NORMAL EDGE-TRANSITIVE CIRCULANT GRAPHS

HYO-SEOB SIM* AND YOUNG-WON KIM

ABSTRACT. A Cayley graph of a finite group $G$ is called normal edge-transitive if its automorphism group has a subgroup which both normalizes $G$ and acts transitively on edges. In this paper, we consider Cayley graphs of finite cyclic groups, namely, finite circulant graphs. We characterize the normal edge-transitive circulant graphs and determine the normal edge-transitive circulant graphs of prime power order in terms of lexicographic products.

1. Introduction

Let $G$ be a finite group and $S$ a subset of $G$ not containing the identity $1_G$. The Cayley graph $X = \text{Cay}(G, S)$ of $G$ on $S$ is a graph defined by

$$V(X) = G, \quad E(X) = \{(g, sg) \mid g \in G, s \in S\}.$$

In particular, if $S^{-1} := \{s^{-1} \mid s \in S\}$ is equal to $S$, then the Cayley graph is said to be undirected. In this case, $(x, y)$ is an edge if and only if $(y, x)$ is an edge, and such a graph can be viewed as a usual undirected graph by coalescing the two edges $(x, y)$ and $(y, x)$ into a single undirected edge.

It is easy to see that the group $G$ acts regularly on the vertex set $G$ by right multiplication, and so $G$ may be viewed as a regular subgroup of the automorphism group of the Cayley graph. In particular, the automorphism group $\text{Aut}X$ of the Cayley graph $X$ acts transitively on the vertex set $G$. The normalizer $N_{\text{Aut}X}(G)$ of the regular subgroup $G$ is the semidirect product

$$N_{\text{Aut}X}(G) = G \cdot \text{Aut}(G, S), \text{ where } \text{Aut}(G, S) := \{\sigma \in \text{Aut}(G) \mid S^\sigma = S\}.$$
A Cayley graph $X = \text{Cay}(G, S)$ is said to be edge-transitive if its automorphism group $\text{Aut}X$ is transitive on the edges. Also, if $X$ is undirected and $\text{Aut}X$ is transitive on the undirected edges, then $X$ is said to be edge-transitive as an undirected graph. It is difficult to find the full automorphism group of a graph in general, and so this makes it difficult to decide whether it is edge-transitive, even for a Cayley graph. As an accessible kind of edge-transitive graphs, Praeger [8] focuses attention on those graphs for which $\mathbf{N}_{\text{Aut}X}(G)$ is transitive on edges, and those undirected graphs $X$ for which $\mathbf{N}_{\text{Aut}X}(G)$ is transitive on the undirected edges. Such a graph is said to be normal edge-transitive, or normal edge-transitive as an undirected graph, respectively. In [8], Praeger gave an approach to analyzing normal edge-transitive Cayley graphs as a subfamily of central importance. Using the strategy suggested in [8] to construct normal edge-transitive Cayley graphs from quotients, Houlis [3] was able to determine the isomorphism types of all connected normal edge-transitive undirected Cayley graphs for $\mathbb{Z}_{pq}$, where $p, q$ are primes; for $G = \mathbb{Z}_p \times \mathbb{Z}_p$, $p$ a prime, Houlis also made a classification which gives all normal edge-transitive undirected Cayley graphs $\text{Cay}(G, S)$ such that $\text{Aut}(G, S)$ acts reducibly on $G$. In this paper, we consider finite circulant graphs, namely Cayley graphs of finite cyclic groups.

Two Cayley graphs $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$ are said to be equivalent if there exists $\alpha \in \text{Aut}(G)$ such that $T = S^\alpha$. Equivalent Cayley graphs are of course isomorphic.

Let $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ denote the additive group of integers modulo $n$, and let $U_n$ denote the multiplicative group of units integers modulo $n$. We may identify $U_n$ with $\text{Aut}(\mathbb{Z}_n)$. The following theorem characterizes all connected normal edge-transitive circulant graphs of order $n$.

**Theorem 1.1.** Every connected normal edge-transitive circulant graph $\text{Cay}(\mathbb{Z}_n, T)$ is equivalent to $\text{Cay}(\mathbb{Z}_n, S)$ for some subgroup $S$ of $U_n$. Conversely, each subgroup $S$ of $U_n$ defines a connected normal edge-transitive circulant graph of order $n$, different choices of subgroups $S$ giving nonisomorphic graphs.

An abelian group $G$ has an automorphism which maps each element to its inverse, and so if an undirected Cayley graph of $G$ is normal edge-transitive as an undirected graph then it is also normal edge-transitive. Therefore, a connected circulant undirected graph of order $n$ is normal
Normal edge-transitive circulant graphs

edge-transitive as an undirected graph if and only if it is isomorphic to 
\( \text{Cay}(\mathbb{Z}_n, S) \) for some subgroup \( S \) of \( U_n \) containing \(-1\).

We focus our attention on the special case when \( n \) is a prime power. 
Let \( p \) be an odd prime. For each positive divisor \( r \) of \( p - 1 \), there is a 
unique subgroup of order \( r \) in the cyclic group \( U_p \). The Cayley graph 
of \( \mathbb{Z}_p^r \) on the subgroup of order \( r \) in \( U_p \) is denoted by \( X(p^i, r) \).

For \( p = 2 \), let \( X(2^i, 1) = \text{Cay}(\mathbb{Z}_{2^i}, \{1\}) \), \( X(2^i, 2) = \text{Cay}(\mathbb{Z}_{2^i}, \{1, -1\}) \), and 
\( X(2^i, 3) = \text{Cay}(\mathbb{Z}_{2^i}, \{1, -1+2^{i-1}\}) \). Denote the Cayley graph of \( \mathbb{Z}_n \) 
on the empty set by \( nK_1 \). Then we have:

**Theorem 1.2.** (i) For an odd prime \( p \) and a positive integer \( m \), 
every connected normal edge transitive circulant graph of order \( p^m \) is 
isomorphic to the lexicographic product \( X(p^i, r)[p^{m-i}K_1] \) for some 
positive divisor \( r \) of \( p - 1 \) and an integer \( i \) with \( 1 \leq i \leq m \), different 
choices of \( i \) or \( r \) giving nonisomorphic graphs. (ii) Every connected normal 
edge transitive circulant graph of order \( 2^m \) is isomorphic to one of 
the lexicographic products \( X(2^i, j)[2^{m-i}K_1] \) for some integers \( i, j \) with 
\( 1 \leq j \leq 3 \leq i \leq m \) or \( 1 \leq j \leq i = 2 \) for \( 3 \leq m \), and \( 1 \leq j \leq i = m \) for 
\( m = 1, 2 \), different choices of \( i \) or \( j \) giving nonisomorphic graphs.

We note that the analogous result can be given for \( n = 2p^m \) for 
an odd prime \( p \) since the automorphism groups of \( \mathbb{Z}_{p^m} \) and \( \mathbb{Z}_{2p^m} \) are 
isomorphic.

2. Basic facts

In this section we give some facts on Cayley graphs, which will be 
useful for our purpose.

First we make some comments about the normalizer \( N_{\text{Aut}X}(G) \) of the 
regular subgroup \( G \). The normalizer of the regular subgroup \( G \) in the 
symmetric group \( \text{Sym}(G) \) is the holomorph of \( G \), that is the semidirect 
product \( G \cdot \text{Aut}(G) \). Thus,

\[
N_{\text{Aut}X}(G) = (G \cdot \text{Aut}(G)) \cap \text{Aut}X = G \cdot (\text{Aut}(G) \cap \text{Aut}X) = G \cdot \text{Aut}(G, S).
\]

The following lemma to characterize normal edge-transitivity is fund-
damental, and a more general description can be also found in [8].
Lemma 2.1. Let \( X = \text{Cay}(G,S) \) be a Cayley graph for a finite group \( G \) with \( S \neq \emptyset \). Then \( X \) is normal edge-transitive if and only if \( \text{Aut}(G,S) \) is transitive on \( S \).

We close this section with some observations about lexicographic products of graphs.

Given two graphs \( X \) and \( Y \) the lexicographic product, \( X[Y] \) is defined as the graph with vertex set \( V(X) \times V(Y) \) and the following adjacency relation:

\[
(x, y) \text{ is adjacent to } (x', y') \text{ in } X[Y] \iff \text{ either } x \text{ is adjacent to } x' \text{ in } X, \\
\text{ or } x = x', y \text{ is adjacent to } y' \text{ in } Y.
\]

We then have the following basic result.

Lemma 2.2. Let \( X = \text{Cay}(G,S) \) be a Cayley graph for a finite group \( G \) with \( S \neq \emptyset \). If \( S \) is a union of cosets of a normal subgroup \( M \) of \( G \) of order \( m \), then \( X \cong \text{Cay}(G/M,S/M)[mK_1] \), where \( S/M \) denotes the set of cosets \( Ms, s \in S \).

Proof. Write \( Y \) for \( \text{Cay}(G/M,S/M) \) and \( Z \) for \( \text{Cay}(M,\emptyset) \). Then \( Z \cong mK_1 \). Let \( T \) be a set of coset representatives for \( M \) in \( G \), so that for every \( g \in G \) there exists a unique \( t \in T \) such that \( Mg = Mt \). Define a map \( \gamma : G \rightarrow G/M \times M \) by \( \gamma(g) = (Mg, gt^{-1}) \). It is routine to show that this map is an isomorphism from \( X \) onto \( Y[Z] \).

3. Proof of Theorem 1.1

For the first part of the theorem, let \( X = \text{Cay}(\mathbb{Z}_n,T) \) be a connected normal edge-transitive circulant graph of order \( n \). Then by Lemma 2.1, \( \text{Aut}(\mathbb{Z}_n,T) \) is transitive on \( T \). Write \( S \) for the subgroup of \( U_n \) corresponding to \( \text{Aut}(\mathbb{Z}_n,T) \) under the identification of \( U_n \) and \( \text{Aut}(\mathbb{Z}_n) \). Since \( \langle T \rangle = \mathbb{Z}_n \), there exists \( t \) in \( T \cap U_n \). Since the action of \( U_n \) on \( \mathbb{Z}_n \) is by multiplication modulo \( n \), it follows that \( T = St \). Therefore the map \( i \mapsto it, i \in \mathbb{Z}_n \) yields an automorphism of \( \mathbb{Z}_n \) that maps \( S \) onto \( T \), and so \( \text{Cay}(\mathbb{Z}_n,S) \) is equivalent to \( \text{Cay}(\mathbb{Z}_n,T) \).

Let \( S \) be a subgroup of \( U_n \). Since \( 1 \in S \), we have \( \mathbb{Z}_n = \langle S \rangle \) and so \( \text{Cay}(\mathbb{Z}_n,S) \) is connected. The subgroup \( \{ a \in U_n \mid Sa = S \} \) acts on \( S \) by
multiplication as $\text{Aut}(\mathbb{Z}_n, S)$ does on $S$. Since $\{a \in U_n \mid Sa = S\} = S$, we see that $\text{Aut}(\mathbb{Z}_n, S)$ is transitive on $S$. It follows from Lemma 2.1 that $\text{Cay}(\mathbb{Z}_n, S)$ is normal edge-transitive.

We now consider the isomorphism problem of connected normal edge-transitive circulant graphs. Ádám [1] conjectured that if two circulant graphs $\text{Cay}(G, S)$ and $\text{Cay}(G, T)$ are isomorphic then they are equivalent; the conjecture was shown to be false in general (see for example, [2]). While the conjecture is true if the number of vertices is either square-free or twice square-free (see [6, 7]). We will show that the conjecture for our case is true, namely:

**Lemma 3.1.** If two connected normal edge-transitive circulant graphs $\text{Cay}(\mathbb{Z}_n, S)$ and $\text{Cay}(\mathbb{Z}_n, T)$ are isomorphic, then they are equivalent.

We note that Klin and Pöschel in [4] first applied the method of Schur rings to solve isomorphism problems of circulant graphs and they succeeded in solving the isomorphism problem for circulant graphs of odd prime-power order in [5]. Our isomorphism problem can be solved by using some basic properties of Schur ring theory.

Let $X = \text{Cay}(\mathbb{Z}_n, S)$ be a Cayley graph of $\mathbb{Z}_n$ on a subset $S$. Let $A$ be the automorphism group of the graph $X$ and let $A_0$ be the subgroup of all automorphisms of $X$ that fix 0. Let $S_1, S_2, \ldots, S_k$ be all orbits of the natural action of $A_0$ on $\mathbb{Z}_n$. Let $\mathbb{Z}[\mathbb{Z}_n]$ be the group ring of $\mathbb{Z}_n$ over the integer ring $\mathbb{Z}$, which consists of the formal sums $c_0\mathbb{Z} + c_1\mathbb{Z} + \ldots + c_{n-1}\mathbb{Z}$, where $c_i$ are integers. For each subset $T = \{t_1, t_2, \ldots, t_s\}$ of $\mathbb{Z}_n$, we denote $t_1 + t_2 + \ldots + t_s$ by $T$ and call it a simple quantity. Then the transitivity module $\mathbb{Z}(\mathbb{Z}_n, A_0)$ belonging to $A_0$ is the module generated by $S_1, S_2, \ldots, S_k$, which are called the basic quantities. It is known as Schur's fundamental theorem (see [9]) that the transitivity module is a subring of the group ring.

Let $X = \text{Cay}(\mathbb{Z}_n, S)$ and $Y = \text{Cay}(\mathbb{Z}_n, T)$ be isomorphic circulants with automorphism groups $A$ and $B$, respectively. Let $\lambda : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ be an isomorphism of $X$ onto $Y$ such that $\lambda(0) = 0$. Since $A$ is vertex-transitive we can choose such $\lambda$. Obviously, we have $B = \lambda A \lambda^{-1}$ and $B_0 = \lambda A_0 \lambda^{-1}$ is the group of all automorphisms of $Y$ that fix 0. The isomorphism $\lambda$ extends to a linear operator of $\mathbb{Z}(\mathbb{Z}_n, A_0)$ onto $\mathbb{Z}(\mathbb{Z}_n, B_0)$. Of course $\lambda$ sends each basic quantity of $\mathbb{Z}(\mathbb{Z}_n, A_0)$ to a basic quantity of $\mathbb{Z}(\mathbb{Z}_n, B_0)$. Let $x$ be an element of $\mathbb{Z}_n$ and let $R(x)$ be the regular representation of $\lambda$ defined by $R(x)(i) = i + x$ for all $i$ in $\mathbb{Z}_n$. Then $\lambda(S_i + x) = R(\lambda(x))\lambda^{-1}R(-\lambda(x))\lambda R(x)(S_i) = R(\lambda(x))\lambda \alpha_0(S_i) = \lambda(S_i) + \ldots$
\( \lambda(x) \) where \( \alpha_0 = \lambda^{-1}R(-\lambda(x))\lambda R(x) \) is an automorphism of \( X \) such that \( \alpha_0(0) = 0. \) Since \( \lambda(S_i \cdot x) = \lambda(S_i + x) \), we have \( \lambda(S_i \cdot x) = \lambda(S_i) \cdot \lambda(x) \). This implies that the linear operator \( \lambda \) preserves multiplication of the subring, and so \( \lambda \) is a ring-isomorphism between \( Z(Z_n, A_0) \) and \( Z(Z_n, B_0) \).

Let \( \alpha \) be an automorphism of \( Z_n \). By Theorem 23.9(a) in [9], \( S_i^\alpha \) is a basic quantity of \( Z(Z_n, A_0) \). By the same idea of the proof of Theorem 23.9(a) in [9], we also have \( \lambda(S_i^\alpha) = \lambda(S_i)^\alpha \). Since \( S \) is again a union of some basic quantities \( S_i \), we have \( \lambda(S^\alpha) = \lambda(S)^\alpha \). Since \( \lambda(S) = T \), we have the following immediate consequence of this observation.

**Lemma 3.2.** If \( \text{Cay}(Z_n, S) \) and \( \text{Cay}(Z_n, T) \) are isomorphic, then \( \text{Aut}(G, S) = \text{Aut}(G, T) \).

Now let \( X = \text{Cay}(Z_n, S) \) and \( Y = \text{Cay}(Z_n, T) \) be isomorphic connected normal edge-transitive circulant graphs. As we have shown in the first part of this section, \( X \) and \( Y \) are equivalent to \( \text{Cay}(Z_n, S') \) and \( \text{Cay}(Z_n, T') \) respectively for some subgroups \( S' \) and \( T' \) of \( U_n \). Then by Lemma 3.2, \( \text{Aut}(G, S') = \text{Aut}(G, T') \), that is \( S' = T' \). This completes the proof of Lemma 3.1, and so Theorem 1.1 is now proved.

4. Proof of Theorem 1.2

Let \( p \) be an odd prime. Then \( U_{p^m} \) is a cyclic group of order \( (p-1)p^{m-1} \). Let \( S \) be a subgroup of \( U_{p^m} \) and let \( B \) be the Sylow \( p \)-subgroup of \( S \). Then \( B = \{ 1 + kp^i \mid k = 0, 1, 2, \ldots, p^{m-i} - 1 \} \) for some integer \( i = 1, 2, \ldots, m \) and \( |B| = p^{m-i} \). Let \( M := \{ kp^i \mid k = 0, 1, 2, \ldots, p^{m-i} - 1 \} \). Then \( M \) is the subgroup of \( Z_{p^m} \) of order \( p^{m-i} \), and \( B = 1 + M \). We see that

\[
S = \bigcup_{a \in S} aB = \bigcup_{a \in S} a(1 + M) = \bigcup_{a \in S} a + M.
\]

So \( S \) is a union of cosets of \( M \) in \( Z_{p^m} \). Let \( r \) denote \( |S/B| \), which is a divisor of \( p-1 \). If \( a + M = a' + M \) for some \( a, a' \) in \( S \), then \( a^{-1}a' \in 1 + M = B \), and so \( aB = a'B \). Therefore \( |S/M| = r \). By Lemma 2.2, we have

\[
\text{Cay}(Z_{p^m}, S) = \text{Cay}(Z_{p^m}/M, S/M)[p^{m-i}K_1].
\]

We want to show that

\[
\text{Cay}(Z_{p^m}/M, S/M)[p^{m-i}K_1] \cong X(p^i, r).
\]
Let $\theta : \mathbb{Z}_{p^m} \rightarrow \mathbb{Z}_{p^i}$ be the natural homomorphism, namely $\theta(x) \equiv x \mod p^i$. Then $\text{Ker}\theta = M$ and $\theta(S)$ is a subgroup of $U_{p^i}$ since $\theta$ preserves the multiplication as well. The homomorphism $\theta$ induces the isomorphism $\bar{\theta}$ from $\mathbb{Z}_{p^m}/M$ onto $\mathbb{Z}_{p^i}$. Note that $\bar{\theta}(S/M) = \theta(S)$. Therefore $\bar{\theta}$ is also an isomorphism between $\text{Cay}(\mathbb{Z}_{p^m}/M, S/M)$ and $\text{Cay}(\mathbb{Z}_{p^i}, \theta(S))$. Since $\theta(S)$ is the unique subgroup of order $r$ in $U_{p^i}$, it follows that $\text{Cay}(\mathbb{Z}_{p^i}, \theta(S)) = X(p^i, r)$. The proof of (i) of the theorem is now complete.

First consider the case when $n = 2^m$. We assume that $m \geq 3$. It is well known that $U_{2^m} = (-1) \cdot (5) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{m-2}}$. For each $i = 2, 3, \ldots, m$, let

$$S_i = \{ 1 + k2^i \mid k = 0, 1, \ldots, 2^{m-i}-1 \}.$$  

Then $S_2, S_3, \ldots, S_m$ consist of all subgroups of $\langle 5 \rangle$. For each $i = 2, \ldots, m-1$, let

$$T_i = S_{i+1} \cup \{ -1 + k2^i \mid 1 \leq k \leq 2^{m-i}-1, k : \text{odd} \}.$$  

Then $T_i$ is a subgroup of $U_{2^m}$ such that $|T_i| = |S_i| = 2^{m-i}$. Let $T$ be a subgroup of $U_n$, and let $\pi$ be the natural projection from $U_n$ onto $\langle 5 \rangle$. Then $\pi(T) = S_i$ for some $i = 2, 3, \ldots, m$. Then there exists a homomorphism $\theta$ from $S_i$ to $(-1)/(\langle -1 \rangle \cap T)$ such that $T = \{ st \mid \theta(s) = t \cdot (-1) \cap T, s \in S_i \}$. If $T$ contains $-1$, then the only such homomorphism is trivial; therefore $T$ is the direct product of $S_i$ and $\langle -1 \rangle$. Suppose that $T$ does not contain $-1$. If $\theta(S_i) = \langle 1 \rangle$, then $\theta$ is the trivial homomorphism, and hence $T = S_i$. If $\theta(S_i) = \langle -1 \rangle$, it follows from $\text{Ker}\theta = S_{i+1}$ and $\theta(S_i) = \langle -1 \rangle \cong \mathbb{Z}_2$ that $T = T_i$ for some $i = 2, \ldots, m-1$. Consequently, we have the following lemma.

**Lemma 4.1.** \{ $S_i, T_j, \langle -1 \rangle \cdot S_i \mid i = 2, 3, \ldots, m, j = 2, 3, \ldots, m-1$ \} is the set of all subgroups of $U_{2^m}$.

We then consider (ii) of the theorem. We first assume that $m \geq 3$. Let $S$ be a subgroup of $U_{2^m}$. Then $S$ is one of those listed in Lemma 4.1. Write $B$ for $S \cap \langle 5 \rangle$. Then $B = \{ 1 + k2^i \mid k = 0, 1, \ldots, 2^{m-i}-1 \}$ for some $i = 2, 3, \ldots, m$. Let $M := \{ k2^i \mid k = 0, 1, 2, \ldots, 2^{m-i}-1 \}$. Then $M$ is a subgroup of order $2^{m-i}$ of $\mathbb{Z}_{2^m}$. Since $B = 1 + M$, $S$ is a union of some cosets of $M$ in $\mathbb{Z}_{2^m}$. In fact either i) $S = 1 + M$, or ii) $S = (1+M) \cup (-1+M)$, or iii) $S = (1+M) \cup (-1+2^{i-1}+M)$, $3 \leq i \leq m$ from Lemma 4.1. Let $\theta : \mathbb{Z}_{2^m} \rightarrow \mathbb{Z}_{2^i}$ be the natural homomorphism
such that \( \theta(x) \equiv x \mod 2^i \). Then \( \text{Ker}\theta = M \), and \( \theta(S) = \{1\} \) for i), \( \theta(S) = \{1, -1\} \) for ii) and \( \theta(S) = \{1, -1 + 2^{i-1}\}, \) \( 3 \leq i \leq m \) for iii). Since \( \text{Cay}(\mathbb{Z}_2^m/M, S/M) \cong \text{Cay}(\mathbb{Z}_2^i, \theta(S)) \), it follows from Lemma 2.2 that \( \text{Cay}(\mathbb{Z}_2^m, S) \cong \text{Cay}(\mathbb{Z}_2^i, \theta(S))[2^{m-i}K_1] \), where \( i \) varies from 2 to \( m \) for i) and ii), while \( i \) varies from 3 to \( m \) for iii). We observe that \( \text{Cay}(\mathbb{Z}_2^i, \theta(S)) = X(2^i, 1), \) \( 2 \leq i \leq m \) for i), \( \text{Cay}(\mathbb{Z}_2^i, \theta(S)) = X(2^i, 2), \) \( 2 \leq i \leq m \) for ii), and \( \text{Cay}(\mathbb{Z}_2^i, \theta(S)) = X(2^i, 3), \) \( 3 \leq i \leq m \) for iii). Consequently \( \text{Cay}(\mathbb{Z}_2^m, S) \cong X(2^i, j)[2^{m-i}K_1] \) where \( 3 \leq i \leq m, \) \( 1 \leq j \leq 3, \) or \( i = 2, \) \( j = 1, 2. \) For \( m = 2 \) or \( 1, \) \( S = \{1\}, \) or \( S = \{1, -1\}, \) and so \( \text{Cay}(\mathbb{Z}_2^m, S) = X(2^m, j) \) where \( 1 \leq j \leq m \). This proves (ii) of the theorem.

ACKNOWLEDGEMENT. The authors thank the referee for several improvements of the exposition.

References


Division of Mathematical Sciences, Pukyong National University, Pusan 608-737, Korea
E-mail: hsim@pknu.ac.kr