Arc-transitive circulant digraphs of odd prime-power order

Ming-Yao Xu\textsuperscript{a,}\textsuperscript{*}\textsuperscript{,1}, Young-Gheel Baik\textsuperscript{b}, Hyo-Seob Sim\textsuperscript{b}

\textsuperscript{a}Department of Mathematics, Shanxi Teachers University, Linfen, Shanxi 041004, People’s Republic of China
\textsuperscript{b}Division of Mathematical Sciences, Pukyong National University, Pusan 608-737, Republic of Korea

Received 30 April 2002; received in revised form 10 February 2004; accepted 7 June 2004

Abstract

In this paper, the full automorphism group of a circulant digraph of prime-power order is investigated, and as a result, a complete classification of arc-transitive circulant graphs of odd prime-power order is given.

© 2004 Elsevier B.V. All rights reserved.

MSC: 05C25; 20B25

Keywords: Circulant; Normal circulant; Arc-transitive graph

1. Introduction

Throughout this paper we consider only finite, simple, (undirected or directed) graphs, and only finite groups.

Let \( p \) be an odd prime number and let \( G = \mathbb{Z}_{p^m} = \{0, 1, \ldots, p^m - 1\} \) be a finite cyclic group of order \( p^m \), written additively. Let \( S \) be a subset of \( G \) not containing the zero element 0. We define the Cayley digraph \( X = \text{Cay}(G, S) \) of \( G \) with respect to \( S \) by

\[
V(X) = G,
E(X) = \{(g, s + g) | g \in G, s \in S\},
\]

and we call \( X \) a \textit{circulant digraph} of order \( p^m \), and \( S \) a \textit{symbol} of \( X \).

Proposition 1.1. Let \( X = \text{Cay}(G, S) \) be a Cayley digraph of \( G \) with respect to \( S \). Then

(1) \( \text{Aut}(X) \) contains the right regular representation \( R(G) \) of \( G \), so \( X \) is vertex-transitive, where \( R(G) = \{R(g) | g \in G\} \) and \( R(g) \) maps \( x \) to \( x + g \) for any \( x \in G \).

(2) \( X \) is connected if and only if \( G = \langle S \rangle \).

(3) \( X \) is undirected if and only if \(-S = S\).

The following fact is well-known:

\textsuperscript{*} This work was supported by the National Natural Science Foundation of China (Proj. No. 10371003).
\textsuperscript{*} Corresponding author. Permanent address: Institute of Mathematics, Peking University, Beijing 100871, People’s Republic of China.
E-mail addresses: xumy\textsuperscript{1}@math.pku.edu.cn (M.-Y. Xu), ygbaik\textsuperscript{1}@pknu.ac.kr (Y.-G. Baik), hsim\textsuperscript{1}@pknu.ac.kr (H.-S. Sim).
\textsuperscript{1} Most of the work in this paper was done when he visited Shanxi Teachers University.

0012-365X/ - see front matter © 2004 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2004.06.012
Proposition 1.2. A digraph $X = (V, E)$ of order $p^m$ is a circulant digraph if and only if $\text{Aut}(X)$ contains a regular subgroup isomorphic to $Z_p^m$.

Let $s$ be a positive integer $s$. An $s$-arc of $X$ is an $(s + 1)$-tuple $(v_0, v_1, \ldots, v_s)$ of vertices such that $\{v_{i-1}, v_i\} \in E(X)$ for $1 \leq i \leq s$ and if $s > 2$, then $v_{i-1} \neq v_{i+1}$ for $1 \leq i \leq s - 1$. We call $X$ an $s$-arc-transitive, if $\text{Aut}(X)$ acts transitively on $V(X)$ and on the set of $s$-arcs; and $X$ is called an $s$-transitive graph if $X$ is $s$-arc-transitive but not $(s + 1)$-arc-transitive. For the case $s = 1$, we simply use $A(X)$ to denote its $1$-arc set and call $1$-arc-transitive graphs arc-transitive.

The purpose of this paper is to classify all arc-transitive circulant graphs and digraphs of order $p^m$, where $p$ is an odd prime. For the case $m = 1$, that is, for the group $G = Z_p$, C.Y. Chao [3] gave such a classification for the undirected case in 1971, and in 1972 J.L. Berggren [2] simplified Chao’s proof; also Chao and Wells [4] did the same thing for the directed case in 1973. Nothing of this kind is known in the literature for $m \geq 2$. On the other hand, Alspach, Conder, Marušić and the first author [1] classified all 2-arc-transitive circulant graphs, and they said in the introductory section of [1] that “Our long-term goal is to classify all arc-transitive circulants”, and that “As a first step towards our long-term goal, we wish to determine which circulants are 2-arc-transitive.” Later, Meng and Wang classified 2-arc-transitive circulant digraphs in 2000, and Li et al. classified all arc-transitive circulants of square-free order in 2001; see [10, 11]. The present paper could be viewed as another step towards this long-term goal.

The method we use in this paper is mainly group-theoretic. The key result is a necessary and sufficient condition for such a circulant (di)graph to be normal, (see Theorems 3.1 and 3.2.) The concept of normality of a Cayley (di)graph was introduced by the first author in [14]. Here we will restate the definition and some basic facts for the normality of circulant (di)graphs.

Let $X = \text{Cay}(G, S)$ be a circulant digraph of order $p^m$ with symbol $S$, and let

$$\text{Aut}(G, S) = \{x \in \text{Aut}(G) | S^x = S\}.$$ 

Obviously, $\text{Aut}(X) \supseteq R(G)\text{Aut}(G, S)$. Let $A = \text{Aut}(X)$. We have

Proposition 1.3 (Godsil and Xu [5, 14]).

1. $N_A(R(G)) = R(G)\text{Aut}(G, S)$;
2. $A = R(G)\text{Aut}(G, S)$ is equivalent to $R(G)$ being normal in $A$.

Definition 1.4. The circulant digraph $X = \text{Cay}(G, S)$ is called normal if $R(G) \triangleleft A = \text{Aut}(X)$.

Proposition 1.5. Let $X = \text{Cay}(G, S)$ be a Cayley digraph of $G$ with respect to $S$, and $A = \text{Aut}(X)$. Let $A_0$ be the stabilizer of the zero element $0$ in $A$. Then $X$ is normal if and only if every element of $A_0$ is an automorphism of the group $G$.

For two graphs $X$ and $Y$, the lexicographic product of $X$ by $Y$, denoted by $X[Y]$ is the graph with vertex set $V(X) \times V(Y)$ such that $(v_1, u_1)$ is adjacent to $(v_2, u_2)$ if and only if either $v_1$ is adjacent to $v_2$ in $X$, or $v_1 = v_2$ and $u_1$ is adjacent to $u_2$ in $Y$, where $v_1, v_2 \in V(X)$ and $u_1, u_2 \in V(Y)$. If in addition, $X$ and $Y$ have the same vertex set then denote by $X - Y$ the graph with vertex set $V(X)$ and having two vertices adjacent if and only if they are adjacent in $X$ but not adjacent in $Y$.

This paper is organized as follows. After this introductory section, in Section 2 we collect some preliminary, mainly group-theoretic results we need later on. In Section 3 we investigate the normality of circulant (di)graphs, and finally in Section 4, we give a complete classification of arc-transitive circulant graphs and digraphs of odd prime power order.

2. Preliminaries

Let $T$ be a nonabelian simple group. We call a group $G$ an almost simple group with socle $T$ if $T \leq G \leq \text{Aut}(T)$, where we identify the group $T$ with its inner automorphism group $\text{Inn}(T)$.

The following result due to Guralnick [6] is of crucial importance to the theme of this article.

Theorem 2.1 (Guralnick [6]). Let $T$ be a nonabelian simple group with a subgroup $H < T$ satisfying $|T : H| = p^d$, $p$ a prime. Then one of the following holds:

1. $T = A_p$ and $H \cong A_{p-1}$ with $n = p^d$.
2. $T = \text{PSL}(n, q)$ and $H$ is the stabilizer of a projective point or a hyperplane in $\text{PG}(n-1, q)$, and $|T : H| = (q^n - 1)/(q - 1) = p^d$. (Note that $n$ must be prime.)
3. $T = \text{PSL}(2, 11)$ and $H \cong A_5$.
4. $T = M_{11}$ and $H \cong M_{10}$.
5. $T = M_{23}$ and $H \cong M_{22}$.
6. $T = \text{PSU}(4, 2) \cong \text{PSp}(4, 3)$ and $H$ is a subgroup of index 27.
Theorem 3.1. Let $p$ be an odd prime and $G = \mathbb{Z}_{p^m}$. Let $S \subseteq G \setminus \{0\}$ and $X = \text{Cay}(G, S)$, which is neither complete nor totally disconnected. If $(|\text{Aut}(G, S)|, p) = 1$, then $X$ is normal.

Proof. Let $A = \text{Aut}(X)$. If $m = 1$, that is, $G = \mathbb{Z}_p$, the conclusion is true by [14, Example 2.2]. So we may assume that $m > 1$.

First, we claim that $(|A_0|, p) = 1$, where $A_0$ is the stabilizer of 0 in $A$. Assume the converse. Then $p || A_0$. Let $P$ be a Sylow $p$-subgroup of $A$ with $P \supseteq R(G)$. Then $P > R(G)$, and hence $N_A(R(G)) \supseteq NP(R(G)) > R(G)$. By Proposition 1.3, $N_A(R(G)) = R(G)\text{Aut}(G, S)$. It follows that $p || \text{Aut}(G, S)$, a contradiction.

Furthermore, in all the above cases apart from $T = A_n$, $n = p^a > p$, and case (6), $H$ is a Hall $p'$-subgroup of $T$.

**Corollary 2.2.** Let $T$ be a nonabelian simple group with a subgroup $H < T$ and a cyclic Sylow $p$-subgroup $C < T$ satisfying $|T : H| = p^a$, $|C| = p^b$, $T = HC$ and $p$ is an odd prime. Then one of the following holds:

1. $T = A_p$ and $H \cong A_{p-1}$ with $a = 1$.
2. $T = PSL(n, q)$ and $H$ is the stabilizer of a projective point or a hyperplane in $PG(n-1, q)$, and $C$ is the Singer cycle. In this case $|T : H| = (q^n - 1)/(q - 1) = p^b$, and $n$ is a prime.
3. $T = PSL(2, 11)$ and $H \cong A_5$, and $p^6 = 11$.
4. $T = M_{11}$ and $H \cong M_{10}$, and $p^6 = 11$.
5. $T = M_{23}$ and $H \cong M_{22}$, and $p^6 = 23$.

In all cases, the permutation representation of $T$ on the cosets of $H$ is doubly transitive.

Table 1

<table>
<thead>
<tr>
<th>$(i)$</th>
<th>$T$</th>
<th>$\text{Aut}(T)$</th>
<th>$\text{Mult}(T)$</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>$A_p$</td>
<td>$S_p$</td>
<td>$Z_2$, if $p \neq 7$</td>
<td>$\text{Mult}(A_7) = Z_6$</td>
</tr>
<tr>
<td>(2)</td>
<td>$PSL(2, q)$</td>
<td>$PGL(2, q)$</td>
<td>$Z_d$, $d = (2, q - 1)$</td>
<td></td>
</tr>
<tr>
<td>(3)</td>
<td>$PSL(n, q)$, $n &gt; 2$</td>
<td>$PGL(n, q) \times Z_2$</td>
<td>$Z_d$, $d = (n, q - 1)$</td>
<td></td>
</tr>
<tr>
<td>(4)</td>
<td>$M_{11}$</td>
<td>$M_{11}$</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>(5)</td>
<td>$M_{23}$</td>
<td>$M_{23}$</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

For later use, in Table 1 we give the automorphism group and the Schur Multiplier of the groups listed in Corollary 2.2. (See [9].)

We need the following two Propositions.

**Proposition 2.3 (Zsigmondy [15]).** Let $p$ and $a$ be integers with $p \geq 2$ and $a \geq 3$. Provided $(p, a) \neq (2, 6)$, there is a prime $r$ such that $r | p^a - 1$ but $r$ does not divide $p^i - 1$ for $1 \leq i < a$.

**Proposition 2.4.** Let $T = PSL(n, q)$ and let $H$ be the stabilizer of a projective point or a hyperplane in $PG(n-1, q)$ as in Case (2) of Corollary 2.2, where $|T : H| = (q^n - 1)/(q - 1) = p^b$, and $n$ is a prime.

(i) Assume that $n = 2$ and $p$ is odd. Then either $p$ is a Fermat prime and $a = 1$, or $p = 3$ and $a = 2$.

(ii) Assume that $n \geq 3$ and $p$ is odd. Then $p | q - 1$.

Proof. (i) In this case $p^a = q + 1$. Since $p$ is odd, $q$ is a power of 2. If $a = 1$, then $p$ is a Fermat prime. If $a = 2$, then $(p - 1)(p + 1) = q$, and hence both $p - 1$ and $p + 1$ are powers of 2. It follows that $p = 3$ and $q = 8$. If $a \geq 3$, by Proposition 2.3 and $2 | p - 1$, $p^a - 1$ would have a prime divisor $\neq 2$, a contradiction.

(ii) Assume the converse, that is, $p | q - 1$. By Proposition 2.3, $q^n - 1$ has a prime divisor $r \neq p$, contradicting the fact that $(q^n - 1)/(q - 1) = p^a$. \(\square\)

Let $G$ be a finite group. $G$ is said to be a Burnside group, if every primitive group which has a regular subgroup isomorphic to $G$ is doubly transitive. (See [13, Definition 25.1].) We have

**Proposition 2.5 (Wielandt [13, Theorem 25.3]).** Every cyclic group of composite order is a Burnside group.

3. Normality of circulants

**Theorem 3.1.** Let $p$ be an odd prime and $G = \mathbb{Z}_{p^m}$. Let $S \subseteq G \setminus \{0\}$ and $X = \text{Cay}(G, S)$, which is neither complete nor totally disconnected. If $(|\text{Aut}(G, S)|, p) = 1$, then $X$ is normal.

Proof. Let $A = \text{Aut}(X)$. If $m = 1$, that is, $G = \mathbb{Z}_p$, the conclusion is true by [14, Example 2.2]. So we may assume that $m > 1$.

First, we claim that $(|A_0|, p) = 1$, where $A_0$ is the stabilizer of 0 in $A$. Assume the converse. Then $p || A_0$. Let $P$ be a Sylow $p$-subgroup of $A$ with $P \supseteq R(G)$. Then $P > R(G)$, and hence $N_A(R(G)) \supseteq NP(R(G)) > R(G)$. By Proposition 1.3, $N_A(R(G)) = R(G)\text{Aut}(G, S)$. It follows that $p || \text{Aut}(G, S)$, a contradiction.
We claim that
\[ \text{Theorem 3.2.} \]
\[ \text{If } p \text{ is the } p \text{-part of } G, \text{ then } p \text{ divides } |G|, \text{ and hence } p \mid |G|. \]
\[ \text{Let } \text{Aut}(G, S), \text{ Aut}(G, S), \text{ the lexicographic product of } (G, S) \text{ and } (G, S), \text{ is not normal in } \text{Aut}(X) \text{; the conclusion holds.} \]
\[ \text{In the remainder of the proof we assume that } X \text{ is connected, that is, } S \text{ contains elements } s \text{ with } (p, s) = 1. \]
\[ \text{Let } P = \left\{ 0, p^{m-1}, 2p^{m-1}, \ldots, (p-1)p^{m-1} \right\}. \]
\[ \text{Let } S_1 = \left\{ s \in S \mid (p, s) = 1, S_1 \subseteq S \right\} \text{ and } S_2 = S \setminus S_1. \]
\[ \text{Let } X_1 = \text{Cay}(G, S_1 \cup S_2) \text{ and } X_2 = \text{Cay}(G, S_2). \]
\[ \text{Since } p \mid |\text{Aut}(G, S), \text{ Aut}(G, S), \text{ the lexicographic product of } G, \text{ which is generated by } x : x \mapsto x(1 + a), \forall a \in G. \]
\[ \text{For any } s \in S_1, \text{ we have } s^{(2)} \subseteq S_1. \]
\[ \text{Since } x^2 = s(1 + p^{m-1}) = s + sp^{m-1}, x^3 = s(1 + p^{m-1})^2 = s + 2sp^{m-1}, \ldots, x^{2p-1} = s(1 + p^{m-1})p-1 = s + s(p-1)p^{m-1}, \]
\[ \text{We claim that } \sigma = \sigma \in \text{Aut}(X). \text{ In fact, letting } B_i = i + (p^{m-1}) \text{ for } 0 \leq i \leq p^{m-1} - 1, \sigma \text{ fixes every block } B_i \text{ setwise.} \]
\[ \text{Consider the graph } X_2. \text{ Since elements in } S_2 \text{ are all multiples of } p, \text{ every edge of } X_2 \text{ is between two blocks } B_i \text{ and } B_j \text{ with } i \equiv j \pmod{p} \text{ and the induced graph } [B_i, B_j] \text{ keeps invariant under the action of } \sigma. \]
\[ \text{So } \sigma \text{ also maps edges of } X_2 \text{ to themselves. Thus, } \sigma \text{ is an automorphism of } X_1 \text{ and also of } X_2, \text{ and } \sigma \text{ is an automorphism of } X. \]
We define a digraph \( G(pm, r) \) \(^{(1)}\).

**Theorem 4.1.** \(^{(1)}\) Let \( p \) be an odd prime and \( m \geq 2 \) be an integer. Let \( G = Z_{pm} \) and \( X = \text{Cay}(G, S) \), and let \( S_1 = \{s \in S | (p, s) = 1\} \). Then \( X \) is normal for \( G \) if and only if \( (G, S) \) is arc-transitive.

**Corollary 3.3.** Chao and Wells \([3,4]\) proved the following result: \( G(p, r) \) for every divisor \( r \) of \( p \) is arc-transitive. Also, since \( \text{Aut}(G(p, r)) = \langle x \rangle \), \( G(p, r) \) is an arc-transitive digraph of order \( p \) with out-valency \( r \).

**Theorem 4.2.** \(^{(1)}\) Every normal arc-transitive circulant digraph of order \( p \) is isomorphic to \( Z_p \times H_r \). The proof is different but Theorem 3.2 is not. The smallest counterexample is: \( G = Z_4 \times \{a\}, S = \{a, -a\}, X = \text{Cay}(G, S) \cong C_4 \), \( \text{Aut}(X) = D_8 \), \( X \) is normal but \( \text{Aut}(G, S) = Z_2 \).

**Remark 3.4.** Theorem 3.1 is also true for the case \( p = 2 \); the proof is different but Theorem 3.2 is not. The smallest counterexample is: \( G = Z_4 \times \{a\}, S = \{a, -a\}, X = \text{Cay}(G, S) \cong C_4 \), \( \text{Aut}(X) = D_8 \), \( X \) is normal but \( \text{Aut}(G, S) = Z_2 \).

## 4. Arc-transitive circulant digraphs

In this section we determine all arc-transitive circulant (di)graphs of order \( pm \), where \( p \) is an odd prime. In the whole section we assume that \( G = Z_{pm} \) is a finite cyclic group of order \( pm \), written additively, and that \( S \subseteq G^* = G - \{0\} \). Let \( X = \text{Cay}(G, S) \) and \( A = \text{Aut}(X) \).

For the case \( m = 1 \), that is, the case \( G = Z_p \), Chao and Wells \([3,4]\) classified the arc-transitive circulant (di)graphs of order \( p \). First we review their classification.

The automorphism group \( \text{Aut}(Z_p) \) of \( Z_p \) is isomorphic to \( Z_{p-1} \). For any positive divisor \( r \) of \( p - 1 \) we use \( H_r \) to denote the unique subgroup of \( \text{Aut}(Z_p) \) of order \( r \), which is isomorphic to \( Z_r \). We identify \( H_r \) with a subgroup of \( Z_{p-1}^* \).

Now we define a digraph \( G(p, r) \) of order \( p \) for each divisor \( r \) of \( p - 1 \) by

\[
V(G(p, r)) = Z_p,
E(G(p, r)) = \{(x, y) | x - y \in H_r\}.
\]

Chao and Wells \([3,4]\) proved the following result:

**Theorem 4.1.** \(^{(2)}\) (1) \( G(p, r) \) is an arc-transitive digraph of order \( p \) with out-valency \( r \) and in-valency \( p - 1 \).

(2) \( G(p, r) \) is undirected if and only if \( r \) is even.

(3) Every arc-transitive digraph of order \( p \) is isomorphic to \( pK_1 \) or \( G(p, r) \) for some divisor \( r \) of \( p - 1 \); the undirected graphs correspond to even divisors \( r \).

(4) \( A = \text{Aut}(G(p, r)) \cong Z_p \times H_r \leq \text{AGL}(1, p) \) acts regularly on the set of arcs for \( r < p - 1 \). \( G(p, p - 1) \) is the complete graph \( K_p \), and so \( \text{Aut}(G(p, p - 1)) = S_p \).

To generalize Chao’s result, we first define a digraph \( G(pm, r) \) for arbitrary \( m \geq 1 \) and for any divisor \( r \) of \( p - 1 \). Note that \( \text{Aut}(Z_{pm}) \cong Z_{pm-1} \times Z_{p-1} \). We use \( H_r \) to denote the unique subgroup of \( \text{Aut}(Z_{pm}) \) of order \( r \), which is isomorphic to \( Z_r \).

We define a digraph \( G(pm, r) \) by

\[
V(G(pm, r)) = Z_{pm},
E(G(pm, r)) = \{(x, y) | x - y \in H_r\}.
\]

**Theorem 4.2.** \(^{(2)}\) (1) \( G(pm, r) \) is an arc-transitive digraph of order \( pm \) with out-valency \( r \) and in-valency \( p - 1 \). \( G(pm, r) \) is undirected if and only if \( r \) is even.

(2) Every normal arc-transitive circulant digraph of order \( pm \) is isomorphic to \( G(pm, r) \) for some divisor \( r \) of \( p - 1 \), and with \( (pm, r) \neq (p, p - 1) \). (Note that \( G(p, p - 1) \) is complete, so it is not normal.)

(3) \( A = \text{Aut}(G(pm, r)) \cong Z_{pm} \times H_r \) acts regularly on the set of arcs for either \( m > 1 \), or \( m = 1 \) and \( r < p - 1 \). So normal arc-transitive circulant (di)graphs are 1-regular.

**Proof.** \(^{(2)}\) (1) By definition \( G(pm, r) = \text{Cay}(G, S) \), where \( S = H_r \). So \( \text{Aut}(G, S) = H_r \), which acts transitively on \( S \), and hence \( G(pm, r) \) is arc-transitive. Also, since \( p | \text{Aut}(G, S) \) and \( X \) is not complete, we have that \( X \) is normal by Theorem 3.1.

(2) Assume that \( X = \text{Cay}(G, S) \) is a normal arc-transitive circulant digraph. By Theorem 3.2, \( p | \text{Aut}(G, S) \), and hence \( \text{Aut}(G, S) \) is the unique subgroup \( H_r \) of order \( r \) of \( \text{Aut}(G) \) for some \( r | p - 1 \). Since \( X \) is arc-transitive, \( A_0 = \text{Aut}(G, S) \) acts transitively on \( S \), so \( S = sH_r \) is a coset of \( H_r \) (in the group \( \text{Aut}(G) \) which is viewed as a multiplicative group). Obviously, \( \text{Cay}(G, sH_r) \cong \text{Cay}(G, H_r) \), so \( X \cong G(pm, r) \). Since \( X \) is normal and it is not complete, we have \( (pm, r) \neq (p, p - 1) \).

(3) follows immediately from the normality of \( X \) and the fact that \( \text{Aut}(G, S) \) is cyclic. \( \square \)
The following two propositions are important for our purpose:

**Proposition 4.3.** For $1 \leq i < m$, $K_{p^i}[p^{m-i}K_1]$ and $G(p^i, r)[p^{m-i}K_1]$ are arc-transitive circulant digraphs of order $p^m$.

**Proposition 4.4.** Let $\overline{X}$ be an arc-transitive circulant digraph of order $p^m$ and $X = \overline{X}[p^kK_1] - p^k\overline{X}$. Then $X$ is arc-transitive but not circulant, and $\text{Aut}(X) = \text{Aut}(\overline{X}) \times S_{p^k}$ which contains a regular subgroup $Z_{p^m} \times Z_{p^k}$, but not $Z_{p^{m+k}}$.

(Proofs of Propositions 4.3 and 4.4 are easy and omitted.)

Since a disconnected circulant digraph is arc-transitive if and only if its connected components are arc-transitive, we only need to consider the connected case. The following theorem gives a classification for connected circulant (di)graphs of odd prime power order.

**Theorem 4.5.** Let $X$ be a connected arc-transitive circulant (di)graph of order $p^m$. Then either $X \cong K_{p^m}$, or $X \cong G(p^m, r)$ for some divisor $r$ of $p - 1$, or $X \cong K_{p^i}[p^{m-i}K_1]$, or $X \cong G(p^i, r)[p^{m-i}K_1]$ for $1 \leq i < m$, and in the second and fourth cases, undirected graphs correspond to even divisors $r$.

**Proof.** Here we only give a proof for the undirected case. For the directed case the proof is essentially the same and is left to the reader.

Assume first that $X$ is normal, then by Theorem 4.2, $X \cong G(p^m, r)$ for some even divisor $r$ of $p - 1$.

In the remainder of the proof we shall assume that $X$ is not complete and is not normal, and that $m > 1$.

By Proposition 2.5, $Z_{p^m}$ is a Burnside group. It follows that $A$ is not primitive since $X$ is not complete. Let $B$ be a smallest block of imprimitivity, and $\mathcal{B} = \{B = B_0, B_1, \ldots, B_{p^m - 1}\}$ the corresponding complete block system. So the length of $B$ is $p^{m-1}$.

Let the quotient graph of $X$ modulo $\mathcal{B}$ be $\overline{X}$. Let $K$ be the kernel of the action of $A$ on $\mathcal{B}$. Since $B$ is also a block of $G = (\mathcal{A}) = Z_{p^m}$, $\mathcal{B}$ is just the set of cosets of the subgroup $H = (a^l)$ of $G$. So $R(H)$, the right translation of $H$, is contained in $K$. That means $K^B$ contains a cyclic regular subgroup isomorphic to $K$. Since $G/K \cong Z_{p^l}$ is contained in $\text{Aut}(\overline{X})$, $\overline{X}$ is a circulant of order $p^l$. We shall distinguish two different cases.

**Case 1:** $m - i > 1$. Since $B$ is the smallest block of $A$, $A^B_{\{B\}}$ is primitive. Since $m - i > 1$, $|H| > p$, and hence $H$ is a Burnside group by Proposition 2.5. It follows that $A^B_{\{B\}}$ is doubly transitive on $B$. Since $1 \neq K^B \cong A^B_{\{B\}}$ and $A^B_{\{B\}}$ has no noncyclic $p$-group, checking the list of doubly-transitive groups in [8], we have $K^B$ is also doubly transitive on $B$. We want to prove that $X$ is a lexicographic product of $\overline{X}$ by $p^{m-1}K_1$, that will complete the proof in this case.

We assume the converse, that is, $X$ is not a lexicographic product of $\overline{X}$ by $p^{m-1}K_1$. Note that there are no edges between vertices inside any block $B$ by [12]. Let us consider the induced graph $[B_1, B_2]$ for any two adjacent blocks $B_1$ and $B_2$. By the assumption, $[B_1, B_2]$ is not bipartite complete. (By the arc-transitivity of the quotient graph $\overline{X}$, $[B_1, B_2]$ are the same for any two adjacent blocks $B_1$ and $B_2$.) Let $K_j$ be the kernel of the action of $K$ on $B_j$ and $K_j$ the kernel on $B_j$. Take a vertex $v \in B_j$. If $K_j$ is transitive on $B_j$, then it is clear that $[B_1, B_2]$ is bipartite complete, a contradiction. Assume that $K_v$ fixes every vertex $B_j$, that is, $K_v \subseteq K_j$. Since $K_v$ is transitive on $B_j \setminus \{v\}$, for any vertex $u \in B_j$ such that $u$ is adjacent to a vertex in $B_j \setminus \{v\}$, we have that $u$ is adjacent to every vertex in $B_j \setminus \{v\}$; and hence $[B_1, B_2] = K_{p,p}$ minus a one-factor because $[B_1, B_2] \neq K_{p,p}$. This implies that $K_1$ fixes every vertex in $B_1$, and hence $K_1 = K_j$, contradicting the fact that $K_v \cong K_j$. So we have $K_v \cong K_j$ and $K_v$ is not transitive on $B_j$. Since $[B_1, B_2] \neq K_{p,p}$, the doubly transitive group $K/K_j \cong K_{[B_j]}$ must be almost simple with socle $\text{PSL}(n, q)$, and $(q^n - 1)/(q - 1) = p^{m-1}$. Since $K_vK_j/K_j$ is a subgroup of $K/K_j$ of $p$-power index at most $[B_j] = p^{m-i}$, we obtain that $|K : K_vK_j| = p^{m-i}$ since $\text{PSL}(n, q)$ has no subgroup of index $(q^n - 1)/(q - 1) = p^{m-i}$ (see [9, Table 5.2.A]).

It follows that $K_v \cong K_j$ and that $K_j = K_1$. By the connectedness and the arc-transitivity of $\overline{X}$, $K_1$ fixes every block pointwise, and hence $K_1 = 1$ and the action of $K$ on any block $B$ is faithful. Now we claim that the representations of $K$ on any two adjacent blocks $B_1$ and $B_2$ are equivalent, and hence $K_1$ fixes a unique vertex in every block $B$. If not, $K$ has socle $\text{PSL}(n, q)$, and by the arc-transitivity of $\overline{X}$ the representations of $K$ on any two adjacent blocks $B_1$ and $B_2$ are not equivalent. Take a Hamilton cycle in $\overline{X}$; it has odd length. So there must be two adjacent blocks such that the representations of $K$ on these two adjacent blocks $B_1$ and $B_2$ are equivalent, a contradiction. Now it is easy to see that $[B_1, B_2] = K_{p,p}$ minus a one-factor, or $[B_1, B_2]$ is perfect by matching. In the latter case the graph $X$ is not connected. So the former happens and $X \cong \overline{X}[p^{m-1}K_1] - p^{m-1}\overline{X}$. By Example 4.4, $X$ is not a circulant, a contradiction.

**Case 2:** $m - i = 1$. By the nonnormality of $X$, the subgroup of order $p$ of $\text{Aut}(G)$ is contained in $\text{Aut}(X)$, which is generated by $z : x \mapsto x(1 + p^{m-i})$, $\forall x \in G$. Since $X$ is connected, there is an $s \in S$ such that $(s, p) = 1$. So we have $s + ks^{m-i} \in S$ for $k = 0, 1, \ldots, p - 1$. Let $B_0 = \langle p^{m-1} \rangle$ and $B_1 = s + \langle p^{m-1} \rangle$. The induced graph $[B_0, B_1] = K_{p,p}$. By the arc-transitivity of...
$X$, we have that for any two adjacent blocks $B_l$ and $B_j$, the induced graph $[B_l, B_j] = K_{p, p}$. It follows that $X$ is a lexicographic product of $X$ and $pK_1$.

Summarizing Cases 1 and 2 we complete the proof of this theorem. □

References