On the automorphism group of integral circulant graphs

Milan Bašić

University of Niš, Faculty of Sciences and Mathematics
Višegradska 33, 18000 Niš, Serbia

e-mail: basic_milan@yahoo.com

Aleksandar Ilić ‡

University of Niš, Faculty of Sciences and Mathematics
Višegradska 33, 18000 Niš, Serbia

e-mail: aleksandari@gmail.com

Submitted: Oct 6, 2009; Accepted: Mar 9, 2011; Published: Mar 31, 2011
Mathematics Subject Classification: 05C60, 05C25

Abstract

The integral circulant graph $X_n(D)$ has the vertex set $Z_n = \{0, 1, 2, \ldots, n-1\}$ and vertices a and b are adjacent, if and only if $\gcd(a-b, n) \in D$, where $D = \{d_1, d_2, \ldots, d_k\}$ is a set of divisors of n. These graphs play an important role in modeling quantum spin networks supporting the perfect state transfer and also have applications in chemical graph theory. In this paper, we deal with the automorphism group of integral circulant graphs and investigate a problem proposed in [W. Klotz, T. Sander, *Some properties of unitary Cayley graphs*, Electr. J. Comb. 14 (2007), #R45]. We determine the size and the structure of the automorphism group of the unitary Cayley graph $X_n(1)$ and the disconnected graph $X_n(d)$. In addition, based on the generalized formula for the number of common neighbors and the wreath product, we completely characterize the automorphism groups $Aut(X_n(1,p))$ for n being a square-free number and p a prime dividing n, and $Aut(X_n(1,p^k))$ for n being a prime power.

1 Introduction

Circulant graphs are Cayley graphs over a cyclic group. The interest of circulant graphs in graph theory and applications has grown during the last two decades. They appeared in coding theory, VLSI design, Ramsey theory and other areas. Recently there is vast research on the interconnection schemes based on the circulant topology – circulant graphs represent an important class of interconnection networks in parallel and distributed computing (see [17]).

Integral circulant graphs as the circulants with integral spectra, were imposed as potential candidates for modeling quantum spin networks with periodic dynamics [12, 30]. Saxena, Severini and Shraplinski [30] studied some parameters of integral circulant graphs such as the diameter, bipartiteness and perfect state transfer. The present authors in [4, 18] calculated the clique and chromatic number of integral circulant graphs with exactly one and two divisors, and also disproved the conjecture that the order of $X_n(D)$ is divisible by the clique and chromatic number.

Various properties of unitary Cayley graphs as a subclass of integral circulant graphs were investigated in some recent papers. In the work of Berrizbeitia and Giudici [6] and in the later paper of Fuchs [11], some lower and upper bounds for the longest induced cycles were given. Bašić et al. [3, 5] established a characterization of integral circulant graphs which allow perfect state transfer. In addition, they proved that there is no perfect state transfer in the class of unitary Cayley graphs except for the hypercubes K_2 and C_4. Klotz and Sander [23] determined the diameter, clique number, chromatic number and eigenvalues of unitary Cayley graphs. The latter group of authors proposed a generalization of unitary Cayley graphs named *gcd-graphs* and proved that they have to be integral. Integral circulant graphs were also characterized by So [32].

Let A be the adjacency matrix of a simple graph G, and $\lambda_1, \lambda_2, \ldots, \lambda_n$ be the eigenvalues of the graph G. The energy of G is defined as the sum of absolute values of its eigenvalues [13, 14]

$$E(G) = \sum_{i=1}^{n} |\lambda_i|.$$

The graph G is said to be hyperenergetic if its energy exceeds the energy of the complete graph K_n, or equivalently if $E(G) > 2n - 2$. This concept was introduced first by Gutman and afterwards has been studied intensively in the literature [2, 7, 15, 16, 31, 33]. Hyperenergetic graphs are important because molecular graphs with maximum energy pertain to maximality stable π-electron systems. It has been proven that for every $n \geq 8$, there exists a hyperenergetic graph of order n [14]. In [19, 20, 21, 29], the authors calculated the energy and distance energy of unitary Cayley graphs and their complements. Furthermore, they establish the necessary and sufficient conditions for X_n to be hyperenergetic.

In this paper we characterize the automorphism group $Aut(X_n)$ of unitary Cayley graphs, and make a step towards characterizing the automorphism group of an arbitrary integral circulant graph. Many authors studied the isomorphisms of circulant and Cayley graphs [26, 28], automorphism groups of Cayley digraphs [10], integral Cayley graphs over Abelian groups [24], rational circulant graphs [22], etc. For the survey on the automorphism groups of circulant graphs see [27]. Following Kovács [25] and Dobson and Morris [8, 9], we start with two cases: $n = p^k$ being a prime power and $n = p_1 p_2 \cdot \ldots \cdot p_k$ being a square-free number. These results are essential for the future research in this field. Furthermore, we generalize the formula given in [23] for counting the number of common neighbors of two arbitrary vertices of X_n.

The paper is organized as follows. In Section 2 we give some preliminary results on integral circulant graphs. In Section 3 we calculate the automorphism group of unitary Cayley graphs and answer the open question from [23] about the ratio of the size of the automorphism group of X_n and the size of the group of affine automorphisms of X_n. In addition, we determine the size of the automorphism group of the disconnected graph $X_n(d)$, where $d \mid n$. In Section 4, we prove the general formula for the number of common neighbors in integral circulant graph $X_n(d_1, d_2)$. Based on this formula, in Section 5 we characterize the automorphism groups of two classes of integral circulant graphs with $|D| = 2$

- $Aut(X_{p^k}(1, p^l))$ with $0 < l < k$,
- $Aut(X_n(1, p))$ with n being a square-free number.

We conclude the paper by posing some open questions for further research.

2 Preliminaries

Let us recall that for a positive integer n and subset $S \subseteq \{0, 1, 2, \ldots, n-1\}$, the circulant graph $G(n, S)$ is the graph with n vertices, labeled with integers modulo n, such that each vertex i is adjacent to $|S|$ other vertices $\{i + s \pmod n \mid s \in S\}$. The set S is called a symbol of $G(n, S)$. As we will consider only undirected graphs, we assume that $s \in S$ if and only if $n - s \in S$, and therefore the vertex i is adjacent to vertices $i \pm s \pmod n$ for each $s \in S$.

Recently, So [32] has characterized integral circulant graphs. Let

$$G_n(d) = \{k \mid \gcd(k, n) = d,\ 1 \leq k < n\}$$

be the set of all positive integers less than n having the same greatest common divisor d with n. Let D_n be the set of positive divisors d of n, with $d \leq \frac{n}{2}$.

Theorem 2.1 ([32]) *A circulant graph $G(n, S)$ is integral if and only if*

$$S = \bigcup_{d \in D} G_n(d)$$

for some set of divisors $D \subseteq D_n$.

Let Γ be a multiplicative group with identity e. For $S \subset \Gamma$, $e \notin S$ and $S^{-1} = \{s^{-1} \mid s \in S\} = S$, the Cayley graph $X = Cay(\Gamma, S)$ is the undirected graph having vertex set $V(X) = \Gamma$ and edge set $E(X) = \{\{a, b\} \mid ab^{-1} \in S\}$. For a positive integer $n > 1$ the unitary Cayley graph $X_n = Cay(Z_n,\ U_n)$ is defined by the additive group of the ring Z_n of integers modulo n and the multiplicative group $U_n = Z_n^*$ of its units. Unitary

Cayley graphs are highly symmetric and have some remarkable properties connecting graph theory, number theory and group theory.

Let D be a set of positive, proper divisors of the integer $n > 1$. Define the gcd-graph $X_n(D)$ having vertex set $Z_n = \{0, 1, \ldots, n-1\}$ and edge set

$$E(X_n(D)) = \{\{a, b\} \mid a, b \in Z_n,\ \gcd(a-b, n) \in D\}.$$

If $D = \{d_1, d_2, \ldots, d_k\}$, then we also write $X_n(D) = X_n(d_1, d_2, \ldots, d_k)$; in particular $X_n(1) = X_n$. Throughout the paper, we let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, where $p_1 < p_2 < \ldots < p_k$ are distinct primes, and $\alpha_i \geq 1$. By Theorem 2.1 we obtain that integral circulant graphs are Cayley graphs of the additive group of Z_n with respect to the Cayley set $S = \bigcup_{d \in D} G_n(d)$ and, thus, they are exactly gcd-graphs. From Corollary 4.2 in [17], the graph $X_n(D)$ is connected if and only if $\gcd(d_1, d_2, \ldots, d_k) = 1$.

In the characterization of the automorphism group, we will use the concept of wreath product (similar as the lexicographical product in graph theory) [27].

Definition 2.1 *Let G and H be permutation groups acting on X and Y, respectively. We define the wreath product of G and H, denoted $G \wr H$, to be the permutation group that acts on $X \times Y$ consisting of all permutations of the form $(x, y) \to (g(x), h_x(y))$, where $g \in G$ and $h_x \in H$.*

3 The automorphism group of unitary Cayley graphs

For a graph G, let $N(a, b)$ denote the number of common neighbors of the vertices a and b. The following theorem is the main tool in describing properties of the automorphisms of unitary Cayley graphs:

Theorem 3.1 *([23]) The number of common neighbors of distinct vertices a and b in the unitary Cayley graph X_n is given by $N(a, b) = F_n(a-b)$, where $F_n(s)$ is defined as*

$$F_n(s) = n \prod_{p \mid n,\ p \ prime} \left(1 - \frac{\varepsilon(p)}{p}\right), \qquad with \qquad \varepsilon(p) = \begin{cases} 1 & if \quad p \mid s \\ 2 & if \quad p \nmid s \end{cases}.$$

Recall that

$$Aut(X_n) = \{f : X_n \to X_n \mid f \text{ is a bijection, and } (a, b) \in E(X_n) \text{ iff } (f(a), f(b)) \in E(X_n)\}$$

We will first determine $|Aut(X_n)|$, with n being a prime power.

Theorem 3.2 *Let $n = p^k$, where p is a prime number and $k \geq 1$. Then*

$$|Aut(X_n)| = p! \left((p^{k-1})!\right)^p.$$

Proof: Let $C_0, C_1, \dots, C_{p-1}$ be the classes modulo p,

$$C_i = \{j \mid 0 \le j < p^k,\ j \equiv i \pmod p\}, \qquad 0 \le i \le p-1.$$

Two vertices a and b from X_n are adjacent if and only if $\gcd(a-b, n) = \gcd(a-b, p^k) = 1$ or equivalently $p \nmid (a-b)$. This means that all vertices from some class C_i are adjacent to the vertices from $X_n \setminus C_i$, while there are no edges between any two vertices from C_i.

Let $f \in Aut(X_n)$ be an automorphism of X_n. Let a and b be two vertices from the class C_i and $f(a) \in C_j$, where $0 \le i, j \le p-1$. It follows that $p \mid a-b$, which implies that a and b are not adjacent, and consequently $f(a)$ and $f(b)$ are not adjacent. From the above consideration, $f(a) - f(b)$ is divisible by p and we conclude that $f(b)$ belongs to the same class modulo p as $f(a)$, i.e. $f(b) \in C_j$. This implies that the vertices from the class C_i are mapped to the vertices from the class C_j. Since we choose an arbitrary index i, we get that the classes are permuted under the automorphism f.

Assume that the class C_i is mapped to the class C_j. Since the vertices from the class C_i form an independent set and the restriction of the automorphism f on the vertices of C_i is a bijection from C_i to C_j, we have all $|C_i|! = (p^{k-1})!$ permutations of the vertices of the class C_i. Finally, taking into account that classes and vertices permute independently, by the product rule we get that the number of automorphisms of X_n equals $p!\left((p^{k-1})!\right)^p$. $\square$

Define the sets

$$C_i^{(j)} = \{0 \le a < n \mid a \equiv i \pmod{p_j}\}, \qquad 1 \le j \le k, \qquad 0 \le i < p_j.$$

In [18] the present authors proved that the chromatic number of X_n is equal to the smallest prime p_1 dividing n and that the color classes of X_n are exactly the classes modulo p_1 and uniquely determined. This means that the maximal independent sets are exactly $C_0^{(1)}, C_1^{(1)}, \dots, C_{p_1-1}^{(1)}$, and the classes modulo p_1 permute under the automorphism f. In the following, we will prove that for an arbitrary prime number p dividing n the classes modulo p permute under the automorphism f.

Lemma 3.3 *For an automorphism f of X_n and prime number p_i dividing n holds:*

$$p_i \mid a-b \qquad \text{if and only if} \qquad p_i \mid f(a) - f(b),$$

where $0 \le a, b \le n-1$ and $1 \le i \le k$.

Proof: Since f^{-1} is an automorphism, we will prove that for a prime number p_i dividing n holds

$$p_i \mid a-b \qquad \Rightarrow \qquad p_i \mid f(a) - f(b),$$

and the opposite direction of the statement follows directly by mapping $a \mapsto f^{-1}(a)$ for $0 \le a \le n-1$.

Suppose that the statement of the lemma is not true and let $2 \le j \le k$ be the greatest index such that $p_j \mid a-b$ and $p_j \nmid f(a) - f(b)$.

First we will consider the pair $(a,b) = (i, i+p_j)$ such that $p_j \nmid f(i) - f(i+p_j)$, where $0 \leq i \leq n-1-p_j$. Using Theorem 3.1 it follows

$$N(i, i+p_j) = F_n(p_j) = (p_1 - 2) \cdot \ldots \cdot (p_{j-1} - 2)(p_j - 1)(p_{j+1} - 2) \cdot \ldots \cdot (p_k - 2) \cdot \frac{n}{p_1 p_2 \ldots p_k}.$$

Since $p_{j+1}, p_{j+2}, \ldots, p_k$ does not divide $f(i) - f(i+p_j)$ we have

$$N(f(i), f(i+p_j)) = (p_1 - \varepsilon(p_1)) \cdot \ldots \cdot (p_{j-1} - \varepsilon(p_{j-1}))(p_j - 2)(p_{j+1} - 2) \cdot \ldots \cdot (p_k - 2) \cdot \frac{n}{p_1 p_2 \ldots p_k}.$$

The automorphism f preserves the number of common neighbors of the vertex pairs $(i, i+p_j)$ and $(f(i), f(i+p_j))$, or equivalently $N(i, i+p_j) = N(f(i), f(i+p_j))$. If $\varepsilon(p_1) = \varepsilon(p_2) = \ldots = \varepsilon(p_{j-1}) = 2$,

$$\frac{N(f(i), f(i+p_j))}{N(i, i+p_j)} = \frac{p_j - 2}{p_j - 1} < 1,$$

which is a contradiction. Thus there exists an index $1 \leq s \leq j-1$, such that $\varepsilon(p_s) = 1$. Similarly, we have

$$\frac{N(f(i), f(i+p_j))}{N(i, i+p_j)} \geq \frac{(p_s - 1)(p_j - 2)}{(p_s - 2)(p_j - 1)} > 1,$$

since $p_s < p_j$. This is again a contradiction, and it follows that $p_j \mid f(i) - f(i+p_j)$.

For an arbitrary $a, b \in X_n$ such $p_j \mid a - b$ and $a < b$ we have

$$p_j \mid (f(a) - f(a+p_j)) + (f(a+p_j) - f(a+2p_j)) + \ldots + (f(b-p_j) - f(b)) = f(a) - f(b),$$

and finally the classes modulo p_j also permute under the automorphism f. This completes the proof. $\square$

Theorem 3.4 *Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ be a canonical representation of n, with prime numbers $p_1 < p_2 < \ldots < p_k$. Then*

$$|Aut(X_n)| = p_1! \cdot p_2! \cdot \ldots \cdot p_k! \cdot \left(\left(\frac{n}{p_1 p_2 \cdot \ldots \cdot p_k} \right)! \right)^{p_1 p_2 \cdot \ldots \cdot p_k}$$

Proof: Let $f \in Aut(X_n)$ be an automorphism of X_n and $m = p_1 p_2 \cdot \ldots \cdot p_k$ be the largest square-free number dividing n. Two vertices a and b from X_n are adjacent if and only if $\gcd(a-b, m) = 1$.

Consider the classes $D_0, D_1, \ldots, D_{m-1}$, defined as follows

$$D_i = \{0 \leq a < n \mid a \equiv i \pmod{m}\}.$$

The size of every class D_i is equal to $\frac{n}{m}$. For an arbitrary vertices $a, b \in D_i$ holds $m \mid a - b$, and every class modulo m is an independent set. By Lemma 3.3, we have that $f(a) - f(b)$ is divisible by m and it follows that the classes $D_0, D_1, \ldots, D_{m-1}$ permute under the automorphism f. Let $a \in D_i$ and $b \in D_j$ be arbitrary vertices from different classes. The vertices a and b are adjacent if and only if

$$\gcd(m(k-l)+(i-j),n)=1$$

for some $0 \leq k,l \leq \frac{n}{m}-1$. Furthermore, if $i-j$ is relatively prime with n, the vertices from D_i and D_j form a complete bipartite induced subgraph of X_n. Otherwise, there are no edges between the classes D_i and D_j. Since the classes $\{D_0, D_1, \ldots, D_{m-1}\}$ permute under the automorphism f and each class is an independent set, for $D_i = f(D_j)$, there are exactly $(\frac{n}{m})!$ possibilities for the restriction of the automorphism f from the vertices of D_i on the vertices of D_j, $i = 0, 1, \ldots, m-1$.

Next we will count the number of permutations of classes D_i. Let i be an arbitrary index such that $0 \leq i \leq m-1$, and let $i_1, i_2, \ldots, i_k$ be the residue of i modulo $p_1, p_2, \ldots, p_k$, respectively. For each $1 \leq s \leq k$, we have $D_i \subseteq C^{(s)}_{i_s}$ implying that

$$D_i \subseteq C^{(1)}_{i_1} \cap C^{(2)}_{i_2} \cap \ldots \cap C^{(k)}_{i_k}.$$

On the other side for these indices $i_1, i_2, \ldots, i_k$, consider the following system of congruences

$$\begin{array}{rcll} x & \equiv & i_1 & \pmod{p_1} \\ x & \equiv & i_2 & \pmod{p_2} \\ & \ldots & & \\ x & \equiv & i_k & \pmod{p_k}. \end{array}$$

According to the Chinese remainder theorem, it follows that there exists a unique solution i of the above system, such that $0 \leq i < m = p_1 p_2 \cdot \ldots \cdot p_k$, and

$$C^{(1)}_{i_1} \cap C^{(2)}_{i_2} \cap \ldots \cap C^{(k)}_{i_k} \subseteq D_i.$$

Finally we conclude that $D_i = C^{(1)}_{i_1} \cap C^{(2)}_{i_2} \cap \ldots \cap C^{(k)}_{i_k}$.

According to Lemma 3.3, for every prime p_s, $1 \leq s \leq k$, the automorphism f permutes the classes $C^{(s)}_0, C^{(s)}_1, \ldots, C^{(s)}_{p_s-1}$. Thus, there exist indices $j_1, j_2, \ldots, j_k$ where $0 \leq j_s < p_s$, $1 \leq s \leq k$, such that $f(C^{(s)}_{i_s}) = C^{(s)}_{j_s}$. Since f is a bijection, we have

$$f(C^{(1)}_{i_1} \cap C^{(2)}_{i_2} \cap \ldots \cap C^{(k)}_{i_k}) = f(C^{(1)}_{i_1}) \cap f(C^{(2)}_{i_2}) \cap \ldots \cap f(C^{(k)}_{i_k}),$$

and $f(D_i) = C^{(1)}_{j_1} \cap C^{(2)}_{j_2} \cap \ldots \cap C^{(k)}_{j_k} = D_j$. If we denote by h_s the permutation of the indices modulo p_s, we can construct a mapping $f(D_i) \mapsto D_j$ if and only if $h_s(i_s) = j_s$, for $s = 1, 2, \ldots, k$. This means that the class $f(D_i)$ is determined by the permutations of classes $C^{(s)}_{j_s}$ for each $1 \leq s \leq k$. Since these permutations are independent, the number of permutations of the classes D_i is bounded from above by the product of the number of permutations of the classes $C^{(s)}_{j_s}$, that is $p_1! \cdot p_2! \cdot \ldots \cdot p_k!$.

Next we will show that the constructed mappings are indeed the automorphisms. For an arbitrary classes $D_{l'}$ and $D_{l''}$ there exist classes $D_{p(l')}$ and $D_{p(l'')}$ such that $f(D_{l'}) = D_{p(l')}$ and $f(D_{l''}) = D_{p(l'')}$, for some permutation p of the indices $0, 1, \ldots, m-1$. The permutation $p(l)$ corresponds to the solution of the following system of congruences, where $h_i : Z_{p_i} \to Z_{p_i}$ represent some permutations of classes $C_j^{(i)}$, $1 \le i \le k$ and $0 \le j \le p_i - 1$,

$$p(l) \equiv \sum_{i=1}^{k} c_{p_i} \cdot h_i(l_i) \pmod{m} \tag{1}$$

for any $0 \le l \le m-1$ and $l_i \equiv l \pmod{p_i}$, $0 \le l_i \le p_i - 1$, for $i = 1, 2, \ldots, k$. Constants c_{p_i} are the solutions of the following system of k congruence equations

$$\begin{array}{rcll} c_{p_i} & \equiv & 1 & \pmod{p_i} \\ c_{p_i} & \equiv & 0 & \pmod{p_j}, \qquad 1 \le j \le k,\ j \ne i. \end{array}$$

The form of the solution (1) follows directly from the Chinese remainder theorem, and we have

$$\begin{array}{rcl} \gcd(p(l') - p(l''), n) = 1 & \Leftrightarrow & \gcd\left(\sum_{i=1}^{k} c_{p_i} \cdot (h_i(l_i') - h_i(l_i'')), n\right) = 1 \\ & \Leftrightarrow & p_i \nmid h_i(l_i') - h_i(l_i''), \quad i = 1, 2, \ldots, k \\ & \Leftrightarrow & p_i \nmid l_i' - l_i'', \quad i = 1, 2, \ldots, k \\ & \Leftrightarrow & \gcd\left(\sum_{i=1}^{k} c_{p_i} \cdot (l_i' - l_i''), n\right) = 1 \\ & \Leftrightarrow & \gcd(l' - l'', n) = 1. \end{array}$$

Therefore, we concluded that there are exactly $p_1! \cdot p_2! \cdot \ldots \cdot p_k!$ possibilities for permuting the classes $\{D_0, D_1, \ldots, D_{m-1}\}$. Since the vertices from the classes can be mapped without restrictions, by the product rule the size of the automorphism group of X_n is equal to

$$p_1! \cdot p_2! \cdot \ldots \cdot p_k! \cdot \left(\left(\frac{n}{m}\right)!\right)^m.$$

□

Let S_n be the symmetric group of degree n. Note that for prime number p, X_p is isomorphic to a complete graph K_p and therefore $Aut(X_p) = S_p$. Also, the permutations of classes modulo m, form a group $S_{p_1} \times S_{p_2} \times \ldots \times S_{p_k}$.

According to the construction of automorphisms of X_n in Theorem 3.4, we conclude that for every permutation of classes modulo m, there are m permutations of vertices in each class. This means that the automorphism group is isomorphic to the wreath product of the permutation group of classes modulo m and the permutation groups of vertices in each class. Thus, we obtain

$$Aut(X_n) = (S_{p_1} \times S_{p_2} \times \ldots \times S_{p_k}) \wr S_{n/m}.$$

Theorem 3.5 *For an arbitrary divisor d of n, and $n' = \frac{n}{d} = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_l^{\beta_l}$ holds*

$$|Aut(X_n(d))| = d! \cdot \left(q_1! \cdot q_2! \cdot \ldots \cdot q_l! \cdot \left(\left(\frac{n'}{q_1 q_2 \cdot \ldots \cdot q_l} \right)! \right)^{q_1 q_2 \cdot \ldots \cdot q_l} \right)^d .$$

Proof: The graph $X_n(d)$ is composed of d connected components $C_0, C_1, \ldots, C_{d-1}$ isomorphic to $X_{n/d}(1)$ [4]. Suppose that f is an automorphism of $X_n(d)$, and let a and b be two arbitrary vertices from a component C_i, $0 \leq i \leq d-1$. Since a and b are connected by a path P in C_i, it follows that $f(a)$ and $f(b)$ are also connected by the image $f(P)$ of the path P under the isomorphism f. This means that $f(a)$ and $f(b)$ belong to the same component C_j, $0 \leq j \leq d-1$. Let $m' = q_1 q_2 \cdot \ldots \cdot q_l$ be the largest square free number dividing n'. The classes C_i permute under the automorphism f, and the size of the automorphism group of each class is given by Theorem 3.4. Finally, the size of the automorphism group of $X_n(d)$ equals

$$d! \cdot \left(q_1! \cdot q_2! \cdot \ldots \cdot q_l! \cdot \left(\left(\frac{n'}{m'} \right)! \right)^{m'} \right)^d .$$

□

From the constructions of the automorphisms in Theorems 3.4 and 3.5 we obtain the following relation

$$Aut(X_n(d)) = S_d \wr Aut(X_{\frac{n}{d}}).$$

For $a, b \in Z_n$, the authors from [23] defined the affine transformation on the vertices of the graph X_n

$$\psi_{a,b} : Z_n \to Z_n \qquad \text{by} \qquad \psi_{a,b}(x) = ax + b \pmod n \qquad \text{for } x \in Z_n.$$

It is proven that $\psi_{a,b}$ is an automorphism of X_n, if and only if $a \in U_n$. Moreover, $A(X_n) = \{\psi_{a,b} \mid a \in U_n, b \in Z_n\}$ is a subgroup of the automorphism group $Aut(X_n)$. We call $A(X_n)$ the group of affine automorphisms of X_n and obviously

$$|A(X_n)| = n \cdot \varphi(n).$$

Motivated by the first open question in [23], we will prove that $|A(X_n)| \leq |Aut(X_n)|$, with equality if and only if $n \in \{2, 3, 4, 6\}$. Consider the ratio

$$\begin{aligned} \frac{|Aut(X_n)|}{|A(X_n)|} &= \frac{p_1! \cdot p_2! \cdot \ldots \cdot p_k!}{p_1 p_2 \cdot \ldots \cdot p_k (p_1 - 1)(p_2 - 1) \cdot \ldots \cdot (p_k - 1)} \left(\frac{(p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1})!}{p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1}} \right)^2 \\ &\quad \cdot ((p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1})!)^{p_1 p_2 \cdot \ldots \cdot p_k - 2}. \end{aligned}$$

The first factor $(p_1 - 2)! \cdot (p_2 - 2)! \cdot \ldots \cdot (p_k - 2)!$ is greater than or equal to 1, with equality if and only if 2 and 3 are the only prime factors of n. The second factor $(p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1} - 1)!$ is also greater than or equal to 1, with equality if and only if n is a square-free number or double square-free number. The third factor $((p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_k^{\alpha_k - 1})!)^{p_1 p_2 \cdot \ldots \cdot p_k - 2}$ is greater than or equal to 1, with equality if and only if n is a square-free number, or $k = 1$ and $p_1 = 2$. It follows that $|A(X_n)| < |Aut(X_n)|$ for $n = 5$ and $n > 6$.

4 The number of common neighbors in $X_n(d_1, d_2)$

Let $d_1 = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}$ and $d_2 = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k}$. If $p^\alpha \mid n$, but $p^{\alpha+1}$ does not divide n, we write $p^\alpha \| n$, i.e. α is the greatest exponent such that p^α divides n. We will set $F_n(s) = 0$ if s is not an integer.

Theorem 4.1 *Let $d_2 > d_1 \geq 1$ be the divisors of n. The number of common neighbors of distinct vertices a and b in the connected integral circulant graph $X_n(d_1, d_2)$ is equal to*

$$F_{n/d_1}\left(\frac{b-a}{d_1}\right) + 2 \cdot \frac{n}{M} \cdot \prod_{p_i \nmid (b-a) d_1 d_2} (p_i - 2) \cdot \prod_{p_i \mid (b-a),\ p_i \nmid d_1 d_2} (p_i - 1) \cdot \prod_{p_i \mid d_1 d_2,\ \alpha_i \neq \beta_i,\ \alpha_i \neq \gamma_i} (p_i - 1)$$

if $\gcd(b-a, d_1) = \gcd(b-a, d_2) = 1,$ *and*

$$F_{n/d_1}\left(\frac{b-a}{d_1}\right) + F_{n/d_2}\left(\frac{b-a}{d_2}\right)$$

otherwise, where $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ *and*

$$M = \prod_{i=1}^{k} p_i^{\min(\max(\beta_i+1, \gamma_i+1), \alpha_i)}.$$

Proof: Let c be the common neighbor of the vertices a and b from $X_n(d_1, d_2)$, where $\gcd(d_1, d_2) = 1$. We have four cases based on the greatest common divisors $\gcd(a-c, n)$ and $\gcd(b-c, n)$.

Case 1. $\gcd(a-c, n) = d_1$ and $\gcd(b-c, n) = d_1$

It follows that $b-a$ is divisible by d_1 and from Theorem 3.1 we have that the number of solutions of the system

$$\gcd\left(\frac{a-c}{d_1}, \frac{n}{d_1}\right) = 1 \qquad \text{and} \qquad \gcd\left(\frac{b-c}{d_1}, \frac{n}{d_1}\right) = 1$$

is $F_{n/d_1}((b-a)/d_1)$.

Case 2. $\gcd(a-c, n) = d_2$ and $gcd(b-c, n) = d_2$

Analogously as in Case 1, we have that the number of common neighbors in this case is $F_{n/d_1}((b-a)/d_2)$ since $d_2 \mid b-a$.

Case 3. $\gcd(a-c, n) = d_1$ and $gcd(b-c, n) = d_2$

Let p be an arbitrary prime number that divides n. Since the divisors d_1 and d_2 are relatively prime, p can divide at most one of d_1 and d_2.

Assume first that p does not divide neither d_1 nor d_2. It follows that

$$c \not\equiv a \pmod p \qquad \text{and} \qquad c \not\equiv b \pmod p$$

If $a \equiv b \pmod p$, then c can take $p-1$ possible residues modulo p; otherwise, there are $p-2$ possibilities.

Assume that $p^\beta \| d_1$. It follows that $p \nmid d_2$, implying that $p \nmid b-c$ and $a \not\equiv b \pmod p$. In this case we have

$$c \equiv a \pmod{p^\beta}.$$

If $p^{\beta+1}$ does not divide n, this equation is sufficient for determine c modulo p^β. Otherwise, we have to take into account that $a-c$ is not divisible by $p^{\beta+1}$,

$$c \not\equiv a \pmod{p^{\beta+1}}.$$

In both cases, since $a \not\equiv b \pmod p$ and $c \equiv a \pmod p$ it follows that $c \not\equiv b \pmod p$. Therefore, we have $p-1$ possibilities for c modulo $p^{\beta+1}$ for $p^{\beta+1} \mid n$ and one possibility otherwise.

Assume now that $p^\gamma \| d_2$. Analogously, if $p^{\gamma+1}$ does not divide n, we have exactly one possibility for c modulo p^γ; otherwise if $p^{\gamma+1}$ divides n, we have $p-1$ possibilities for c modulo $p^{\gamma+1}$.

According to the Chinese remainder theorem, we are solving the system of congruences modulo M. For primes p_i with $\beta_i = \gamma_i = 0$ we have $p_i \| M$. Otherwise, either $\beta_i > 0$ or $\gamma_i > 0$, and we have $p_i^{\min(\beta_i+1,\alpha)} \| M$ or $p_i^{\min(\gamma_i+1,\alpha)} \| M$. If p_i does not divide d_1 and d_2, we have $p_i - 2$ possibilities for $p_i \nmid (b-a)$ and $p_i - 1$ possibilities for $p_i \mid (b-a)$. For $\alpha_i = \beta_i$, we have only one possibility modulo p^{β_i}, while for $\alpha_i \neq \beta_i$ there are $p-1$ possibilities modulo p^{β_i+1}. Analogously, we have symmetric expression for the divisor d_2.

This gives us

$$S = \prod_{p_i \nmid (b-a)d_1d_2} (p_i - 2) \cdot \prod_{p_i \mid (b-a),\ p_i \nmid d_1d_2} (p_i - 1) \cdot \prod_{p_i \mid d_1,\ \alpha_i \neq \beta_i} (p_i - 1) \cdot \prod_{p_i \mid d_2,\ \alpha_i \neq \gamma_i} (p_i - 1)$$

solutions for c modulo M, and it follows that there are $\frac{n}{M} \cdot S$ solutions with $0 \leq c < n$.

Case 4. $\gcd(a-c, n) = d_2$ and $\gcd(b-c, n) = d_1$

Analogously as in Case 3, we have

$$S = \prod_{p_i \nmid (b-a)d_1d_2} (p_i - 2) \cdot \prod_{p_i \mid (b-a),\ p_i \nmid d_1d_2} (p_i - 1) \cdot \prod_{p_i \mid d_1d_2,\ \alpha_i \neq \beta_i,\ \alpha_i \neq \gamma_i} (p_i - 1)$$

solutions for c.

Finally, after adding all contributions we get the formula for the number of common neighbors for a and b. □

These results can be further generalized for an arbitrary integral circulant graph $X_n(d_1, d_2, \ldots, d_k)$, by considering the pairs of divisors (d_i, d_j), $1 \leq i < j \leq k$.

5 The automorphism group of further integral circulant graphs

5.1 n being a prime power

Lemma 5.1 *Let $n = p^k$ and $d = p^l$, where p is odd prime such that $2 \le l < k$ and $D = \{1, d\}$. For an automorphism f of $X_n(1, d)$ it holds that*

$$p^s \mid a - b \qquad \text{if and only if} \qquad p^s \mid f(a) - f(b),$$

where $0 \le a, b \le n - 1$ and $l \le s \le l + 1$.

Proof: Let $0 \le a, b \le n - 1$ be two vertices of $X_n(1, d)$ such that $a = b + p^s$. Suppose that p^s does not divide $f(a) - f(b)$. Since the automorphism f preserves the number of common neighbors of pairs (a, b) and $(f(a), f(b))$, these numbers must be equal. According to Theorem 4.1 the number of common neighbors of a and b is given by:

$$N(a,b) = F_{p^k}(p^s) + F_{p^{k-l}}(p^{s-l}) = \begin{cases} p^{k-1}(p-1) + p^{k-l-1}(p-2), & s = l \\ p^{k-1}(p-1) + p^{k-l-1}(p-1), & s > l. \end{cases}$$

Case 1. $s = l$.

If $p \mid f(a) - f(b)$, it holds that

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) = p^{k-1}(p-1) < N(a, b).$$

If $p \nmid f(a) - f(b)$, we have

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) + 2 \cdot \frac{p^k}{p^{l+1}} \cdot (p-1) = p^{k-1}(p-2) + 2p^{k-l-1}(p-1),$$

and $N(a, b) - N(f(a), f(b)) = p^{k-1} - p^{k-l} \ge 0$. Since $l > 1$, in both cases we have $N(f(a), f(b)) \ne N(a, b)$, which is a contradiction and finally $p^l \mid f(a) - f(b)$.

Case 2. $s = l + 1$.

Suppose that $p^l \mid f(a) - f(b)$. Since $p^{l+1} \nmid f(a) - f(b)$, we have

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) + F_{p^{k-l}}\left(\frac{f(a) - f(b)}{p^l}\right) = p^{k-1}(p-1) + p^{k-l-1}(p-2),$$

and thus $N(f(a), f(b)) < N(a, b)$.

Suppose that $p^l \nmid f(a) - f(b)$.

If $p \mid f(a) - f(b)$ then $N(f(a), f(b)) = F_n(f(a) - f(b)) = p^{k-1}(p-1) < N(a, b)$. If $p \nmid f(a) - f(b)$ then

$$N(f(a), f(b)) = F_{p^k}(f(a) - f(b)) + 2\frac{p^k}{p^{l+1}} \cdot (p-1) = p^{k-1}(p-2) + 2p^{k-l-1}(p-1),$$

and $N(a, b) - N(f(a), f(b)) = p^{k-l-1}(p^l - p + 1) > 0$.

In both cases holds $N(f(a), f(b)) \ne N(a, b)$, which is a contradiction and finally $p^{l+1} \mid f(a) - f(b)$. $\square$

Theorem 5.2 *Let $n = p^k$ and $d = p^l$, where p is odd prime, $1 \leq l \leq k-1$ and $D = \{1, d\}$. Then*

$$|Aut(X_n(D))| = \begin{cases} (p^2)! \cdot \left(p^{k-2}!\right)^{p^2} & \text{if } l = 1; \\ (p^{l-1}!)^p \cdot (p!)^{p^l+1} \cdot (p^{k-l-1}!)^{p^{l+1}} & \text{if } l > 1. \end{cases}$$

Proof: Let f be an automorphism of $X_n(1, d)$. Two vertices a and b from $X_n(1, d)$ are adjacent iff $p \nmid (a - b)$ or $p^l \| a - b$. We will distinguish three cases depending on the relation of l and k.

Case 1. $l = 1$.

Let $C_0, C_1, \ldots, C_{p^2-1}$ be the partition of $\{0, 1, \ldots, p^k - 1\}$ modulo p^2. It is easy to verify that arbitrary two vertices a and b from different classes are adjacent, since p^2 does not divide $a - b$, and therefore $\gcd(a - b, p^k) \in \{1, p\}$. Every class C_i, $0 \leq i \leq p^2 - 1$ forms an independent set, and therefore the classes C_i permute under the automorphism f. By the product rule, it follows

$$|Aut(X_{p^k}(1, p))| = (p^2)! \cdot \left(p^{k-2}!\right)^{p^2}.$$

Case 2. $3 \leq l + 1 = k$.

Let $\{C_i\}$ be a partition of the set of vertices $X_n(D)$ given by

$$C_i = \{\ 0 \leq a < p^{l+1} \mid a \equiv i \pmod{p^l}\}, \qquad 0 \leq i \leq p^l - 1.$$

According to Lemma 5.1 these classes permute under the automorphism f. For arbitrary vertices a and b from the same class C_i it holds that $p^l \mid (a - b)$ where $0 \leq (a - b)/p^l \leq p - 1$, which means that $p^{l+1} \nmid a - b$ and thus C_i is a clique. If $a \in C_i$, $b \in C_j$ and $i \neq j$ then $p^l \nmid a - b$. We conclude that if $p \mid i - j$, then there are no edges connecting two vertices from the classes C_i and C_j; while for $p \nmid i - j$ the classes C_i and C_j form a clique.

According to Theorem 3.2, the number of permutations of classes C_i is equal to

$$|Aut(X_{p^l})| = p! \cdot (p^{l-1}!)^p,$$

and the number of permutations of vertices of a class C_i is equal to $|C_i|!$. Since the size of every class modulo p^l is equal to p and by the product rule, we finally obtain

$$|Aut(X_{p^{l+1}}(1, p^l))| = p!(p^{l-1}!)^p \cdot (p!)^{p^l} = (p^{l-1}!)^p \cdot (p!)^{p^l+1}.$$

Case 3. $3 \leq l + 1 < k$.

Let $\{D_i\}$ be a partition of the set of vertices $X_n(D)$ given by,

$$D_i = \{\ 0 \leq a < p^k \mid a \equiv i \pmod{p^{l+1}}\}, \qquad 0 \leq i \leq p^{l+1} - 1.$$

Since the difference of any two vertices from the same class is divisible by p^{l+1}, these vertices are not adjacent. So, the classes D_i form independent sets.

The vertices $a \in D_i$ and $b \in D_j$, $i \neq j$, are adjacent if and only if

$$gcd(i-j, p^k) \in \{1, p^l\} \qquad \Leftrightarrow \qquad gcd(i-j, p^{l+1}) \in \{1, p^l\}.$$

Using Lemma 5.1, the classes D_i permute under the automorphism f. That is, by Case 2 the number of permutations of classes D_i is equal to the size of the automorphism group $|Aut(X_{p^{l+1}}(1, p^l))|$. The number of permutations of vertices in each class is $|D_i|!$. Thus, by the product rule we obtain

$$|Aut(X_{p^k}(1, p^l))| = |Aut(X_{p^{l+1}}(1, p^l))| \cdot (p^{k-l-1}!)^{p^{l+1}} = (p^{l-1}!)^p \cdot (p!)^{p^l+1} \cdot (p^{k-l-1}!)^{p^{l+1}}.$$

$\square$

According to the construction of the automorphisms of $X_n(D)$ in Theorem 5.2, we conclude that for every permutation of classes D_i modulo p^{l+1}, there are p^{l+1} permutations of vertices in each of these classes (Case 3). This means that the automorphism group $Aut(X_{p^k}(1, p^l))$ is isomorphic to the wreath product of the automorphism group $Aut(X_{p^{l+1}}(1, p^l))$ of classes modulo p^{l+1} and the permutation groups of vertices in each of these classes

$$Aut(X_{p^k}(1, p^l)) = Aut(X_{p^{l+1}}(1, p^l)) \wr S_{p^{k-l-1}}.$$

Furthermore, according to Case 2, the automorphism group of classes modulo p^{l+1} is isomorphic to the wreath product of the automorphism group $Aut(X_{p^l})$ of classes C_i and the permutation groups of vertices in each of these classes

$$Aut(X_{p^{l+1}}(1, p^l)) = Aut(X_{p^l}) \wr S_p.$$

Using Theorem 3.4 we have

$$Aut(X_{p^l}) = S_p \wr S_{p^{l-1}},$$

and finally

$$Aut(X_{p^k}(1, p^l)) = ((S_p \wr S_{p^{l-1}}) \wr S_p) \wr S_{p^{k-l-1}}.$$

Therefore, we completely determine the size and the structure of the automorphism group of $X_n(D)$, with prime power order $n = p^k$ for $|D| \in \{1, 2\}$. Notice that in these cases the automorphism group is either the wreath product of two permutation groups or the wreath product of four permutation groups. This result improves Theorem 6.2 given in [27].

5.2 n being a square-free number

Lemma 5.3 *Let n be a square-free number, $p > 1$ an arbitrary prime divisor of n, and $2^m \| \frac{n}{p}$. For an automorphism f of $X_n(1, p)$ and prime number $p_i \neq 2$ dividing $\frac{n}{p}$ holds*

$$2^m p_i \mid a - b \qquad \text{if and only if} \qquad 2^m p_i \mid f(a) - f(b),$$

where $0 \leq a, b \leq n-1$ and $1 \leq i \leq k$.

Proof: Notice that since n is a square-free number, we have $m \in \{0, 1\}$.

Assume first that $\frac{n}{p}$ is odd.

We will prove that if $p_i \mid a-b$ then $p_i \mid f(a)-f(b)$. Let p_i be the maximal prime divisor of $\frac{n}{p}$ and set $a = b + p_i$. Suppose that p_i does not divide $f(a) - f(b)$. Since the automorphism f preserves the number of common neighbors of pairs (a, b) and $(f(a), f(b))$, these numbers must be equal. According to Theorem 4.1 the number of common neighbors of a and b is given by

$$N(a,b) = F_n(p_i) + 2(p_i - 1) \prod_{q|\frac{n}{p},\ q \neq p_i} (q-2) = (p_i - 1) \cdot p \cdot \prod_{q|\frac{n}{p},\ q \neq p_i} (q-2).$$

Now, we distinguish two different cases depending on the greatest common divisor of $f(a) - f(b)$ and p.

Case 1. $p \mid f(a) - f(b)$.

According to Theorem 4.1 the number of common neighbors of $f(a)$ and $f(b)$ is given by

$$N(f(a), f(b)) = F_n(f(a) - f(b)) + F_{\frac{n}{p}}\left(\frac{f(a) - f(b)}{p}\right) = (p_i - 2) \cdot p \cdot \prod_{q|\frac{n}{p},\ q \neq p_i} (q - \varepsilon(q)).$$

If $\gcd(f(a) - f(b), \frac{n}{p}) > 1$, there exists a prime number r dividing both $f(a) - f(b)$ and $\frac{n}{p}$. The ratio of $N(f(a), f(b))$ and $N(a, b)$ equals

$$\frac{N(f(a), f(b))}{N(a,b)} = \frac{(p_i - 2)(r-1)}{(p_i - 1)(r-2)} \cdot \frac{\prod_{q|\frac{n}{p},\ q \neq p_i, r} (q - \varepsilon(q))}{\prod_{q|\frac{n}{p},\ q \neq p_i, r} (q-2)} \cdot \frac{p}{p} > 1. \quad (2)$$

It is clear that the second factor is greater than or equal to 1. The first factor is greater than 1, since p_i is the maximal prime number dividing $\frac{n}{p}$ and $p_i > r$. This means that $N(f(a), f(b)) > N(a, b)$, which is a contradiction.

Assume now that $\gcd(f(a) - f(b), \frac{n}{p}) = 1$. The ratio of $N(f(a), f(b))$ and $N(a, b)$ is given by

$$\frac{N(f(a), f(b))}{N(a,b)} = \frac{(p_i - 2) \cdot p}{(p_i - 1) \cdot p} < 1. \quad (3)$$

Notice that the ratio of $N(f(a), f(b))$ and $N(a, b)$ is defined in both cases, since $\frac{n}{p}$ is odd and thus $\prod_{q|\frac{n}{p}} (q - 2) \neq 0$. Therefore, we obtain a contradiction and p_i divides $f(a) - f(b)$.

Case 2. $\gcd(f(a) - f(b), p) = 1$.

According to Theorem 4.1 the number of common neighbors of $f(a)$ and $f(b)$ is given by

$$N(f(a), f(b)) = F_n(f(b) - f(a)) + 2(p_i - 2) \prod_{q|\frac{n}{p},\ q \neq p_i} (q - \varepsilon(q)) = (p_i - 2) \cdot p \cdot \prod_{q|\frac{n}{p},\ q \neq p_i} (q - \varepsilon(q)).$$

Similarly as in the previous case, we conclude that $N(f(a), f(b)) \neq N(a, b)$, which is a contradiction and p_i divides $f(a) - f(b)$.

For an arbitrary $a, b \in X_n(1, p)$ such $p_i \mid a - b$ and $a < b$ we have

$$p_i \mid (f(a) - f(a + p_i)) + (f(a + p_i) - f(a + 2p_i)) + \ldots + (f(b - p_i) - f(b)) = f(a) - f(b).$$

Theretofore, the classes modulo p_i also permute under the automorphism f.

Assume now that $\frac{n}{p}$ is even.

Let p_i be the maximal prime divisor of $\frac{n}{p}$ and set $a = b + 2p_i$. Suppose that $2p_i$ does not divide $f(a) - f(b)$. Since $p \nmid 2p_i$, according to Theorem 4.1 the number of common neighbors of a and b is given by:

$$N(a, b) = F_n(2p_i) + 2(p_i - 1) \prod_{q \mid \frac{n}{p},\ q \neq 2, p_i} (q - 2) = (p_i - 1) \cdot p \cdot \prod_{q \mid \frac{n}{p},\ q \neq 2, p_i} (q - 2) > 0.$$

We distinguish similarly two different cases depending on the greatest common divisor of $f(a) - f(b)$ and p.

Case 1. $p \mid f(a) - f(b)$.

According to Theorem 4.1 the number of common neighbors of $f(a)$ and $f(b)$ is given by

$$N(f(a), f(b)) = F_n(f(a) - f(b)) + F_{\frac{n}{p}} \left(\frac{f(a) - f(b)}{p} \right) = (p_i - 2) \cdot p \cdot \prod_{q \mid \frac{n}{p},\ q \neq p_i} (q - \varepsilon(q))$$

If $f(a) - f(b)$ is odd, then for $q = 2$ we have $q - \varepsilon(q) = 0$ and $N(f(a), f(b)) = 0 < N(a, b)$, which is a contradiction. Otherwise, we again conclude that $N(f(a), f(b)) \neq N(a, b)$ since we have the same formulas as (2) and (3).

Case 2. $\gcd(f(a) - f(b), p) = 1$.

Similarly, according to Theorem 4.1 the number of common neighbors of $f(a)$ and $f(b)$ is given by

$$N(f(a), f(b)) = F_n(f(b) - f(a)) + 2(p_i - 2) \prod_{q \mid \frac{n}{p},\ q \neq p_i} (q - \varepsilon(q)) = (p_i - 2) \cdot p \cdot \prod_{q \mid \frac{n}{p},\ q \neq p_i} (q - \varepsilon(q)).$$

If $f(a) - f(b)$ is odd, then $N(f(a), f(b)) = 0$, and we have again a contradiction. Otherwise, we conclude that $N(f(a), f(b)) \neq N(a, b)$, which is contradiction in both cases and $2p_i$ divides $f(a) - f(b)$.

For an arbitrary $a, b \in X_n(1, p)$ such $2p_i \mid a - b$ and $a < b$ we have

$$p_i \mid (f(a) - f(a + 2p_i)) + (f(a + 2p_i) - f(a + 4p_i)) + \ldots + (f(b - 2p_i) - f(b)) = f(a) - f(b).$$

Therefore, the classes modulo $2p_i$ also permute under the automorphism f.

We can now apply mathematical induction on the number of prime divisors of $n = p_1 p_2 \cdot \ldots \cdot p_k$, by considering the prime divisors in decreasing order. Using the same arguments as above we can prove that for arbitrary p_i dividing n, if $2^m p_i \mid a-b$ then $2^m p_i \mid f(a)-f(b)$ (in all formulas for calculating the number of common neighbors of $f(a)$ and $f(b)$ we have $\varepsilon(q)=1$ for $q>p_i$).

Since f^{-1} is an automorphism as well, the opposite direction of the statement follows directly. This concludes the proof. □

Theorem 5.4 *Let n be a square free number and p an arbitrary prime divisor of n. The size of the automorphism group of $X_n(1,p)$ is equal to*

$$|Aut(X_n(1,p))| = \prod_{q \mid \frac{n}{p},\ q \ prime} q! \cdot (p!)^{\frac{n}{p}}.$$

Proof: Let $f \in Aut(X_n(1,p))$ be an automorphism of $X_n(1,p)$. Define the sets C_i as follows:

$$C_i = \{0 \le a \le n-1 \mid a \equiv i \pmod{\frac{n}{p}}\}$$

for $0 \le i \le \frac{n}{p}-1$. According to Lemma 5.3, the classes C_i permute under the automorphism f, since

$$\frac{n}{p} \mid a-b \quad \Leftrightarrow \quad \frac{n}{p} \mid f(a)-f(b)$$

holds for all pairs of vertices $0 \le a,b \le n-1$. For the special case $n=2p$, the graph is bipartite and the classes C_0 and C_1 permute under the automorphism f. Therefore, for any class C_i there exist a class $C_{h(i)}$ such that $f(C_i)=C_{h(i)}$, for some permutation h of indices $0,1,\ldots,\frac{n}{p}-1$. The vertices $a \in C_i$ and $b \in C_j$ are adjacent if and only if

$$\gcd\left(\frac{n}{p}(k-l)+(i-j), n\right) \in \{1,p\}$$

for some $0 \le k,l \le p-1$. It follows that the edge $\{a,b\}$ exists only if $i-j$ and $\frac{n}{p}$ are relatively prime. In the same way, notice that the vertices from the same modulo class form an independent set, since for the vertices $a,b \in C_i$ holds $\frac{n}{p} \mid \gcd(a-b,n)$ and thus $\gcd(a-b,n) \notin \{1,p\}$. For $\gcd(i-j,\frac{n}{p})=1$, the vertices from the classes C_i and C_j form a complete bipartite subgraph.

As the structure of the subgraph induced by the vertices from C_i and C_j depends only on the difference $i-j$, we obtain that the induced subgraphs consisting of the vertices from C_i and C_j are isomorphic to each other for all pairs (i,j) with $\gcd(i-j,\frac{n}{p})=1$. The same conclusion holds for the pairs (i,j) such that $\gcd(i-j,\frac{n}{p}) \ne 1$, since in this case there are no edges between C_i and C_j. We can construct a new graph G' with the vertex set $Z_{n/p}$ and two vertices i and j are adjacent if and only if the classes C_i and C_j form a complete bipartite graph, i. e. $\gcd(i-j,\frac{n}{p})=1$. It easily follows that this graph G' is isomorphic to $X_{n/p}$ and that each vertex i corresponds to the class C_i. Finally, according to Theorem 3.4 the number of permutations of these classes equals $\prod_{q\mid n,\ q \ne p} q!$, which is exactly the size of the automorphism group of the unitary Cayley graph $Aut(X_{n/p})$.

Assume that the class C_i is mapped to the class C_j. Since the vertices from the class C_i form an independent set and the restriction of the automorphism f on the vertices of C_i is a bijection from C_i to C_j, we have all $|C_i|! = p!$ permutations of the vertices of the class C_i. Finally, taking into account that classes and vertices permute independently, by the product rule the size of the automorphism group is

$$\prod_{q | \frac{n}{p}} q! \cdot (p!)^{\frac{n}{p}}.$$

□

Similarly, the automorphism group of a graph with square-free order and $D = \{1, p\}$ is the wreath product of the group of class permutations C_i and the groups of permutations of vertices in each of these classes

$$Aut(X_n(1,p)) = \Big(\prod_{q | \frac{n}{p}} S_q\Big) \wr S_p.$$

6 Concluding remarks

In this paper, we determine the automorphism group of unitary Cayley graphs X_n, and make a step in describing the automorphism group of integral circulant graphs by examining two special cases – n being a prime power or a square-free number [22, 27]. Our proofs are based on the fact that for some primes p dividing n, the classes modulo p permute under the automorphism f. Furthermore, we determine the number of common neighbors of two arbitrary vertices in $X_n(d_1, d_2)$. This is a main tool for the proof that classes permute by some prime modulo and therefore for the characterization of the automorphism group of $X_n(d_1, d_2)$. The idea of considering the number of common neighbors turns out to be essential for the general case $X_n(D)$, but it requires many cases.

Examples suggest that for an arbitrary integral circulant graph $X_n(D)$ and some primes p dividing n, the classes modulo p permute under the automorphism f. For the future research we propose the full characterization of the automorphism groups of integral circulant graphs using this approach. We believe that the automorphism groups are the product or/and wreath product of permutation groups of prime power degree.

Remark

One of the referees points out that at about the same time Akhtar et al. in [1] independently obtained similar result concerning the automorphism of unitary Cayley graph G_R of a finite ring R. We have read paper [1], and found that the main idea of their algebraic proof is different than our number-theoretical approach. Akhtar et al. considered another generalization of unitary Cayley graphs and emphasized the dependence of automorphisms on the underlying algebraic structure of the rings concerned. In our paper we tried to characterize the automorphism group of all integral circulant graphs based on the idea that for some divisors $d \mid n$ the classes modulo d permute under arbitrary automorphism. We illustrate these permutations of classes on some special cases of n, using the generalized formula for the number of common neighbors. Moreover, our approach can be used for establishing some upper bounds on the size of the automorphism group of integral circulant graphs. The idea of partitioning vertices into classes modulo d was used in earlier papers [4, 18] for characterizing the clique and chromatic number of integral circulant graphs, and we believe that it can be extended for the full characterization of integral circulant graphs.

Acknowledgement. This work was supported by Research Grants 174010, 174013 and 174033 of Serbian Ministry of Science and Technological Development. The authors are grateful to the anonymous referees whose valuable comments resulted in improvements to this article.

References

[1] R. Akhtar, M. Bogess, T. Jackson-Henderson, I. Jiménez, R. Karpman, A. Kinzel, D. Pritikin, *On the unitary Cayley graph of a finite ring*, Electron. J. Combin. 16 (2009) #R117.

[2] S. Akbari, F. Moazami, S. Zare, *Kneser Graphs and their Complements are Hyperenergetic*, MATCH Commun. Math. Comput. Chem. 61 (2009) 361–368.

[3] M. Bašić, M. Petković, D. Stevanović, *Perfect state transfer in integral circulant graphs*, Appl. Math. Letters 22 (2009) 1117–1121.

[4] M. Bašić, A. Ilić, *On the clique number of integral circulant graphs*, Appl. Math. Letters 22 (2009) 1406–1411.

[5] M. Bašić, M. Petković, *Some classes of integral circulant graphs either allowing or not allowing perfect state transfer*, Appl. Math. Letters 22 (2009) 1609–1615.

[6] P. Berrizbeitia, R. E. Giudici, *On cycles in the sequence of unitary Cayley graphs*, Discrete Math. 282 (2004) 239–243.

[7] S. Blackburn, I. Shparlinski, *On the average energy of circulant graphs*, Linear Algebra Appl. 428 (2008) 1956–1963.

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

[9] E. Dobson, *Automorphism groups of metacirculant graphs of order a product of two distinct primes*, Combin. Prob. Comput. 15 (2006) 105–130.

[10] E. Dobson, I. Kovács, *Automorphism groups of Cayley digraphs of Z_p^3*, Electron. J. Combin. 16 (2009) #R149.

[11] E. Fuchs, *Longest induced cycles in circulant graphs*, Electr. J. Comb. 12 (2005) 1–12.

[12] C. Godsil, *Periodic Graphs*, Electr. J. Comb. 18 (2011) #P23.

[13] I. Gutman, *The energy of a graph*, Ber. Math. Stat. Sekt. Forschungszent. Graz 103 (1978) 1–22.

[14] I. Gutman, *The energy of a graph: old and new results*, Algebraic Combinatorics and Applications, Springer, Berlin, 2001, 196–211.

[15] I. Gutman, *Hyperenergetic molecular graphs*, J. Serb. Chem. Soc. 64 (1999) 199–205.

[16] W. H. Haemers, *Strongly regular graphs with maximal energy*, Linear Algebra Appl. 429 (2008) 2719–2723.

[17] F. K. Hwang, *A survey on multi-loop networks*, Theor. Comput. Sci. 299 (2003) 107–121.

[18] A. Ilić, M. Bašić, *On the chromatic number of integral circulant graphs*, Comput. Math. Appl. 60 (2009) 144–150.

[19] A. Ilić, *The energy of unitary Cayley graphs*, Linear Algebra Appl. 431 (2009) 1881–1889.

[20] A. Ilić, *Distance spectra and distance energy of integral circulant graphs*, Linear Algebra Appl. 433 (2010) 1005–1014.

[21] A. Ilić, M. Bašić, I Gutman, *Triply Equienergetic Graphs*, MATCH Commun. Math. Comput. Chem. 64 (2010) 189–200.

[22] M. Klin, I. Kovács, *Automorphism groups of rational circulant graphs through the use of Schur rings*, arXiv:1008.0751 [math.CO], 2010.

[23] W. Klotz, T. Sander, *Some properties of unitary Cayley graphs*, Electr. J. Comb. 14 (2007) #R45.

[24] W. Klotz, T. Sander, *Integral Cayley graphs over abelian groups*, Electron. J. Combin. 17 (2010) #R81.

[25] I. Kovács, *On automorphisms of circulant digraphs on p^m vertices, p an odd prime*, Linear Algebra Appl. 356 (2002) 231–252.

[26] C. H. Li, *On isomorphisms of connected Cayley graphs*, Discrete Math. 178 (1998) 109–122.

[27] J. Morris, *Automorphism groups of circulant graphs – a survey*, in A. Bondy, J. Fonlupt, J. L. Fouquet, J. C. Fournier, and J. L. Ramirez Alfonsin (Eds.), Graph Theory in Paris (Trends in Mathematics), Birkhäuser, 2007.

[28] M. E. Muzychuk, *A solution of the isomorphism problem for circulant graphs*, Proc. London Math. Soc. (3) 88 (2004) 1–41.

[29] H. N. Ramaswamy, C. R. Veena, *On the Energy of Unitary Cayley Graphs*, Electron. J. Combin. 16 (2009) #N24.

[30] N. Saxena, S. Severini, I. Shparlinski, *Parameters of integral circulant graphs and periodic quantum dynamics*, Int. J. Quant. Inf. 5 (2007) 417–430.

[31] I. Shparlinski, *On the energy of some circulant graphs*, Linear Algebra Appl. 414 (2006) 378–382.

[32] W. So, *Integral circulant graphs*, Discrete Math. 306 (2006) 153–158.

[33] W. So, *Remarks on some graphs with large number of edges*, MATCH Commun. Math. Comput. Chem. 61 (2009) 351–359.