creative commons

ARS MATHEMATICA CONTEMPORANEA

ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 15 (2018) 205–223
https://doi.org/10.26493/1855-3974.1419.3e9
(Also available at http://amc-journal.eu)

Enumerating regular graph coverings whose covering transformation groups are $\mathbb{Z}_2$-extensions of a cyclic group*

Jian-Bing Liu †
Mathematics, Beijing Jiaotong University, Beijing, 100044, P.R. China

Jaeun Lee
Mathematics, Yeungnam University, Kyongsan, 38541 Korea

Jin Ho Kwak
Mathematics, POSTECH, Pohang, 37673 Korea
Mathematics, Beijing Jiaotong University, Beijing, 100044, P.R. China

Received 9 June 2017, accepted 12 October 2017, published online 20 June 2018

Abstract

Several types of the isomorphism classes of graph coverings have been enumerated by many authors. In 1988, Hofmeister enumerated the double covers of a graph, and this work was extended to n-fold coverings of a graph by the second and third authors. For *regular* coverings of a graph, their isomorphism classes were enumerated when the covering transformation group is a finite abelian or dihedral group. In this paper, we enumerate the isomorphism classes of graph coverings when the covering transformation group is a $\mathbb{Z}_2$-extension of a cyclic group, including generalized quaternion and semi-dihedral groups.

Keywords: Graphs, regular coverings, voltage assignments, enumeration, Möbius functions (on a lattice), group extensions.

Math. Subj. Class.: 05C30, 20F28, 20K27

*The authors are grateful to anonymous referees for their valuable comments. The authors also would like to thank Young-Soo Kwon for illuminating discussions and remarks. This work was partially supported by the National Natural Science Foundation of China (11671030).

†Corresponding author
E-mail addresses: jl0068@mix.wvu.edu (Jian-Bing Liu), julee@ynu.ac.kr (Jaeun Lee), jinkwak@postech.ac.kr (Jin Ho Kwak)

This work is licensed under https://creativecommons.org/licenses/by/3.0/

1 Introduction

Throughout this paper, all graphs and groups are assumed to be finite. Let G be a connected simple graph with vertex set $V(G)$ and edge set $E(G)$. The *neighborhood* of a vertex $v \in V(G)$, denoted by $N(v)$, is the set of vertices adjacent to v. We use $|X|$ for the cardinality of a set X. The number $\beta = |E(G)| - |V(G)| + 1$ is equal to the number of independent cycles in G and it is referred to as the *Betti number* of G.

Two graphs G and H are *isomorphic* if there exists a one-to-one correspondence between their vertex sets which preserves adjacency, and such a correspondence is called an *isomorphism* between G and H. An *automorphism* of a graph G is an isomorphism of G onto itself. Thus, an automorphism of G is a permutation of the vertex set $V(G)$ which preserves adjacency. Obviously, the automorphisms of G form a permutation group, $\mathrm{Aut}(G)$, under composition, which acts on the vertex set $V(G)$.

A graph $\widetilde{G}$ is called a *covering* of G with projection $p\colon \widetilde{G} \to G$ if there is a surjection $p\colon V(\widetilde{G}) \to V(G)$ such that $p|_{N(\tilde{v})}\colon N(\tilde{v}) \to N(v)$ is a bijection for any vertex $v \in V(G)$ and $\tilde{v} \in p^{-1}(v)$. Also, we sometimes say that the projection $p\colon \widetilde{G} \to G$ is a covering, and an *n-fold covering* if p is n-to-one. A covering $p\colon \widetilde{G} \to G$ is said to be *regular* (simply, *$\mathcal{A}$-covering*) if there is a subgroup $\mathcal{A}$ of the automorphism group $\mathrm{Aut}(\widetilde{G})$ of $\widetilde{G}$ acting freely on $\widetilde{G}$ so that the graph G is isomorphic to the quotient graph $\widetilde{G}/\mathcal{A}$, say by h, and the quotient map $\widetilde{G} \to \widetilde{G}/\mathcal{A}$ is the composition $h \circ p$ of p and h. The *fiber* of an edge or a vertex is its preimage under p.

Two coverings $p_i\colon \widetilde{G}_i \to G$, $i = 1, 2$, are *isomorphic* if there exists a graph isomorphism $\Phi\colon \widetilde{G}_1 \to \widetilde{G}_2$ such that $p_2 \circ \Phi = p_1$, that is, the diagram

$$\begin{array}{ccc} \widetilde{G}_1 & \xrightarrow{\ \Phi\ } & \widetilde{G}_2 \\ & {\scriptstyle p_1}\searrow \quad \swarrow{\scriptstyle p_2} & \\ & G & \end{array}$$

commutes. Such a Φ is called a *covering isomorphism*. A *covering transformation* is just a covering automorphism.

Every edge of a graph G gives rise to a pair of oppositely directed edges. By $e^{-1} = vu$, we mean the reverse edge to a directed edge $e = uv$. We denote the set of directed edges of G by $D(G)$. Let $\mathcal{A}$ be a finite group. An *ordinary voltage assignment* (or, *$\mathcal{A}$-voltage assignment*) of G is a function $\phi\colon D(G) \to \mathcal{A}$ with the property that $\phi(e^{-1}) = \phi(e)^{-1}$ for each $e \in D(G)$. The values of ϕ are called *voltages*, and $\mathcal{A}$ is called the *voltage group*. The *ordinary derived graph* $G \times_\phi \mathcal{A}$ derived from an ordinary voltage assignment $\phi\colon D(G) \to \mathcal{A}$ has as its vertex set $V(G) \times \mathcal{A}$, and as its edge set $E(G) \times \mathcal{A}$, so that an edge (e, g) of $G \times_\phi \mathcal{A}$ joins a vertex (u, g) to $(v, \phi(e)g)$ for $e = uv \in D(G)$ and $g \in \mathcal{A}$. In the (ordinary) derived graph $G \times_\phi \mathcal{A}$, a vertex (u, g) is denoted by u_g and an edge (e, g) is denoted by e_g. The first coordinate projection $p_\phi\colon G \times_\phi \mathcal{A} \to G$ commutes with the left multiplication action of the $\phi(e)$ and the right multiplication action of $\mathcal{A}$ on the fibers, which is free and transitive, so that p_ϕ is a regular $|\mathcal{A}|$-fold covering, called simply an *$\mathcal{A}$-covering*. Moreover, if the covering graph $G \times_\phi \mathcal{A}$ is connected, then the group $\mathcal{A}$ becomes the covering transformation group of the $\mathcal{A}$-covering.

For a group $\mathcal{A}$, let $C^1(G; \mathcal{A})$ denote the set of $\mathcal{A}$-voltage assignments ϕ of G. Choose a spanning tree T of G, and let

$$C^1_T(G; \mathcal{A}) = \{\phi \in C^1(G; \mathcal{A}) : \phi(uv) \text{ is the identity for each } uv \in D(T)\}.$$

Gross and Tucker [4] showed that every $\mathcal{A}$-covering $\widetilde{G}$ of a graph G can be derived from an $\mathcal{A}$-voltage assignment ϕ in $C_T^1(G;\mathcal{A})$, say it *T-reduced.* From now on, let T denote a fixed spanning tree of a graph G, and we consider only an $\mathcal{A}$-voltage assignment ϕ in $C_T^1(G;\mathcal{A})$.

The enumeration problem of coverings became subject of investigation by many authors starting from the classical paper by Hurwitz published more then 100 years ago. In particular, enumeration of graph coverings became possible after the paper by Hall ([6]) published in 1949. In 1988, Hofmeister [8] counted double covers of graphs. Liskovets enumerated connected non-isomorphic coverings of the graph with a given Betti number, see [19, 20]. The number of connected and disconnected coverings were determined by Kwak and Lee in [15]. Later, Kwak, Lee and A. D. Mednykh counted cyclic and dihedral coverings over surfaces and graphs with prescribed topological characteristics, see [16, 17].

Following notations in [14], let $\mathrm{Iso}^R(G;n)$ denote the number of the isomorphism classes of regular (connected or disconnected) n-fold coverings of G, and use $\mathrm{Isoc}^R(G;n)$ for their connected ones. Similarly, let $\mathrm{Iso}(G;\mathcal{A})$ denote the number of the isomorphism classes of (connected or disconnected) $\mathcal{A}$-coverings of G, and use $\mathrm{Isoc}(G;\mathcal{A})$ for their connected ones. By the properties of regularity of coverings, one can see that the number of the isomorphism classes of (connected or disconnected) n-fold regular coverings of a graph G is the sum of numbers of the isomorphism classes of connected d-fold regular coverings of G, where d runs over all divisors of n:

$$\mathrm{Iso}^R(G;n) = \sum_{d|n} \mathrm{Isoc}^R(G;d).$$

Moreover, the number of the isomorphism classes of connected n-fold regular coverings of G is the sum of the numbers of the isomorphism classes of connected $\mathcal{A}$-coverings of G, where $\mathcal{A}$ runs over all non-isomorphic groups of order n:

$$\mathrm{Isoc}^R(G;n) = \sum_{\mathcal{A}} \mathrm{Isoc}(G;\mathcal{A}).$$

Consequently, it just needs to determine the numbers $\mathrm{Isoc}(G;\mathcal{A})$ for every finite group $\mathcal{A}$. Hong, Kwak and Lee [9] obtained an algebraic characterization of two isomorphic graph regular coverings given as follows.

Lemma 1.1. *Let $\phi \in C_T^1(G;\mathcal{A})$ and $\psi \in C_T^1(G;\mathcal{B})$ be any two ordinary voltage assignments in G. If their derived (regular) coverings $p_\phi\colon G\times_\phi \mathcal{A} \to G$ and $p_\psi\colon G\times_\psi \mathcal{B}\to G$ are connected, then they are isomorphic if and only if there exists a group isomorphism $\sigma\colon \mathcal{A}\to\mathcal{B}$ such that $\psi(uv)=\sigma(\phi(uv))$ for all $uv\in D(G)-D(T)$.*

In particular, if two voltages ϕ and ψ in $C_T^1(G;\mathcal{A})$ derive connected coverings, then the derived coverings are isomorphic if and only if there exists a group automorphism $\sigma\in \mathrm{Aut}(\mathcal{A})$ such that

$$\psi(uv)=\sigma(\phi(uv))$$

for all $uv\in D(G)-D(T)$.

With a linear ordering of the cotree edges of G, the set $C_T^1(G;\mathcal{A})$ of T-reduced $\mathcal{A}$-voltage assignments of G can be identified as

$$C_T^1(G;\mathcal{A}) = \mathcal{A}\times\cdots\times\mathcal{A}\ \ (\beta \text{ times}),$$

that is, an $\mathcal{A}$-voltage assignment ϕ of G can be identified as a β-tuple $(g_1, \ldots, g_\beta)$ of group elements $g_i \in \mathcal{A}$. Moreover, such a β-tuple of g's derives a connected covering if and only if it is transitive. It means by definition that the subgroup $\langle g_1, \ldots, g_\beta \rangle$ generated by them acts transitively on the group $\mathcal{A}$ (under the left translation on $\mathcal{A}$), or equivalently $\{g_1, g_2, \ldots, g_\beta\}$ generates the whole group $\mathcal{A}$.

Note that the automorphism group $\mathrm{Aut}(\mathcal{A})$ of $\mathcal{A}$ can act on the set of transitive β-tuples of group elements $g_i \in \mathcal{A}$ coordinatewisely, and any two transitive β-tuples of elements in $\mathcal{A}$ belong to the same orbit under the action if and only if they derive (connected) isomorphic $\mathcal{A}$-coverings, by Lemma 1.1.

Clearly, the $\mathrm{Aut}(\mathcal{A})$-action on the set of transitive β-tuples of group elements $g_i \in \mathcal{A}$ is free (having no fixed element), and hence Burnside's counting Lemma gives a counting formula for $\mathrm{Isoc}(G; \mathcal{A})$ as follows.

Theorem 1.2 ([14])**.** *For any finite group $\mathcal{A}$,*

$$\mathrm{Isoc}(G; \mathcal{A}) = \frac{|\Omega(\mathcal{A}; \beta)|}{|\mathrm{Aut}(\mathcal{A})|},$$

where $\Omega(\mathcal{A}; \beta) = \{(g_1, g_2, \ldots, g_\beta) \in \mathcal{A}^\beta \mid \{g_1, g_2, \ldots, g_\beta\}$ *generates* $\mathcal{A}\}$.

Note that the set $\Omega(\mathcal{A}; \beta)$ can be identified as the set of epimorphisms from the free group generated by β elements onto the group $\mathcal{A}$.

To determine the number $\mathrm{Isoc}(G; \mathcal{A})$, we need to estimate $|\mathrm{Aut}(\mathcal{A})|$ and $|\Omega(\mathcal{A}; \beta)|$. The number $|\mathrm{Aut}(\mathcal{A})|$ can certainly be determined for a few groups $\mathcal{A}$. For example, one can refer to [14] for $|\mathrm{Aut}(\mathcal{A})|$ when $\mathcal{A}$ is abelian or dihedral groups. Also, one can see recent two papers [1], [7] for abelian case.

The other number $|\Omega(\mathcal{A}; \beta)|$ can be determined by a direct counting and it can also be determined in terms of the Möbius function defined on the subgroups lattice of $\mathcal{A}$, as shown in [17]. The Möbius function assigns an integer $\mu(\mathcal{K})$ to each subgroup $\mathcal{K}$ of $\mathcal{A}$ by the recursive formula

$$\sum_{\mathcal{H} \geq \mathcal{K}} \mu(\mathcal{H}) = \begin{cases} 1 & \text{if } \mathcal{K} = \mathcal{A}, \\ 0 & \text{if } \mathcal{K} < \mathcal{A}. \end{cases}$$

Jones ([12, 13]) used the Möbius function to count the normal subgroups of a surface group or a crystallographic group, and applied it to count certain covering surfaces. We see that

$$|\mathcal{A}|^\beta = \sum_{\mathcal{K} \leq \mathcal{A}} |\Omega(\mathcal{K}; \beta)|.$$

It follows from the Möbius inversion that

$$|\Omega(\mathcal{A}; \beta)| = \sum_{\mathcal{K} \leq \mathcal{A}} \mu(\mathcal{K}) |\mathcal{K}|^\beta.$$

The next theorem is deduced from Theorem 1.2.

Theorem 1.3. *For any finite group $\mathcal{A}$,*

$$\mathrm{Isoc}(G; \mathcal{A}) = \frac{1}{|\mathrm{Aut}(\mathcal{A})|} \sum_{\mathcal{K} \leq \mathcal{A}} \mu(\mathcal{K}) |\mathcal{K}|^\beta.$$

Now, we have two ways of computing $|\Omega(\mathcal{A};\beta)|$, by a direct counting and by using the Möbius function on the subgroups lattice of $\mathcal{A}$. For example, when $\mathcal{A}$ is cyclic or dihedral, $\mathrm{Isoc}(G;\mathcal{A})$ was determined by Kwak, Lee and Mednykh in [17] in terms of the Möbius function. However, it is not easy to determine the Möbius function on the subgroups lattice of any abelian group $\mathcal{A}$. For an abelian group $\mathcal{A}$, $\mathrm{Isoc}(G;\mathcal{A})$ was determined in [14] by a direct counting method.

This paper is organized as follows. In a coming section, we review an extension of a group, giving a classification of $\mathbb{Z}_2$-extensions of a cyclic p-group and a discussion on $\mathbb{Z}_2$-extensions of a cyclic group. In Sections 3 and 4, we determine the number $\mathrm{Isoc}(G;\mathcal{A})$ when $\mathcal{A}$ is a $\mathbb{Z}_2$-extension of a cyclic p-group, or $\mathbb{Z}_2$-extensions of any cyclic group, as main results in this paper. In Section 5, we try to extend our discussion to a $\mathbb{Z}_2$-extension of an abelian group, by considering two special cases of them.

2 Review on extensions of groups

We review briefly an extension of a group with some recent results to use it in this paper.

Let $\mathcal{N}$ and $\mathcal{Q}$ be two groups. A group $\mathcal{A}$ is an *extension* of $\mathcal{N}$ by $\mathcal{Q}$ (or a $\mathcal{Q}$-*extension* of $\mathcal{N}$) if $\mathcal{N}$ is a normal subgroup of $\mathcal{A}$ and the quotient group $\mathcal{A}/\mathcal{N} \cong \mathcal{Q}$. Or equivalently, a sequence

$$1 \to \mathcal{N} \xrightarrow{\iota} \mathcal{A} \xrightarrow{\pi} \mathcal{Q} \to 1$$

is exact. The extension is *split* if $\mathcal{N}$ has a complement in $\mathcal{A}$. By a *complement* of $\mathcal{N}$ in $\mathcal{A}$, we mean a subgroup $\mathcal{H}$ satisfying $\mathcal{A} = \mathcal{N}\mathcal{H}$ and $\mathcal{N} \cap \mathcal{H} = 1$. Otherwise, the extension is *nonsplit*.

Let us assume that the given extension is split. For a complement $\mathcal{H}$ of $\mathcal{N}$ in $\mathcal{A}$, one has $\mathcal{H} \cong \mathcal{A}/\mathcal{N}$. So we can view $\mathcal{Q}$ as a subgroup of $\mathcal{A}$. A trivial case is an (internal) direct product of two groups $\mathcal{N}$ and $\mathcal{Q}$: $\mathcal{A} = \mathcal{N}\mathcal{Q}$ with $\mathcal{N} \cap \mathcal{Q} = 1$ and a trivial commutator $[\mathcal{N}, \mathcal{Q}] = 1$. For all nontrivial cases, it holds $\mathcal{A} = \mathcal{N}\mathcal{Q}$ with $\mathcal{N} \cap \mathcal{Q} = 1$, but the commutator $[\mathcal{N}, \mathcal{Q}]$ is not trivial and the multiplication in $\mathcal{N}$ is twisted by an action of the elements of $\mathcal{Q}$, that is, for $n_i \in \mathcal{N}$ and $q_j \in \mathcal{Q}$ with $i, j \in \{1, 2\}$,

$$(n_1 q_1)(n_2 q_2) = n_1 (q_1 n_2 q_1^{-1}) q_1 q_2 = n_1 n_2^{\alpha(q_1)^{-1}} q_1 q_2,$$

where $\alpha \colon \mathcal{Q} \to \mathrm{Aut}(\mathcal{N})$ is a homomorphism defined by $\alpha(q)^{-1} = \mathrm{Inn}(q^{-1})$. The *semidirect product* $\mathcal{A} = \mathcal{N} \rtimes_\alpha \mathcal{Q}$ of $\mathcal{N}$ by $\mathcal{Q}$ with respect to α is defined on the set

$$\mathcal{A} = \{(n, q) \mid n \in \mathcal{N}, q \in \mathcal{Q}\}$$

with a multiplication

$$(n_1, q_1)(n_2, q_2) = (n_1 n_2^{\alpha(q_1)^{-1}}, q_1 q_2).$$

The semidirect product $\mathcal{A} = \mathcal{N} \rtimes_\alpha \mathcal{Q}$ is in fact a group with $(n, q)^{-1} = (n^{-\alpha(q)}, q^{-1})$. If we identify $\mathcal{Q}$ and $\mathcal{N}$ with $\{(1, q) \mid q \in \mathcal{Q}\}$ and $\{(n, 1) \mid n \in \mathcal{N}\}$, respectively, then $\mathcal{A} = \mathcal{N}\mathcal{Q} = \mathcal{Q}\mathcal{N}$ and $\mathcal{N} \cap \mathcal{Q} = 1$. So a semidirect product $\mathcal{A} = \mathcal{N} \rtimes_\alpha \mathcal{Q}$ is a split extension of $\mathcal{N}$ by $\mathcal{Q}$. Consequently an extension of $\mathcal{N}$ by $\mathcal{Q}$ is split if and only if $\mathcal{A}$ is a semidirect product of $\mathcal{N}$ by $\mathcal{Q}$.

A (split or nonsplit) extension of a cyclic group by another cyclic group is called a *metacyclic group*. The next two lemmas are famous in finite group theory, see [11] and [10], respectively.

Lemma 2.1 (Hölder)**.** *Let $\mathcal{A}$ be a metacyclic group which is an extension of a cyclic group of order n by a cyclic group of order m. Then $\mathcal{A}$ has the following presentation*

$$\mathcal{A} = \langle a, b \mid a^n = 1, b^m = a^t, b^{-1}ab = a^r \rangle, \tag{2.1}$$

where n, m, t and r satisfy

$$r^m \equiv 1 \pmod{n}, \quad t(r-1) \equiv 0 \pmod{n}. \tag{2.2}$$

Conversely, for any parameters n, m, t, r satisfying Equation (2.2)*, the relations in Equation* (2.1) *define a metacyclic group which is an extension of a cyclic group of order n by a cyclic group of order m.*

A subgroup $\mathcal{N}$ of $\mathcal{A}$ is a *Hall subgroup* if $|\mathcal{N}|$ is coprime to $|\mathcal{A} : \mathcal{N}|$.

Lemma 2.2 (Schur-Zassenhaus)**.** *Let $\mathcal{N}$ be a normal Hall subgroup of $\mathcal{A}$. Then*

(1) $\mathcal{N}$ has a complement in $\mathcal{A}$.

(2) If $\mathcal{H}$ and $\mathcal{K}$ are two complements of $\mathcal{N}$ in $\mathcal{A}$, then there is an element $n \in \mathcal{N}$ such that $n^{-1}\mathcal{H}n = \mathcal{K}$.

By Lemmas 2.1 and 2.2, one can show that a $\mathbb{Z}_2$-extension of a cyclic p-group with odd prime p is a cyclic or a dihedral group. Now, let $p = 2$.

The following theorems in this section come from an unpublished manuscript [18] Chapter 3 by Kwak and Xu. Since the authors cannot find these theorems in any other sources, we add their proofs in this paper.

Theorem 2.3. *Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic 2-group $\mathbb{Z}_{2^{n-1}}$ with $n \geq 4$. Then $\mathcal{A}$ is isomorphic to one of following six groups.*

(1) (*the cyclic group*)
$\mathbb{Z}_{2^n} = \langle b \mid a^{2^{n-1}} = 1, b^2 = a \rangle$,

(2) (*the non-cyclic abelian group*)
$\mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_2 = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, b^{-1}ab = a \rangle$,

(3) (*the dihedral group*)
$\mathbb{D}_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, b^{-1}ab = a^{-1} \rangle$,

(4) (*the generalized quaternion group*)
$\mathbb{Q}_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^{2^{n-2}}, b^{-1}ab = a^{-1} \rangle$,

(5) (*the ordinary metacyclic group*)
$\mathbb{M}_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, b^{-1}ab = a^{1+2^{n-2}} \rangle$,

(6) (*the semidihedral group*)
$\mathbb{SD}_{2^n} = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = 1, b^{-1}ab = a^{-1+2^{n-2}} \rangle$.

All the six groups are not isomorphic one another.

Proof. Since (1) and (2) are trivial cases, we assume that $\mathcal{A}$ is not abelian. By Lemma 2.1, $\mathcal{A}$ has the following presentation:

$$\mathcal{A} = \langle a, b \mid a^{2^{n-1}} = 1, b^2 = a^t, b^{-1}ab = a^r \rangle,$$

where t and r satisfy

$$r^2 \equiv 1 \pmod{2^{n-1}}, \quad t(r-1) \equiv 0 \pmod{2^{n-1}}.$$

By $\mathcal{A}$ non-abelian, one has $r \equiv -1$ or $\pm 1 + 2^{n-2} \pmod{2^{n-1}}$, the latter two cases can happen only when $n \geq 4$. If $r \equiv -1$ or $-1+2^{n-2} \pmod{2^{n-1}}$, then $2^{n-1} \mid 2t$ and hence $2^{n-2} \mid t$, it follows that $t \equiv 0$ or $2^{n-2} \pmod{2^{n-1}}$. Now we consider the three cases separately.

(i) $r \equiv -1 \pmod{2^{n-1}}$. In this case we get the dihedral group (3) and the generalized quaternion group (4) depending on $t \equiv 0$ or $2^{n-2} \pmod{2^{n-1}}$, respectively. These two groups are not isomorphic. Note that the following cases (ii) and (iii) happen only when $n \geq 4$. So, when $n = 3$ we have only the above two groups.

(ii) $r \equiv -1 + 2^{n-2} \pmod{2^{n-1}}$. In this case $t \equiv 0 \pmod{2^{n-2}}$. Thus $b^2 = 1$ or $a^{2^{n-2}}$. If $b^2 = a^{2^{n-2}}$, letting $b_1 = ba$, then

$$b_1^2 = (ba)^2 = b^2(b^{-1}ab)a = b^2a^{-1+2^{n-2}}a = a^{2^{n-2}}a^{2^{n-2}} = 1.$$

Thus we get the group (6).

(iii) $r \equiv 1 + 2^{n-2} \pmod{2^{n-1}}$. In this case, one has $t \cdot 2^{n-2} \equiv 0 \pmod{2^{n-1}}$ which implies that t is even. Let $t = 2s$. Since $n \geq 4$, there is a j satisfying $j(1 + 2^{n-3}) + s \equiv 0 \pmod{2^{n-2}}$. Let $b_1 = ba^j$. Then

$$b_1^2 = b^2(b^{-1}a^jb)a^j = b^2a^{j(2+2^{n-2})} = a^{2(j(1+2^{n-3})+s)} = 1.$$

Now the generators a, b_1 satisfy the relations in the group (5), with b instead of b_1.

Finally, we shall show that the mentioned four non-abelian groups are not isomorphic, and we assume that $n \geq 4$. It is easy to see that in these four cases the derived group $\mathcal{A}' = \langle [a,b] \rangle$. We calculate the commutator $[a,b]$ and get

$$[a,b] = a^{-1}b^{-1}ab = \begin{cases} a^{-2} & \text{for the groups (3) and (4),} \\ a^{2^{n-2}} & \text{for the group (5),} \\ a^{-2+2^{n-2}} & \text{for the group (6).} \end{cases}$$

So, one has $|\mathcal{A}'| = 2$ for (5), and $|\mathcal{A}'| = 2^{n-2}$ for the others. It follows that the group (5) is not isomorphic to any one of the rest. To prove the rest three groups are not isomorphic, we calculate the square of the elements of the form ba^i outside $\langle a \rangle$. We have

$$(ba^i)^2 = b^2(b^{-1}a^ib)a^i = \begin{cases} 1 & \text{for the group (3),} \\ a^{2^{n-2}} & \text{for the group (4),} \\ a^{i2^{n-2}} & \text{for the group (6).} \end{cases}$$

This shows that the subgroup of order 2^{n-1} in $\mathcal{A}$ is unique, and outside this subgroup $\langle a \rangle$, all elements are of order 2 in the group (3), order 4 in the group (4), and some are of order 2 and the others are of order 4 in the group (6). Therefore, all the four groups are not isomorphic to one another. □

Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n$, where $n = p_0^{\alpha_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ is the prime decomposition with $p_0 = 2$. First, we consider the case that n is odd, that is, $\alpha_0 = 0$.

Theorem 2.4. *Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ with n odd. Then, $\mathcal{A}$ has a presentation*

$$\mathcal{A} = \langle a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = b^2 = 1, [a_i, a_j] = 1, b^{-1} a_i b = a_i^{r_i} \text{ for all } i, j \rangle,$$

where $r_i^2 \equiv 1 \pmod{p_i^{\alpha_i}}$ for all i. There are 2^s non-isomorphic such extended groups.

Proof. By Lemma 2.2, $\mathcal{A}$ is split. Since $\mathcal{A}$ is a metacyclic group, by Lemma 2.1, $\mathcal{A}$ has the presentation

$$\mathcal{A} = \langle a, b \mid a^n = b^2 = 1, b^{-1} a b = a^r \rangle,$$

with $r^2 \equiv 1 \pmod{n}$. The action of b on each element of $\mathbb{Z}_n$ by conjugacy is an automorphism of $\mathbb{Z}_n$ of order at most 2. Since $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}_{p_s^{\alpha_s}})$, the b-conjugation on $\mathbb{Z}_n$ corresponds to an s-tuple $(r_1, \ldots, r_s)$ with $r_i \equiv \pm 1 \pmod{p_i^{\alpha_i}}$ for $i \in \{1, \ldots, s\}$. Thus the s-tuple $(r_1, \ldots, r_s)$ has 2^s choices and $\mathcal{A}$ is presented by

$$\mathcal{A} = \langle a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = b^2 = 1, [a_i, a_j] = 1, b^{-1} a_i b = a_i^{r_i} \text{ for all } i, j \rangle.$$

To finish the proof, it suffices to show that different s-tuples $(r_1, \ldots, r_s)$ give non-isomorphic groups. It is easy to see that $\mathbb{Z}_{p_i^{\alpha_i}}$ is a subgroup of the center of $\mathcal{A}$ if and only if $r_i = 1$. Hence the groups with different s-tuples $(r_1, \ldots, r_s)$ have different center of $\mathcal{A}$. Therefore, there are 2^s non-isomorphic $\mathbb{Z}_2$-extensions of $\mathbb{Z}_n$. □

Next we consider the case of even n. Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ with $p_0 = 2$. We deal with three cases $\alpha_0 = 1, 2$ or $\alpha_0 \geq 3$ in the next theorem. First we determine the Sylow 2-subgroup $\mathcal{S}_0$ of $\mathcal{A}$ which is a $\mathbb{Z}_2$-extension of $\mathbb{Z}_{2^{\alpha_0}} = \langle a_0 \rangle$. This has been done by Theorem 2.3. Namely,

$$\mathcal{S}_0 = \langle a_0, b_0 \mid a_0^{2^{\alpha_0}} = 1, b_0^2 = a_0^{t_0}, b_0^{-1} a_0 b_0 = a_0^{r_0} \rangle,$$

where $t_0 = 0, 1$ or $2^{\alpha - 1}$, $r_0 = \pm 1$ or $\pm 1 + 2^{\alpha_0 - 1}$ depending on the types of $\mathcal{S}_0$ in Theorem 2.3. Next, take $b = b_0$. Thus each Sylow 2-subgroup and each element of order at most 2 in $\mathrm{Aut}(\mathbb{Z}_{p_1^{\alpha_1}}) \times \cdots \times \mathrm{Aut}(\mathbb{Z}_{p_s^{\alpha_s}})$ gives a unique $\mathbb{Z}_2$-extension of $\mathbb{Z}_n$.

Theorem 2.5. *Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ with $p_0 = 2$.*

(1) If $\alpha_0 = 1$, then $\mathcal{A}$ has the following presentations

- *(i) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = b^2 = 1, [a_i, a_j] = 1, b^{-1} a_i b = a_i^{r_i}$ for all $i, j \rangle$, ($\mathcal{S}_0 = \mathbb{Z}_2 \times \mathbb{Z}_2$).*
- *(ii) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = 1, b^2 = a_0, [a_i, a_j] = 1, b^{-1} a_i b = a_i^{r_i}$ for all $i, j \rangle$, ($\mathcal{S}_0 = \mathbb{Z}_4$).*

There are 2^{s+1} non-isomorphic groups.

(2) If $\alpha_0 = 2$, then $\mathcal{A}$ has the following presentations

(i) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = b^2 = 1, [a_i, a_j] = 1, b^{-1}a_i b = a_i^{r_i} \text{ for all } i, j\rangle$, $(\mathcal{S}_0 = \mathbb{Z}_4 \times \mathbb{Z}_2 \text{ or } \mathbb{D}_8)$.

(ii) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = 1, b^2 = a_0, [a_i, a_j] = 1, b^{-1}a_i b = a_i^{r_i} \text{ for all } i, j\rangle$, $(\mathcal{S}_0 = \mathbb{Z}_8)$.

(iii) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = 1, b^2 = a_0^2, [a_i, a_j] = 1, b^{-1}a_i b = a_i^{r_i} \text{ for all } i, j\rangle$, $(\mathcal{S}_0 = \mathbb{Q}_8)$.

There are 2^{s+1} *non-isomorphic groups.*

(3) If $\alpha_0 \geq 3$*, then* $\mathcal{A}$ *has the following presentations*

(i) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = b^2 = 1, [a_i, a_j] = 1, b^{-1}a_i b = a_i^{r_i} \text{ for all } i, j\rangle$, $(\mathcal{S}_0 = \mathbb{Z}_{2^{\alpha_0}} \times \mathbb{Z}_2,\ \mathbb{D}_{2^{\alpha_0+1}},\ \mathbb{SD}_{2^{\alpha_0+1}},\ \text{or } \mathbb{M}_{2^{\alpha_0+1}})$.

(ii) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = 1, b^2 = a_0, [a_i, a_j] = 1, b^{-1}a_i b = a_i^{r_i} \text{ for all } i, j\rangle$, $(\mathcal{S}_0 = \mathbb{Z}_{2^{\alpha_0+1}})$.

(iii) $\mathcal{A} = \langle a_0, a_1, \ldots, a_s, b \mid a_i^{p_i^{\alpha_i}} = 1, b^2 = a_0^{2^{\alpha_0-1}}, [a_i, a_j] = 1, b^{-1}a_i b = a_i^{r_i} \text{ for all } i, j\rangle$, $(\mathcal{S}_0 = \mathbb{Q}_{2^{\alpha_0+1}})$.

There are $6 \cdot 2^s$ *non-isomorphic groups.*

For each extension group $\mathcal{A}$ appeared so far, the number $\mathrm{Isoc}(G; \mathcal{A})$ shall be determined in the next section.

3 In cases of $\mathbb{Z}_2$-extensions of a cyclic p-group

For each group $\mathcal{A}$ in the classification of $\mathbb{Z}_2$-extensions of a cyclic p-group listed in the previous section, we aim to determine the number $\mathrm{Isoc}(G; \mathcal{A})$ in this section. However, for an abelian or a dihedral group $\mathcal{A}$, it has already been done in [14]. Hence, we need to do it only for each group $\mathcal{A}$ listed in the last three cases of Theorem 2.3. For a $\mathbb{Z}_2$-extension $\mathcal{A}$ of a finite group $\mathcal{H}$, we call an element x *normal type* if $x \in \mathcal{H}$ and *quotient type* otherwise. Note that $\mathcal{H}$ is normal in $\mathcal{A}$, and a product of any two normal type elements is normal type. For any two quotient type elements $ab, a'b$, their product is $aba'b = ab^2b^{-1}a'b$, and hence a product of any two quotient type elements is normal type. A *word* in $\{x_1, \ldots, x_s\}$ is any expression of the form $y_1^{i_1} \cdots y_k^{i_k}$ where $y_1, \ldots, y_k \in \{x_1, \ldots, x_s\}$ and $i_1, \ldots, i_k \in \{1, -1\}$, denoted by $w(x_1, \ldots, x_s)$. The number k is known as the *length* of the word. When writing words, it is common to use exponential notation as an abbreviation.

Lemma 3.1. *Let* $\mathcal{A}$ *be a* $\mathbb{Z}_2$*-extension of a finite group* $\mathcal{H}$*. For a subset* $\mathcal{I}$ *of* $S = \{1, \ldots, \beta\}$*, let*

$$\Omega_{\mathcal{I}}(\mathcal{A}; \beta) = \{(x_1, \ldots, x_\beta) \in \Omega(\mathcal{A}; \beta) : x_i \text{ is quotient type for exactly indices } i \in \mathcal{I}\}.$$

Then $|\Omega(\mathcal{A}; \beta)| = (2^\beta - 1)|\Omega_{\{1\}}(\mathcal{A}; \beta)|$.

Proof. Recall that

$$\Omega(\mathcal{A}; \beta) = \{(x_1, \ldots, x_\beta) \in \mathcal{A}^\beta : \langle x_1, \ldots, x_\beta\rangle = \mathcal{A}\}.$$

For each tuple $(x_1, \ldots, x_\beta) \in \Omega(\mathcal{A}; \beta)$, at least one of entries x_i should be quotient type to generate the whole group $\mathcal{A}$. Then,

$$\Omega(\mathcal{A}; \beta) = \bigcup_{\emptyset \neq \mathcal{I} \subseteq S} \Omega_{\mathcal{I}}(\mathcal{A}; \beta), \quad \text{disjoint union},$$

and

$$|\Omega(\mathcal{A}; \beta)| = \sum_{\emptyset \neq \mathcal{I} \subseteq S} |\Omega_{\mathcal{I}}(\mathcal{A}; \beta)|.$$

For any non-empty subset $\mathcal{I}$ of S, choose an index $j_0 \in \mathcal{I}$ and define a map $\phi\colon \Omega_{\mathcal{I}}(\mathcal{A}; \beta) \to \Omega_{\{j_0\}}(\mathcal{A}; \beta)$ by replacing all quotient type entries x_i for $i \in \mathcal{I}$ by $x_{j_0} x_i$ except x_{j_0}. Then one can see that ϕ is well-defined and bijective. It follows $|\Omega_{\mathcal{I}}(\mathcal{A}; \beta)| = (2^\beta - 1)|\Omega_{\{j_0\}}(\mathcal{A}; \beta)|$. One can assume that $j_0 = 1$ for convenience. □

Lemma 3.2. *Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a finite group $\mathcal{H}$. If each x_i is normal type except x_1, then $\langle x_1, \ldots, x_\beta \rangle = \mathcal{A}$ if and only if $\langle x_1^2, x_2, \ldots, x_\beta, x_1^{-1} x_2 x_1, \ldots, x_1^{-1} x_\beta x_1 \rangle = \mathcal{H}$.*

Proof. Assume $\langle x_1^2, x_2, \ldots, x_\beta, x_1^{-1} x_2 x_1, \ldots x_1^{-1} x_\beta x_1 \rangle = \mathcal{H}$ and each x_i is normal type except x_1. Then $\langle x_1, \ldots, x_\beta \rangle = \langle x_1, x_1^2, x_2, \ldots, x_\beta, x_1^{-1} x_2 x_1, \ldots x_1^{-1} x_\beta x_1 \rangle = \langle x_1, \mathcal{H} \rangle = \mathcal{A}$. Now assume that $\langle x_1, \ldots, x_\beta \rangle = \mathcal{A}$. For any $g \in \mathcal{A}$, g can be expressed by a word $w(x_1, \ldots, x_\beta)$. For odd k, $x_i x_1^k = x_1 \cdot (x_1^{-1} x_i x_1) \cdot (x_1^2)^{(k-1)/2}$ and for even k, $x_i x_1^k = x_i \cdot (x_1^{k/2})$. Rewrite g, one has

$$g = w(x_1, \ldots, x_\beta) = x_1^\ell w(x_1^2, x_2, \ldots, x_\beta, x_1^{-1} x_2 x_1, \ldots, x_1^{-1} x_\beta x_1), \quad \ell = 0, 1.$$

It follows that g is normal type if and only if $\ell = 0$. Therefore, $\langle x_1^2, x_2, \ldots, x_\beta, x_1^{-1} x_2 x_1, \ldots, x_1^{-1} x_\beta x_1 \rangle = \mathcal{H}$. □

Corollary 3.3. *Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n$. If each x_i is a normal type element except x_1, then $\langle x_1, \ldots, x_\beta \rangle = \mathcal{A}$ if and only if $\langle x_1^2, x_2, \ldots, x_\beta \rangle = \mathbb{Z}_n$.*

We determine $|\Omega(\mathcal{A}; \beta)|$ and $|\mathrm{Aut}(\mathcal{A})|$ for each group $\mathcal{A}$ listed in the last three cases of Theorem 2.3 in the following.

Lemma 3.4. *Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_{2^{n-1}}$ and let $\mathcal{A}$ be non-abelian. Then $|\Omega(\mathcal{A}; \beta)| = 2^{(n-2)\beta+1}(2^\beta - 1)(2^{\beta-1} - 1)$.*

Proof. By Lemma 3.1, it just needs to determine $\Omega_{\{1\}}(\mathcal{A}; \beta)$. By Corollary 3.3, $\langle x_1^2, x_2, \ldots, x_s \rangle = \mathbb{Z}_{2^{n-1}}$ if and only if $(x_1, \ldots, x_s) \in \Omega_{\{1\}}(\mathcal{A}; \beta)$. By the last three cases of Theorem 2.5, one can assume $b^2 = a^t$ with $t = 0$ or 2^{n-2} for a generator a of $\mathbb{Z}_{2^{n-1}}$. Note that x_1 is quotient type, say $x_1 = ba^i$. Then $x_1^2 = b^2 \cdot b^{-1} a^i b \cdot a^i = b^2 a^{i(1+r)} = a^{t+i(1+r)}$ with $r \in \{-1, \pm 1 + 2^{n-2}\}$. Suppose x_1^2 generates $\mathbb{Z}_{2^{n-1}}$. Then $t + i(1 + r) \equiv 1 \pmod 2$. But it is impossible by checking case by case. So $\langle x_2, \ldots, x_s \rangle = \mathbb{Z}_{2^{n-1}}$. By $|\Omega(\mathbb{Z}_{2^{n-1}}; \beta - 1)| = 2^{(n-2)(\beta-1)}(2^{\beta-1} - 1)$, which was shown by Kwak et al. in [14], it follows $|\Omega(\mathcal{A}; \beta)| = (2^\beta - 1)2^{n-1}|\Omega(\mathbb{Z}_{2^{n-1}}; \beta - 1)| = 2^{(n-2)\beta+1}(2^\beta - 1)(2^{\beta-1} - 1)$. □

Lemma 3.5. *For $n \geq 4$,*

(1) $|\mathrm{Aut}(\mathbb{Z}_{2^n})| = 2^{n-1}$,

(2) $|\mathrm{Aut}(\mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_2)| = 2^n$,

(3) $|\mathrm{Aut}(\mathbb{D}_{2^n})| = 2^{2n-3}$,

(4) $|\mathrm{Aut}(\mathbb{Q}_{2^n})| = 2^{2n-3}$,

(5) $|\mathrm{Aut}(\mathbb{M}_{2^n})| = 2^n$,

(6) $|\mathrm{Aut}(\mathbb{SD}_{2^n})| = 2^{2n-4}$.

Proof. Since the first three cases have been shown in [14], we only need to show the last three cases. To do this separately, let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_{2^{n-1}}$ and let an automorphism $\sigma \in \mathrm{Aut}(\mathcal{A})$ be of the form $a \mapsto a^i b^k, b \mapsto a^j b^\ell$ with $0 \le i, j \le 2^{n-1} - 1$ and $0 \le k, \ell \le 1$.

(4) Since the identity $(a^i b)^2 = bb^{-1}a^i ba^i b = b^2$ gives the orders $o(a^i b) = 4$ and $o(a) = 2^{n-1} \neq 4$ for $n \ge 4$, the image $\sigma(a_i)$ should be of the form a^i with $(i, 2^{n-1}) = 1$. The surjectivity of σ implies that the choices of $\sigma(b)$ are $a^j b$ with $j = 0, \ldots, 2^{n-1} - 1$. Moreover, all of such possible choices $\sigma(a)$ and $\sigma(b)$ satisfy the defining relations of $\mathbb{Q}_{2^n}$. Hence $|\mathrm{Aut}(\mathbb{Q}_{2^n})| = 2^{2n-3}$ by counting the choices of $\sigma(a)$ and $\sigma(b)$, that is, the choices of i, j, k, ℓ.

(5) If $k = 0$, then $\sigma(a) = a^i$ for some i with $(i, 2^{n-1}) = 1$. If $k = 1$, then $\sigma(a) = a^i b$ for some i with $(i, 2^{n-1}) = 1$, because the order preserving condition says $o(a^i b) = o(a) = 2^{n-1}$, and $(a^i b)^m = b^m a^{i(1+\cdots+r^{m-1})}$ for all $m \ge 1$, where $r = 1 + 2^{n-2}$. Next, we determine the possible values of $\sigma(b)$. If $\ell = 0$, then j should be 2^{n-2}. In this case, all possible values $\sigma(a)$ and $\sigma(b)$ do not satisfy the defining relations of $\mathbb{M}_{2^n}$. Thus it should be $\ell = 1$. Now the order condition $o(a^k b) = o(b) = 2$ implies $j = 2^{n-2}$ or 0. Consequently, σ has four different forms.

(i) $a \mapsto a^i, b \mapsto b$,
(ii) $a \mapsto a^i, b \mapsto a^{2^{n-2}} b$,
(iii) $a \mapsto a^i b, b \mapsto b$,
(iv) $a \mapsto a^i b, b \mapsto a^{2^{n-2}} b$.

In these four cases, $\sigma(a)$ and $\sigma(b)$ satisfy the defining relations of $\mathbb{M}_{2^n}$. Therefore, the four different cases give $|\mathrm{Aut}(\mathbb{M}_{2^n})| = 2^n$.

(6) Since $(a^i b)^2 = a^{i \cdot 2^{n-2}}$, one gets $o(a^i b) = 2$ for even i and $o(a^i b) = 4$ for odd i. Hence σ should be of the form $a \mapsto a^i, b \mapsto a^j b$ with $(i, 2^{n-1}) = 1$ and j even. Moreover, all such possible values $\sigma(a)$ and $\sigma(b)$ satisfy the defining relations of $\mathbb{SD}_{2^n}$. So $|\mathrm{Aut}(\mathbb{SD}_{2^n})| = 2^{2n-4}$. □

As a special case, $|\mathrm{Aut}(\mathbb{Q}_8)| = 24$ which is not included in the above lemma. From Theorem 1.2 and Lemmas 3.4 and 3.5, one can get the following theorem.

Theorem 3.6. *For a $\mathbb{Z}_2$-extension of $\mathcal{A}$ a cyclic group $\mathbb{Z}_{2^{n-1}}$ for $n \ge 2$,*

$$\mathrm{Isoc}(G; \mathcal{A}) = \begin{cases} 2^{(\beta-1)(n-1)}(2^\beta - 1) & \text{if } \mathcal{A} \text{ is } \mathbb{Z}_{2^n}, \\ 2^{(\beta-2)(n-2)+(n-3)}(2^\beta - 1)(2^{\beta-1} - 1) & \text{if } \mathcal{A} \text{ is } \mathbb{Z}_{2^{n-1}} \times \mathbb{Z}_2, \\ 2^{(\beta-2)(n-2)}(2^\beta - 1)(2^{\beta-1} - 1) & \text{if } \mathcal{A} \text{ is } \mathbb{D}_{2^n} \text{ for } n \ge 3, \\ 2^{(\beta-2)}(2^\beta - 1)(2^{\beta-1} - 1)/3 & \text{if } \mathcal{A} \text{ is } \mathbb{Q}_8, \\ 2^{(\beta-2)(n-2)}(2^\beta - 1)(2^{\beta-1} - 1) & \text{if } \mathcal{A} \text{ is } \mathbb{Q}_{2^n} \text{ for } n \ge 4, \\ 2^{(\beta-1)(n-2)-1}(2^\beta - 1)(2^{\beta-1} - 1) & \text{if } \mathcal{A} \text{ is } \mathbb{M}_{2^n} \text{ for } n \ge 4, \\ 2^{(\beta-2)(n-2)+1}(2^\beta - 1)(2^{\beta-1} - 1) & \text{if } \mathcal{A} \text{ is } \mathbb{SD}_{2^n} \text{ for } n \ge 4, \end{cases}$$

where the first three cases were shown in [14].

By using the Möbius function, $\mathrm{Isoc}(G;\mathcal{A})$ can also be determined. For example, for a generalized quaternion group $\mathbb{Q}_{2^n}$, a proper subgroup $\mathcal{S}$ of $\mathbb{Q}_{2^n}$ is isomorphic to $\mathbb{Z}_{2^m}$ or $\mathbb{Q}_{2^m}^{(i)}$, where $\mathbb{Z}_{2^m} = \langle a^{2^{n-m-1}}\rangle$ and $\mathbb{Q}_{2^m}^{(i)} = \langle a^{2^{n-m}}, a^i b\rangle$ for $m \in \{1,\dots,n-1\}$ and $i \in \{0,\dots,2^{n-m}-1\}$. From the subgroups lattice of $\mathbb{Q}_{2^n}$, see Figure 1, one has

$$\mu(S) = \begin{cases} 1 & \text{if } \mathcal{S} = \mathbb{Q}_{2^n}, \\ -1 & \text{if } \mathcal{S} = \mathbb{Z}_{2^{n-1}}, \mathbb{Q}_{2^{n-1}}^{(0)} \text{ or } \mathbb{Q}_{2^{n-1}}^{(1)}, \\ 2 & \text{if } \mathcal{S} = \mathbb{Z}_{2^{n-2}}, \\ 0 & \text{otherwise.} \end{cases}$$

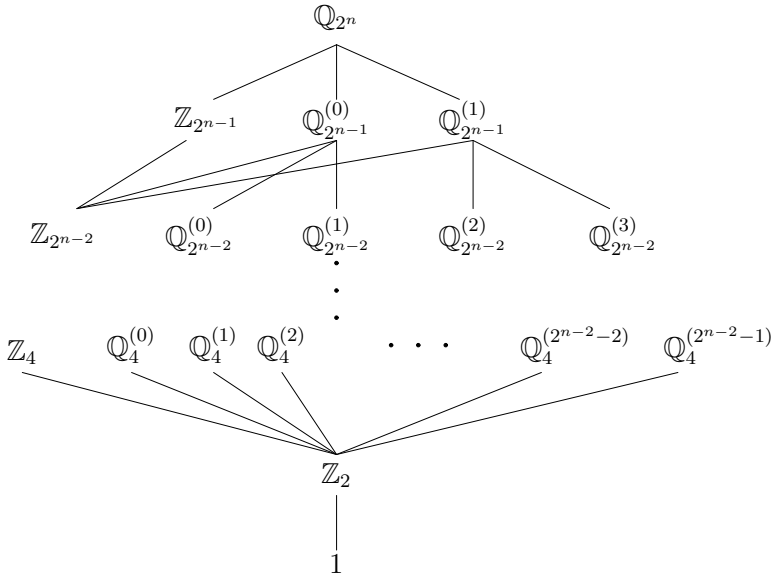

Figure 1: The subgroup lattice of $\mathbb{Q}_{2^n}$.

It follows from Theorem 1.3

$$\mathrm{Isoc}(G;\mathbb{Q}_{2^n}) = \begin{cases} \frac{1}{3}(2^{3\beta-3} - 3\cdot 2^{2\beta-3} + 2^{\beta-2}) & \text{if } n = 3, \\ \frac{1}{2^{2n-3}}(2^{\beta n} - 3\cdot 2^{\beta(n-1)} + 2^{\beta(n-2)+1}) & \text{if } n > 3, \end{cases}$$

which coincides with the formula given in Theorem 3.6.

If $\mathcal{A} \cong \mathbb{M}_{2^n}$, then every proper subgroup $\mathcal{S}$ of $\mathbb{M}_{2^n}$ is isomorphic to $\mathbb{Z}_m$ or $\mathbb{M}_{2^m}^{(i)}$ for $m \in \{2,\dots,n-1\}$ and $i \in \{0,1\}$, where $\mathbb{Z}_{2^m} = \langle a^{2^{n-m-1}}\rangle$, $\mathbb{M}_{2^m}^{(0)} = \langle a^{2^{n-m}}, b\rangle$ and $\mathbb{M}_{2^m}^{(1)} = \langle a^{2^{n-m}}, a^{2^{n-m-1}}b\rangle$. If $m = 1$, then $\mathcal{S}$ is isomorphic to $\mathbb{Z}_2^{(0)} = \langle a^{n-2}\rangle$ or $\mathbb{Z}_2^{(1)} = \langle a^{n-2}b\rangle$. Now from the subgroups lattice of $\mathbb{M}_{2^n}$ illustrated in Figure 2 and $|\mathrm{Aut}(\mathbb{M}_{2^n})| = 2^n$, one can have

$$\mathrm{Isoc}(G;\mathbb{M}_{2^n}) = \frac{1}{2^n}(2^{n\beta} - 3\cdot 2^{(n-1)\beta} + 2^{(n-2)\beta+1}),$$

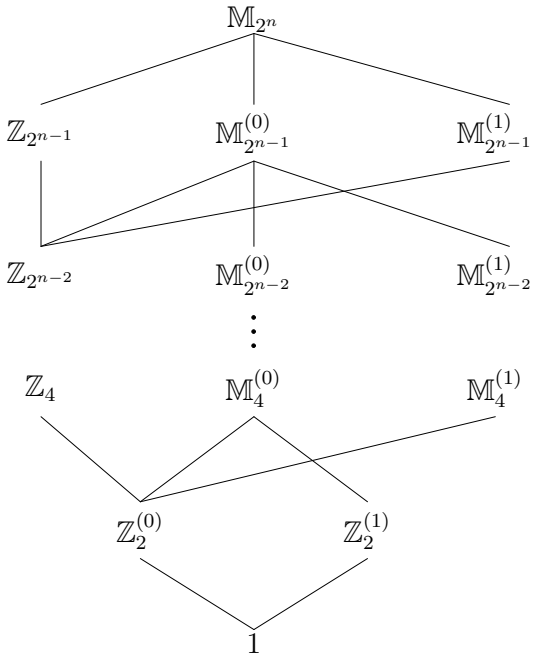

Figure 2: The subgroup lattice of $\mathbb{M}_{2^n}$.

which coincides exactly with the result in Theorem 3.6.

Also, by using the Möbius function, one can show that

$$\mathrm{Isoc}(G;\mathbb{SD}_{2^n}) = \frac{1}{2^{2n-4}}(2^{n\beta} - 3\cdot 2^{(n-1)\beta} + 2^{(n-2)\beta+1}).$$

For some small β and n, the numbers $\mathrm{Isoc}(G;\mathcal{A})$ are tabulated in Table 1.

Table 1: The number Isoc for small β and n.

	Isoc						
(β,n)	$\mathbb{Z}_{2^n}$	$\mathbb{Z}_{2^{n-1}}\times\mathbb{Z}_2$	$\mathbb{D}_{2^n}$	$\mathbb{Q}_{2^n}$	$\mathbb{M}_{2^n}$	$\mathbb{SD}_{2^n}$	$\mathcal{A}$
$(2,3)$	12	3	3	1	0	0	22
$(2,4)$	24	6	3	6	24	6	69
$(2,4)$	48	12	3	6	48	6	123
$(3,3)$	112	42	42	56	0	0	252
$(3,4)$	448	168	84	168	672	168	1708
$(3,5)$	1792	672	168	336	2688	336	5992
$(4,3)$	960	420	420	560	0	0	2360
$(4,4)$	7680	3360	1680	3360	13440	3360	32880
$(4,5)$	61440	26880	6720	13440	107520	13440	229440

4 In cases of $\mathbb{Z}_2$-extensions of any cyclic groups

In this section we determine $\mathrm{Isoc}(G;\mathcal{A})$ for a $\mathbb{Z}_2$-extension $\mathcal{A}$ of a cyclic group $\mathbb{Z}_n$ (of any order n, not necessarily to be a p-group). Again, let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ and let $n = p_0^{\alpha_0} p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the prime decomposition with $p_0 = 2$. Let the b-conjugation on $\mathbb{Z}_n$ correspond to an $(s+1)$-tuple $(r_0, r_1, \ldots, r_s)$, where $r_0 \in \{\pm 1, \pm 1 + 2^{\alpha_0 - 1}\}$ and $r_i = \pm 1$ for $i \in \{1, \ldots, s\}$ with -1 in exactly t entries $\ell_1, \ldots, \ell_t$. Let $n = 2^{\alpha_0} n_1 n_2$ with $n_1 = \prod_{j=1}^{t} p_{\ell_j}^{\alpha_{\ell_j}}$. Then $\mathcal{A}$ is isomorphic to $\mathcal{B} \times \mathbb{Z}_{n_2}$ where $\mathcal{B}$ is a $\mathbb{Z}_2$-extension of $\mathbb{Z}_{n_1}$ since any element of $\mathbb{Z}_{n_2}$ commutes with each element of $\mathcal{A}$. Since $(|\mathcal{B}|, |\mathbb{Z}_{n_1}|) = 1$, one has $\mathrm{Isoc}(G; \mathcal{B} \times \mathbb{Z}_{n_1}) = \mathrm{Isoc}(G;\mathcal{B}) \cdot \mathrm{Isoc}(G; \mathbb{Z}_{n_1})$, as shown in [14]. Because $\mathrm{Isoc}(G; \mathbb{Z}_{n_1})$ has already been determined, we just need to determine $\mathrm{Isoc}(G;\mathcal{B})$.

Lemma 4.1. *Let $\mathcal{B}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ with $p_0 = 2$ and $s \geq 1$, and let $n = 2^{\alpha_0} m$. Let the b-conjugation on $\mathbb{Z}_n$ correspond to an $(s+1)$-tuple $(r_0, r_1, \ldots, r_s)$, where $r_0 \in \{\pm 1, \pm 1 + 2^{\alpha_0 - 1}\}$ and all other r_i's are -1. Then*

$$|\Omega(\mathcal{B};\beta)| = \begin{cases} (2^\beta - 1) m 2^{\alpha_0 \beta} |\Omega(\mathbb{Z}_m; \beta - 1)| & \text{if } 2^{\alpha_0 + 1} \mid o(b), \\ (2^\beta - 1) m 2^{\alpha_0} |\Omega(\mathbb{Z}_{2^{\alpha_0} m}; \beta - 1)| & \text{otherwise.} \end{cases}$$

Proof. By Theorem 2.5, one can assume $b^2 = a_0^t$ with $t \in \{0, 1, 2^{\alpha_0 - 1}\}$. By Lemma 3.1, it just needs to determine $|\Omega_{\{1\}}(\mathcal{B};\beta)|$. Take $(x_1, \ldots, x_\beta) \in \Omega_{\{1\}}(\mathcal{A};\beta)$. Note that x_1 is a quotient type element and other x_i's are all normal type. Since

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times Z_{p_s^{\alpha_s}},$$

any element of $\mathbb{Z}_n$ can be presented $g_i h_i$ with $g_i \in \mathbb{Z}_{p_0^{\alpha_0}}$ and $h_i \in \prod_{i=1}^{\beta} \mathbb{Z}_{p_i^{\alpha_i}}$. So x_1 can be presented by $g_1 h_1 b$ and other x_i's can be presented by $g_i h_i$. By Corollary 3.3, $\langle x_1, \ldots, x_\beta \rangle = \mathcal{B}$ if and only if $\langle x_1^2, x_2, \ldots, x_\beta \rangle = \mathbb{Z}_n$. By $x_1^2 = (g_1 h_1 b)^2 = b^2 g_1^{1+r_0}$, one has $\langle b^2 g_1^{1+r_0}, g_2 h_2, \ldots, g_\beta h_\beta \rangle = \mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$. Recall that $b^2 = a_0^t \in \mathbb{Z}_{p_0^{\alpha_0}}$ with $p_0 = 2$, then $\langle b^2 g_1^{1+r_0}, g_2, \ldots, g_\beta \rangle = \mathbb{Z}_{p_0^{\alpha_0}}$ and $\langle h_2, \ldots, h_\beta \rangle = \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$. So $(b^2 g_1^{1+r_0}, g_2, \ldots, g_\beta) \in \Omega(\mathbb{Z}_{2^{\alpha_0}}; \beta)$, $(h_2, \ldots, h_\beta) \in \Omega(\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}; \beta - 1)$. To count the choice of $(x_1, \ldots, x_\beta)$, equivalently to count the number of $(g_1, \ldots, g_\beta)$ and $(h_1, \ldots, h_\beta)$. When computing $x_1^2 = b^2 g_1^{1+r_0}$, h_1 can be any element of $\prod_{i=1}^{\beta} \mathbb{Z}_{p_i^{\alpha_i}}$, and it follows h_1 has m choices by $m = \prod_{i=1}^{\beta} p_i^{\alpha_i}$. The number of choices of $(h_2, \ldots, h_\beta)$ is equal to $|\Omega(\mathbb{Z}_m; \beta - 1)|$. Hence number of choices of $(h_1, \ldots, h_\beta)$ is $m|\Omega(\mathbb{Z}_m; \beta - 1)|$. Now we determine the number of choices of $(g_1, \ldots, g_\beta)$ in the following.

Assume that $2^{\alpha_0 + 1} \mid o(b)$ and it follows $t = 1$. Then the Sylow 2-subgroup of $\mathcal{B}$ is $\mathbb{Z}_{2^{\alpha_0 + 1}}$. By Theorem 2.5, $\langle b^2 \rangle = \langle a_0 \rangle = \mathbb{Z}_{2^{\alpha_0}}$ and $r_0 = 1$. Since $g_1 \in \mathbb{Z}_{2^{\alpha_0}}$, one has $\langle b^2 g_1^{1+r_0} \rangle = \langle b^2 g_1^2 \rangle = \langle b^2 \rangle = \mathbb{Z}_{2^{\alpha_0}}$. By $\langle b^2 g_1^{1+r_0}, g_2, \ldots, g_\beta \rangle = \langle b^2 \rangle = \mathbb{Z}_{2^{\alpha_0}}$, $(g_1, \ldots, g_\beta)$ has $2^{\alpha_0 \beta}$ choices. So $|\Omega_{\{1\}}(\mathcal{B};\beta)| = 2^{\alpha_0 \beta} m |\Omega(\mathbb{Z}_m; \beta - 1)|$, and it follows $|\Omega(\mathcal{B};\beta)| = (2^\beta - 1) m 2^{\alpha_0 \beta} |\Omega(\mathbb{Z}_m; \beta - 1)|$.

If $2^{\alpha_0 + 1}$ does not divide $o(b)$, then, by Theorem 2.5, $b^2 = a_0^t$ with $t \in \{0, 2^{\alpha_0 - 1}\}$. If $t = 0$, then $b^2 = 1$ and $r_0 \in \{\pm 1, \pm 1 + 2^{\alpha_0 - 1}\}$. It follows $b^2 g_1^{1+r_0} = 1, g_1^2, g_1^{2^{\alpha_0 - 1}}$ or $g_1^{2 + 2^{\alpha_0 - 1}}$. So g^{1+r_0} can not be the generator of $\mathbb{Z}_{2^{\alpha_0}}$. If $t = 2^{\alpha_0 - 1}$, then $r_0 = -1$. Then $b^2 g_1^{1+r_0} = a_0^{2^{\alpha_0 - 1}}$, again, $b^2 g_1^{1+r_0}$ can not generate $\mathbb{Z}_{2^{\alpha_0}}$. So $\langle b^2 g_1^{1+r_0}, g_2, \ldots, g_\beta \rangle = \mathbb{Z}_{2^{\alpha_0}}$ if and only if $\langle g_2, \ldots, g_\beta \rangle = \mathbb{Z}_{2^{\alpha_0}}$. It follows $(g_2, \ldots, g_\beta) \in \Omega(\mathbb{Z}_{2^{\alpha_0}}; \beta - 1)$ and g_1

is any element in $\mathbb{Z}_{2^{\alpha_0}}$. Then $(g_1, \ldots, g_\beta)$ has $2^{\alpha_0}|\Omega(\mathbb{Z}_{2^{\alpha_0}}; \beta-1)|$ choices. So $|\Omega(\mathcal{B}; \beta)| = (2^\beta - 1)m2^{\alpha_0}|\Omega(\mathbb{Z}_{2^{\alpha_0}m}; \beta - 1)|$. □

Lemma 4.2. *Let $\mathcal{B}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ with $p_0 = 2$ and $s \geq 1$, and let $n = 2^{\alpha_0}m$. Let the b-conjugation on $\mathbb{Z}_n$ correspond to an $(s+1)$-tuple $(r_0, r_1, \ldots, r_s)$, where $r_0 \in \{\pm 1, \pm 1 + 2^{\alpha_0 - 1}\}$ and all other r_i's are -1.*

(1) If $r_0 = 1$, then

$$|\mathrm{Aut}(\mathcal{B})| = \begin{cases} 2^{\alpha_0}m\varphi(n) & \text{if } 2^{\alpha_0+1} \mid o(b), \\ 2m\varphi(n) & \text{otherwise.} \end{cases}$$

(2) If $r_0 = -1$, then $|\mathrm{Aut}(\mathcal{B})| = 2^{\alpha_0}m\varphi(n)$.

(3) If $r_0 = 1 + 2^{\alpha_0 - 1}$, then $|\mathrm{Aut}(\mathcal{B})| = 2m\varphi(n)$.

(4) If $r_0 = -1 + 2^{\alpha_0 - 1}$, then $|\mathrm{Aut}(\mathcal{B})| = 2^{\alpha_0 - 1}m\varphi(n)$.

Proof. Again, one can assume that $b^2 = a_0^t$ with $t \in \{0, 1, 2^{\alpha_0 - 1}\}$. For an automorphism σ of $\mathcal{B}$, $\sigma(a_k)$ should be of the form $a_k^{i_k}$ with $(i_k, p_k^{\alpha_k}) = 1$ for $k \in \{1, \ldots, s\}$ since σ is order-preserving. Suppose that $\sigma(a_0)$ is quotient type, then $b^{-1}a_k b = a_k$ since $\sigma(a_0)$ commutes with $\sigma(a_k)$ for each k. So $r_i = 1$ for each $i \in \{1, \ldots, s\}$, which is a contradiction. Then $\sigma(a_0)$ is normal type, say $\sigma(a_0) = a_0^{i_0}$ with $(i_0, 2^{\alpha_0}) = 1$. Assume $\sigma(b) = a_0^{u_0}a_1^{u_1} \cdots a_s^{u_s}b$. We need to count the number of choices of $u_0, \ldots, u_\beta$. By computing, $(a_0^{u_0}a_1^{u_1} \cdots a_s^{u_s}b)^2 = b^2 a_0^{u_0(1+r_0)} \cdots a_\beta^{u_\beta(1+r_\beta)} = b^2 a_0^{u_0(1+r_0)}$. Note that $o(\sigma(b)) = o(b)$ and $o(b)$ is even. By hypothesis, $r_1 = \cdots = r_\beta = -1$, and it follows $(\sigma(b))^2 = b^2 a_0^{u_0(1+r_0)}$. Then u_i can be any element of $\mathbb{Z}_{p_i^{\alpha_i}}$ for $i \in \{1, \ldots, s\}$. Now it needs to determine the number of choices of u_0.

(1) If $r_0 = 1$ and $o(b) = 2^{\alpha_0+1}$, then $(\sigma(b))^2 = b^2 a_0^{2u_0}$. By Theorem 2.5, $b^2 = a_0$ in this case. Then $o(b^2 a_0^{2u_0}) = o(b^2) = 2^{\alpha_0}$, and it follows u_0 has 2^{α_0} choices. Hence $|\mathrm{Aut}(\mathcal{B})| = 2^{\alpha_0}m\varphi(n)$. If $r_0 = 1$ and $o(b) = 2$, then u_0 can be 0 or $2^{\alpha_0 - 1}$. So $|\mathrm{Aut}(\mathcal{B})| = 2m\varphi(n)$.

(2) If $r_0 = -1$, then $(\sigma(b))^2 = b^2$ and $o(b)$ is 2 or 4, by Theorem 2.5. So u_0 can be any element of $\mathbb{Z}_{2^{\alpha_0}}$ and has 2^{α_0} choices. It follows $|\mathrm{Aut}(\mathcal{B})| = 2^{\alpha_0}m\varphi(n)$.

(3) If $r_0 = 1 + 2^{\alpha_0 - 1}$, then $o(b) = 2$. So $(\sigma(b))^2 = b^2 a_0^{u_0(2+2^{\alpha_0-1})} = a_0^{u_0(2+2^{\alpha_0-1})} = 1$. If follows $u_0(2 + 2^{\alpha_0 - 1}) \equiv 0 \pmod{2^{\alpha_0}}$. Then u_0 has 2 choices: 0 or $2^{\alpha_0 - 1}$. Hence $|\mathrm{Aut}(\mathcal{B})| = 2m\varphi(n)$.

(4) If $r_0 = -1 + 2^{\alpha_0 - 1}$, then $o(b) = 2$. So $(\sigma(b))^2 = a_0^{u_0 2^{\alpha_0 - 1}} = 1$. Then $u_0 2^{\alpha_0 - 1} \equiv 0 \pmod{2^{\alpha_0}}$, and it follows u_0 has $2^{\alpha_R 0 - 1}$ choices. Hence $|\mathrm{Aut}(\mathcal{B})| = 2^{\alpha_0 - 1}m\varphi(n)$. □

The next lemma follows from Theorem 1.2 and Lemmas 4.1 and 4.2.

Lemma 4.3. *Let $\mathcal{B}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ and let $n = p_0^{\alpha_0}p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ be the prime decomposition with $p_0 = 2$. Let the b-conjugation on $\mathbb{Z}_n$ correspond to an $(s+1)$-tuple $(r_0, r_1, \ldots, r_s)$, where $r_0 \in \{\pm 1, \pm 1 + 2^{\alpha_0 - 1}\}$ and all other r_i's are -1.*

(1) If $r_0 = 1$,

$$\mathrm{Isoc}(G;\mathcal{B}) = \begin{cases} \frac{1}{\varphi(n)}(2^\beta - 1)2^{\alpha_0\beta-\alpha_0}\prod_{i=1}^{s} p_i^{(\alpha_i-1)(\beta-1)}(p_i^{\beta-1}-1) & \text{if } 2^{\alpha_0+1} \mid o(b), \\ \frac{1}{\varphi(n)}(2^\beta - 1)2^{\alpha_0-1}\prod_{i=0}^{s} p_i^{(\alpha_i-1)(\beta-1)}(p_i^{\beta-1}-1) & \text{otherwise}. \end{cases}$$

(2) If $r_0 = -1$, *then*

$$\mathrm{Isoc}(G;\mathcal{B}) = \frac{1}{\varphi(n)}(2^\beta - 1)\prod_{i=0}^{s} p_i^{(\alpha_i-1)(\beta-1)}(p_i^{\beta-1}-1).$$

(3) If $r_0 = 1 + 2^{\alpha_0-1}$, *then*

$$\mathrm{Isoc}(G;\mathcal{B}) = \frac{1}{\varphi(n)}2^{\alpha_0-1}(2^\beta - 1)\prod_{i=0}^{s} p_i^{(\alpha_i-1)(\beta-1)}(p_i^{\beta-1}-1).$$

(4) If $r_0 = -1 + 2^{\alpha_0-1}$, *then*

$$\mathrm{Isoc}(G;\mathcal{B}) = \frac{1}{\varphi(n)}2(2^\beta - 1)\prod_{i=0}^{s} p_i^{(\alpha_i-1)(\beta-1)}(p_i^{\beta-1}-1).$$

Now one can get main theorem of this section.

Theorem 4.4. *Let* $\mathcal{A}$ *be a* $\mathbb{Z}_2$*-extension of a cyclic group* $\mathbb{Z}_n \cong \mathbb{Z}_{p_0^{\alpha_0}} \times \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}}$ *and let* $n = p_0^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ *be the prime decomposition with* $p_0 = 2$. *Let the* b*-conjugation on* $\mathbb{Z}_n$ *correspond to an* $(s+1)$*-tuple* $(r_0, r_1, \ldots, r_s)$, *where* $r_0 \in \{\pm 1, \pm 1 + 2^{\alpha_0-1}\}$ *and* $r_i = \pm 1$ *for* $i \in \{1, \ldots, s\}$ *with* -1 *in exactly* t *entries* $\ell_1, \ldots, \ell_t$. *Let* $\mathcal{J} = \{\ell_1, \ldots, \ell_t\}$, $\mathcal{K} = \{1, \ldots, s\} - \mathcal{J}$ *and*

$$\mathfrak{N} = \frac{1}{\varphi(n)}(2^\beta - 1)\prod_{i\in\mathcal{J}} p_i^{(\alpha_i-1)(\beta-1)}(p_i^{\beta-1}-1)\prod_{i\in\mathcal{K}} p_i^{(\alpha_i-1)\beta}(p_i^{\beta}-1).$$

Then $\mathrm{Isoc}(G;\mathcal{A}) = \mathfrak{T}\mathfrak{N}$, *where*

$$\mathfrak{T} = \begin{cases} 2^{\alpha_0\beta-\alpha_0} & \text{if } r_0 = 1 \text{ and } 2^{\alpha_0+1} \mid o(b), \\ 2^{(\alpha_0-1)\beta}(2^{\beta-1}-1) & \text{if } r_0 = 1 \text{ and } 2^{\alpha_0+1} \nmid o(b), \\ 2^{(\alpha_0-1)(\beta-1)}(2^{\beta-1}-1) & \text{if } r_0 = -1, \\ 2^{(\alpha_0-1)\beta}(2^{\beta-1}-1) & \text{if } r_0 = 1 + 2^{\alpha_0-1}, \\ 2^{(\alpha_0-1)(\beta-1)-1}(2^{\beta-1}-1) & \text{if } r_0 = 1 + 2^{\alpha_0-1}. \end{cases}$$

Example 4.5. Let $\mathcal{A}$ be a $\mathbb{Z}_2$-extension of a cyclic group $\mathbb{Z}_{1260} \cong \mathbb{Z}_4 \times \mathbb{Z}_{3^2} \times \mathbb{Z}_5 \times \mathbb{Z}_7 = \langle a_0\rangle \times \langle a_1\rangle \times \langle a_2\rangle \times \langle a_3\rangle$. By Theorem 2.5, the b-conjugation on $\mathbb{Z}_n$ corresponds to a 4-tuple (r_0, r_1, r_2, r_3), where $r_i = \pm 1$ for $i \in \{0, 1, 2, 3\}$. Take $(r_0, r_1, r_2, r_3) = (1, -1, -1, 1)$ and $\beta = 3$ as an example. One has $\mathrm{Isoc}(G;\mathcal{A}) = \mathrm{Isoc}(G;\mathcal{B})\,\mathrm{Isoc}(G;\mathbb{Z}_7)$, where $\mathcal{B}$ is a $\mathbb{Z}_2$-extension of $\mathbb{Z}_{180}$. By Lemmas 4.1 and 4.2, $|\Omega(\mathcal{B};3)| = (2^3-1)|\Omega_1(\mathcal{B};3)| = 34836480$ and $|\mathrm{Aut}(\mathcal{B})| = 4320$. It follows that $\mathrm{Isoc}(G;\mathcal{B}) = 8064$. By $\mathrm{Isoc}(G;\mathbb{Z}_7) = 57$, one gets $\mathrm{Isoc}(G;\mathcal{A}) = 459648$.

5 In cases of $\mathbb{Z}_2$-extensions of an abelian group

Naturally, we are interested in extending the counting problem of the previous two sections to the case of a $\mathbb{Z}_2$-extension of an abelian group. To do this, we need to classify $\mathbb{Z}_2$-extensions of an arbitrary abelian group, but we can not give a complete answer so far, see Section 6. So we just count two special cases, generalized dihedral groups or generalized dicyclic groups.

5.1 With generalized dihedral groups

Let $\mathcal{H}$ be an abelian group. A *generalized dihedral group* $\mathrm{Dih}(\mathcal{H})$, as a $\mathbb{Z}_2$-extension of $\mathcal{H}$, is defined with relations

$$b^2 = 1, b^{-1}ab = a^{-1}, \quad \text{for all } a \in \mathcal{H}.$$

It is a semidirect product of $\mathcal{H}$ and $\mathbb{Z}_2$, with $\mathbb{Z}_2$ acting on $\mathcal{H}$ by inverting elements. When $\mathcal{H}$ is cyclic, $\mathrm{Dih}(\mathcal{H})$ is just a dihedral group.

Lemma 5.1. *$\mathcal{H}$ is a characteristic subgroup of* $\mathrm{Dih}(\mathcal{H})$.

Proof. Take an automorphism $\sigma \in \mathrm{Aut}(\mathrm{Dih}(\mathcal{H}))$. Note that the order of a quotient type element is 2. For any element a of odd order in $\mathrm{Dih}(\mathcal{H})$, $\sigma(a)$ should be normal type since σ is order-preserving. For an element a_0 of even order, suppose that $\sigma(a_0)$ is a quotient type element. Since a_0 commutes with a as an element of odd order, $\sigma(a_0)$ commutes $\sigma(a)$. Then b commutes a, which is a contradiction. Then $\sigma(a) \in \mathcal{H}$ for any $a \in \mathcal{H}$. Hence $\mathcal{H}$ is a characteristic subgroup of $\mathrm{Dih}(\mathcal{H})$. □

Now, $|\mathrm{Aut}(\mathrm{Dih}(\mathcal{H}))| = |\mathcal{H}| \cdot |\mathrm{Aut}(\mathcal{H})|$. By Lemmas 3.1 and 3.2, one can show that $|\Omega(\mathrm{Dih}(\mathcal{H}); \beta)| = (2^\beta - 1)|\Omega_{\{1\}}(\mathcal{H}; \beta - 1)| = (2^\beta - 1)|\mathcal{H}||\Omega(\mathcal{H}; \beta - 1)|$. Each abelian group can be decomposed into direct product of abelian p-group, namely, $\mathcal{H} \cong \mathcal{H}_{p_1} \times \cdots \times \mathcal{H}_{p_s}$ with p_i prime. Then $|\Omega(\mathrm{Dih}(\mathcal{H}); \beta)| = (2^\beta - 1)|\mathcal{H}||\Omega(\mathcal{H}_{p_1}; \beta - 1)| \cdots |\Omega(\mathcal{H}_{p_s}; \beta - 1)|$. It just needs to determine $\mathrm{Isoc}(G; \mathrm{Dih}(\mathcal{H}_p))$ for a prime integer p. Since $|\Omega(\mathcal{H}_p; \beta - 1)|$ is determined in [14], one gets

Theorem 5.2. *For a generalized dihedral group* $\mathrm{Dih}(\mathcal{H}_p)$ *and* $\mathcal{H}_p = m_1\mathbb{Z}_{p^{s_1}} \times \cdots \times m_\ell\mathbb{Z}_{p^{s_\ell}}$ *with* $m_1, \ldots, m_\ell$ *and* $s_1, \ldots, s_\ell$ *are positive integers satisfying* $s_\ell < \cdots < s_1$*, one can obtain*

$$\mathrm{Isoc}(G; \mathrm{Dih}(\mathcal{H}_p)) = (2^\beta - 1)p^{f(\beta-1, m_i, s_i)} \frac{\prod_{i=1}^{m} p^{\beta - i} - 1}{\prod_{j=1}^{\ell} \prod_{h=1}^{m_j} p^{m_j - h + 1} - 1},$$

where $m = m_1 + \cdots + m_\ell$ *and*

$$f(\beta - 1, m_i, s_i) = (\beta - 1 - m)\left(\sum_{i=1}^{\ell} m_i(s_i - 1)\right) + \sum_{i=1}^{\ell-1} m_i \left(\sum_{j=i+1}^{\ell} m_j(s_i - s_j - 1)\right).$$

5.2 With generalized dicyclic groups

A *generalized dicyclic group* $\mathrm{Dic}(\mathcal{H})$, as another $\mathbb{Z}_2$-extension of an abelian group $\mathcal{H}$, is defined with relations

$$b^2 = c, b^{-1}ab = a^{-1},$$

where c is an involution of $\mathcal{H}$ and a is an arbitrary element of $\mathcal{H}$. Similarly, one can have the coming lemma.

Lemma 5.3. *$\mathcal{H}$ is a characteristic group of $\mathrm{Dic}(\mathcal{H})$. Hence*

$$|\mathrm{Aut}(\mathrm{Dic}(\mathcal{H}))| = |\mathcal{H}| \cdot |\mathrm{Aut}(\mathcal{H})|.$$

Theorem 5.4. *For a generalized dicyclic group $\mathrm{Dic}(\mathcal{H}_p)$ and $\mathcal{H}_p = m_1\mathbb{Z}_{p^{s_1}} \times \cdots \times m_\ell\mathbb{Z}_{p^{s_\ell}}$ with $m_1, \ldots, m_\ell$ and $s_1, \ldots, s_\ell$ are positive integers satisfying $s_\ell < \cdots < s_1$, one can obtain*

$$\mathrm{Isoc}(G; \mathrm{Dih}(\mathcal{H}_p)) = 2(2^\beta - 1)p^{f(\beta-1,m_i,s_i)} \frac{\prod_{i=1}^{m} p^{\beta-i} - 1}{\prod_{j=1}^{\ell}\prod_{h=1}^{m_j} p^{m_j-h+1} - 1},$$

where $m = m_1 + \cdots + m_\ell$ and

$$f(\beta-1, m_i, s_i) = (\beta - 1 - m)\left(\sum_{i=1}^{\ell} m_i(s_i - 1)\right) + \sum_{i=1}^{\ell-1} m_i \left(\sum_{j=i+1}^{\ell} m_j(s_i - s_j - 1)\right).$$

6 Further remarks

In this paper, we enumerate the regular coverings of a graph whose covering transformation groups are $\mathbb{Z}_2$-extensions of a cyclic group. However, we could not give a complete answer of this problem if $\mathcal{A}$ is a $\mathbb{Z}_2$-extension of any abelian group $\mathcal{H}$.

However, we cannot answer the same enumeration problem when the cyclic group is replaced by an abelian group, even by an elementary abelian p-group. In fact the difficulty for authors is how to determine all involutions of $\mathrm{Aut}(\mathcal{H})$. The counting problem has studied by many researchers, for example, in [21], it gave a generating function for the number of involutions of $\mathrm{GL}(n, p)$ which is isomorphic to automorphism group of $\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$. For more results, see [2], [5], [3] and so on. But it is still hard for us to determine the specific form of each involution of $\mathrm{GL}(n, p)$.

For further possible problems unsolved in this paper, we list in the following.

(1) $\mathrm{Isoc}(G; \mathcal{A})$ if $\mathcal{A}$ is a $\mathbb{Z}_2$-extension of any abelian group.

(2) $\mathrm{Isoc}(G; \mathcal{A})$ if $\mathcal{A}$ is a $\mathbb{Z}_p$-extension of any cyclic group.

(3) $\mathrm{Isoc}(G; \mathcal{A})$ if $\mathcal{A}$ is any metacyclic group.

References

[1] J. N. S. Bidwell and M. J. Curran, Automorphisms of finite abelian groups, *Math. Proc. R. Ir. Acad.* **110A** (2010), 57–71, doi:10.3318/pria.2010.110.1.57.

[2] D. Ž. Djoković, Product of two involutions, *Arch. Math.* **18** (1967), 582–584, doi:10.1007/bf01898863.

[3] J. Fulman, R. Guralnick and D. Stanton, Asymptotics of the number of involutions in finite classical groups, *J. Group Theory* **20** (2017), 871–902, doi:10.1515/jgth-2017-0011.

[4] J. L. Gross and T. W. Tucker, Generating all graph coverings by permutation voltage assignments, *Discrete Math.* **18** (1977), 273–283, doi:10.1016/0012-365x(77)90131-5.

[5] W. H. Gustafson, P. R. Halmos and H. Radjavi, Products of involutions, *Linear Algebra Appl.* **13** (1976), 157–162, doi:10.1016/0024-3795(76)90054-9.

[6] M. Hall, Jr., Subgroups of finite index in free groups, *Canad. J. Math.* **1** (1949), 187–190, doi:10.4153/cjm-1949-017-2.

[7] C. J. Hillar and D. L. Rhea, Automorphisms of finite abelian groups, *Amer. Math. Monthly* **114** (2007), 917–923, doi:10.1080/00029890.2007.11920485.

[8] M. Hofmeister, Counting double covers of graphs, *J. Graph Theory* **12** (1988), 437–444, doi:10.1002/jgt.3190120316.

[9] S. Hong, J. H. Kwak and J. Lee, Regular graph coverings whose covering transformation groups have the isomorphism extension property, *Discrete Math.* **148** (1996), 85–105, doi:10.1016/0012-365x(94)00266-l.

[10] I. M. Isaacs, *Finite Group Theory*, volume 92 of *Graduate Studies in Mathematics*, American Mathematical Society, Providence, Rhode Island, 2008, doi:10.1090/gsm/092.

[11] D. L. Johnson, *Presentations of Groups*, volume 15 of *London Mathematical Society Student Texts*, Cambridge University Press, Cambridge, 2nd edition, 1997, doi:10.1017/cbo9781139168410.

[12] G. A. Jones, Enumeration of homomorphisms and surface-coverings, *Quart. J. Math. Oxford* **46** (1995), 485–507, doi:10.1093/qmath/46.4.485.

[13] G. A. Jones, Counting subgroups of non-Euclidean crystallographic groups, *Math. Scand.* **84** (1999), 23–39, doi:10.7146/math.scand.a-13930.

[14] J. H. Kwak, J.-H. Chun and J. Lee, Enumeration of regular graph coverings having finite abelian covering transformation groups, *SIAM J. Discrete Math.* **11** (1998), 273–285, doi:10.1137/s0895480196304428.

[15] J. H. Kwak and J. Lee, Enumeration of connected graph coverings, *J. Graph Theory* **23** (1996), 105–109, doi:10.1002/(sici)1097-0118(199606)22:2⟨105::aid-jgt2⟩3.0.co;2-r.

[16] J. H. Kwak and J. Lee, Distribution of branched $\mathbb{D}_p$-coverings of surfaces, *Discrete Math.* **183** (1998), 193–212, doi:10.1016/s0012-365x(97)00030-7.

[17] J. H. Kwak, J. Lee and A. Mednykh, Coverings, enumeration and hurwitz problems, in: J. Koolen, J. H. Kwak and M.-Y. Xu (eds.), *Applications of Group Theory to Combinatorics*, CRC Press, London, pp. 71–107, 2008, selected papers from the Com^{2}MaC Conference on Applications of Group Theory to Combinatorics, Pohang, Korea, 9 – 12 July 2007.

[18] J. H. Kwak and M. Y. Xu, *Finite Group Theory for Combinatorists*, unpublished.

[19] V. Liskovets, Reductive enumeration under mutually orthogonal group actions, *Acta Appl. Math.* **52** (1998), 91–120, doi:10.1023/a:1005950823566.

[20] V. A. Liskovets, On the enumeration of subgroups of a free group, *Dokl. Akad. Nauk BSSR* **15** (1971), 6–9.

[21] K. E. Morrison, Integer sequences and matrices over finite fields, *J. Integer Seq.* **9** (2006), Article 06.2.1, `https://cs.uwaterloo.ca/journals/JIS/VOL9/Morrison/morrison37.html`.