))$ and $l \in \mathbb{Z}_n^*$ such that $l \not\equiv \pm 1 \pmod{d}$,*

if $\beta \in \mathrm{End}(\Gamma(\mathbb{Z}_n, lS))$, then β is either an automorphism of $\Gamma(\mathbb{Z}_n, S)$ or a constant.

Proof. Let $\beta \in \mathrm{End}(\Gamma(\mathbb{Z}_n, S))$ and $l \in \mathbb{Z}_n^*$ with $l \not\equiv \pm 1 \pmod{d}$. Suppose that $\beta \in \mathrm{End}(\Gamma(\mathbb{Z}_n, lS))$. Note that $k - 1 \notin \mathbb{Z}_n^*$ implies that $d \geq 2$. Suppose that β is not constant. We want to show that β is an automorphism of $\Gamma(\mathbb{Z}_n, S)$. By Lemma 6.8, $\beta(x + s) \neq \beta(x)$ for every $x \in \mathbb{Z}_n$. Let $x_0 \in \mathbb{Z}_n$. Consider the path

$$x_0 \xrightarrow{s} x_1 \xrightarrow{s} x_2 \xrightarrow{s} \cdots \xrightarrow{s} x_{ls}$$

in $\Gamma(\mathbb{Z}_n, S)$, and the corresponding path of images

$$\beta(x_0) \to \beta(x_1) \to \beta(x_2) \to \cdots \to \beta(x_{ls}). \tag{6.10}$$

Let m_1 be the number of edges in (6.10) labeled s, and m_2 the number of edges in (6.10) labeled t. Note that $m_1 + m_2 = l$ since $\beta(x + s) \neq \beta(x)$ for every $x \in \mathbb{Z}_n$, so no edge in (6.10) can be labeled 0. As $\beta \in \mathrm{End}(\Gamma(\mathbb{Z}_n, lS))$ and $x_0 \xrightarrow{ls} x_{ls}$, we have $\beta(x_0) \xrightarrow{u} \beta(x_{ls})$, where $u \in \{0, ls, lt\}$. We will consider these possibilities in turn.

- If $u = 0$, then we have (in $\mathbb{Z}_n$)

  $$m_1 s + m_2 t = 0 \Rightarrow (l - m_2)s + m_2 sk = 0 \Rightarrow m_2(k - 1) = -l,$$

  which is impossible as l is a unit in $\mathbb{Z}_n$ and $k - 1$ is not.
- If $u = ls$, then (in $\mathbb{Z}_n$)

  $$m_1 s + m_2 t = ls \Rightarrow (l - m_2)s + m_2 sk = ls \Rightarrow m_2(k - 1) = 0,$$

  which implies that $d = \frac{n}{\gcd(n,k-1)}$ divides m_2 in $\mathbb{Z}$.
- If $u = lt$, then (in $\mathbb{Z}_n$)

  $$m_1 s + m_2 t = lt \Rightarrow m_1 s + (l - m_1)sk = lsk \Rightarrow m_1(1 - k) = 0,$$

  which implies that d divides m_1 in $\mathbb{Z}$.

So d divides either m_1 or m_2. We may assume that d divides m_1. Then $l = m_1 + m_2 \equiv m_2 \pmod{d}$, and so $m_2 \not\equiv \pm 1 \pmod{d}$. Consider the path

$$x_1 \xrightarrow{s} x_2 \xrightarrow{s} x_3 \xrightarrow{s} \cdots \xrightarrow{s} x_{ls} \xrightarrow{s} x_{(l+1)s}$$

in $\Gamma(\mathbb{Z}_n, S)$, and the corresponding path of images

$$\beta(x_1) \to \beta(x_2) \to \beta(x_3) \to \cdots \to \beta(x_{ls}) \to \beta(x_{(l+1)s}). \tag{6.11}$$

Define m_1' and m_2' in the analogous way to m_1 and m_2, but with respect to (6.11). As the paths (6.10) and (6.11) overlap, we have $m_2 - m_2' \in \{-1, 0, 1\}$. Our prior argument for (6.10), applied to (6.11), shows that d divides m_1' or d divides m_2'. The latter is impossible since it would imply $m_2 \equiv \pm 1 \pmod{d}$ or $m_2 \equiv 0 \pmod{d}$. However, we know that $m_2 \not\equiv \pm 1 \pmod{d}$. Moreover, $m_2 \not\equiv 0 \pmod{d}$ since otherwise d would divide $l = m_1 + m_2$, which is not possible since $d \geq 2$, d divides n, and l is a unit in $\mathbb{Z}_n$.

Hence d divides m_1', and so d divides $m_1 - m_1'$. Since we also have $m_1 - m_1' \in \{-1, 0, 1\}$ and $d \geq 2$, it follows that $m_1 = m_1'$ (which implies $m_2 = m_2'$). This is only possible if the label in $\beta(x_0) \to \beta(x_1)$ is the same as the label in $\beta(x_{ls}) \to \beta(x_{(l+1)s})$.

Consider the cycle

$$0 \xrightarrow{s} s \xrightarrow{s} 2s \xrightarrow{s} \cdots \xrightarrow{s} (n-1)s \xrightarrow{s} 0$$

in $\Gamma(\mathbb{Z}_n, S)$, and the corresponding cycle of images

$$\beta(0) \to \beta(s) \to \beta(2s) \to \cdots \to \beta((n-1)s) \to \beta(0). \tag{6.12}$$

By the foregoing argument, the labels of edges in (6.12) form a pattern that is periodic with period l. As l is a unit in $\mathbb{Z}_n$, such a pattern is only possible when all edges are labeled s or all edges are are labeled t. In both cases, β is an automorphism of $\Gamma(\mathbb{Z}_n, S)$. □

Corollary 6.12. *Let $S = \{0, s, t\}$, where $s, t \in \mathbb{Z}_n^*$ and $s \neq t, -t$. Let $k = s^{-1}t$, $d = \frac{n}{\gcd(n, k-1)}$, and $k - 1 \notin \mathbb{Z}_n^*$. Suppose that there exists $\beta \in \mathrm{End}(\Gamma(\mathbb{Z}_n, S))$ that is not an automorphism or a constant. Then for every $l \in \mathbb{Z}_n^*$ such that $l \not\equiv \pm 1 \pmod{d}$, $l \notin U_S(\mathbb{Z}_n)$.*

Proof. By [4, (4.2)], $U_S(\mathbb{Z}_n) = \{k \in \mathbb{Z}_n^* : \mathrm{End}(\Gamma(\mathbb{Z}_n, S)) = \mathrm{End}(\Gamma(\mathbb{Z}_n, kS))\}$. Hence, the result follows from Lemma 6.11. □

Corollary 6.12 allows us to eliminate units from consideration for $U_S(\mathbb{Z}_n)$ in those cases when we know that there is at least one endomorphism that is not an automorphism or a constant, which can reduce the complexity when working with concrete examples. Moreover, in suitable situations, Corollary 6.12 allows us to obtain further results.

For example, consider $n = 2p$, where $p > 2$ is prime, and let t be odd with $p < t < 2p$. Let $S = \{0, 1, t\}$. We have $k = t$, $\gcd(k - 1, n) = 2$, and $d = p$. Note that in this case $k - 1$ is not a unit and $d < k + 1$, hence our previous results do not apply.

If $l \in \mathbb{Z}_n^*$ with $l \equiv \pm 1 (\mathrm{mod}\ d)$, then l is either one of the trivial units ± 1, or $l = p \pm 1$. However, $p - 1$ and $p + 1$ are both even and hence are not units. It then follows by Corollary 6.12 that $U_S(\mathbb{Z}_n)$ can only be either $\{1, -1\}$ or $\mathbb{Z}_n^*$, with $U_S(\mathbb{Z}_n) = \{-1, 1\}$ if $\mathrm{End}(\Gamma(\mathbb{Z}_n, S))$ contains an endomorphism that is neither an automorphism nor a constant, and $U_S(\mathbb{Z}_n) = \mathbb{Z}_n^*$ otherwise.

7. Problems

To extend the results of Section 6, the following problems must be solved.

Problem 1: Determine $U_{\mathrm{S}}(\mathbb{Z}_n)$ for the circulant digraphs considered in Corollary 6.5 such that $W(S) = \emptyset$. (Note that $W(S) = \emptyset$ if and only if $(S \cap (-S), +)$ is a subgroup of $(\mathbb{Z}_n, +)$.)

Problem 2: Determine $U_{\mathrm{S}}(\mathbb{Z}_n)$ for the circulant digraphs considered in Corollary 6.5 such that $W(S) \neq \emptyset$ but $x + y \notin -S$ for all $(x, y) \in W(S)$.

Problem 3: Determine $U_{\mathrm{S}}(\mathbb{Z}_n)$ for reflexive 3-circulant digraphs other than those considered in Corollary 6.10.

Another natural problem that so far has received little or no attention is the following. We recall that a *core* is a graph in which all endomorphisms are automorphisms.

Problem 4: Classify the core circulant digraphs.

A particular instance of Problem 4 is its restriction to the types of circulant digraphs considered in this paper.

Problem 5: Classify the core circulant digraphs of small valency and the core unit circulant digraphs.

8. Acknowledgments

The authors are grateful to the anonymous referees for their careful and detailed reports. These contained numerous helpful comments and suggestions that led to important improvements in the paper.

The first author acknowledges that this work was developed within FCT projects CAUL (PEst-OE/MAT/UI0143/2014) and CEMAT-CIÊNCIAS (UID/Multi/04621/2013). The second author has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. PCOFUND-GA-2009-246542 and from the Foundation for Science and Technology of Portugal under PCOFUND-GA-2009-246542 and SFRH/BCC/52684/2014, and acknowledges that this work was developed within FCT projects CAUL (PEst-OE/MAT/UI0143/2014) and CEMAT-CIÊNCIAS (UID/Multi/04621/2013). The last author is supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

References

[1] M.E. Adams, S. Bulman-Fleming, and M. Gould, Endomorphism properties of algebraic structures, *Proceedings of the Tennessee Topology Conference (Nashville, TN, 1996)*, 1–17, World Sci. Publishing, River Edge, NJ, 1997.

[2] R. Akhtar, T. Jackson-Henderson, R. Karpman, M. Boggess, I. Jiménez, A. Kinzel, and D. Pritikin, On the unitary Cayley graph of a finite ring, *Electron. J. Combin.* **16** (2009), no. 1, Research Paper 117, 13.

[3] B. Alspach and T.D. Parsons, Isomorphism of circulant graphs and digraphs, *Discrete Math.* **25** (1979), 97–108.

[4] J. Araújo, E. Dobson, and J. Konieczny, Automorphisms of endomorphism semigroups of reflexive digraphs, *Math. Nachr.* **283** (2010), 939–964.

[5] J. Araújo, V.H. Fernandes, M. Jesus, V. Maltcev and J. D. Mitchell. Automorphisms of partial endomorphism semigroups. *Publicationes Mathematicae Debrecen* **79** (1–2) (2011), 23–39.

[6] J. Araújo and M. Kinyon, Inverse semigroups with idempotent-fixing automorphisms. *Semigroup Forum* **89** (2014), no. 2, 469–474.

[7] J. Araújo and J. Konieczny, Dense relations are determined by their endomorphism monoids, *Semigroup Forum* **70** (2005), 302–306.
[8] J. Araújo and J. Konieczny, Automorphism groups of centralizers of idempotents, *J. Algebra* **269** (2003), no. 1, 227–239.
[9] J. Araújo and J. Konieczny, Automorphisms of the endomorphism monoids of relatively free bands, *Proc. Edinb. Math. Soc.* (2) **50** (2007), no. 1, 1–21.
[10] J. Araújo and J. Konieczny, A method of finding automorphism groups of endomorphism monoids of relational systems. *Discrete Math.* **307** 13, (2007), 1609–1620.
[11] J. Araújo and J. Konieczny, Automorphisms of endomorphism monoids of 1-simple free algebras. *Comm. Algebra* **37** 1, (2009), 83–94.
[12] J. Araújo and J. Konieczny, General theorems on automorphisms of semigroups and their applications. *Journal of the Australian Mathematical Society* **87** 1, (2009), 1–17.
[13] L. Babai, Isomorphism problem for a class of point-symmetric structures, *Acta Math. Acad. Sci. Hungar.* **29** (1977), 329–336.
[14] S. Bhoumik, E. Dobson, and J. Morris, Asymptotic automorphism groups of circulant graphs and digraphs, *Ars Math. Contemp.*, **7** (2014), 487–506.
[15] 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)* **66** (2002), 325–333.
[16] J.D. Dixon and B. Mortimer, "Permutation groups," Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.
[17] E. Dobson and J. Morris, Toida's conjecture is true, *Electron. J. Combin.* **9** (2002), Research Paper 35, 14 pp. (electronic).
[18] E. Dobson and J. Morris, On automorphism groups of circulant digraphs of square-free order, *Discrete Math.* **299** (2005), 79–98.
[19] E. Dobson and J. Morris, Automorphism groups of wreath product digraphs, *Electron. J. Combin.* **16** (2009), Research Paper 17, 30 pp.
[20] S.A. Evdokimov and I.N. Ponomarenko, Characterization of cyclotomic schemes and normal Schur rings over a cyclic group, *St. Petersburg Math. J.* **14** (2003), 189–221.
[21] W. Klotz and T. Sander, Some properties of unitary Cayley graphs, *Electron. J. Combin.* **14** (2007), Research Paper 45, 12 pp. (electronic).
[22] L.M. Gluskĭn, Semi-groups of isotone transformations, (Russian) *Uspehi Mat. Nauk 16* (1961), 157–162.
[23] K.H. Leung and S.H. Man, On Schur rings over cyclic groups. II, *J. Algebra* **183** (1996), 273–285.
[24] K.H. Leung and S.H. Man, On Schur rings over cyclic groups, *Israel J. Math.* **106** (1998), 251–267.
[25] I. Levi, Automorphisms of normal transformation semigroups. *Proc. Edinburgh Math. Soc. (2)* **28** (1985), 185–205.
[26] I. Levi. Automorphisms of normal partial transformation semigroups, *Glasgow Math. J.* **29** (1987), 149–157.
[27] I. Levi. On the inner automorphisms of finite transformation semigroups, *Proc. Edinburgh Math. Soc. (2)* **39** (1996), 27–30.
[28] C.H. Li, On isomorphisms of connected Cayley graphs, *Discrete Math.* **178** (1998), 109–122.
[29] C.H. Li, Permutation groups with a cyclic regular subgroup and arc transitive circulants, *J. Algebraic Combin.* **21** (2005), 131–136.
[30] A.E. Liber, On symmetric generalized groups, *Mat. Sbornik N.S.* **33** (1953), 531–544. (Russian)
[31] K.D. Magill, Semigroup structures for families of functions, I. Some homomorphism theorems, *J. Austral. Math. Soc.* **7** (1967), 81–94.
[32] A.I. Mal'cev, Symmetric groupoids, *Mat. Sbornik N.S.* **31** (1952), 136–151. (Russian)
[33] G. Mashevitzky, B.M. Schein, and G.I. Zhitomirski, Automorphisms of the endomorphism semigroup of a free inverse semigroup, *Comm. Alg. 34* (2006), 3569–3584.
[34] J.D.P. Meldrum, "Wreath products of groups and semigroups," Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 74, Longman, Harlow, 1995.
[35] M. Muzychuk, M. Klin, and R. Pöschel, The isomorphism problem for circulant graphs via Schur ring theory, *Codes and association schemes (Piscataway, NJ, 1999)*, 241–264, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001.
[36] J. Schreier. Über Abbildungen einer abstrakten Menge Auf ihre Teilmengen. *Fund. Math.* **28** (1936), 261–264.
[37] R.P. Sullivan. Automorphisms of transformation semigroups. *J. Australian Math. Soc.* **20** (1975), part 1, 77–84.
[38] È.G. Šutov. Homomorphisms of the semigroup of all partial transformations. *Izv. Vysš. Učebn. Zaved. Matematika* **3** (1961), 177–184. (Russian)
[39] J.S.V. Symons. *Normal transformation semigroups.* J. Austral. Math. Soc. Ser. A **22** (1976), no. 4, 385–390.
[40] W.T. Tutte, A family of cubical graphs, *Proc. Cambridge Philos. Soc.* **43** (1947), 459–474.
[41] Ju.M. Važenin, The elementary definability and elementary characterizability of classes of reflexive graphs, *Izv. Vysš. Učebn. Matematika 1972*, no. 7(122), 3–11. (Russian)

[42] H. Wielandt, *Permutation groups through invariant relations and invariant functions*, lectures given at The Ohio State University, Columbus, Ohio, 1969.
[43] H. Wielandt, "Mathematische Werke/Mathematical works. Vol. 1," Walter de Gruyter & Co., Berlin, 1994.
[44] M.Y. Xu, Automorphism groups and isomorphisms of Cayley digraphs, *Discrete Math.* **182** (1998), 309–319.
[45] H. Yang and X. Yang. Automorphisms of partition order-decreasing transformation monoids. *Semigroup Forum* **85** (2012), no. 3, 513–524.

Universidade Aberta and CEMAT-Ciências Faculdade de Ciências, Universidade de Lisboa, 1749-016, Lisboa, Portugal
E-mail address: jjaraujo@fc.ul.pt

Department of Physics and Mathematics, University of Hull, Kingston upon Hull, HU6 7RX, United Kingdom
E-mail address: W.Bentz@hull.ac.uk

Department of Mathematics and Statistics, Mississippi State University, PO Drawer MA Mississippi State, MS 39762 USA, and IAM, University of Primorska, Koper 6000, Slovenia
E-mail address: dobson@math.msstate.edu

Department of Mathematics, University of Mary Washington, Fredericksburg, VA 22408, USA
E-mail address: jkoniecz@umw.edu

Department of Math and CS, University of Lethbridge, Lethbridge, AB T1K 3M4, Canada
E-mail address: joy.morris@uleth.ca