

AUTOMORPHISM GROUPS AND STRUCTURE OF 4-VALENT CAYLEY GRAPHS ON DIHEDRAL GROUPS

AMITAYU BANERJEE

ABSTRACT. Let G be a finite group and $S \subseteq G \setminus \{e\}$ be an inverse-closed subset of G . The undirected Cayley graph $\text{Cay}(G, S)$ has vertex set G , where two vertices x and y are adjacent if and only if $xy^{-1} \in S$. Kaseasbeh and Erfanian (Proyecciones (Antofagasta) 40(6): 1683–1691, 2021) determined the structure of all $\text{Cay}(D_{2n}, S)$ with $|S| \leq 3$, where D_{2n} denotes the dihedral group of order $2n$. We extend their work by analyzing the structure of all $\text{Cay}(D_{2n}, S)$ with $|S| = 4$. Our main results are as follows:

- (1) By applying a result of Burnside and Schur from 1911 in the formulation of Evdokimov and Ponomarenko (Bull. Lond. Math. Soc. 37(4): 535–546, 2005), we prove that if $S = \{r^{\pm 1}, r^{\pm t_1}, \dots, r^{\pm t_{k-1}}\}$ with $t_i \geq 2$ contains distinct rotations and $p > Q = \max_{a,b}(ab + M)$ for $M = \max\{1, t_1, \dots, t_{k-1}\}$, then $\text{Aut}(\text{Cay}(D_{2p}, S)) \cong (R(\mathbb{Z}_p) \rtimes \langle p-1 \rangle) \wr \mathbb{Z}_2$, where $R(\mathbb{Z}_p)$ denotes the right regular representation of $\mathbb{Z}_p$.
- (2) If S is a set of $4 \leq 2k < n$ distinct rotations, then $\text{Cay}(D_{2n}, S)$ is the disjoint union of two isomorphic circulant graphs on n vertices.
- (3) Let $S = \{r^{a_1}s, \dots, r^{a_k}s\} \subseteq D_{2n}$ be a set of distinct reflections where $4 \leq k < n$. If S is a generating set, then $\Gamma = \text{Cay}(D_{2n}, S)$ is bipartite and a disjoint union of k perfect matchings. This generalizes a result of Ahmad Fadzil, Sarmin, and Erfanian (Matematika: Mjiam 35(3): 371–376, 2019). Moreover, if $\gcd(k, n) = 1$, Γ is normal, and $\Delta = \{a_i - a_j : 1 \leq i < j \leq k\}$, then $\text{Aut}(\Gamma) = R(G) \rtimes H$ where $H \leq \{u \in (\mathbb{Z}_n)^\times : u\Delta = \Delta\}$.

1. INTRODUCTION

The study of automorphism groups of Cayley graphs is one of the central topics in algebraic graph theory. Cayley graphs on dihedral groups, in particular, have received significant attention as a rich class of examples for this research (cf. [3, 5, 6, 8, 9, 10], among others). Previous research work has largely focused on Cayley graphs with valency at most 3. In particular, Kong [5] studied the automorphism group of connected cubic Cayley graphs of dihedral groups of order $2^n p^m$ where $n \geq 2$ and p is an odd prime, while Kaseasbeh and Erfanian [3] determined the structure of all $\text{Cay}(D_{2n}, S)$, where $n \geq 3$ and $|S| \leq 3$. These studies provide a foundation for understanding higher-valency cases. Classification of 4-valent one-regular normal Cayley graphs on dihedral groups were also investigated in [6, 8, 9]. Notably, Wang and Xu [9] provided a classification of the normal 4-valent one-regular Cayley graphs of dihedral groups, identifying specific exceptions and proved that all 4-valent one-regular Cayley graph X of dihedral groups are normal except that $n = 4s$, and $X \cong \text{Cay}(G, \{a, a^{-1}, a^i b, a^{-i} b\})$ where $i^2 \equiv \pm 1 \pmod{2s}$, $2 \leq i \leq 2s - 2$. However, a complete understanding of all 4-valent Cayley graphs over dihedral groups, including their structural properties and automorphism groups for different types of generating sets, remains an open area. In this paper, we extend this line of research by investigating the structure of 4-valent

2020 *Mathematics Subject Classification.* 05C25, 20B25, 05E18.

Key words and phrases. Cayley graph, Dihedral group, Automorphism group, Affine group, Valency.

Cayley graphs on dihedral groups and the automorphism groups of n -valent Cayley graphs on dihedral groups for $n \geq 4$ when the generating set consists exclusively of rotations or reflections.

1.1. Results. Apart from the main results stated in the Abstract, we prove the following:

- (1) If S contains two rotations and two reflections, then $\text{Cay}(D_{2n}, S)$ is formed by two isomorphic circulant graphs connected by two inter-layer perfect matchings.
- (2) Let $n \geq 3$ and $k \in \{1, \dots, n-1\}$ be such that if n is even, then $k \neq \frac{n}{2}$. Then, the graph $\text{Cay}(D_{2n}, S)$ is normal and $\text{Aut}(\text{Cay}(D_{2n}, S)) \cong R(D_{2n}) \rtimes C_2$ if $S = \{r, r^{-1}, s, sr^k\}$.
- (3) If S contains three rotations and one reflection, then $\text{Cay}(D_{2n}, S)$ is formed by two isomorphic circulant graphs connected by a single inter-layer perfect matching.
- (4) If S contains three reflections and one rotation, then $\text{Cay}(D_{2n}, S)$ consists of two circulant subgraphs (with intra-layer edges linking vertices at distance $n/2$) connected by three inter-layer perfect matchings.

Remark. The normality of all 4-valent one-regular Cayley graphs of dihedral groups was determined by Wang and Xu [9], who showed that such graphs are normal except for a few exceptional families. The result stated in (2) provides an explicit construction for determining the structure of $\text{Aut}(\text{Cay}(D_{2n}, S))$ for $S = \{r, r^{-1}, s, sr^k\}$, which differs from the approach used in [9].

2. PRELIMINARIES

Definition 2.1. Let $\Gamma = (V, E)$ be a graph. A *matching* in Γ is a subset $M \subseteq E$ such that no two edges in M share a common vertex. The matching M is called a *perfect matching* if every vertex of Γ is incident with exactly one edge in M . The *n -Crown graph* for an integer $n \geq 3$ is the graph with vertex set $V = \{x_1, \dots, x_n, y_1, \dots, y_n\}$ and edge set $E = \{\{x_i, y_j\} : 1 \leq i, j \leq n, i \neq j\}$. This graph is also known as the complete bipartite graph $K_{n,n}$ from which a perfect matching (specifically, the set of edges $\{x_i, y_i\}$ for each $1 \leq i \leq n$) has been removed.

Definition 2.2. Let G be a group that acts on a set X such that $|X| \geq 2$. The action of G on X is *2-transitive* if and only if for any $x_1, x_2, y_1, y_2 \in X$ such that $x_1 \neq x_2$ and $y_1 \neq y_2$ there is $g \in G$ such that $gx_1 = y_1$ and $gx_2 = y_2$ and the action of G on X is *transitive* if for any $x, y \in X, x \neq y$ there exists $g \in G$ so that $gx = y$. Let $\text{Orb}_G(x) = \{gx : g \in G\}$ be the orbit of $x \in X$ and $\text{Stab}_G(x) = \{g \in G : gx = x\}$ be the stabilizer of x under the action of G .

The *Orbit-Stabilizer theorem* states that the size of the orbit is the index of the stabilizer, that is $|\text{Orb}_G(x)| = [G : \text{Stab}_G(x)]$. We also recall that different orbits of the action are disjoint and form a partition of X i.e., $X = \bigcup \{\text{Orb}_G(x) : x \in X\}$.

Definition 2.3. A group G is called a *semidirect product* of N by Q , denoted by $G = N \rtimes Q$, if G contains subgroups N and Q such that: (1). $N \trianglelefteq G$ (that is, N is a normal subgroup of G), (2). $NQ = G$, and (3). $N \cap Q = \{1\}$.

Definition 2.4. The *affine group* $\text{AGL}(1, n)$ is the semidirect product of the group of translations $\mathbb{Z}_n$ and the group of automorphisms $\text{Aut}(\mathbb{Z}_n)$. Alternatively, it is the group of functions $x \mapsto ax + b$ where $a \in \mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n$, where $\mathbb{Z}_n^*$ is the multiplicative group of integers modulo n which consists of the set of integers k with $1 \leq k < n$ such that $\gcd(k, n) = 1$ and the group operation is multiplicative modulo n . If n is a prime then $\mathbb{Z}_n^*$ contains all non-zero integer modulo n .

Definition 2.5. Let G be a finite group and let $S \subseteq G \setminus \{e\}$ be an inverse-closed subset of $G \setminus \{e\}$ i.e., $S = S^{-1}$, where $S^{-1} := \{s^{-1} : s \in S\}$. The *undirected Cayley graph* $\text{Cay}(G, S)$ is the graph with a set of vertices G , and the vertices u and v are adjacent in $\text{Cay}(G, S)$ if and only if $uv^{-1} \in S$. The size of the set S is called the *valency* of $\text{Cay}(G, S)$. It is known that $\text{Cay}(G, S)$ is connected if and only if S is a generating set of G .

Definition 2.6. Let G be a group. The *right regular representation* of G , denoted by $R(G)$, is the permutation group $R(G) = \{\rho_g \mid g \in G\} \subseteq \text{Sym}(G)$, where ρ_g is the map $\rho_g : G \rightarrow G$ defined by $\rho_g(x) = xg$ for all $x \in G$. For an abelian group, left and right translations are the same. The automorphism group of a Cayley graph $\text{Cay}(G, S)$ is denoted by $\text{Aut}(\text{Cay}(G, S))$.

It is known that $R(G)$ is a subgroup of $\text{Aut}(\text{Cay}(G, S))$.

Definition 2.7. The *stabilizer of vertex v in $\text{Aut}(\text{Cay}(G, S))$* is denoted by $\text{Aut}(\text{Cay}(G, S))_v$. Given a group G and a subset $S \subseteq G$, let $\text{Aut}(G, S) = \{\alpha \in \text{Aut}(G) \mid \alpha(S) = S\}$.

If $\Gamma = \text{Cay}(G, S)$, then $\text{Aut}(G, S)$ is a subgroup of the stabilizer $\text{Aut}(\Gamma)_1$, where 1 is the identity element of the group G . It is also known that $R(G) \rtimes \text{Aut}(G, S) \leq \text{Aut}(\Gamma)$.

Definition 2.8. A Cayley graph $\Gamma = \text{Cay}(G, S)$ is *normal* if $R(G)$ is a normal subgroup of $\text{Aut}(\Gamma)$ i.e., $R(G) \trianglelefteq \text{Aut}(\Gamma)$. The graph Γ is normal if and only if $\text{Aut}(\Gamma) = R(G) \rtimes \text{Aut}(G, S)$.

Fact 2.9. The following holds:

- (1) ([4]) $\text{Cay}(G, S)$ is normal if and only if $\text{Aut}(\text{Cay}(G, S))_e = \text{Aut}(G, S)$.
- (2) (Burnside-Schur; [2]) Every primitive finite permutation group containing a regular cyclic subgroup is either 2-transitive or permutationally isomorphic to a subgroup of the affine group $\text{AGL}(1, p)$ where p is a prime.
- (3) For any integer $n > 1$, $\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.
- (4) If the action of G on X is 2-transitive, then the action of $\text{Stab}_G(x)$ on $X \setminus \{x\}$ is transitive for all $x \in X$.

Since any transitive permutation group of prime degree is primitive, we obtain the following.

Corollary 2.10. (of Fact 2.9(2)) *Let p be a prime. Let $G \leq S_p$ be a transitive permutation group of degree p that contains a regular cyclic subgroup. Then G is primitive and G is either*

- (1) *isomorphic to a subgroup of the affine group $\text{AGL}(1, p) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^*$, or*
- (2) *G is 2-transitive.*

Throughout the manuscript, we will use the following notations.

- $D_{2n} = \langle r, s \mid r^n = e, s^2 = e, srs = r^{-1} \rangle$ be the dihedral group of order $2n$,
- $\mathbb{Z}_n$ denotes cyclic group of order n ,
- $R = \{r^i : i \in \mathbb{Z}_n\}$ be the set of all rotations, and
- $F = \{sr^i : i \in \mathbb{Z}_n\}$ be the set of all reflections. Thus, $D_{2n} = R \cup F$.
- The indices of rotations and reflections are taken modulo n whenever we work with $\text{Cay}(D_{2n}, S)$.
- We refer to edges connecting two rotations or two reflections as *intra-layer edges*, and those connecting a rotation with a reflection as *inter-layer edges*.

- For graphs G_1 and G_2 , we denote by $G_1 + G_2$ the *disjoint union* of G_1 and G_2 .

Let $S \subset D_{2n}$ satisfy $e \notin S$, $S = S^{-1}$ and $|S| = 4$. Then $\Gamma := \text{Cay}(D_{2n}, S)$ falls into exactly one of the following mutually exclusive types:

- Case (I)**— $S \subseteq R$. Then $S = \{r^{\pm a}, r^{\pm b}\}$ for some $a, b \in \mathbb{Z}_n$ (possibly $a \equiv \pm b \pmod{n}$).
- Case (II)**— $S \subseteq F$. Then $S = \{sr^{a_1}, sr^{a_2}, sr^{a_3}, sr^{a_4}\}$ for some $a_1, a_2, a_3, a_4 \in \mathbb{Z}_n$. Clearly, $S = S^{-1}$ since each reflection is an involution.
- Case (III)**— S contains exactly two rotations and two reflections. Then, for some $a, b_1, b_2 \in \mathbb{Z}_n$, $S = \{r^{\pm a}, sr^{b_1}, sr^{b_2}\}$.
- Case (IV)**— S contains exactly three rotations and one reflection. This case occurs only when n is even. Then three rotations in S must consist of one inverse pair and the unique element of order two, that is $r^{n/2}$. Thus, $S = \{r^{\pm a}, r^{n/2}, sr^b\}$, for some $a, b \in \mathbb{Z}_n$.
- Case (V)**— S contains exactly three reflections and one rotation. This case arises only when n is even and the rotation in S must be $r^{n/2}$. Hence, $S = \{sr^{a_1}, sr^{a_2}, sr^{a_3}, r^{n/2}\}$, for some $a_1, a_2, a_3 \in \mathbb{Z}_n$.

In sections 3–6, we will analyze the above-mentioned cases.

3. ONLY ROTATIONS

Proposition 3.1. *Assume $S \subseteq R \setminus \{e\}$ is inverse-closed with $|S| = 2k < n$ for some $k \geq 2$. Choose representatives $a_1, \dots, a_k \in \mathbb{Z}_n$ such that $S = \{r^{\pm a_1}, \dots, r^{\pm a_k}\}$. Let $T = \{\pm a_1, \dots, \pm a_k\}$, $G_1 = \text{Cay}(D_{2n}, S)$, $G_2 = \text{Cay}(\mathbb{Z}_n, T)$, and $d = \gcd(n, a_1, \dots, a_k)$. Then:*

- (1) $\text{Cay}(D_{2n}, S) \cong \text{Cay}(\mathbb{Z}_n, T) + \text{Cay}(\mathbb{Z}_n, T)$.
- (2) If $d = 1$, then G_2 is connected. So G_1 has 2 components isomorphic to G_2 .
- (3) If $d > 1$, write $n = dn'$ and $a_i = da'_i$ for all i , and set $T' = \{\pm a'_1, \dots, \pm a'_k\} \subset \mathbb{Z}_{n'}$. Then G_2 decomposes into d components isomorphic to $\text{Cay}(\mathbb{Z}_{n'}, T')$. Consequently, $G_1 \cong G_2 + G_2$ splits into $2d$ components isomorphic to $\text{Cay}(\mathbb{Z}_{n'}, T')$.

Proof. (1). The vertex set of $\text{Cay}(D_{2n}, S)$ is $D_{2n} = R \cup F$. For any rotation $r^t \in R$, if $g \in R$, then $gr^t \in R$, while if $g \in F$, then $gr^t \in F$. Thus, every edge $\{g, gr^t\}$ produced by a rotation generator $r^t \in S$ is an intra-layer edge. Consequently, no generator in S produces an edge joining R to F . Therefore, $\text{Cay}(D_{2n}, S)$ splits into two vertex-disjoint subgraphs induced on R and on F . Consider the induced subgraph Γ_R of $\text{Cay}(D_{2n}, S)$ on R . If $t \in T$, then Γ_R contains the edge $\{r^i, r^{i+t}\}$. Hence $\Gamma_R \cong \text{Cay}(\mathbb{Z}_n, T)$. Similarly, the induced subgraph Γ_F on F is isomorphic to $\text{Cay}(\mathbb{Z}_n, T)$. In particular, the map $\varphi : R \rightarrow F$ defined by $\varphi(r^i) = sr^i$ is a bijection, and for any $t \in T$, $\{\varphi(r^i), \varphi(r^{i+t})\} = \{sr^i, sr^{i+t}\} = \{sr^i, (sr^i)r^t\}$. Thus, edges inside R correspond exactly to edges inside F under φ , so $\Gamma_F \cong \Gamma_R$. Consequently, $\text{Cay}(D_{2n}, S) = \Gamma_R + \Gamma_F \cong \text{Cay}(\mathbb{Z}_n, T) + \text{Cay}(\mathbb{Z}_n, T)$.

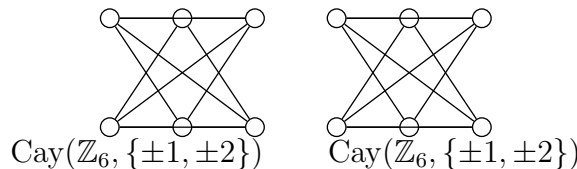


FIGURE 1. The graph $\text{Cay}(D_{12}, \{r^{\pm 1}, r^{\pm 2}\})$ can be expressed as $K_{2,2,2} + K_{2,2,2}$.

(2). We know that $\text{Cay}(\mathbb{Z}_n, T)$ is connected if and only if T is a generating set of $\mathbb{Z}_n$. The subgroup generated by T is $\langle T \rangle = \{x_1 a_1 + \dots + x_k a_k \pmod{n} : x_i \in \mathbb{Z}\} = d\mathbb{Z}_n = \{0, d, 2d, \dots, n-d\}$. Hence $\text{Cay}(\mathbb{Z}_n, T)$ is connected if and only if $\langle T \rangle = \mathbb{Z}_n$, which is equivalent to $d = \gcd(n, a_1, \dots, a_k) = 1$.

(3). We recall that $d = \gcd(n, a_1, \dots, a_k)$, $n = dn'$, $a_i = da'_i$ for $i = 1, \dots, k$. Let $\{C_j : 0 \leq j \leq d-1\}$ be a partition of $\mathbb{Z}_n$ where $C_j = \{j + kd : k = 0, \dots, n'-1\}$. The graph G_2 is the disjoint union of induced subgraphs on C_j 's. In particular, if $x \in C_j$ and $t \in T$, then t is a multiple of d (since each a_i is). Thus, $x+t \in C_j$ since $x+t \equiv x \pmod{d}$. Consequently, no edge $\{x, x+t\}$ joins C_i and C_j for $i \neq j$. Fix $0 \leq j \leq d-1$. The map $\psi_j : C_j \rightarrow \mathbb{Z}_{n'}, \psi_j(j + kd) \equiv k \pmod{n'}$, is a graph isomorphism from the induced subgraph on C_j to $\text{Cay}(\mathbb{Z}_{n'}, T')$, where $T' = \{\pm a'_1, \dots, \pm a'_k\}$. Therefore, there are exactly d identical components, each isomorphic to $\text{Cay}(\mathbb{Z}_{n'}, T')$. Since $\gcd(n', a'_1, \dots, a'_k) = 1$, $\langle T' \rangle = \mathbb{Z}_{n'}$, and thus $\text{Cay}(\mathbb{Z}_{n'}, T')$ is connected. $\square$

n	T	$\text{Cay}(\mathbb{Z}_n, T)$	S	$\text{Cay}(D_{2n}, S)$
4	$\{\pm 1, \pm 2\}$	Complete graph K_4	$\{r^{\pm 1}, r^{\pm 2}\}$	$K_4 + K_4$
6	$\{\pm 1, \pm 2\}$	Octahedral graph $(K_{2,2,2})$	$\{r^{\pm 1}, r^{\pm 2}\}$	$K_{2,2,2} + K_{2,2,2}$
6	$\{\pm 1, \pm 3\}$	$\text{Circ}(6; \{1, 3\})$	$\{r^{\pm 1}, r^{\pm 3}\}$	$\text{Circ}(6; \{1, 3\}) + \text{Circ}(6; \{1, 3\})$
8	$\{\pm 1, \pm 3\}$	complete bipartite graph $K_{4,4}$	$\{r^{\pm 1}, r^{\pm 3}\}$	$K_{4,4} + K_{4,4}$

TABLE 1. Examples of $\text{Cay}(\mathbb{Z}_n, T)$ and $\text{Cay}(D_{2n}, S)$ for $n \leq 8$.

3.1. Automorphism groups.

Lemma 3.2. *Let $p \geq 3$ be a prime. Let H be a proper subgroup of $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$. Let T be a generating set of $\mathbb{Z}_p$ that is invariant under the action of H but not under any larger subgroup of $\text{Aut}(\mathbb{Z}_p)$. If $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$ and the action of $\text{Aut}(\Gamma)$ on the set of vertices is not 2-transitive, then $\text{Aut}(\Gamma) \cong R(\mathbb{Z}_p) \rtimes H$.*

Proof. Denote $A = \text{Aut}(\Gamma)$ and $R(\mathbb{Z}_p) = \{R_a : x \mapsto x + a \mid a \in \mathbb{Z}_p\}$.

Claim 3.3. Γ is normal.

Proof. All connected Cayley graphs of $\mathbb{Z}_p$ are normal except the complete graph K_p by Galois and Burnside's theorems (cf. [7, pg. 82]). The condition that $\text{Aut}(\Gamma)$ is not 2-transitive effectively excludes the case $\Gamma = K_p$. Thus, Γ is normal. We provide an alternative argument to show that Γ is normal using Burnside-Schur's theorem. By the definition of a Cayley graph, the group of right translations $R(\mathbb{Z}_p)$ is a subgroup of A and is isomorphic to $\mathbb{Z}_p$. Since automorphism groups of Cayley graphs are vertex-transitive, A is a transitive permutation group. Moreover, $R(\mathbb{Z}_p)$ is a regular cyclic subgroup of S_p since $R(\mathbb{Z}_p) \cong \mathbb{Z}_p$, each $R_a \in R(\mathbb{Z}_p)$ is a permutation of $\mathbb{Z}_p$ and that the action of $\mathbb{Z}_p$ is regular (i.e., transitive and free). Since A is not 2-transitive, by Corollary 2.10, A is isomorphic to a subgroup of the affine group $\text{AGL}(1, p) = \{x \mapsto ax + b : a \in \mathbb{Z}_p^*, b \in \mathbb{Z}_p\}$.

- (1) Any automorphism α of Γ can be written as a composition of a translation R_b and an element of A_0 where for all $b \in \mathbb{Z}_p$, $R_b(x) = x + b$. We recall that $A_0 = \{m_c : c \in \mathbb{Z}_p^*, cT = T\} = \text{Aut}(\mathbb{Z}_p, T)$ where $m_c : x \mapsto cx$ is a map for $c \in \mathbb{Z}_p^*$. Thus, $\alpha = R_b(m_c(x)) = R_b(cx) = cx + b$ for some $b \in \mathbb{Z}_p$ and $c \in \mathbb{Z}_p^*$. Thus, $A \subseteq \text{AGL}(1, p)$. Since $\text{AGL}(1, p) \leq \text{Sym}(\mathbb{Z}_p)$ and $A \leq \text{Sym}(\mathbb{Z}_p)$, we have $A \leq \text{AGL}(1, p)$.

- (2) Write elements of $\text{AGL}(1, p)$ as pairs (u, b) acting by $(u, b) : x \mapsto ux + b$. The group operation is $(u_1, b_1)(u_2, b_2) = (u_1u_2, u_1b_2 + b_1)$ and inverses are $(u, b)^{-1} = (u^{-1}, -u^{-1}b)$. Thus the translation $t_a : x \mapsto x + a$ is the pair $(1, a)$. For any $(u, b) \in \text{AGL}(1, p)$,

$$(u, b)(1, a)(u, b)^{-1} = (u, b)(1, a)(u^{-1}, -u^{-1}b) = (1, ua),$$

which is again a translation. Hence conjugation by every element of $\text{AGL}(1, p)$ preserves the set of translations, so $R(\mathbb{Z}_p) = \{(1, a) : a \in \mathbb{Z}_p\} \trianglelefteq \text{AGL}(1, p)$.

Since $R(\mathbb{Z}_p) \trianglelefteq \text{AGL}(1, p)$, $A \leq \text{AGL}(1, p)$, and $R(\mathbb{Z}_p) \leq A$, we have $R(\mathbb{Z}_p) \trianglelefteq A$. Thus, Γ is normal. $\square$

Claim 3.4. $\text{Aut}(\mathbb{Z}_p, T) = H$.

Proof. Let $A_0 = \{\alpha \in A : \alpha(0) = 0\}$ denote the stabilizer of 0 in A . Since automorphisms preserve adjacency, $\alpha(T) = T$ for all $\alpha \in A_0$. Thus, $A_0 = \{\alpha \in A : \alpha(T) = T\}$.

Subclaim 3.5. *Let p be a prime and let $T \subseteq \mathbb{Z}_p$ be a generating, inverse-closed subset. For each $c \in \mathbb{Z}_p^\times$ define $m_c : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ by $m_c(x) = cx$. Then $A_0 = \{m_c : c \in \mathbb{Z}_p^\times, cT = T\} = \text{Aut}(\mathbb{Z}_p, T)$.*

Proof. By Claim 3.3 and Fact 2.9(1), the Cayley graph $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$ is normal and hence $\text{Aut}(\text{Cay}(G, S))_e = \text{Aut}(G, S)$. Thus, for any Cayley graph on a cyclic group of prime order, every automorphism fixing the identity element is a *group automorphism*. Since the group automorphisms of $(\mathbb{Z}_p, +)$ are exactly the multipliers $m_c : x \mapsto cx$ with $c \in \mathbb{Z}_p^\times$, we have $A_0 \subseteq \{m_c : c \in \mathbb{Z}_p^\times\}$. Moreover, for any such m_c ,

$$\{x, x + t\} \text{ is an edge} \iff t \in T \iff ct \in cT \iff \{cx, cx + ct\} \text{ is an edge}.$$

Thus m_c is an automorphism of Γ if and only if $cT = T$. Conversely, any $\alpha \in A_0$ must satisfy $\alpha(T) = T$, so $\alpha = m_c$ for some c with $cT = T$. Therefore $A_0 = \{m_c : c \in \mathbb{Z}_p^\times, cT = T\}$. $\square$

Since T is a generating set of $\mathbb{Z}_p$ that is invariant under the action of H but not under any larger subgroup of $\text{Aut}(\mathbb{Z}_p)$, we have $H = \{h \in \mathbb{Z}_p^* : hT = T\}$. We can see that $\text{Aut}(\mathbb{Z}_p, T) = \{m_h : x \mapsto hx \mid h \in H\}$. Pick any m_h for $h \in H$. For all adjacent pairs $\{x, y\}$, $y - x \in T \implies m_h(y) - m_h(x) = h(y - x) \in hT = T$. Thus, $m_h \in \text{Aut}(\mathbb{Z}_p, T)$ as $m_h(0) = 0$. On the other hand, if $\alpha \in \text{Aut}(\mathbb{Z}_p, T)$, then $\alpha = m_c$ for some $c \in \mathbb{Z}_p^*$ and $cT = T$. So, $c \in H$ and $\alpha = m_c \in \{m_h : x \mapsto hx \mid h \in H\}$. $\square$

By claims 3.3 and 3.4, we have $A = \text{Aut}(\Gamma) = R(\mathbb{Z}_p) \rtimes \text{Aut}(\mathbb{Z}_p, T) \cong R(\mathbb{Z}_p) \rtimes H$. This completes the proof of Lemma 3.2. $\square$

Theorem 3.6. *Let $p \geq 3$ be prime. Let $S = \{r^{\pm a_1}, \dots, r^{\pm a_k}\} \subseteq R \setminus \{e\}$ and let $T = \{\pm a_1, \dots, \pm a_k\}$ denote the exponents of the rotations in S such that the following hold:*

- (1) H is a proper subgroup of $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^*$ and T is invariant under the action of H , but T is not invariant under any subgroup of $\text{Aut}(\mathbb{Z}_p)$ strictly larger than H .
- (2) If $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$, then the action of $\text{Aut}(\Gamma)$ on the set of vertices is not 2-transitive.
- (3) $\gcd(p, a_1, \dots, a_k) = 1$.

Then, $\text{Aut}(\text{Cay}(D_{2p}, S)) \cong (R(\mathbb{Z}_p) \rtimes H) \wr C_2$.

Proof. By Proposition 3.1 and the hypothesis $\gcd(p, a_1, \dots, a_k) = 1$, the graph $\text{Cay}(D_{2p}, S)$ is the disjoint union of two components, each isomorphic to the connected circulant graph $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$. Moreover, $\text{Aut}(\text{Cay}(D_{2p}, S))$ is the wreath product of $\text{Aut}(\Gamma)$ with the symmetric group on two elements, S_2 , i.e., $\text{Aut}(\text{Cay}(D_{2p}, S)) \cong \text{Aut}(\Gamma) \wr S_2$ and T is a generating set of $\mathbb{Z}_p$. By Lemma 3.2, we have $\text{Aut}(\Gamma) \cong R(\mathbb{Z}_p) \rtimes H$. Since $S_2 \cong C_2$, we obtain $\text{Aut}(\text{Cay}(D_{2p}, S)) \cong (\text{Aut}(\Gamma)) \wr S_2 \cong (R(\mathbb{Z}_p) \rtimes H) \wr C_2$. $\square$

Theorem 3.7. *Fix an integer $k \geq 2$. Let $T = \{1, -1, t_1, -t_1, \dots, t_{k-1}, -t_{k-1}\} \subset \mathbb{Z}_p$ and*

$$S = \{r^{\pm 1}, r^{\pm t_1}, \dots, r^{\pm t_{k-1}}\} \subset R \setminus \{e\} \text{ for some integers } t_1, \dots, t_{k-1} \geq 2.$$

Let $M := \max\{1, t_1, \dots, t_{k-1}\}$, $Q := \max_{a,b \in \{1, t_1, \dots, t_{k-1}\}}(ab + M)$ and p be a prime with $p > Q$. Then $\text{Aut}(\text{Cay}(D_{2p}, S)) \cong (R(\mathbb{Z}_p) \rtimes H) \wr C_2$, where $H = \langle p-1 \rangle = \{1, p-1\} \subset \mathbb{Z}_p^\times$.

Proof. Clearly, $\gcd(p, 1, t_1, \dots, t_{k-1}) = 1$. In view of Theorem 3.6, it is enough to show that T is invariant under the action of H but not under any larger subgroup of $\text{Aut}(\mathbb{Z}_p)$ and if $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$, then the action of $\text{Aut}(\Gamma)$ on the set of vertices is not 2-transitive. We proceed by verifying these properties in three steps.

Claim 3.8. *T is invariant under the action of H .*

Proof. For the units $1, -1 \in \mathbb{Z}_p^*$, $1T = T$ and $(-1)T = T$. $\square$

Claim 3.9. *T is not invariant under any subgroup of $\text{Aut}(\mathbb{Z}_p)$ larger than H .*

Proof. Suppose, for contradiction, there exists $m \in \mathbb{Z}_p^\times \setminus \{1, p-1\}$ with $mT = T$. As $1 \in T$, we must have $m \in T$. Hence $m \in \{\pm t_a\}$ for some $a \in \{1, \dots, k-1\}$. Consider the case $m = t_a$ (the $m = -t_a$ case is identical up to signs). Then

$$mT = \{t_a, -t_a, t_a^2, -t_a^2, t_a t_b, -t_a t_b \ (b = 1, \dots, k-1)\}.$$

Since we have $mT = T$, each element on the left must equal (mod p) one of the elements of $T = \{\pm 1, \pm t_1, \dots, \pm t_{k-1}\}$. In particular, t_a^2 is congruent modulo p to some $s \in T$. But for every such s we have

$$0 < |t_a^2 - s| \leq t_a^2 + M \leq Q < p.$$

Hence, we have $t_a^2 \equiv s \pmod{p}$. This is impossible since $t_a^2 \not\equiv \pm 1$ and $t_a^2 \not\equiv \pm t_b$ (as $t_a^2 > t_a \geq t_b$ except in degenerate coincidence which our inequality rules out). Similarly, each product $t_a t_b$ appearing in mT cannot equal any element of T by the same magnitude bound and hence cannot be congruent to an element of T modulo p . Therefore no such m exists, a contradiction. Thus T is not invariant under any subgroup strictly larger than H . $\square$

Claim 3.10. $\text{Aut}(\Gamma)_0 = \{m \in \mathbb{Z}_p^\times : mT = T\} = \{1, -1\}$ where 0 is the identity of the group $\mathbb{Z}_p$.

Proof. By the arguments in the proof of Lemma 3.2, the Cayley graph $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$ is normal and $\text{Aut}(\mathbb{Z}_p, T) = H = \{1, -1\}$. By Fact 2.9 (1), we obtain $\text{Aut}(\Gamma)_0 = \text{Aut}(\mathbb{Z}_p, T) = \{1, -1\}$. $\square$

Claim 3.11. *Let $\Gamma = \text{Cay}(\mathbb{Z}_p, T)$. The action of $\text{Aut}(\Gamma)$ on the set of vertices is not 2-transitive.*

Proof. If the action of $A = \text{Aut}(\Gamma)$ on the vertex set $\mathbb{Z}_p$ is 2-transitive, then for any fixed point x_0 the stabilizer $A_{x_0} = \text{Stab}_A(x_0)$ acts transitively on the remaining $p-1$ vertices i.e., on all vertices of $\mathbb{Z}_p \setminus \{x_0\}$. Thus, for all $y_1, y_2 \in \mathbb{Z}_p \setminus \{x_0\}$, there exists $g \in A_{x_0}$ such that $g(y_1) = y_2$.

Thus, $\text{Orb}_{A_{x_0}}(y) = \{g(y) : g \in A_{x_0}\} = \mathbb{Z}_p \setminus \{x_0\}$; so $|\text{Orb}_{A_{x_0}}(y)| = p - 1$. By the Orbit-Stabilizer Theorem,

$$|A_{x_0}| = |\text{Orb}_{A_{x_0}}(y)| \cdot |(A_{x_0})_y| = (p - 1) \cdot |(A_{x_0})_y|,$$

so $|A_{x_0}|$ is a multiple of $p - 1$. In particular, $|A_{x_0}| \geq p - 1$. By Claim 3.10, we have $|A_{x_0}| = 2$. Since $p > Q \geq 3$ because each $t_i \geq 2$, this is impossible. $\square$

$\square$

Corollary 3.12. $\text{Aut}(\text{Cay}(D_{2p}, S)) \cong (R(\mathbb{Z}_p) \rtimes H) \wr \mathbb{Z}_2$ if $p > 5$ is a prime, $H = \langle p - 1 \rangle = \{1, p - 1\} \subset \mathbb{Z}_p^\times$, and $S = \{r, r^{p-1}, r^2, r^{p-2}\}$.

The following table list the Automorphism groups of $\text{Cay}(D_{2p}, S)$ for specific primes p and shows how the choice of proper subgroups of $\mathbb{Z}_p^*$ influences the structure of the generating set.

p	$H < \mathbb{Z}_p^*$	$T = \{\pm a, \pm b\}$	$\text{Aut}(\text{Cay}(D_{2p}, S))$	Graph structure of $\Gamma' = \text{Cay}(D_{2p}, S)$
7	$H = \{1, 6\}$	$\{1, 2, 5, 6\}$	$(L(\mathbb{Z}_7) \rtimes H) \wr \mathbb{Z}_2$	Γ' has two components isomorphic to $\text{Circ}(7; \{1, 2\})$.
11	$H = \{1, 10\}$	$\{1, 2, 9, 10\}$	$(L(\mathbb{Z}_{11}) \rtimes H) \wr \mathbb{Z}_2$	Γ' has two components isomorphic to $\text{Circ}(11; \{1, 2\})$.
13	$H = \{1, 12\}$	$\{1, 2, 11, 12\}$	$(L(\mathbb{Z}_{13}) \rtimes H) \wr \mathbb{Z}_2$	Γ' has two components isomorphic to $\text{Circ}(13; \{1, 2\})$.
17	$H = \{1, 4, 13, 16\}$	$\{1, 4, 13, 16\}$	$(L(\mathbb{Z}_{17}) \rtimes H) \wr \mathbb{Z}_2$	Γ' has two components isomorphic to $\text{Circ}(17; \{1, 4\})$.

TABLE 2. Automorphism groups and graph structures of $\text{Cay}(D_{2p}, S)$ based on the choice of proper subgroups of $\mathbb{Z}_p^*$ for specific primes p

4. FOUR REFLECTIONS

Ahmad Fadzil–Sarmin–Erfanian [1, Proposition 2] proved that if $n \geq 3$ and S contains all n reflections of D_{2n} , then $\text{Cay}(D_{2n}, S) = K_{n,n}$.

Proposition 4.1. Fix $n, k \geq 4$. Let $S \subseteq D_{2n}$ be a set of k reflections. Then $\text{Cay}(D_{2n}, S)$ is a complete bipartite graph if and only if $k = n$ and S contains all n reflections of D_{2n} . Moreover, if these conditions are met, then $\text{Cay}(D_{2n}, S) \cong K_{n,n}$.

Proof. Suppose $\Gamma = (V(\Gamma), E(\Gamma)) = \text{Cay}(D_{2n}, S)$ is a complete bipartite graph, say K_{m_1, m_2} . Since Γ is k -regular, we have $m_1 = m_2 = k$. Thus, $V(\Gamma) = 2n = 2k$. Since $\Gamma = K_{k,k}$, every vertex in R must be connected to every vertex in F . The neighbors of the identity element e are the generators in S . For e to be connected to all k reflections $s, sr, \dots, sr^{k-1}$, the set S must contain all of these reflections. Conversely, if S is the complete set of reflections then [1, Proposition 2] implies $\text{Cay}(D_{2n}, S) \cong K_{n,n}$. $\square$

We generalize [1, Proposition 2] due to Ahmad Fadzil, Sarmin, and Erfanian as follows.

Proposition 4.2. Fix $k \leq n$. Let $S = \{sr^{a_1}, \dots, sr^{a_k}\} \subseteq D_{2n}$ for some $a_1, \dots, a_k \in \mathbb{Z}_n$ be a generating set of distinct reflections. Let $M_{a_j} = \{\{r^i, sr^{a_j-i}\} : i \in \mathbb{Z}_n\}$ be a collection of edges for each $j \in \{1, \dots, k\}$ and $\Gamma = \text{Cay}(D_{2n}, S)$. The following holds:

- (1) Each M_{a_j} is a perfect matching between R and F .
- (2) The matchings M_{a_j} and M_{a_ℓ} are edge-disjoint whenever $a_j \not\equiv a_\ell \pmod{n}$.
- (3) Γ is bipartite with bipartitions R and F , and its edge set decomposes as $E(\Gamma) = \bigcup_{j=1}^k M_{a_j}$, the disjoint union of k perfect matchings.

Proof. (1). Fix $1 \leq j \leq k$. Consider the bijection $\varphi_j : R \rightarrow F$ given by $\varphi_j(r^i) = r^i s r^{a_j} = s r^{a_j-i}$. The mapping φ_j has inverse $\varphi_j^{-1}(s r^k) = r^{a_j-k}$. Thus M_{a_j} pairs each $r^i \in R$ with $\varphi_j(r^i) \in F$, and every vertex of R and F appears in exactly one pair. Thus, M_{a_j} is a perfect matching between R and F .

(2). For the sake of contradiction, suppose $\{r^i, s r^{a_j-i}\} = \{r^t, s r^{a_\ell-t}\}$ for some $i, t \in \mathbb{Z}_n$. The rotation endpoints must coincide, so $r^i = r^t$ and thus $i \equiv t \pmod{n}$. Furthermore, $s r^{a_j-i} = s r^{a_\ell-t}$ implies $a_j - i \equiv a_\ell - t \pmod{n}$. Thus, $a_j \equiv a_\ell \pmod{n}$.

(3). In order to show that $E(\Gamma) = \bigcup_{j=1}^k M_{a_j}$, it suffices to show that $E(\Gamma) \subseteq \bigcup_{j=1}^k M_{a_j}$ and $M_{a_j} \subseteq E(\Gamma)$ for each $1 \leq j \leq k$.

Claim 4.3. $E(\Gamma) \subseteq \bigcup_{j=1}^k M_{a_j}$.

Proof. By the definition of Γ , for any $g \in D_{2n}$ and $x \in S$ there is an edge $\{g, gx\}$. If $x = s r^{a_j}$ and $g = r^i \in R$, then $gx = r^i(s r^{a_j}) = s r^{a_j-i} \in F$, so the edge $\{r^i, s r^{a_j-i}\}$ lies in M_{a_j} . If the edge starts from a reflection vertex $g = s r^k \in F$, and is generated by $x = s r^{a_j} \in S$, then $gx = (s r^k)(s r^{a_j}) = (s r^k s) r^{a_j} = (s r^k s^{-1}) r^{a_j} = r^{-k} r^{a_j} = r^{a_j-k} \in R$. We claim that $\{s r^k, r^{a_j-k}\} \in M_{a_j}$. Let $i = a_j - k$ and consider $r^i \in R$. Since $s r^{a_j-i} = s r^{a_j-(a_j-k)} = s r^k$, the edge $\{r^{a_j-k}, s r^k\}$ lies in M_{a_j} , and this is the same edge as $\{s r^k, r^{a_j-k}\}$. $\square$

Claim 4.4. $M_{a_j} \subseteq E(\Gamma)$ for each $1 \leq j \leq k$.

Proof. By the definition of a Cayley graph, an edge exists between r^i and $r^i(s r^{a_j})$ (which is $s r^{a_j-i}$) because $s r^{a_j} \in S$. So, any element $\{r^i, s r^{a_j-i}\}$ in M_{a_j} is generated by multiplying the element $r^i \in D_{2n}$ by the generator $s r^{a_j} \in S$. Therefore, it is an edge of Γ . $\square$

Clearly, all edges are between R and F , so Γ is bipartite with bipartitions R and F . $\square$

Corollary 4.5. Let S be a set of $n-1$ reflections from D_{2n} . Then $\text{Cay}(D_{2n}, S) \cong n\text{-Crown graph}$.

Proof. We can write $S = F \setminus \{s r^{i_0}\}$ for some $i_0 \in \mathbb{Z}_n$ where $F = \{s r^k : k \in \mathbb{Z}_n\}$. The rest follows from Proposition 4.2 and the fact that S is a generating set since Γ is the union of $n-1$ perfect matchings between R and F , that is, the n -Crown graph. $\square$

4.1. Automorphism groups. The following lemma reveals a relationship between the automorphism group of a normal, connected Cayley graph $\text{Cay}(D_{2n}, S)$, where S consists entirely of reflections, and the stabilizer of the exponents of the elements of S under the action of $\text{AGL}(1, n)$.

Lemma 4.6. Let $n \geq 5$ be any integer and $4 \leq k < n$. Let $S = \{r^{a_1} s, \dots, r^{a_k} s\} \subseteq D_{2n}$ be a set of distinct reflections, $A = \{a_1, \dots, a_k\} \subseteq \mathbb{Z}_n$, and $\Delta = \{a_i - a_j \mid 1 \leq i, j \leq k\}$. Assume that the following hold:

- (i) $\Gamma = \text{Cay}(G, S)$ is normal,
- (ii) $d = \gcd(n, a_i - a_j, 1 \leq i < j \leq k) = 1$.

Then $\text{Aut}(\Gamma) \cong R(D_{2n}) \rtimes \{(u, v) \in (\mathbb{Z}_n)^\times \ltimes \mathbb{Z}_n : uA + v = A\}$.

Proof. Since $d = 1$, we have Γ is connected and S is a generating set. Since S contains only reflections, S is symmetric.

Claim 4.7. $\text{Aut}(G, S) \cong \{(u, v) \in (\mathbb{Z}_n)^\times \ltimes \mathbb{Z}_n : uA + v = A\}$, i.e. the stabiliser of A in the affine group $\text{AGL}(1, n)$.

Proof. Given $\psi_{u,v} : r \mapsto r^u, s \mapsto r^v s$, there is a natural correspondence

$$\Phi : \text{Aut}(G, S) \longrightarrow \text{AGL}(1, n), \quad \psi_{u,v} \longmapsto (u, v).$$

We can see that $\psi_{u,v} \in \text{Aut}(G, S) \iff uA + v = A$, that is, the affine map $x \mapsto ux + v$ stabilises A . For $a_i \in A$, we have $\psi_{u,v}(r^{a_i} s) = (r^u)^{a_i} r^v s = r^{ua_i + v} s$. Hence $\psi_{u,v}(S) = \{r^{ua_i + v} s : a_i \in A\} = \{r^x s : x \in uA + v\}$, where $uA + v := \{ua + v : a \in A\} \subseteq \mathbb{Z}_n$. Therefore, $\psi_{u,v}(S) = S \iff \{r^x s : x \in uA + v\} = \{r^x s : x \in A\} \iff uA + v = A$. Thus, $\psi_{u,v} \in \text{Aut}(G, S) \iff uA + v = A$. Hence Φ identifies $\text{Aut}(G, S)$ isomorphically with the affine stabiliser of A in $\text{AGL}(1, n)$, i.e., $\text{Aut}(G, S) \cong \{(u, v) \in (\mathbb{Z}_n)^\times \ltimes \mathbb{Z}_n : uA + v = A\}$. $\square$

Since Γ is normal, $\text{Aut}(\Gamma) \cong R(G) \rtimes \{(u, v) \in (\mathbb{Z}_n)^\times \ltimes \mathbb{Z}_n : uA + v = A\}$ by Claim 4.7. $\square$

Theorem 4.8. Let $4 \leq k < n$ be integers such that $\gcd(n, k) = 1$. Let $S = \{r^{a_1} s, \dots, r^{a_k} s\} \subseteq G = D_{2n}$ be a set of distinct reflections, and $\Delta = \{a_i - a_j : 1 \leq i < j \leq k\}$. Assume

- (i) $\Gamma = \text{Cay}(G, S)$ is normal,
- (ii) $d = \gcd(n, a_i - a_j : 1 \leq i < j \leq k) = 1$.

Then $\text{Aut}(\Gamma) = R(G) \rtimes H$, such that $H \leq (U_0, \times)$ where $U_0 := \{u \in (\mathbb{Z}_n)^\times : u\Delta = \Delta\}$ and $\times$ is multiplication modulo n .

Proof. Since Γ is normal, we have $\text{Aut}(\Gamma) = R(G) \rtimes \text{Aut}(G, S)$. Let $A = \{a_1, \dots, a_k\}$. By the arguments in the proof of Lemma 4.6, if $\psi_{u,v}$ maps $r \mapsto r^u$ and $s \mapsto r^v s$ then $\text{Aut}(G, S) = \{\psi_{u,v} : (u, v) \in (\mathbb{Z}_n)^\times \ltimes \mathbb{Z}_n, uA + v = A\}$. Let $\pi : (\text{Aut}(G, S), \circ) \rightarrow (\mathbb{Z}_n)^\times$ be the function that maps $\psi_{u,v} \mapsto u$ where $\circ$ is the operation defined by $\psi_{u_1, v_1} \circ \psi_{u_2, v_2} = \psi_{u_1 u_2, v_1 + u_1 v_2}$ for any $\psi_{u_1, v_1}, \psi_{u_2, v_2} \in \text{Aut}(G, S)$. Since $\pi(\psi_{u_1, v_1} \circ \psi_{u_2, v_2}) = u_1 u_2 = \pi(\psi_{u_1, v_1}) \pi(\psi_{u_2, v_2})$, π is a homomorphism.

Claim 4.9. $\pi(\text{Aut}(G, S)) \subseteq U_0$.

Proof. If $\psi_{u,v} \in \text{Aut}(G, S)$ then $uA + v = A$. Thus, for every $x \in A$, there exists $y \in A$ such that $ux + v = y$, and conversely, for every $y \in A$, there exists $x \in A$ satisfying $ux + v = y$. For any $x, y \in A$, there exists $x', y' \in A$ such that $x' = ux + v$ and $y' = uy + v$. Thus, $x' - y' = (ux + v) - (uy + v) = u(x - y)$. Furthermore, $x' - y' \in \Delta$. Thus, $u\delta \in \Delta$ for all $\delta \in \Delta$. So, $u\Delta \subseteq \Delta$ where $u\Delta := \{u\delta : \delta \in \Delta\}$. Since u is a unit in $\mathbb{Z}_n$, it has a multiplicative inverse $u^{-1} \in (\mathbb{Z}_n)^\times$. By the same reasoning as above, we can see that $u^{-1}\Delta \subseteq \Delta$. Multiplying both sides by u , we obtain $\Delta \subseteq u\Delta$. Consequently, $u\Delta = \Delta$. $\square$

Claim 4.10. $\ker(\pi)$ is trivial, and hence π is an injective homomorphism.

Proof. The kernel of π is $\ker(\pi) = \{\psi_{1,v} : \psi_{1,v} \in \text{Aut}(G, S)\}$. If $\psi_{1,v} \in \ker(\pi)$, then $A + v = A$. Let $\mathcal{G} = (\mathbb{Z}_n, +)$. Fix $v \in \mathbb{Z}_n$. Let $\langle v \rangle \leq \mathcal{G}$ denote the cyclic subgroup generated by v , and let $\langle v \rangle$ act on $\mathbb{Z}_n$ by translations $k \cdot x \equiv x + kv \pmod{n}$, ($k \in \mathbb{Z}$).

Subclaim 4.11. *Let m be the order of v in $\mathcal{G}$, i.e. the smallest positive integer with $mv \equiv 0 \pmod{n}$. Then for every $x \in \mathbb{Z}_n$, $|\text{Orb}_{\langle v \rangle}(x)| = m$. In particular, m divides n .*

Proof. The subgroup $\langle v \rangle = \{0, v, \dots, (m-1)v\}$ has m elements and $\text{Orb}_{\langle v \rangle}(x) = \{x + g : g \in \langle v \rangle\}$. Since m is the least positive integer with $mv \equiv 0 \pmod{n}$, the elements $x, x+v, \dots, x+(m-1)v$ are all distinct and $x + mv \equiv x \pmod{n}$. Thus, $|\text{Orb}_{\langle v \rangle}(x)| = m$. Finally, since $\langle v \rangle$ is a subgroup of the finite group $(\mathbb{Z}_n, +)$ of order n , Lagrange's theorem gives $m \mid n$. $\square$

Since $A = \bigcup_{x \in A} \{\text{Orb}_{\langle v \rangle}(x)\}$ is a disjoint union of orbits, we have $|A| = tm = k$ if A is the union of t -orbits, hence $m \mid k$. By Subclaim 4.11, $m \mid n$ and thus $m = 1$ since we assumed $\gcd(n, k) = 1$. Therefore, $v = 0$. So, the identity automorphism $\psi_{1,0}$ is the only element in $\ker(\pi)$. $\square$

Claim 4.12. $(\text{Aut}(G, S), \circ) \cong (\pi(\text{Aut}(G, S)), \times) \leq (U_0, \times)$.

Proof. By the arguments of Claim 4.10, there exists a unique $v(u)$ such that $uA + v(u) = A$ for any $u \in \pi(\text{Aut}(G, S))$.¹ Then $\psi_{u,v(u)} \in \text{Aut}(G, S)$ and $\pi(\psi_{u,v(u)}) = u$, so $\pi : \text{Aut}(G, S) \rightarrow \pi(\text{Aut}(G, S))$ is surjective. Since π is a monomorphism, π induces an isomorphism. Thus, $(\text{Aut}(G, S), \circ) \cong (\pi(\text{Aut}(G, S)), \times)$. By Claim 4.9, we have $(\pi(\text{Aut}(G, S)), \times) \leq (U_0, \times)$. $\square$

This completes the proof of Theorem 4.8. $\square$

5. TWO ROTATIONS AND TWO REFLECTIONS

Proposition 5.1. *Assume that S contains exactly two rotations and two reflections. Then, there exist integers $a, b_1, b_2 \in \mathbb{Z}_n$ such that $S = \{r^{\pm a}, sr^{b_1}, sr^{b_2}\}$ where $a \not\equiv 0, n/2 \pmod{n}$. Let $T = \{\pm a\} \subset \mathbb{Z}_n$, $M_{b_j} = \{\{r^i, sr^{b_j-i}\} : i \in \mathbb{Z}_n\}$ for $j \in \{1, 2\}$, and $\Gamma = \text{Cay}(D_{2n}, S)$. Then*

$$V(\Gamma) = R \cup F, \quad \text{and} \quad E(\Gamma) = E(\text{Cay}(\mathbb{Z}_n, T)) \cup E(\text{Cay}(\mathbb{Z}_n, T)) \cup M_{b_1} \cup M_{b_2}.$$

So Γ is obtained by taking two identical circulant layers (on R and F) and adding the two inter-layer perfect matchings M_{b_1}, M_{b_2} .

Proof. We can see that R and F partition D_{2n} into the rotation and reflection cosets. Multiplying by a rotation preserves the coset and multiplying by a reflection swaps cosets. Hence, rotation generators yield intra-layer edges and reflection generators yield inter-layer edges. For $i \in \mathbb{Z}_n$, $\{r^i, r^{i+a}\}$, and $\{r^i, r^{i-a}\}$ are edges of $\Gamma[R]$, so $\Gamma[R] \cong \text{Cay}(\mathbb{Z}_n, \{\pm a\})$. Similarly, $\Gamma[F] \cong \text{Cay}(\mathbb{Z}_n, \{\pm a\})$. For $j = 1, 2$, each reflection sr^{b_j} pairs r^i with $r^i(sr^{b_j}) = (r^i s)r^{b_j} = (sr^{-i})r^{b_j} = sr^{b_j-i}$, producing the perfect matching $M_{b_j} = \{\{r^i, sr^{b_j-i}\} : i \in \mathbb{Z}_n\}$. Thus, $E(\Gamma) = E(\Gamma[R]) \cup E(\Gamma[F]) \cup M_{b_1} \cup M_{b_2}$. $\square$

5.1. Automorphism groups.

Theorem 5.2. *Let $n \geq 3$ be an integer and $k \in \{1, \dots, n-1\}$ be such that if n is even, then $k \neq n/2$. Let $S = \{r, r^{-1}, s, sr^k\}$. Then $\Gamma = \text{Cay}(D_{2n}, S)$ is normal and $\text{Aut}(\Gamma) \cong R(D_{2n}) \rtimes C_2$.*

Proof. The proof follows from a direct case analysis on the possible images of r and s under automorphisms of D_{2n} ; see Appendix A for details. $\square$

¹Indeed, if $uA + v = uA + v'$ then $uA = uA + (v - v')$. Applying u^{-1} elementwise to both sides yields $A = A + u^{-1}(v - v')$. Thus $u^{-1}(v - v')$ fixes A , and the orbit-count argument (as in Claim 4.10) forces $u^{-1}(v - v') \equiv 0 \pmod{n}$, hence $v = v'$.

6. ONE ROTATION OR ONE REFLECTION

Proposition 6.1. *Suppose S contains exactly three rotations and one reflection. Then n is even, and there exist integers $a, b \in \mathbb{Z}_n$ such that $S = \{r^a, r^{-a}, r^{n/2}, sr^b\}$ where $a \not\equiv 0, n/2 \pmod{n}$. Let $\Gamma = \text{Cay}(D_{2n}, S)$, $T = \{\pm a, n/2\} \subset \mathbb{Z}_n$. For the reflection sr^b define the perfect matching $M_b = \{\{r^i, sr^{b-i}\} : i \in \mathbb{Z}_n\}$. Then $E(\Gamma) = E(\text{Cay}(\mathbb{Z}_n, T)) \cup E(\text{Cay}(\mathbb{Z}_n, T)) \cup M_b$. In particular, Γ is formed by two isomorphic circulant graphs connected by a single inter-layer perfect matching.*

Proof. For any $r^t \in R$ and any $g \in D_{2n}$, gr^t and g belong to the same coset, and for any $sr^u \in F$ and any $g \in D_{2n}$, $g(sr^u)$ and g belongs to the opposite coset. Thus, the generators r^a, r^{-a} , and $r^{n/2}$ produce only intra-layer edges. In particular, for every $i \in \mathbb{Z}_n$,

$$\{r^i, r^{i \pm a}\}, \{r^i, r^{i+n/2}\}, \{sr^i, sr^{i \pm a}\}, \{sr^i, sr^{i+n/2}\} \in E(\Gamma).$$

Therefore, $\Gamma[R] \cong \Gamma[F] \cong \text{Cay}(\mathbb{Z}_n, T)$. Furthermore, $sr^b \in S$ produces the inter-layer edges. For each $i \in \mathbb{Z}_n$, $r^i(sr^b) = sr^{b-i} \in F$, so the edges arising from sr^b are $\{r^i, sr^{b-i}\}$ for $i \in \mathbb{Z}_n$. The set $M_b = \{\{r^i, sr^{b-i}\} : i \in \mathbb{Z}_n\}$ is a perfect matching. Consequently, $E(\Gamma) = E(\Gamma[R]) \cup E(\Gamma[F]) \cup M_b$. As $\Gamma[R] \cong \text{Cay}(\mathbb{Z}_n, T)$ and $\Gamma[F] \cong \text{Cay}(\mathbb{Z}_n, T)$, the graph structure can be described as two identical circulant graphs connected by a perfect matching. $\square$

Proposition 6.2. *Assume that S is a symmetric generating set for D_{2n} with three distinct reflections and one rotation. Then n is even and there exist distinct integers $a_1, a_2, a_3 \in \mathbb{Z}_n$ such that $S = \{sr^{a_1}, sr^{a_2}, sr^{a_3}, r^{n/2}\}$. Let $\Gamma = \text{Cay}(D_{2n}, S)$. For $j = 1, 2, 3$, define the perfect matchings: $M_{a_j} = \{\{r^i, sr^{a_j-i}\} : i \in \mathbb{Z}_n\}$, $N_R = \{\{r^i, r^{i+n/2}\} : i \in \mathbb{Z}_n\}$, and $N_F = \{\{sr^i, sr^{i+n/2}\} : i \in \mathbb{Z}_n\}$. Then $\Gamma = (R \cup F, N_R \cup N_F \cup M_{a_1} \cup M_{a_2} \cup M_{a_3})$.*

Proof. For $j \in \{1, 2, 3\}$, we consider the action of generators sr^{a_j} and $r^{n/2}$ on vertices of Γ .

- For $i \in \mathbb{Z}_n$, we have $r^i(sr^{a_j}) = r^i(r^{-a_j}s) = r^{i-a_j}s = sr^{a_j-i}$. So the edges produced by the generator sr^{a_j} on rotation vertices are of the form $\{r^i, sr^{a_j-i}\}$. These edges form the perfect matching M_{a_j} between the set of rotations R and the set of reflections F .
- For $y \in \mathbb{Z}_n$, we have $(sr^y)(sr^{a_j}) = r^{a_j-y}$. Thus the edges produced by the generator sr^{a_j} on reflection vertices are of the form $\{sr^y, r^{a_j-y}\}$ for $y \in \mathbb{Z}_n$. If we set $i = a_j - y$, then $\{sr^y, r^{a_j-y}\} = \{sr^{a_j-i}, r^i\} \in M_{a_j}$. Thus, the edges generated by sr^{a_j} acting on reflection vertices are already defined in M_{a_j} .
- For rotation $r^{n/2}$, since $(r^{n/2})^2 = e$ we have for each i , $r^i r^{n/2} = r^{i+n/2} \in R$ and $(sr^i) r^{n/2} = sr^{i+n/2} \in F$, so $r^{n/2}$ induces the perfect matchings N_R on R and N_F on F .

The total set of edges in Γ is the union of the matchings induced by each generator in S . Each of the reflection generators sr^{a_i} , $1 \leq i \leq 3$ induces a perfect matching M_{a_i} . The rotation generator $r^{n/2}$ induces the perfect matchings N_R and N_F . Thus, $E(\Gamma) = N_R \cup N_F \cup M_{a_1} \cup M_{a_2} \cup M_{a_3}$. $\square$

Funding The author was supported by the EKÖP-24-4-II-ELTE-996 University Excellence scholarship program of the Ministry for Culture and Innovation from the source of the National Research, Development and Innovation fund.

REFERENCES

- [1] A. F. Ahmad Fadzil, N. H. Sarmin, and A. Erfanian. The Energy of Cayley Graphs for a Generating Subset of the Dihedral Groups, *MATEMATIKA: MJIAM* **35** no.3 (2019), 371–376. doi: <https://doi.org/10.11113/matematika.v35.n3.1115>
- [2] S. Evdokimov, and I. Ponomarenko, A New Look at the Burnside–Schur Theorem, *Bull. Lond. Math. Soc.* **37** no.4 (2005), 535–546. doi: <https://doi.org/10.1112/S0024609305004340>
- [3] S. AL. Kaseasbeh and A. Erfanian, The structure of Cayley graphs of dihedral groups of Valencies 1, 2 and 3, *Proyecciones (Antofagasta)* **40** no.6 (2021), 1683–1691. doi: <https://doi.org/10.22199/issn.0717-6279-4357-4429>
- [4] X. Huang, Q. Huang, and L. Lu, Automorphism Groups of a Class of Cubic Cayley Graphs on Symmetric Groups, *Algebra Colloq.* **24** no. 4 (2017), 541–550. doi: <https://doi.org/10.1142/S1005386717000359>
- [5] X. Kong, Automorphism Groups of Cubic Cayley Graphs of Dihedral Groups of Order $2^n p^m$ ($n \geq 2$ and p Odd Prime), *JAMP* **8** no.12 (2020), 3075–3084. doi: <https://doi.org/10.4236/jamp.2020.812226>
- [6] J.H. Kwak and J.M. Oh, One-regular normal Cayley graphs on dihedral groups of valency 4 or 6 with cyclic vertex stabilizer, *Acta Math. Sinica* **22** (2006), 1305–1320. doi: <https://doi.org/10.1007/s10114-005-0752-9>
- [7] Z.P. Lu and M.Y. Xu, On the normality of Cayley graphs of order pq , *Australas. J. Combin.* **27** (2003), 81–93.
- [8] C.Q. Wang and Z.Y. Zhou, One-Regularity of 4-Valent and Normal Cayley Graphs of Dihedral Groups, *Acta Math. Sinica, Chin. Ser.* **49** no. 3 (2006), 669–678. doi: <https://doi.org/10.12386/A2006sxxb0084>
- [9] C. Wang and M. Xu, Non-normal one-regular and 4-valent Cayley graphs of dihedral groups D_{2n} , *Eur. j. comb.* **27** no. 5 (2006), 750–766. doi:<https://doi.org/10.1016/j.ejc.2004.12.007>
- [10] C. Zhou and Y.Q. Feng, Automorphism Groups of Connected Cubic Cayley Graphs of Order $4p$, *Algebra Colloq.* **14** no. 2 (2007), 351–359. doi:<https://doi.org/10.1142/S100538670700034X>

7. APPENDIX A

In this section, we write the detailed proof of Theorem 5.2. The set $S = \{r, r^{-1}, s, sr^k\}$, contains both r and s . Therefore, the subgroup $\langle S \rangle$ generated by S , is equal to D_{2n} and Γ is connected.

Claim 7.1. $\text{Aut}(G, S) = \{\text{id}, \phi\}$, where $\phi : r \mapsto r^{-1}, s \mapsto sr^k$ and id is the identity automorphism.

Proof. Every automorphism of D_{2n} is of the form $\psi_{u,v} : r \mapsto r^u, s \mapsto r^v s$, where $u \in (\mathbb{Z}_n)^\times$ and $v \in \mathbb{Z}_n$. For $\psi_{u,v}$ to be in $\text{Aut}(G, S)$, it must map the set S to itself.

- (1) Since $r \in S$, its image r^u must be in S . The only elements of order $n \geq 3$ in S are r and r^{-1} . So, we must have $r^u = r$ or $r^u = r^{-1}$, which implies $u \equiv \pm 1 \pmod{n}$.
- (2) Similarly, since $s \in S$, its image $r^v s$ must be in S . The only involutions in S are s and sr^k . Thus, $r^v s = s$ or $r^v s = sr^k$.

Now we analyze the cases for u and v :

- **Case $u \equiv 1 \pmod{n}$:** Then $\psi_{u,v}$ maps r to r . Then $\psi_{u,v}\{s, sr^k\} = \{s, sr^k\}$. Clearly, $\psi_{u,v}(s) = r^v s$ and $\psi_{u,v}(sr^k) = (r^v s)r^k = r^v(r^{-k}s) = r^{v-k}s$. Thus $\{r^v s, r^{v-k}s\} = \{s, sr^k\}$.
 - **Subcase $r^v s = s$:** If $r^v s = s$, then $v = 0$. Consequently, $\psi_{1,0} = \text{id} \in \text{Aut}(G, S)$.
 - **Subcase $r^v s = sr^k$:** If $r^v s = sr^k$ and $r^{v-k}s = s$, then $v \equiv -k \pmod{n}$. We have $r^{-2k}s = s$. This implies $r^{-2k} = 1$ and $2k \equiv 0 \pmod{n}$. However, the hypothesis of Theorem 5.2 states that if n is even, $k \neq n/2$, which means $2k \not\equiv 0 \pmod{n}$. Thus, this subcase is impossible.
- **Case $u \equiv -1 \pmod{n}$:** Then $\psi_{u,v}$ maps r to r^{-1} . Then $\psi_{u,v}\{s, sr^k\} = \{s, sr^k\}$. Clearly, $\psi_{u,v}(s) = r^v s$ and $\psi_{u,v}(sr^k) = (r^v s)r^{-k} = r^v(r^k s) = r^{v+k}s$. Thus $\{r^v s, r^{v+k}s\} = \{s, sr^k\}$.

- **Subcase $r^v s = s$ and $r^{v+k} s = sr^k$:** The first equation implies $v \equiv 0 \pmod{n}$. The second equation becomes $r^k s = sr^k$, which is $r^k s = r^{-k} s$. Thus,

$$(r^k s)s = (r^{-k} s)s \implies r^k s^2 = r^{-k} s^2 \implies r^k = r^{-k}.$$

Multiplying both sides by r^k gives $r^k r^k = r^{-k} r^k$, which simplifies to $r^{2k} = r^0 = 1$. This implies $2k \equiv 0 \pmod{n}$, since the order of r is n . This is excluded by the hypothesis of Theorem 5.2. Thus, this subcase is impossible.

- **Subcase $r^v s = sr^k$ and $r^{v+k} s = s$:** The second equation implies $v + k \equiv 0 \pmod{n}$, so $v \equiv -k \pmod{n}$. Let's check if the mapping $\psi_{-1,-k}$ preserves the set S :

$$* \psi_{-1,-k}(r) = r^{-1} \in S.$$

$$* \psi_{-1,-k}(s) = r^{-k} s = sr^k \in S.$$

$$* \psi_{-1,-k}(sr^k) = \psi_{-1,-k}(s)\psi_{-1,-k}(r)^k = (sr^k)(r^{-1})^k = sr^k r^{-k} = s \in S.$$

This mapping, which we denote by ϕ , maps S to S and is a valid automorphism of D_{2n} . Since $k \not\equiv 0 \pmod{n}$, ϕ is not the identity. Moreover, $\phi^2 = \text{id}$ since $\phi^2(r) = \phi(r^{-1}) = r$ and $\phi^2(s) = \phi(sr^k) = s$.

Therefore, the only possible automorphism for this case is $\phi = \psi_{-1,-k}$.

Since $\phi \neq \text{id}$, $\text{Aut}(G, S) \supseteq \{\text{id}, \phi\}$. Furthermore, from the analysis above, these are the only two possibilities. So $\text{Aut}(G, S) = \{\text{id}, \phi\}$, and since $\phi^2 = \text{id}$, this group is isomorphic to C_2 . $\square$

Claim 7.2. Γ is normal, and consequently, $\text{Aut}(\Gamma) = R(D_{2n}) \rtimes \text{Aut}(G, S) \cong R(D_{2n}) \rtimes C_2$.

Proof. In view of Fact 2.9 (1), it suffices to show that $\text{Aut}(\Gamma)_e = \{\text{id}, \phi\}$. Let $\alpha \in \text{Aut}(\Gamma)$ with $\alpha(e) = e$. Since automorphisms preserve adjacency, $\alpha(N_\Gamma(e)) = N_\Gamma(e) = S = \{r, r^{-1}, s, sr^k\}$ where $N_\Gamma(e)$ denotes the open neighborhood of e in Γ . Additionally, α must preserve the order of elements. For $n \geq 3$, the elements r and r^{-1} are rotations of order n , whereas s and sr^k are reflections of order 2. Since $n \neq 2$, these sets have distinct orders, so $\alpha\{r, r^{-1}\} = \{r, r^{-1}\}$ and $\alpha\{s, sr^k\} = \{s, sr^k\}$. This gives four possibilities:

- (1) **Case (I):** $\alpha(r) = r$ and $\alpha(s) = s$. Since α fixes the generators, we have $\alpha = \text{id}$.
- (2) **Case (II):** $\alpha(r) = r$ and $\alpha(s) = sr^k$. Since $\alpha(e) = e$, we have $\alpha(rr^{-1}) = \alpha(r)\alpha(r^{-1}) = r\alpha(r^{-1}) = e$. Thus, $\alpha(r^{-1}) = r^{-1}$. Furthermore, $\alpha(sr^k) = \alpha(s)\alpha(r)^k = (sr^k)r^k = (r^{-k}s)r^k = r^{-k}(sr^k) = r^{-k}(r^{-k}s) = r^{-2k}s = sr^{2k}$. Since $\alpha(S) = S$, we have

$$\{\alpha(r), \alpha(r^{-1}), \alpha(s), \alpha(sr^k)\} = \{r, r^{-1}, s, sr^k\}.$$

Thus $sr^{2k} = s$, so $r^{2k} = 1$ and $2k \equiv 0 \pmod{n}$, which are excluded by the theorem's hypothesis. Thus, this case is impossible.

- (3) **Case (III):** $\alpha(r) = r^{-1}$ and $\alpha(s) = s$. Then $\alpha(r^{-1}) = r$ and $\alpha(sr^k) = \alpha(s)\alpha(r)^k = s(r^{-1})^k = sr^{-k}$. Similar to Case(II), we obtain $sr^{-k} = sr^k$, so $r^{-k} = r^k$, and $r^{2k} = 1$. This means $2k \equiv 0 \pmod{n}$. Therefore, similar to Case(II), this case is also impossible.
- (4) **Case (IV):** $\alpha(r) = r^{-1}$ and $\alpha(s) = sr^k$. Then $\alpha(r^{-1}) = r$ and $\alpha(sr^k) = \alpha(s)\alpha(r)^k = (sr^k)(r^{-1})^k = sr^k r^{-k} = s$. Thus $\alpha(S) = S$ and α is the automorphism ϕ from Claim 7.1.

Since these are the only four possibilities for α acting on the generators, the only automorphisms in $\text{Aut}(\Gamma)_e$ are id and ϕ . Hence, $\text{Aut}(\Gamma)_e = \{\text{id}, \phi\} = \text{Aut}(G, S)$ and we are done. $\square$