Scientific Research Publishing

Journal of Applied Mathematics and Physics, 2020, 8, 3075-3084
https://www.scirp.org/journal/jamp
ISSN Online: 2327-4379
ISSN Print: 2327-4352

Automorphism Groups of Cubic Cayley Graphs of Dihedral Groups of Order $2^n p^m$ ($n \geq 2$ and p Odd Prime)

Xianfen Kong

Department of Foundational Mathematics, Xi'an Jiaotong-Liverpool University, Suzhou, China
Email: xianfen.kong@xjtlu.edu.cn

How to cite this paper: Kong, X.F. (2020) Automorphism Groups of Cubic Cayley Graphs of Dihedral Groups of Order $2^n p^m$ ($n \geq 2$ and p Odd Prime). *Journal of Applied Mathematics and Physics*, **8**, 3075-3084.
https://doi.org/10.4236/jamp.2020.812226

Received: December 10, 2020
Accepted: December 28, 2020
Published: December 31, 2020

Abstract

For a prime p, let $D_{2^n p^m}$ be the dihedral group $< a,b \mid a^{2^{n-1}p^m} = b^2 = 1, b^{-1}ab = a^{-1} >$ of order $2^n p^m$ and $Cay(G,S)$ be a connected cubic Cayley graph on G with respect to a generating system of three elements S such that S does not contain the identity and $S^{-1} = S$. In this paper, the automorphism groups of cubic Cayley graphs of dihedral groups of order $2^n p^m$ where $n \geq 2$ and p is odd prime are completely given. When $S \equiv \{b, ab, a^{2^{n-1}p^m} b\}$, the automorphism group $Aut(Cay(G,S)) \cong \mathbb{Z}_2^{2^{n-2}p^m} \rtimes D_{2^{n-1}p^m}$. Except in this case, the automorphism group $Aut(Cay(G,S))$ is the semidirect product $R(G) \rtimes Aut(G,S)$ where $R(G)$ is the right regular representation of G and $Aut(G,S) = \{\alpha \in Aut(G) \mid S^\alpha = S\}$.

Keywords

Automorphism Group, Dihedral Group, Cayley Graph

1. Introduction

An *automorphism* of a graph X is a permutation σ of vertex set of X with the property that, for any vertices u and v, we have $\{u^\sigma, v^\sigma\}$ is an edge of X if and only if $\{u,v\}$ is the edge of X. As usual, we use u^σ to denote the image of the vertex u under the permutation σ and $\{u,v\}$ to denote the edge joining vertices u and v. All automorphisms of graph X form a group under the composite operation of mapping. This group is called the *full automorphism group* of graph X, denoted by A in this paper.

For a graph *X*, we denote vertex set and edge set of X by $V(X)$ and $E(X)$. A_v is the stabilizer of vertex v in the automorphism group of *X*. $X_k(v)$ denotes the set of vertices at distance *k* from vertex *v*. D_{2n} means the dihedral group of order 2*n*. A graph is called *vertex-transitive* if its automorphism group *A* is transitive on the vertex set $V(X)$. An *s-arc* in a graph is an ordered $(s+1)$-tuple $(v_0, v_1, \ldots, v_{s-1}, v_s)$ of vertices of the graph such that v_{i-1} is adjacent to v_i for $1 \le i \le s$ and $v_{i-1} \ne v_{i+1}$ for $1 \le i \le s$. A graph is said to be *s-arc-transitive* if the automorphism group *A* acts transitively on the set of all s-arcs in *X*. When $s = 1$, 1-arc called *arc* and 1-arc transitive is called *arc-transitive* or *symmetric*.

Throughout this paper, graphs are finite, simple and undirected.

Let *G* be a finite group and *S* be a subset of *G* such that $1 \notin S$. The *Cayley graph* $X = Cay(G, S)$ on *G* with respect to *S* is defined to have vertex set $V(X) = G$ and edge set $E(X) = \{\{g, sg\} \mid g \in G \text{ and } s \in S\}$. Let set $S^{-1} = \{s^{-1} \mid s \in S\}$. If $S^{-1} = S$, $Cay(G, S)$ is undirected. If *S* is a generating system of *G*, $Cay(G, S)$ is connected. Two subsets *S* and *T* of group *G* are called *equivalent* if there exists a group automorphism of group *G* mapping *S* to *T*: $S^\alpha = T$ for some $\alpha \in Aut(G)$. Denote by $S \equiv T$. If *S* and *T* are equivalent, Cayley graphs $Cay(G, S)$ and $Cay(G, S)$ are isomorphic.

The right regular representation $R(G)$ of group *G* is a subgroup of the the automorphism group *A* of the Cayley graph *X*. In particular by [1], if $R(G)$ is the full automorphism group of *X* then $X = Cay(G, S)$ is called a *GRR* (for *graphical regular representation*) of *G*. A Cayley graph is *normal* if $R(G)$ is a normal subgroup of *A*. $R(G)$ is transitive on *G* hence Cayley graph is vertex-transitive. Denote $Aut(G, S) = \{\alpha \in Aut(G) \mid S^\alpha = S\}$, the set of all automorphism of group *G* preserving *S*. $Aut(G, S)$ is also a subgroup of the automorphism group of Cayley graph. In particular, $Aut(G, S)$ is a subgroup of stabilizer of vertex identity A_1. By [2] the normalizer of $R(G)$ in *A* is the semi-direct product of $R(G)$ and $Aut(G, S)$: $N_A(R(G)) = R(G) \rtimes Aut(G, S)$. By [3] Proposition 1.5 *X* is normal if and only if $A_1 = Aut(G, S)$. Cayley graph *X* is normal if and only if the automorphism group of *X* is $A = R(G) \rtimes Aut(G, S)$. Normality provides an approach to find automorphism groups of Cayley graphs.

In [4] the automorphism group of connected cubic Cayley graphs of order 4*p* is given. In [5] the automorphism group of connected cubic Cayley graphs of order 32*p* is given. In this paper, the automorphism group of connected cubic Cayley graphs of dihedral groups of order $2^n p^m$ where $n \ge 2$ and *p* is odd is given.

Summarising theorem 4.1, 4.2, 4.3 in Part 4 gives the main results.

Theorem 1.1. Let $G = D_{2^n p^m}$ be a dihedral group where $n \ge 2$ and *p* is an odd prime number. *S* is an inverse-closed generating system of three elements without identity element. Then Cayley graph $Cay(G, S)$ is *GRR* except the following cases:

1) $S \equiv \{b, ab, a^k b\}$ where $k^2 \equiv 1\left(\bmod 2^{n-1} p^m\right)$ and $\gcd(k, 2^{n-1} p^m) = 1$, $Aut(X) \cong G : \mathbb{Z}_2$.

2) $S \equiv \{b, ab, a^{2^{n-1} p^m} b\}$, $Aut(X) \cong \mathbb{Z}_2^{2^{n-2} p^m} \rtimes D_{2^{n-1} p^m}$.

3) $S \equiv \{a, a^{-1}, b\}$, $Aut(X) = G : \mathbb{Z}_2$.

4) $S \equiv \{b, ab, a^{2^{n-2} p^m}\}$, $Aut(X) = G : \mathbb{Z}_2$.

2. Preliminary

Results used to prove main theorem are listed here.

Proposition 2.1. Suppose that $G = < a, b \mid a^n = b^2 = 1, b^{-1} ab = a^{-1} >$ is a dihedral group, then the automorphism group $Aut(G)$ of G has the following properties.

1) Any automorphism of G can be defined as $a \mapsto a^i$ and $b \mapsto a^j b$ where $i \in \mathbb{Z}_n^*$ and $j \in \mathbb{Z}_n$.

2) $Aut(G) = < \alpha > \rtimes < \beta > \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$ where $\alpha : a \mapsto a, b \mapsto ab; \beta : a \mapsto a^i, b \mapsto b, i \in \mathbb{Z}_n^*$.

Proposition 2.2. Suppose G is a finite group and subsets $S \equiv T$, then $Cay(G, S) \cong Cay(G, T)$.

Proposition 2.3. Let $G = < a, b \mid a^n = b^2 = 1, b^{-1} ab = a^{-1} >$ be the dihedral group of order $2n$. Subsets $\{b, ab, a^k b\} \equiv \{b, ab, a^{1-k} b\}$.

Proof Let $\sigma \in Aut(G) : a \mapsto a^{-1}, b \mapsto ab$ then $\{b, ab, a^k b\}^\sigma = \{b, ab, a^{1-k} b\}$.

The following sufficient and necessary condition of normality of Cayley graph is from paper [6].

Proposition 2.4. Let $X = Cay(G, S)$ be connected. Then X is a normal Cayley graph of G if and only if the following conditions are satisfied:

1) For each $\varphi \in A_1$ there exists $\sigma \in Aut(G)$ such that $\varphi|_{X_1(1)} = \sigma|_{X_1(1)}$;

2) For each $\varphi \in A_1$, $\varphi|_{X_1(1)} = 1_{X_1(1)}$ implies $\varphi|_{X_2(1)} = 1_{X_2(1)}$.

A classification of locally primitive Cayley graphs of dihedral groups from paper [7] will be used.

Proposition 2.5. Let X be a locally-primitive Cayley graph of a dihedral group of order $2n$. Then one of the following statements is true, where q is a prime power.

1) X is 2-arc-transitive, and one of the following holds:

a) $X = K_{2n}, K_{n,n}$ or $K_{n,n} - nK_2$;

b) $X = \mathcal{HD}(11, 5, 2)$ or $\mathcal{HD}(11, 6, 2)$, the incidence or non-incidence graph of the Hadamard design on 11 points;

c) $X = \mathcal{PH}(d, q)$ or $\mathcal{PH}'(d, q)$, the point-hyperplane incidence or non-incidence graph of $(d-1)$-dimension projective geometry $PG(d-1, q)$, where $d \ge 3$;

d) $X = K_{q+1}^{2d}$, where d is a divisor of $\frac{q-1}{2}$ if $q \equiv 1$ (mod 4), and a divisor of $q-1$ if $q \equiv 3$ (mod 4) respectively.

2) $X = \mathcal{ND}_{2n,r,k}$ is a normal Cayley graph and is not 2-arc-transitive, where $n = r^t p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} \ge 13$ with $r, p_1, p_2, \cdots, p_s$ distinct odd primes, $t \le 1$, $s \ge 1$ and $r \mid (p_i - 1)$ for each *i*. There are exactly $(r-1)^{s-1}$ non-isomorphism such

graphs for a given order $2n$.

3. Lemmas and Propositions

In the following, group G means that $G=<a,b\,|\,a^{2^{n-1}p^m}=b^2=1, b^{-1}ab=a^{-1}>$ be dihedral group of order $2^n p^m$ where $n\ge 2$ and p is an odd prime number.

Proposition 3.1. If $S=\{a^ib,a^jb,a^rb\}$ is a generating system of G of three elements, then $S\equiv\{b,ab,a^kb\}$ for some $2\le k\le 2^{n-1}p^m-1$.

There are two types of S classified by the number of subsets of two elements generating G.

Type 1: S has only one subset of two elements generating G.

Type 2: S has exactly two subsets of two elements generating G. In this case, $S\equiv\{b,ab,a^kb\}$ where $\gcd(k,2^{n-1}p^m)=1$.

The proof of Proposition 3.1 will be done by the following three lemmas.

Lemma 3.1. If $S=\{a^ib,a^jb,a^rb\}$ is a generating system of G of three elements, then S is equivalent to a subset of type $\{b,ab,a^kb\}$ for some $2\le k\le 2^{n-1}p^m-1$.

Proof By proposition 2.1 in preliminary, automorphism group Aut(G) of dihedral group G is transitive on the set of involutions $\{a^ib\,|\,0\le i\le 2^{n-1}p^m-1\}$. One may assume that $b\in S$ and $S=\{b,a^ib,a^jb\}$ be a generating system of G of three elements. S has three subsets of two elements: $\{b,a^ib\},\{b,a^jb\}$ and $\{a^ib,a^jb\}$.

Note that, subset $T\subset G$ is a generating system of G if and only if T^α is a generating system of G for any $\alpha\in Aut(G)$.

Suppose that subset $\{b,a^xb\}$ ($x=i$ or j) generates G. Let $\alpha\in Aut(G)$: $a\mapsto a^x, b\mapsto b$, then $\{b,ab,a^kb\}^\alpha=\{b,a^ib,a^jb\}$ for some $k\ne 0,1$. Hence $S\equiv\{b,ab,a^kb\}$.

Assume that both subset $\{b,a^ib\}$ and $\{b,a^jb\}$ do not generate G. Next will show that $\{a^ib,a^jb\}$ must be able to generate G.

$G=<S>=<b,a^ib,a^jb>=<a^i,a^j><b>=<a^{\gcd(i,j)}><b>$. Hence $\gcd(i,j)$ and $2^{n-1}p^m$ are mutually prime.

$G\ne<b,a^ib>=<a^i><b>$. Hence i and $2^{n-1}p^m$ are not mutually prime.

Similarly, $G\ne<b,a^jb>$ implies that j and $2^{n-1}p^m$ are also not mutually prime.

$(\gcd(i,j),2^{n-1}p^m)=1$, $(i,2^{n-1}p^m)\ne 1$ and $(j,2^{n-1}p^m)\ne 1$ imply that, for i and j, one number is power of 2 and the other one is power of p. Thus $i-j$ and $2^{n-1}p^m$ are mutually prime.

Hence, $\{a^ib,a^jb\}$ is a generating system of G since $<a^ib,a^jb>=<a^{i-j}><a^ib>=G$.

Let $\alpha\in Aut(G)$: $a\mapsto a^{i-j}, b\mapsto a^jb$. Then $\{b,ab,a^kb\}^\alpha=\{b,a^ib,a^jb\}$ for some k. $S\equiv\{b,ab,a^kb\}$. ■

Corollary 3.1. If $S=\{a^ib,a^jb,a^rb\}$ is a generating system of G of three elements, there exists at least one subset of two elements generating G.

Lemma 3.2. If $S=\{a^ib,a^jb,a^rb\}$ is a generating system of G of three elements, there are only one or two subsets of two elements of S generating *G*.

Proof By Lemma 3.1, we assume that $S=\{b,ab,a^kb\}$ where $k\neq 0,1$. S has three subsets of two elements: $\{b,ab\},\{b,a^kb\}$ and $\{ab,a^kb\}$. Next we will show that it is impossible that all three subsets of two elements generating *G*.

$<b,a^kb>=<a^k><b>$ is a dihedral subgroup of *G*. $<ab,a^kb>=<a^{k-1}><ab>$ is also a dihedral subgroup of *G*.

For k and $k-1$, one is an even number and the other one is an odd number. The orders of elements a^k and a^{k-1} are different: $\circ(a^k)\neq\circ(a^{k-1})$. This implies that at least one subset of $\{b,a^kb\}$ and $\{ab,a^kb\}$ does not generate *G*.

Hence there are only one or two subsets of two elements of *S* generating *G*. ■

Lemma 3.3. Let $S=\{a^ib,a^jb,a^rb\}$ be a generating system of *G* of three elements and *S* has two subsets of two elements generating *G*. If $S\equiv\{b,ab,a^kb\}$, either $\gcd(k,2^{n-1}p^m)=1$ or $\gcd(1-k,2^{n-1}p^m)=1$.

Proposition 3.2. Suppose that $S=\{a^ib,a^jb,a^rb\}$ is a generating system of *G* of three elements and $S\equiv\{b,ab,a^kb\}$.

(1) If *S* has only one subset of two elements generating *G*, then $Aut(G,S)=1$.

(2) If *S* has two subsets of two elements generating *G*, then $Aut(G,S)=1$ except the following two cases. $Aut(G,S)\cong\mathbb{Z}_2$ if $k^2\equiv 1(\bmod 2^{n-1}p^m)$ and $\gcd(k,2^{n-1}p^m)=1$; $Aut(G,S)\cong\mathbb{Z}_2$ if $(1-k)^2\equiv 1(\bmod 2^{n-1}p^m)$ and $\gcd(1-k,2^{n-1}p^m)=1$.

Proof (1) If there is only one subset of two elements in $S=\{b,ab,a^kb\}$ generating *G*, then $G\neq<b,a^kb>$, $G\neq<ab,a^kb>$ and $G=<b,ab>$. For any $\sigma\in Aut(G,S)$, $\{b,ab\}^\sigma$ is also a generating system of *G*. $\{b,ab\}^\sigma=\{b,ab\}$. Since $S^\sigma=S$. Hence $a^kb=S-\{b,ab\}$ is fixed by σ. $(a^kb)^\sigma=a^kb$.

If $b^\sigma=b$ and $(ab)^\sigma=ab$ then $a^\sigma=(abb)^\sigma=(ab)^\sigma b^\sigma=abb=a$, hence $\sigma=1$.

If $b^\sigma=ab$ and $(ab)^\sigma=b$, then $a^\sigma=(abb)^\sigma=(ab)^\sigma b^\sigma=bab=a^{-1}$. This implies that $a^kb=(a^kb)^\sigma=(a^k)^\sigma b^\sigma=a^{-k}ab=a^{1-k}b$. Thus $a^k=a^{1-k}$. This is a contradiction. For *k* and $1-k$, one is an even number and the other one is an odd number. This implies that the orders of the element a^k and a^{1-k} are not equal: $\circ(a^k)\neq\circ(a^{1-k})$.

Hence $Aut(G,S)=1$.

(2) If there are two subsets of two elements of *S* generating *G*, we assume that $\gcd(k,2^{n-1}p^m)=1$. $G=<b,ab>=<b,a^kb>$ and $G\neq<ab,a^kb>$.

Since subset $\{ab,a^kb\}$ is the only subset of two elements not generating *G*, $\{ab,a^kb\}^\sigma=\{ab,a^kb\}$ for any $\sigma\in Aut(G,S)$. $b=S-\{ab,a^kb\}$ is fixed by σ. $(ab)^\sigma=ab$ or a^kb.

If $(ab)^\sigma=ab$, then $\sigma=1$.

If $(ab)^\sigma=a^kb$, then $a^\sigma=(abb)^\sigma=(ab)^\sigma b^\sigma=a^kbb=a^k$. $(a^kb)^\sigma=(a^k)^\sigma b^\sigma=(a^k)^kb=a^{k^2}b=ab$. So $k^2\equiv 1(\bmod 2^{n-1}p^m)$.

Hence $Aut(G,S)=1$ if $k^2\not\equiv 1(\bmod 2^{n-1}p^m)$. $Aut(G,S)\cong\mathbb{Z}_2$ if $k^2\equiv 1(\bmod 2^{n-1}p^m)$.

Similarly, when $\gcd(1-k,2^{n-1}p^m)=1$, $Aut(G,S)=1$ if $(1-k)^2 \not\equiv 1(\bmod 2^{n-1}p^m)$. $Aut(G,S)\cong \mathbb{Z}_2$ if $(1-k)^2 \equiv 1(\bmod 2^{n-1}p^m)$. ■

Proposition 3.3. Suppose that *S* is inverse-closed generating system of three elements of *G*, then $S\equiv\{a,a^{-1},b\}$, $\{b,ab,a^{2^{n-2}p^m}\}$ or $\{b,ab,a^kb\}(k\neq 0,1)$.

Proof Since *S* contains three elements and inverse-closed, there must be an involution in *S*. There are two orbits of involutions in *G* under the action of group automorphism $Aut(G)$: $\{a^{2^{n-2}p^m}\}$ and $\{a^ib \mid 0\le i\le 2^{n-1}p^m-1\}$.

Suppose that $a^{2^{n-2}p^m}\in S$. $S-\{a^{2^{n-2}p^m}\}$ is also inverse-closed hence it is a set of two involutions from orbit $\{a^ib \mid 0\le i\le 2^{n-1}p^m-1\}$. *S* generating *G* implies that $S-\{a^{2^{n-2}p^m}\}$ also generates *G*. We get $S\equiv\{b,ab,a^{2^{n-2}p^m}\}$.

Suppose that *S* contains an involution from $\{a^ib \mid 0\le i\le 2^{n-1}p^m-1\}$. $Aut(G)$ is transitive on this orbit, we can assume that $b\in S$. If $S-\{b\}$ contains an involution, $S\equiv\{b,ab,a^kb\}(k\neq 0,1)$ by Proposition 3.1 and 2.1. If $S-\{b\}$ contains no involutions, $S\equiv\{b,a,a^{-1}\}$ by Proposition 2.1. ■

4. Results

By Proposition 3.3, we only need to discuss $X=Cay(G,S)$ for $S=\{a,a^{-1},b\},\{b,ab,a^{2^{n-2}p^m}\}$ and $\{b,ab,a^kb\}(k\neq 0,1)$.

Firstly, we discuss $X=Cay(G,\{b,ab,a^kb\})(k\neq 0,1)$.

Theorem 4.1. Suppose that $S=\{a^ib,a^jb,a^mb\}$ is a generating system of three involutions of *G* and $S\equiv\{b,ab,a^kb\}$.

X is GRR except the following cases.

(1) When $\gcd(k,2^{n-2}p^m)=1$, $k^2\equiv 1(\bmod 2^{n-1}p^m)$ and $k\neq 2^{n-2}p^m+1$ then $Aut(X)\cong R(G):\mathbb{Z}_2$.

(2) When $\gcd(1-k,2^{n-2}p^m)=1$, $(1-k)^2\equiv 1(\bmod 2^{n-1}p^m)$ and $k\neq 2^{n-2}p^m$ then $Aut(X)\cong R(G):\mathbb{Z}_2$.

(3) If $k=2^{n-2}p^m+1$ or $k=2^{n-2}p^m$, then $Aut(X)\cong \mathbb{Z}_2^{2^{n-2}p^m}\rtimes D_{2^{n-1}p^m}$.

Proof Let $S=\{b,ab,a^kb\}$ where $2\le k\le 2^{n-1}p^m-1$ and $X=Cay(G,S)$. Classify *X* in two cases: there are 4-cycles in *X* and there is no 4-cycle in *X*.

(1) Note that $X_2(1)=\{a,a^k,a^{-1},a^{k-1},a^{-k},a^{1-k}\}$ is the set of vertices at distance 2 from vertex 1.

If there are 4-cycles in *X*, some vertices in $X_2(1)$ are coincident. Solving $a=a^{k-1}$ and $a^{-1}=a^{1-k}$ we get $k=2$. Solving $a=a^{-k}$ and $a^k=a^{-1}$ we get $k=-1$. Solving $a^k=a^{-k}$ we get $k=2^{n-2}p^m$. Solving $a^{k-1}=a^{1-k}$ we get $k=2^{n-2}p^m+1$. There is no solution for other equations. Note that -1 and $2^{n-2}p^m+1$ are two solutions of equation $k^2\equiv 1(\bmod 2^{n-1}p^m)$. 2 and $2^{n-2}p^m$ are two solutions of equation $(1-k)^2\equiv 1(\bmod 2^{n-1}p^m)$. Since $\{b,ab,a^2b\}\equiv\{b,ab,a^{-1}b\}$ and $\{b,ab,a^{2^{n-2}p^m}b\}\equiv\{b,ab,a^{2^{n-2}p^m+1}b\}$ we only discuss $k=2$ and $k=2^{n-2}p^m$.

(1.1) When $k=2$, $X=C_{2^{n-1}p^m}\times K_2$ is a cylinder as **Figure 1**. Hence $A\cong D_{2^np^m}\times\mathbb{Z}_2$.

(1.2) When $k=2^{n-2}p^m$, *X* is a thickened 2-cover of the cycle graph $C_{2^{n-1}p^m}$ as **Figure 2**. All 4-cycles in *X* form an imprimitive block system of *A* and the

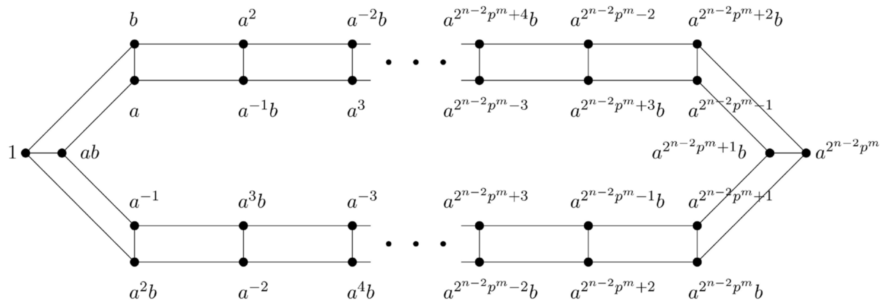

Figure 1. $X = Cay(G,\{b,ab,a^2b\})$.

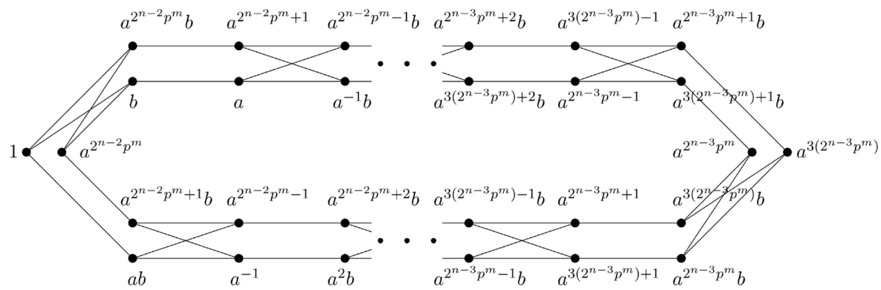

Figure 2. $X = Cay(G,\{b,ab,a^{2^{n-2}p^m}b\})$.

kernel of the action of A on the imprimitive block system is isomorphic to $\mathbb{Z}_2^{2^{n-2}p^m}$. Thus $A \cong Z_2^{2^{n-2}p^m} \rtimes D_{2^{n-1}p^m}$.

(2) Suppose that there is no 4-cycle in X. We will count 6-cycles passing through vertex 1.

$X_3(1) = \{a^{-k}b, a^{-1}b, a^{1-k}b, a^{2-k}b, a^{k-1}b, a^{k+1}b, a^2b, a^{2k-1}b, a^{2k}b\}$ is the set of vertices at distance 3 from vertex 1.

a) Solving $a^{2k}b = a^{2-k}b$ and $a^{2k-1}b = a^{1-k}b$, we get $3k \equiv 2(\text{mod}\, 2^{n-1}p^m)$. Solving $a^{2k}b = a^{1-k}b$ and $a^{2k-1}b = a^{-k}b$, we get $3k \equiv 1(\text{mod}\, 2^{n-1}p^m)$. Solving $a^{k-1}b = a^2b$ and $a^{-1}b = a^{2-k}b$ we get $k = 3$. Solving $a^{-k} = a^2$ and $a^{k+1} = a^{-1}$ we get $k = -2$. There is no solution for other equations.

The induced subgraph of the set of vertices at distance less than or equal to 3 from vertex 1 in X are isomorphic in these four cases. The following uses $Cay(G,\{b,ab,a^3b\})$ as representative to discuss. See **Figure 3**.

We count the number of 6-cycles passing through vertex 1. There are four 6-cycles through edge $\{1,b\}$. There are five 6-cycles through edge $\{1,ab\}$. There are three 6-cycles through edge $\{1,a^3b\}$. For any $\sigma \in A_1$, A_1 fixes edged $\{1,b\},\{1,ab\},\{1,a^3b\}$ and hence σ fixes vertices set $X_1(1) = \{b,ab,a^3b\}$ pointwise. σ fixes all vertices on X by the connectivity of X and the transitivity of A on $V(X)$. Hence $A_1 = 1$. X is GRR.

b) Suppose that $k \not\equiv 3$, $k \not\equiv -2$, $3k \not\equiv 2$, $3k \not\equiv 1$ (mod $2^{n-1}p^m$). Then the induced subgraph of the set of vertices at distance less than or equal to 3 from vertex 1 in X is the as **Figure 4**.

Firstly, show that the action of A_1 on $X_1(1)$ is faithful.

Let $\sigma \in A_1$ and σ fixes $X_1(1)$ pointwise. Passing through vertices $\{1,b,ab\}$,

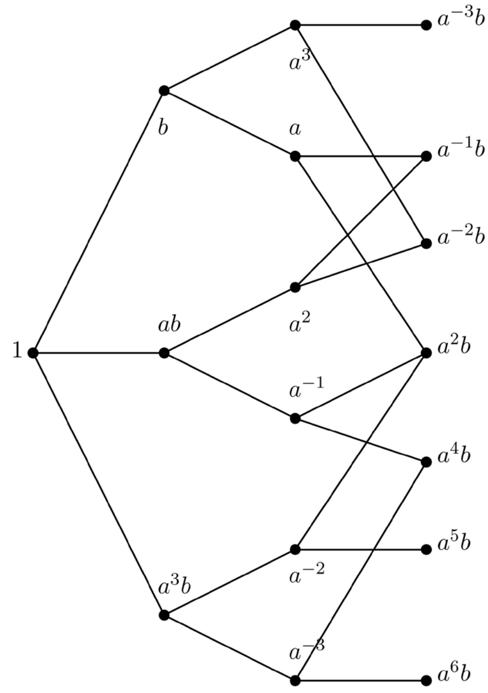

Figure 3. $X =$ induced subgraph of $Cay(G,\{b,ab,a^3b\})$.

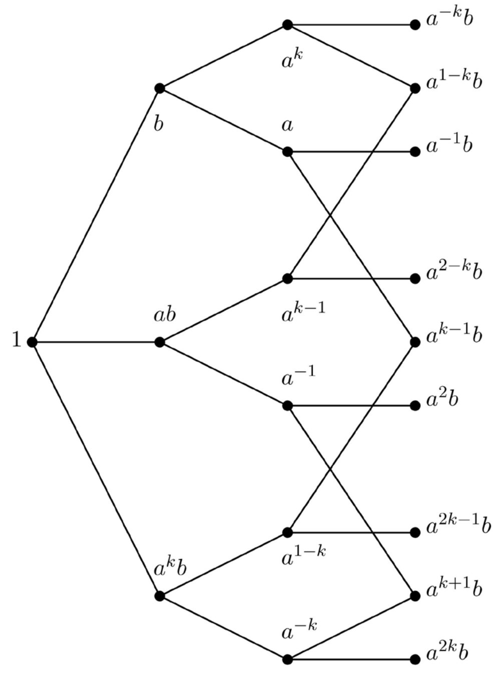

Figure 4. $X =$ induced subgraph $Cay(G,\{b,ab,a^kb\})$.

there is a unique 6-cycle $[1,b,a^k,a^{1-k}b,a^{k-1},ab] \triangleq C_1$. Passing through vertices $\{1,b,a^kb\}$, there is a unique 6-cycle $[1,b,a,a^{k-1}b,a^{1-k},a^kb] \triangleq C_2$. Passing through vertices $\{1,ab,a^kb\}$, there is a unique 6-cycle $[1,ab,a^{-1},a^{k+1}b,a^{-k},a^kb] \triangleq C_3$. For any $\alpha \in A$, the image of a cycle of length *l* under α is also a cycle of length *l*. Note that $\sigma \in A_1$ fixes $\{1,b,ab,a^kb\}$ pointwise, hence C_1^σ is also a 6-cycle passing through vertices $1, b, ab$. Hence $C_1^\sigma = C_1$. Follow the same argument, $C_2^\sigma = C_2, C_3^\sigma = C_3$. So σ fixes all vertices on cycles C_1, C_2, C_3. In particular, σ fixes $X_2(1)$ pointwise. By the connectivity of X and the transitivity of A on $V(X)$, we get A_1 acts on $X_1(1) = S$ faithfully.

Next, show that X is normal.

A_1 acting on $X_1(1)$ faithfully implies that A_1 is isomorphic to a subgroup of symmetric group of degree 3. $A_1 \lesssim S_3$.

If $A_1 \cong A_3$ or S_3, then A_1 is transitive on $X_1(1)$. Since $|X_1(1)| = 3$ is prime, X is a locally-primitive Cayley graph. Theorem 1.5 in [7] gives a classification of locally primitive Cayley graphs of dihedral groups which has been listed as Proposition 2.5 in this paper.

Since the order of G is $2^n p^m$ where $n \ge 2$ and p is odd, $Cay(G, S)$ is not on the list of locally-primitive Cayley graphs. Thus, A_1 is not transitive on $X_1(1)$. $A_1 \cong \mathbb{Z}_1$ or $\mathbb{Z}_2$. $|A : R(G)| = |A_1| = 1$ or 2, $R(G) \trianglelefteq A$. X is normal. $A = R(G) \rtimes Aut(G, S)$.

By Proposition 3.2 and part(1) of this proof, $A = R(G) : \mathbb{Z}_2$ if $k^2 \equiv 1(\bmod 2^{n-1} p^m)$, $k \ne 2^{n-2} p^m + 1$ and $\gcd(k, 2^{n-1} p^m) = 1$ or $(1-k)^2 \equiv 1(\bmod 2^{n-1} p^m)$, $k \ne 2^{n-2} p^m$ and $\gcd(1-k, 2^{n-1} p^m) = 1$. ■

Theorem 4.2. Suppose that $S \equiv \{a, a^{-1}, b\}$, then X is normal and $A = G : \mathbb{Z}_2$.

Proof Suppose that $S \equiv \{a, a^{-1}, b\}$ and $X = Cay(G, S)$. Cayley graph X is also a cylinder as **Figure 5**. Hence $A = D_{2^n p^m} \times \mathbb{Z}_2$. ■

Theorem 4.3. Suppose that $S \equiv \{b, ab, a^{2^{n-2} p^m}\}$, then X is normal and $A = G : \mathbb{Z}_2$.

Proof Suppose that $S \equiv \{b, ab, a^{2^{n-2} p^m}\}$ and $X = Cay(G, S)$. The Cayley graph is an Möbius ladder as **Figure 6**. Hence, $A = D_{2^n p^m} \rtimes \mathbb{Z}_2$. ■

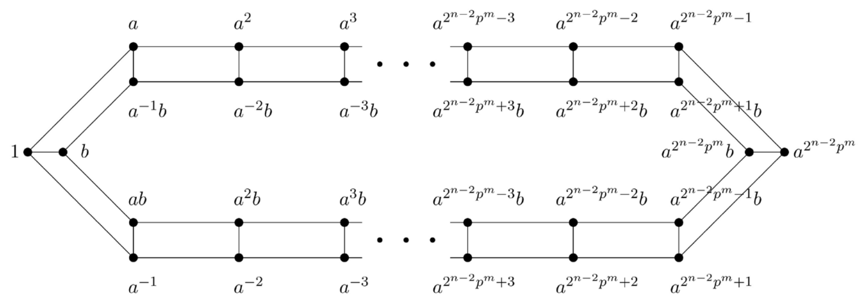

Figure 5. $X = Cay(G, \{a, a^{-1}, b\})$

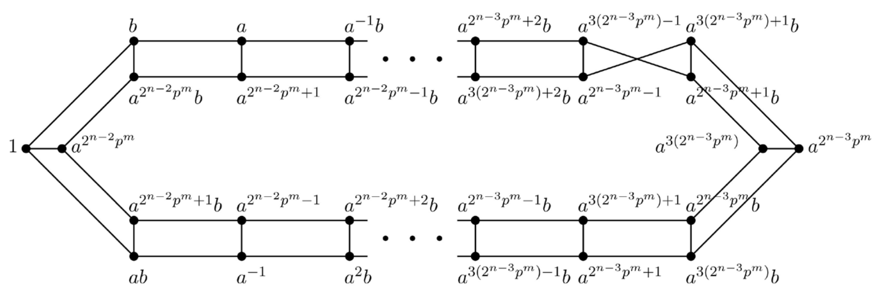

Figure 6. $X = Cay(G, \{b, ab^{-1}, a^{2^{n-2}} p^m\})$

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Godsil, C.D. (1981) GRRs for Nonsolvable Groups. In: *Algebraic Methods in Graph Theory*, Colloq. Math. Soc. Janos Bolyai, Amsterdam-New York, Vol. I, II (Szeged, 1978), 221-239.

[2] Godsil, C.D. (1981) On the Full Automorphism Group of a Graph. *Combinatorica*, **1**, 243-256. https://doi.org/10.1007/BF02579330

[3] Xu, M.Y. (1998) Automorphism Groups and Isomorphisms of Cayley Digraphs. *Discrete Mathematics*, **182**, 309-319. https://doi.org/10.1016/S0012-365X(97)00152-0

[4] Zhou, C.X. and Feng, Y.-Q. (2007) Automorphism Groups of Connected Cubic Cayley Graphs of Order 4*p*. *Algebra Colloquium*, **14**, 351-359. https://doi.org/10.1142/S100538670700034X

[5] Xie, J.H., Yang, X. and Xu, S.J. (2019) The Normality of 3-Valent Cayley Graphs of Dihedral Groups of Order 32*p*. *Journal of Guangxi Teachers Education University* (*Natural Science Edition*), **36**, 6-12.

[6] Pan, J.M. (2014) Locally Primitive Cayley Graphs of Dihedral Groups. *European Journal of Combinatorics*, **36**, 39-52. https://doi.org/10.1016/j.ejc.2013.06.041

[7] Wang, C.Q., Wang, D.J. and Xu, M.Y. (1998) Normal Cayley Graphs of Finite Groups. *Science in China* (*Series A*), **41**, 242-251. https://doi.org/10.1007/BF02879042