

# Automorphism groups of circulant graphs — a survey

Joy Morris

**Abstract.** A circulant (di)graph is a (di)graph on  $n$  vertices that admits a cyclic automorphism of order  $n$ . This paper provides a survey of the work that has been done on finding the automorphism groups of circulant (di)graphs, including the generalisation in which the edges of the (di)graph have been assigned colours that are invariant under the aforementioned cyclic automorphism.

**Mathematics Subject Classification (2000).** 05C25.

**Keywords.** circulant graphs, automorphism groups, algorithms.

## 1. Introduction

The aim of this paper is to provide a history and overview of work that has been done on finding the automorphism groups of circulant graphs. We will focus on structural theorems about these automorphism groups, and on efficient algorithms based on these theorems, that can be used to determine the automorphism group of certain classes of circulant graphs.

We must begin this discussion by defining the terms that will be central to the topic. In what follows, we sometimes refer simply to “graphs” or to “digraphs,” but all of our definitions, and many of the results on automorphism groups, can be generalised to the case of “colour digraphs:” that is, digraphs whose edges not only have directions, but colours.

**Definition 1.1.** Two graphs  $X = X(V, E)$  and  $Y = Y(V', E')$  are said to be **isomorphic** if there is a bijective mapping  $\phi$  from the vertex set  $V$  to the vertex set  $V'$  such that  $(u, v) \in E$  if and only if  $(\phi(u), \phi(v)) \in E'$ . The mapping  $\phi$  is called an **isomorphism**. We denote the fact that  $X$  and  $Y$  are isomorphic by  $X \cong Y$ .

---

The author gratefully acknowledges support from the National Science and Engineering Research Council of Canada (NSERC)..

That is, an isomorphism between two graphs is a bijection on the vertices that preserves edges and nonedges. In the case of digraphs, an isomorphism must also preserve the directions assigned to the edges, and in the case of colour (di)graphs, the colours must also be preserved.

This definition has the following special case:

**Definition 1.2.** An **automorphism** of a (colour) (di)graph is an isomorphism from the (colour) (di)graph to itself.

When we put all of the automorphisms of a (colour) (di)graph together, the result is a group:

**Definition 1.3.** The set of all automorphisms of a graph  $X$  forms a group, denoted  $\text{Aut}(X)$ , the **automorphism group** of  $X$ .

Now that we know what automorphism groups of graphs are, we must define circulant graphs.

**Definition 1.4.** A **circulant graph**  $X(n; S)$  is a Cayley graph on  $\mathbb{Z}_n$ . That is, it is a graph whose vertices are labelled  $\{0, 1, \dots, n-1\}$ , with two vertices labelled  $i$  and  $j$  adjacent iff  $i - j \pmod{n} \in S$ , where  $S \subset \mathbb{Z}_n$  has  $S = -S$  and  $0 \notin S$ .

For a circulant digraph, the condition that  $S = -S$  is removed. For a colour circulant (di)graph, each element of  $S$  also has an associated (not necessarily distinct) colour, which is assigned to every edge whose existence is a consequence of that element of  $S$ .

With these basic definitions in hand, we can explore the history of the question: what do the automorphism groups of circulant graphs look like, and how can we find them?

Although we define most of the terms used in this paper, for permutation group theoretic terms that are not defined, the reader is referred to Wielandt's book on permutation groups [42], which has recently come back into print in his collected works [43]. Another good source is Dixon and Mortimer's book [11]. Throughout this paper, the symmetric group on  $n$  points is denoted by  $\mathcal{S}_n$ .

## 2. History

In 1936, König [27] asked the following question: "When can a given abstract group be interpreted as the group of a graph and if this is the case, how can the corresponding graph be constructed? This same question could be asked for directed graphs." (This quote is from the English translation published by Birkhäuser in 1990). By the group of a graph, he is referring to the automorphism group.

This question was answered by Frucht, in 1938 [18]. The answer was yes; in fact, it went further: there are infinitely many such graphs for any group  $G$ .

By no means was this the end of the matter. One method of construction involved the creation of graphs on large numbers of vertices, that encoded the colour information from the Cayley colour digraph of a group, into structured

subgraphs. This construction led to graphs that had, in general, many more vertices than the order of the group.

One major area of research that spun off from this, was the search for “graphical regular representations” of a particular group  $G$ : that is, graphs whose automorphism group is isomorphic to  $G$ , and whose number of vertices is equal to the order of  $G$ . This is not a topic that we will pursue further in this paper, however.

A related question was presumably also considered by mathematicians. That is, given a particular representation of permutation group  $G$ , is there a graph  $X$  for which  $\text{Aut}(X) \cong G$  as permutation groups? We know of no reference for this question prior to 1974, however [3].

The answer to this question did not prove to be so straightforward. For example, if  $\rho = (0\ 1\ 2\ \dots\ n)$ , no graph has  $\langle \rho \rangle$  as its automorphism group, because the reflection that maps  $a$  to  $-a$  for every  $0 \leq a \leq n$  will always be an automorphism of any such graph. Another way of explaining this, is that the dihedral group acting on  $n$  elements has the same orbits on unordered pairs  $(i, j)$  as  $Z_n$  has. This shows that there is not always a graph  $X$  whose automorphism group is a particular representation of a permutation group.

Although it is not our aim to discuss this version of the question, we will give here the most significant results that have been obtained on it.

The first result is due to Hemminger [21], in 1967.

**Theorem 2.1.** *Let  $G$  be a transitive abelian permutation group that is abstractly isomorphic to  $Z_{n_1} \times \dots \times Z_{n_k}$ . Then if the number of factors in the direct product of order 2 is not 2, 3, or 4, and the number of factors of order 3 is not 2, there is a directed graph whose automorphism group is isomorphic to  $G$ .*

In 1981, Godsil [20] proved the following result.

**Theorem 2.2.** *Let  $G$  be a finite permutation group. A necessary condition for the Cayley graph  $X = X(G; S)$  to have  $G$  as its automorphism group, is that the subgroup of  $G$  that fixes some vertex of  $X$ , is isomorphic to the automorphisms of  $G$  that fix  $S$  set-wise.*

He also proved that this condition is sufficient for many  $p$ -groups, and obtained necessary and sufficient conditions for the occurrence of the dihedral groups of order  $2^k$ , and of certain Frobenius groups, as the full automorphism groups of vertex-transitive graphs and digraphs.

In 1989, a paper by Zelikovskij [44] appeared in Russian. We are unaware of a translation, so can only report the main result as stated in the English summary: that for every finite abelian permutation group  $G$  whose order is relatively prime to 30, the paper provides necessary and sufficient conditions for the existence of a simple graph whose automorphism group is isomorphic to  $G$ . Note that the facts that Zelikovskij produces a simple graph and apparently does not require transitivity, represent improvements over Hemminger’s result, although he does not cover all of the orders that Hemminger does.

In 1999, Peisert proved [36] the following result.

**Theorem 2.3.** *If two permutation groups each have representations as automorphism groups of graphs, then the direct product of these representations, will also have a graph for which it is isomorphic to the automorphism group, unless the two original groups are isomorphic as permutation groups, transitive, and have a unique graph for which they are the automorphism group (up to isomorphism).*

The approach this question that we will follow in this paper, is to ask what is the automorphism group of a given graph  $X$ ? Again, the answer is not easy, so we will limit our consideration to circulant graphs.

### 3. Algorithms for finding automorphism groups

As one focus of this paper will be finding efficient algorithms for calculating the automorphism group of a graph, it is necessary to spend some time considering what makes an algorithm “efficient” in this regard.

There is, after all, a very straightforward algorithm that is guaranteed to find the automorphism group of any graph on  $n$  vertices: simply consider every possible permutation in  $\mathcal{S}_n$ , and include those that turn out to be automorphisms of our graph. As  $\mathcal{S}_n$  has order  $n!$ , this algorithm is exponential in  $n$ .

Depending on our goal, it may not be possible to do any better than this. Specifically, if our goal is to list every automorphism in the automorphism group, then as there may be as many as  $n!$  elements, generating the list in anything less than exponential time will not be feasible in general.

If the number of prime factors of  $n$  is bounded with a sufficiently low bound, then we actually can do more than this. In such cases, the number of subgroups of  $\mathcal{S}_n$  that can be automorphism groups of circulant graphs may be sufficiently small that we can choose the automorphism group of our graph from a short list. We will not be listing all of its elements, but we may be able to describe its structure precisely without the use of generating sets, as for example by saying it is isomorphic to  $\mathcal{S}_p \times \mathcal{S}_q$ .

However, when the number of prime factors is unbounded, we lose this ability to explicitly describe the automorphism group. Thus, when we consider algorithms intended to determine the automorphism group of a circulant graph on a number of vertices whose number of factors is unbounded, what we are looking for is not an explicit listing of all of the elements of the group, but the provision of a generating set for the group.

Each of the algorithms that we provide below, runs in polynomial time in the number of vertices of the graph, and provides either a generating set for the automorphism group of the graph, or (where possible) a precise structural description of the automorphism group.

#### 4. Circulant graphs on a prime number of vertices

In 1973, Alspach proved the following result on the automorphism groups of circulant graphs on a prime number of vertices.

**Theorem 4.1.** [2] *Let  $p$  be prime. If  $S = \emptyset$  or  $S = \mathbb{Z}_p^*$ , then  $\text{Aut}(X) = \mathcal{S}_p$ ; otherwise,  $\text{Aut}(X) = \{T_{a,b} : a \in E(S), b \in \mathbb{Z}_p\}$ , where  $T_{a,b}(v_i) = v_{ai+b}$ , and  $E(S)$  is the largest even-order subgroup of  $\mathbb{Z}_p^*$  such that  $S$  is a union of cosets of  $E(S)$ .*

Notice that since  $S = -S$ ,  $S$  must be a union of cosets of  $\{1, -1\}$ , so  $E(S)$  can always be found.

This leads to the following algorithm for finding the automorphism group of such a graph.

**Algorithm for finding  $\text{Aut}(X)$ :**

1. If  $S = \emptyset$  or  $S = \mathbb{Z}_p^*$ ,  $\text{Aut}(X) = \mathcal{S}_p$ .
2. For each even-order subgroup  $H$  of  $\mathbb{Z}_p^*$ , verify whether  $S$  is a union of cosets of  $H$ .
3. Since  $\mathbb{Z}_p^*$  is cyclic, there is one  $H$  of every order dividing  $p - 1$ . Set  $E(S)$  to be the largest  $H$  that satisfies (2).
4. If  $\text{Aut}(X) \neq \mathcal{S}_p$ ,  $\text{Aut}(X) = \{T_{a,b} : a \in E(S), b \in \mathbb{Z}_p\}$ .

Proof of Alspach's theorem relies on the following theorem by Burnside.

**Theorem 4.2.** [8] *If  $G$  is a transitive group acting on a prime number  $p$  of elements, then either  $G$  is doubly transitive or  $G = \{T_{a,b} : a \in H < \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$ .*

Although the algorithm given above may be the most natural way to create an algorithm from the statement of Alspach's theorem, we will re-state the algorithm slightly differently. The purpose of this, is to provide a closer parallel to the algorithms that we will be constructing subsequently, to cover other possible numbers of vertices.

**Alternate algorithm:**

1. Find  $A$ , the set of all multipliers  $a \in \mathbb{Z}_p^*$  for which  $aS = S$ .
2. If  $A = \mathbb{Z}_p^*$ , then  $\text{Aut}(X) = \mathcal{S}_p$ .
3. Otherwise,  $\text{Aut}(X) = \{T_{a,b} : a \in A, b \in \mathbb{Z}_p\}$ .

Before presenting any generalisations of this algorithm, the concept of wreath products will be required.

#### 5. Wreath products

Although we will present a formal definition of the wreath product of two graphs in a moment, we will first give a description which may make the formal presentation easier to follow. If we are taking a wreath product of two (di)graphs,  $X$  and  $Y$ , we replace every vertex of  $X$  by a copy of the (di)graph  $Y$ . Between two copies of  $Y$ , we include all edges (or all arcs in a particular direction) if there was an edge

(or an arc in the appropriate direction) between the corresponding vertices of  $X$ . Now for the formal definition.

**Definition 5.1.** The wreath product of the (di)graph  $X$  with the (di)graph  $Y$ , denoted  $X \wr Y$ , is defined in the following way.

The vertices of  $X \wr Y$  are the ordered pairs  $(x, y)$  where  $x$  is a vertex of  $X$  and  $y$  is a vertex of  $Y$ . There is an arc (or edge) from the vertex  $(x_1, y_1)$  to the vertex  $(x_2, y_2)$  if and only if one of the following holds:

1.  $x_1 = x_2$  and  $(y_1, y_2)$  is an arc (or edge) of  $Y$ ; or
2.  $(x_1, x_2)$  is an arc (or edge) of  $X$ .

We say two sets of vertices  $A$  and  $B$  are **wreathed** if either  $ab$  is an edge for every  $a \in A$  and every  $b \in B$ , or  $ab$  is a nonedge for every  $a \in A$  and every  $b \in B$ .

In graph theory, what we have called the “wreath” product is also often called the “lexicographic” product, and has also been called the “composition” of graphs. The notion of a wreath product is also defined on groups; in fact, the term “wreath product” comes from group theory. Although it can be defined on abstract groups, we will only be considering permutation groups, where the definition is simpler, so it is this definition that we provide.

**Definition 5.2.** The wreath product of two permutation groups,  $H$  and  $K$ , acting on sets  $U$  and  $V$  respectively, is the group of all permutations  $f$  of  $U \times V$  for which there exist  $h \in H$  and an element  $k_u$  of  $K$  for each  $u \in U$  such that

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

for all  $(u, v) \in U \times V$ . It is written  $H \wr K$ .

It is easy to verify that

$$\text{Aut}(X) \wr \text{Aut}(Y) \leq \text{Aut}(X \wr Y)$$

is true for any graphs  $X$  and  $Y$ ; in fact, it is often the case that equality holds.

## 6. Circulant graphs on $pq$ vertices, or $p^n$ vertices

The following theorem, proven by Klin and Pöschel in 1978, characterises the automorphism groups of circulant graphs on  $pq$  vertices, where  $p$  and  $q$  are distinct primes.

**Theorem 6.1.** [25] *If  $G$  is the automorphism group of a circulant graph on  $pq$  vertices, then  $G$  is one of:*

1.  $\mathcal{S}_{pq}$ ;
2.  $A_1 \wr A_2$ , or  $A_2 \wr A_1$ , where  $A_1$  and  $A_2$  are automorphism groups of circulant graphs on  $p$  and  $q$  vertices, respectively;
3.  $\mathcal{S}_p \times A_2$ , or  $A_1 \times \mathcal{S}_q$ , where  $A_1$  and  $A_2$  are automorphism groups of circulant graphs on  $p$  and  $q$  vertices, respectively; or,
4.  $\{T_{a,b} : a \in A \leq \mathbb{Z}_n^*, b \in Z_n\}$  (a subgroup of the holomorph).

The following algorithm can be constructed from this characterisation, to determine the automorphism group of a graph on  $pq$  vertices.

**Algorithm:**

1. If  $S = \emptyset$  or  $S = \mathbb{Z}_{pq} - \{0\}$ , then  $\text{Aut}(X) = \mathcal{S}_{pq}$ . END.
2. If  $(v_0 \ v_p \ v_{2p} \dots \ v_{(q-1)p}) \in \text{Aut}(X)$ , then  $\text{Aut}(X) = A_1 \wr A_2$ , where  $A_1$  is the automorphism group of the induced subgraph of  $X$  on the vertices  $\{v_0, v_q, \dots, v_{(p-1)q}\}$  and  $A_2$  is the automorphism group of the induced subgraph of  $X$  on the vertices  $\{v_0, v_p, \dots, v_{(q-1)p}\}$ . Use the previous algorithm (for finding the automorphism group of a circulant graph on a prime number of vertices) to find  $A_1$  and  $A_2$ . END.
3. Repeat (2) with the roles of  $p$  and  $q$  reversed.
4. Let  $A$  be the group of all multipliers  $a$  in  $\mathbb{Z}_{pq}^*$  for which  $aS = S$ .
5. Define  $E_p$  by  $E_p = \{T_{a,b} : a \in A, a \equiv 1 \pmod{p}, b \in q\mathbb{Z}_p\}$ ; if  $E_p \cong \text{AGL}(1, p)$  then  $\text{Aut}(X) = \mathcal{S}_p \times A_2$ , where  $A_2$  is as in step (2). Use the previous algorithm to find  $A_2$ . END.
6. Repeat (4) with the roles of  $p$  and  $q$  reversed, and  $A_1$  taking the role of  $A_2$ . END.
7. Otherwise,  $\text{Aut}(X) = \{T_{a,b} : a \in A, b \in \mathbb{Z}_{pq}\}$ .

The full automorphism group of circulant graphs on  $p^n$  vertices has been determined, first by Klin and Pöschel, and later independently by Dobson; both results are unpublished.

The full result is technical, but this nice result gets much of the way:

**Theorem 6.2.** [12, 26] *A circulant graph on  $p^n$  vertices is either a wreath product, or its automorphism group has a normal Sylow  $p$ -subgroup.*

## 7. The square-free case

There is no known characterisation for the automorphism groups of circulant graphs in the general square-free case that is as straightforward as the results we have described above, when the number of vertices is  $p$  or  $pq$  and  $p, q$  are distinct primes.

However, Dobson and Morris [14] did prove the following structural theorem about the automorphism groups of circulant graphs of arbitrary square-free order. The definition of a group being 2-closed is quite technical, but the important thing to know about 2-closed groups is that the automorphism group of a vertex-transitive graph or digraph is always 2-closed. The terms used in the second point of this theorem are defined later in this paper, in the section “A Strategy,” for readers who are interested.

**Theorem 7.1.** *Let  $mk$  be a square-free integer and  $G \leq \mathcal{S}_{mk}$  be 2-closed and contain a regular cyclic subgroup,  $\langle \rho \rangle$ . Then one of the following is true:*

1.  $G = G_1 \cap G_2$ , where  $G_1 = \mathcal{S}_r \wr H_1$  and  $G_2 = H_2 \wr \mathcal{S}_k$ , where  $H_1$  is a 2-closed group of degree  $mk/r$ ,  $H_2$  is a 2-closed group of order  $m$ , and  $r|m$ ; or

2. *there exists a complete block system  $\mathcal{B}$  of  $G$  consisting of  $m$  blocks of size  $k$ , and there exists  $H \triangleleft G$  such that  $H$  is transitive, 2-closed, and  $\langle \rho \rangle \leq H = H_1 \times H_2$  (with the canonical action), where  $H_1 \leq \mathcal{S}_m$  is 2-closed and  $H_2 \leq \mathcal{S}_k$  is 2-closed and primitive.*

Unlike the previous structural results by Alspach, and by Klin and Pöschel, this clearly does not provide a clear, short list of groups from among which the automorphism group of a circulant graph on any square-free number of vertices must be chosen. However, it is sufficient to allow Dobson and Morris, in a subsequent paper [15], to construct the following algorithm that will determine the automorphism group of any such graph.

**General algorithm ( $n$  square-free)**

**Inputs:** The number  $n$  of vertices of  $X$ , and the connection set  $S \subseteq \mathbb{Z}_n$ .

1. Let  $A$  be the group of all multipliers  $a$  in  $\mathbb{Z}_n^*$  for which  $aS = S$ .
2. For each prime divisor  $p$  of  $n$ , define  $E_p$  by  $E_p = \{T_{a,b} : a \in A, a \equiv 1 \pmod{p}, b \in \frac{n}{p}\mathbb{Z}_p\}$ ; if  $E_p \cong \text{AGL}(1, p)$  then define  $E_p = \mathcal{S}_p$ .
3. Let  $p_1, \dots, p_t$  be all primes such that  $E_p = \mathcal{S}_p$ .
  - (a) For each pair of distinct primes  $p_i, p_j$ , if the transposition that switches  $n/p_i + kp_i p_j$  with  $n/p_j + kp_i p_j$  for every  $0 \leq k \leq n/p_i p_j$  and fixes all other vertices is an automorphism of  $X$ , then  $E_{p_i p_j} = \mathcal{S}_{p_i p_j}$ . Otherwise,  $E_{p_i p_j} = E_{p_i} E_{p_j}$ .
  - (b) Define a relation  $R$  on  $\{p_1, \dots, p_t\}$  by  $p_i R p_j$  iff there exists a sequence of primes  $p_{k_1}, \dots, p_{k_s}$  where  $p_i = p_{k_1}, p_j = p_{k_s}$  such that  $E_{\text{lcm}(p_{k_1}, p_{k_1+1})} = \mathcal{S}_{\text{lcm}(p_{k_1}, p_{k_1+1})}$ . This is an equivalence relation. For each equivalence class  $\mathcal{E}_i$ , let  $m_i = \prod_{j \in \mathcal{E}_i} p_j$ , then let  $E_{m_i} = \mathcal{S}_{m_i}$ .
  - (c) For any divisor  $m$  of  $n$ ,

$$E_m = \prod_{\mathcal{E}} \mathcal{S}_{\text{gcd}(m_i, m)} \prod_{p | \text{gcd}(n/p_1 \dots p_t, m)} E_p.$$

4. For each composite divisor  $m$  of  $n$ , let  $A_m = \{a \in A : a \equiv 1 \pmod{\frac{n}{m}}\}$ , and let  $A_n = A$ . Define  $E'_m = \langle E_m, A_m \rangle$ .
5. Let  $G = E'_n$ . For each complete block system of  $E'_n$ ,  $\mathcal{B}$ , consisting of  $n/k$  blocks of size  $k$ , do:
  - (a) For each complete block system of  $E'_n$ ,  $\mathcal{D}$ , consisting of  $n/kk'$  blocks of size  $kk'$ , determine whether or not

$$\rho^{n/k} |_{D_0},$$

the mapping that acts as  $\rho^{n/k}$  on the vertices of  $D_0$ , and fixes all other vertices, is an automorphism of  $X$ . If it is, let our new  $G$  be the group generated by the old  $G$  together with every  $E'_k |_D$ , where  $D \in \mathcal{D}$ ; if not, leave  $G$  unchanged.

6.  $G$  is the automorphism group of  $X$ .

To avoid some technical details, we have oversimplified some of the notation in this algorithm; the astute reader may observe, for example, that if we define  $E_p = \mathcal{S}_p$ , then  $E_p$  is acting on  $p$  vertices, and subsequent products involving

$E_p$  ( $E_m = E_p E_q$ , etc.) may not be properly defined. These issues are properly addressed in the paper that presents the algorithm, but as the intent of this paper was only to give the flavour of the algorithm, the technical details seemed likely to unnecessarily complicate our presentation.

In the same paper, Dobson and Morris prove that this algorithm runs in polynomial time on the number of vertices of the graph.

## 8. A Strategy

In this section, we outline a general strategy that is often used to obtain structural results about circulant graphs.

**Definition 8.1.** Let  $V$  be a set, and  $G$  a permutation group acting on the elements of  $V$ . The subset  $B \subseteq V$  is a  $G$ -**block** if for every  $g \in G$ , either  $g(B) = B$ , or  $g(B) \cap B = \emptyset$ .

In some cases, the group  $G$  is clear from the context and we simply refer to  $B$  as a block.

It is a simple matter to realise that if  $B$  is a  $G$ -block, then for any  $g \in G$ ,  $g(B)$  will also be a  $G$ -block. Also, intersections of  $G$ -blocks remain  $G$ -blocks.

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

Notice that any singleton in  $V$ , and the entire set  $V$ , are always  $G$ -blocks.

The **size** of the block  $B$  is the cardinality of the set  $B$ . A block  $B$  is **nontrivial** if the size of  $B$  is neither 1 nor the cardinality of  $V$ .

**Definition 8.2.** The transitive permutation group  $G$  is said to be **imprimitive** if  $G$  admits nontrivial blocks. If  $G$  is transitive but not imprimitive, then  $G$  is said to be **primitive**.

The notion of transitivity for permutation groups can be generalised.

**Definition 8.3.** The permutation group  $G$  acting on the set  $V$  is  $k$ -**transitive** if given any two  $k$ -tuples  $(v_1, \dots, v_k)$  and  $(u_1, \dots, u_k)$  with  $v_1, \dots, v_k, u_1, \dots, u_k \in V$ , there exists some  $g \in G$  such that  $g(v_i) = u_i$  for  $1 \leq i \leq k$ .

In particular, we often say that a 2-transitive group is doubly transitive.

**Definition 8.4.** The abstract group  $G$  is a **Burnside group** if every primitive permutation group containing the regular representation of  $G$  as a transitive subgroup is doubly transitive.

Burnside gave the first example of such a group, hence the name. This is extremely useful in the theory of circulant graphs, due to the following theorem.

**Theorem 8.5 (Theorem 25.3, [42]).** *Every cyclic group of composite order is a Burnside group.*

In particular, if  $n$  is composite, the automorphism group of a circulant graph of order  $n$  is either doubly transitive or imprimitive.

**Corollary 8.6.** *For any circulant graph  $X = X(n; S)$ , one of the following holds:*

1.  $\text{Aut}(X) = \mathcal{S}_n$ ;
2.  $\text{Aut}(X)$  is imprimitive; or
3.  $n$  is prime.

This can be used repeatedly to show that the minimal blocks of a circulant graph must either have prime size, or the induced subgraph on these vertices is complete or empty.

We can also use this to determine additional information about how  $\text{Aut}(X)$  acts upon any blocks - once again, this action must be imprimitive or doubly transitive unless there are a prime number of blocks.

## 9. Related problems

In this section, we discuss a number of problems that are closely related to finding the automorphism group of a circulant graph.

### 9.1. The Cayley Isomorphism problem for circulants

One of the most-studied problems related to finding the automorphism group of circulant graphs, is the Cayley Isomorphism, or CI, problem.

**Definition 9.1.** A circulant graph  $X = X(n; S)$  is said to have the **Cayley Isomorphism (CI) property** if whenever  $Y = Y(n; S')$  is isomorphic to  $X$ , there is some  $a \in \mathbb{Z}_n^*$  for which  $aS = S'$ .

The cyclic group of order  $n$  is said to have the Cayley Isomorphism (CI) property if every circulant graph  $X(n; S)$  has the CI property.

The CI problem, of course, is to determine which graphs (or which groups) have the CI property. When applied to digraphs, the CI property is referred to as the DCI property (for “directed Cayley Isomorphism” property).

**Theorem 9.2.** [5, 6] *A circulant graph  $X$  on  $n$  vertices has the CI property if and only if any two  $n$ -cycles in  $\text{Aut}(X)$  are conjugate in  $\text{Aut}(X)$ .*

So, knowing that a graph has the CI-property gives us significant information about its automorphism group.

We give a brief history of the major results on this problem.

In 1967, Àdàm conjectured [1] that all cyclic groups are CI-groups. Elspas and Turner proved in 1970 that this was not the case [17], and that, in fact,  $\mathbb{Z}_{p^2}$  is not CI for  $p \geq 5$ . There were also many positive results on this conjecture, however. First, in 1967, Turner proved that  $\mathbb{Z}_p$  is CI [40]. In a computer search, McKay [32] found that  $\mathbb{Z}_n$  is CI, when  $n \leq 37$  and  $n \neq 16, 24, 25, 27, 36$ . In 1977, Babai [6] proved that  $\mathbb{Z}_{2p}$  is CI, which was generalised in 1979 by Alspach and Parsons [5], who proved that  $\mathbb{Z}_{pq}$  is CI. In 1983, Godsil [19] proved that  $\mathbb{Z}_{4p}$  is

CI. Muzychuk completed the work in 1997 [34, 35] by showing that  $\mathbb{Z}_n$  is DCI if and only if  $n \in \{k, 2k, 4k\}$  where  $k$  is odd and squarefree;  $\mathbb{Z}_n$  is CI if and only if  $n \in \{8, 9, 18\}$  or  $\mathbb{Z}_n$  is DCI.

This problem has also been studied for particular families of graphs; Huang and Meng proved in 1996 [22], that  $X(n; S)$  has the CI property if  $S$  is a minimal generating set for  $\mathbb{Z}_n$ . In 1977, Toida conjectured that if  $S \subseteq \mathbb{Z}_n^*$  then  $X(n; S)$  is CI [39]. This conjecture was proven by Klin, Pöschel and Muzychuk [24], and independently by Dobson and Morris [13].

The special case where the connection set,  $S$ , is small, has also been studied. In 1977, Toida [39] proved that if  $|S| \leq 3$ ,  $X(n; S)$  is CI. In 1988, Sun [38] was the first to prove that if  $|S| = 4$ ,  $X(n; S)$  is CI, although others later also proved this result. In 1995, Li proved that if  $|S| = 5$ ,  $X(n; S)$  is CI [28].

This is by no means intended as a full history of work that has been done on the CI problem; for further information, the reader is referred to Li's survey of the problem [29].

## 9.2. Edge-transitivity, arc-transitivity, 2-arc-transitivity

**Definition 9.3.** A  $k$ -arc is a list  $v_1, \dots, v_k$  of vertices for which any two sequential vertices are adjacent, and any 3 sequential vertices are distinct.

This definition allows us to consider graphs whose automorphism groups are transitive on the set of  $k$ -arcs of the graph, for various values of  $k$ ; for our purposes, we will only consider  $k = 1$  and  $k = 2$ .

The following theorem was proven by Chao [9] in 1971; the proof was simplified by Berggren [7] in 1972.

**Theorem 9.4.** *A circulant graph on  $p$  vertices is edge-transitive iff  $S = \emptyset$  or  $S$  is a coset of an even order subgroup  $H \leq \mathbb{Z}_p^*$ .*

Notice that in the case of circulant graphs, the reflection is an automorphism, so arc-transitivity is equivalent to edge-transitivity.

This result, and those that follow, provide significant information about how the automorphism group of a graph can act on the edge set of the graph. They are therefore related to finding the automorphism group, although they do not directly provide much information about the automorphism group of an arbitrary circulant graph.

The above theorem was extended to classifications of arc-transitive graphs on  $pq$  vertices, for any distinct primes  $p$  and  $q$ , in papers by Cheng and Oxley [10], who classified the graphs on  $2p$  vertices; Wang and Xu [41], who classified the graphs on  $3p$  vertices; and Praeger, Wang and Xu [37], who completed the classification.

In 2001, the following classification was obtained of arc-transitive circulants on a square-free number of vertices, by Li, Marušič and Morris [30].

**Theorem 9.5.** *If  $X$  is an arc-transitive circulant graph of square-free order  $n$ , then one of the following holds:*

1.  $X = K_n$ ;
2.  $\text{Aut}(X)$  contains a cyclic regular normal subgroup; or
3.  $X = Y \wr \bar{K}_b$ , or  $X = Y \wr \bar{K}_b - bY$ , where  $n = mb$ , and  $Y$  is an arc-transitive circulant of order  $m$ .

Another approach has been taken to classifying edge-transitive circulant graphs, using the more stringent condition that the complement must also be edge-transitive. The following result was proven by Zhang in 1996 [45].

**Theorem 9.6.** *If  $G$  and  $\bar{G}$  are both edge-transitive circulants, then  $G$  is one of:  $mK_n$ ,  $\overline{mK_n}$ , or a self-complementary Paley graph ( $n$  is prime,  $1 \pmod{4}$ ) and  $S = \{a^2 : a \in \mathbb{Z}_n^*\}$ ).*

The property of 2-arc-transitivity is stronger than arc-transitivity, but accordingly tells us more about the action of the automorphism group. Circulant graphs that are 2-arc-transitive have been fully classified by Alspach, Conder, Marušič and Xu [4], as follows.

**Theorem 9.7.** *A connected 2-arc-transitive circulant graph is one of:*

1.  $K_n$  (exactly 2-arc-transitive);
2.  $K_{n/2, n/2}$  (exactly 3-arc-transitive);
3.  $K_{n/2, n/2}$  minus a 1-factor,  $n \geq 10$ ,  $n/2$  odd (exactly 2-arc-transitive);
4.  $C_n$  ( $k$ -arc-transitive for every  $k \geq 0$ )

### 9.3. Other regular subgroups in $\text{Aut}(X)$

The automorphism group of any circulant graph will have a cyclic subgroup that acts regularly on the vertices of the graph. (A permutation group on a set  $V$  is said to act regularly if for any pair of points in  $V$ , there is exactly one permutation in the group that maps one to the other.) Sometimes, the automorphism group of a graph may have multiple, nonisomorphic, regular subgroups. This is of interest from a different perspective, because it means that the graph in question can be represented as a Cayley graph on some noncyclic group, besides being a circulant graph. From our perspective, knowing the regular subgroups of the automorphism group may be useful in determining the automorphism group.

There are only a few results of note on this topic. The first result was proven by Joseph in the special case  $n = p^2$  [23], and extended by Morris [33] to all prime powers.

**Theorem 9.8.** *If  $n = p^e$ ,  $X$  is a circulant graph on  $n$  vertices, and  $\text{Aut}(X)$  contains a regular subgroup that is not cyclic, then  $X$  is isomorphic to a wreath product of smaller circulant graphs.*

Recently, Marušič and Morris [31] proved the following results.

**Theorem 9.9.** *Let  $X = X(n; S)$  be a circulant graph, and  $\mathbb{Z}_n^*(S)$  be the subgroup of  $\mathbb{Z}_n^*$  that fixes  $S$  set-wise. Then if  $\gcd(n, |\mathbb{Z}_n^*(S)|) > 1$ , the automorphism group of  $X$  has a noncyclic regular subgroup.*

*In fact, if  $p$  is any prime divisor of  $\gcd(n, |\mathbb{Z}_n^*(S)|)$ , then the automorphism group of  $X$  contains a regular subgroup that is isomorphic to  $\mathbb{Z}_p \times \mathbb{Z}_{n/p}$ .*

They also show that the converse is not true in general; that is, there may be noncyclic regular subgroups in the automorphism group even if this greatest common divisor is 1.

In the same paper, they prove the following result. The condition that we must have a normal circulant means that the regular cyclic group must be normal in the automorphism group of the graph.

**Theorem 9.10.** *Let  $X$  be a normal circulant graph of order  $n$ ,  $n$  not divisible by 4. Then if the automorphism group of  $X$  has a noncyclic regular subgroup, that group must be metacyclic, generated by two cyclic subgroups whose orders are relatively prime.*

## 10. Concluding remarks

Efficient algorithms have been found for determining the automorphism group of a circulant graph, when the number of vertices is any product of distinct primes. In the case where the number of vertices is a prime power, structural theorems about the automorphism groups exist (in unpublished form), but no algorithms have been constructed. No work has been done on combining these into results that may hold when the number of vertices is divisible by at least two distinct primes, but is not square-free. There is, therefore, a great deal of room for more results on this problem.

Unfortunately, in the results that we have seen, the complexity (of the proofs) seems to be growing. The result on circulant graphs on a square-free number of vertices is the culmination of two densely-packed, long papers; the first provides a structural theorem, and the second the algorithm. The result that deals with circulant graphs whose number of vertices is a prime power seems to be unpublished to this point, largely because of its length and complexity. It may be that new techniques will need to be developed before the problem can be completed in its full generality.

Of course, circulant graphs are just one very small step towards answering the general question with which we began, of finding the automorphism group of any graph. In full generality, this problem seems unmanageable, but it may be that for some other classes of graphs, the solution turns out to be feasible, or even easy.

## References

- [1] Àdàm, A., Research problem 2–10. *J. Combin. Theory* **2** (1967), 309.
- [2] Alspach, B., Point-symmetric graphs and digraphs of prime order and transitive permutation groups of prime degree. *J. Combinatorial Theory Ser. B* **15** (1973), 12–17.

- [3] Alspach, B., On constructing the graphs with a given permutation group as their group, *Proc. Fifth Southeastern Conf. Combin., Graph Theory and Computing* (1974), 187–208.
- [4] Alspach, B., Conder, M., Marušič, D., and Xu, M.-Y. A classification of 2-arc-transitive circulants. *J. Algebraic Combin.* **5** (1996), 83–86.
- [5] Alspach, B., and Parsons, T. D., Isomorphism of circulant graphs and digraphs, *Discrete Math.* **25** (1979), 97–108.
- [6] Babai, L., Isomorphism problem for a class of point-symmetric structures, *Acta Math. Sci. Acad. Hung.* **29** (1977), 329–336.
- [7] Berggren, J. L., An algebraic characterization of symmetric graphs with a prime number of vertices, *Bull. Austral. Math. Soc.* **7** (1972), 131–134.
- [8] Burnside, W., On some properties of groups of odd order, *J. London Math. Soc.* **33** (1901), 162–185.
- [9] Chao, C. Y., On the classification of symmetric graphs with a prime number of vertices, *Trans. Amer. Math. Soc.* **158** (1971), 247–256.
- [10] Cheng, Y. and Oxley, J., On weakly symmetric graphs of order twice a prime. *J. Combin. Theory Ser. B* **42** (1987), 196–211.
- [11] Dixon, J.D., and Mortimer, B., *Permutation Groups*, Springer-Verlag New York, Berlin, Heidelberg, Graduate Texts in Mathematics, **163**, 1996.
- [12] Dobson, E., An extension of a classical result of Burnside, *unpublished manuscript*.
- [13] Dobson, E., and Morris, J., Toida’s conjecture is true, *Electronic J. Combin.*, **9(1)** (2002), R35.
- [14] Dobson, E., and Morris, J., On automorphism groups of circulant digraphs of square-free order, *Discrete Math.*, to appear.
- [15] Dobson, E., and Morris, J., Automorphism groups of circulant digraphs of square-free order, in preparation.
- [16] Dobson, E., and Witte, D., Transitive permutation groups of prime-squared degree, *J. Algebraic Combin.* **16** (2002), 43–69.
- [17] Elspas, B., and Turner, J., Graphs with circulant adjacency matrices, *J. Combin. Theory* **9** (1970), 297–307.
- [18] Frucht, R., Herstellung von Graphen mit vorgegebener abstrakter Gruppe. *Compositio Math.*, **6** (1938), 239–250.
- [19] Godsil, C. D., On Cayley graph isomorphisms, *Ars Combin.* **15** (1983), 231–246.
- [20] Godsil, C. D., On the full automorphism group of a graph. *Combinatorica* **1** (1981), 243–256.
- [21] Hemminger, R. L., Directed graphs with transitive abelian groups. *Amer. Math. Monthly* **74** (1967), 1233–1234.
- [22] Huang, Q. X., and Meng, J. X., On the isomorphisms and automorphism groups of circulants, *Graphs Combin.* **12** (1996), 179–187.
- [23] Joseph, A. The isomorphism problem for Cayley digraphs on groups of prime-squared order. *Discrete Math.* **141** (1995), 173–183.
- [24] Klin, M.H., Muzychuk, M., and Pöschel, R. The isomorphism problem for circulant graphs via Schur ring theory, *Codes and Association Schemes*, American Math. Society, 2001.

- [25] Klin, M. H., and Pöschel, R., The König problem, the isomorphism problem for cyclic graphs and the method of Schur, Proceedings of the Inter. Coll. on Algebraic methods in graph theory, Szeged 1978, *Coll. Mat. Soc. János Bolyai* **27**.
- [26] Klin, M.H. and R. Pöschel, The isomorphism problem for circulant digraphs with  $p^n$  vertices, *unpublished manuscript* (1980).
- [27] König, D., *Theorie der Endlichen und Unendlichen Graphen*, Akademische Verlagsgesellschaft, Leipzig, 1936.
- [28] Li, C. H., Isomorphisms and classification of Cayley graphs of small valencies on finite abelian groups, *Australas. J. Combin.* **12** (1995), 3–14.
- [29] Li, C. H., On isomorphisms of finite Cayley graphs—a survey. *Discrete Math.* **256** (2002), 301–334.
- [30] Li, C. H., Marušič, D., and Morris, J., Classifying arc-transitive circulants of square-free order. *J. Algebraic Combin.* **14** (2001), 145–151.
- [31] Marušič, D. and Morris, J., Normal circulant graphs with noncyclic regular subgroups, *J. Graph Theory*, to appear.
- [32] McKay, B. D., unpublished computer search for cyclic CI-groups.
- [33] Morris, J., Isomorphic Cayley graphs on nonisomorphic groups. *J. Graph Theory* **31** (1999), 345–362.
- [34] Muzychuk, M., Àdàm’s conjecture is true in the square-free case, *J. Combin. Theory A* **72** (1995), 118–134.
- [35] Muzychuk, M., On Àdàm’s conjecture for circulant graphs, *Disc. Math.* **167/168** (1997), 497–510.
- [36] Peisert, W. Direct product and uniqueness of automorphism groups of graphs. *Discrete Math.* **207** (1999), 189–197.
- [37] Praeger, C. E., Wang, R. J. and Xu, M. Y. Symmetric graphs of order a product of two distinct primes. *J. Combin. Theory Ser. B* **58** (1993), 299–318.
- [38] Sun, L., Isomorphisms of circulant graphs, *Chinese Ann. Math.* **9A** (1988), 259–266.
- [39] Toida, S., A note on Àdàm’s conjecture, *J. Combin. Theory B* **23** (1977), 239–246.
- [40] Turner, J., Point-symmetric graphs with a prime number of points, *J. Combin. Theory* **3** (1967), 136–145.
- [41] Wang, R. J. and Xu, M. Y., A classification of symmetric graphs of order  $3p$ . *J. Combin. Theory Ser. B* **58** (1993), 197–216.
- [42] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York, 1964.
- [43] Wielandt, H., *Mathematische Werke/Mathematical works*. Vol. 1. Group theory, edited and with a preface by Bertram Huppert and Hans Schneider, Walter de Gruyter & Co., Berlin, 1994.
- [44] Zelikovskij, A.Z., Knig’s problem for Abelian permutation groups. *Izv. Akad. Nauk BSSR, Ser. Fiz.-Mat. Nauk* **5** (1989), 34–39.
- [45] Zhang, H., On edge transitive circulant graphs. *Tokyo J. Math.* **19** (1996), 51–55

Joy Morris  
Department of Mathematics and Computer Science  
University of Lethbridge  
Lethbridge, AB. T1K 6R4. Canada  
e-mail: [joy@cs.uleth.ca](mailto:joy@cs.uleth.ca)