THESIS ON NATURAL AND EXACT SCIENCES B126

Some Classes of Finite 2-Groups and Their Endomorphism Semigroups

TATJANA TAMBERG

TUT
PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Sciences
Department of Mathematics

Dissertation is accepted for the defence of the degree of Doctor of Philosophy in Applied Mathematics on February 9, 2012

Supervisor: Peeter Puusemp, PhD, Prof., Dept. of Mathematics, Tallinn University of Technology

Opponents: Professor Markku Niemenmaa, University of Oulu

Professor Kalle Kaarli, University of Tartu

Defence of the thesis: May 9, 2012

Declaration: Hereby I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology has not been submitted for any academic degree.

/Tatjana Tamberg/

ISSN 1406-4723
ISBN 978-9949-23-252-9 (publication)
ISBN 978-9949-23-253-6 (PDF)

LOODUS- JA TÄPPISTEADUSED B126

Mõnedest lõplike 2-rühmade klassidest ja nende endomorfismipoolrühmadest

TATJANA TAMBERG

TTÜ
KIRJASTUS

Contents

Introduction

Motives and aims of the thesis

Suppose S and T are two mathematical structures of the same type. Let $\mathrm{End}(S)$ and $\mathrm{End}(T)$ be the semigroups of all endomorphisms of S and T, respectively. Suppose that $\mathrm{End}(S)$ and $\mathrm{End}(T)$ are isomorphic. What can be said about interrelations of S and T? This problem is quite popular in different investigations. Of course, if S and T are isomorphic, then $\mathrm{End}(S)$ and $\mathrm{End}(T)$ are isomorphic as well. In many cases the converse holds also. For example, it holds for Boolean algebras [41] and Boolean rings [18, 19]. An overview of the results on endomorphism properties of different algebraic structures is presented in [1]. Let us give a short overview on state of the art of this problem for semigroups and groups.

In general, considering the problem mentioned for semigroups, we can say that a semigroup cannot be characterized by its endomorphism semigroup in the class of all semigroups. Z. Hedrlin and J. Lambek [13] proved that for every monoid M and every cardinal α there exist α non-isomorphic semigroups whose endomorphism monoids are isomorphic to M. Therefore, it is natural to choose two semigroups S and T from a certain class (or variety) $\mathcal{K}$ of semigroups and study the interrelation between them in the case when the senigroups $\mathrm{End}(S)$ and $\mathrm{End}(T)$ are isomorphic. It is done for some varieties of bands by B. M. Schein [40, 41] and M. Demlová and V. Koubek [6]. Recall that a *band* is an idempotent semigroup. For example, B. M. Schein [40] proved that the endomorphism semigroups of two semilattices (i. e., commutative bands) S and T are isomorphic if and only if S and T are either isomorphic or dually ordered chains. He proved also that there exist at most four non-isomorphic normal bands (i. e., bands that satisfy the identity $xyzx = xzyx$) with isomorphic endomorphism monoids. M. Demlová and V. Koubek [6] obtained similar results for the variety of bands defined by the identity $xyx = xy$ and for the variety of bands defined by the identity $xyxz = xyz$.

Another class of semigroups which is often investigated in the context of their endomorphism semigroups is the class of Clifford semigroups. A. H. Clifford [4] characterized the semigroups that *admit relative inverses*. A semigroup S admits relative inverses if it satisfies the following condition: for each $a \in S$ there exist $e, b \in S$ such that $ea = ae = a$ and $ab = ba = e$. Later these semigroups were called *Clifford semigroups*. The endomorphisms of various Clifford semigroups were studied in detail by M. Samman and J. D. P. Meldrum [39]. Some characterizations of the regularity of endomorphism semigroups of Clifford semigroups are given by S. Worawiset [43]. Seminear-rings of endomorphisms Clifford semigroups

were studied by N. D. Gilbert and M. Samman [7]. They did it under the assumption that a Clifford semigroup S is isomorphic to the direct product $S = G \times \Lambda$ of a group G and a semilattice Λ. In this case the endomorphism semigroups $\mathrm{End}(S)$ are isomorphic to the direct product $\mathrm{End}(G) \times \mathrm{End}(\Lambda)$ of the endomorphism semigroups of G and Λ, and the problem of the recoverability of these Clifford semigroups by their endomorphism semigroups is reduced to the same problem for groups.

Considering the problem of the recoverability of groups by their endomorphism semigroups, much more is known. We have especially diverse information on endomorphisms of Abelian groups, because the endomorphisms of a Abelian group form a ring under the composition and the sum, and, therefore, it is possible to use methods of the theory of rings. An excellent overview of the present situation in the theory of endomorphism rings of Abelian groups is given by P. A. Krylov, A. V. Mikhalev and A. A. Tuganbaev in their book [15] which is based on their papers [17, 16]. In general, for a given group G there exist many groups H such that the semigroups $\mathrm{End}(G)$ and $\mathrm{End}(H)$ are isomorphic, and, for a given Abelian group G there exist many Abelian groups H such that their endomorphism rings $\mathrm{End}(G)$ and $\mathrm{End}(H)$ are isomorphic. Let us give some examples.

A. L. Corner [5] proved that every countable reduced torsion-free ring with unity is isomorphic to the endomorphism rings of countable many countable reduced torsion-free Abelian groups. It follows that the additive group $\mathbb{Z}$ of integers is not determined by its endomorphism ring in the class of all Abelian groups, although there exist classes of Abelian groups that can be described by their endomorphism rings or endomorphism semigroups. For example, R. Baer [3] and I. Kaplansky [14] proved that if endomorphism rings of two torsion Abelian groups are isomorphic then these groups are isomorphic as well. P. Puusemp [29] generalized this result and proved that if endomorphism semigroups of two torsion Abelian groups are isomorphic then these groups are also isomorphic. Examples of Abelian groups which are determined by their endomorphism semigroups in the class of all groups are finite Abelian groups [36], bounded Abelian groups [29] and non-torsion divisible Abelian groups [27]. It follows that the additive group $\mathbb{Q}$ of rational numbers is determined by its endomorphism semigroup in the class of all groups. The same holds for the additive group $\mathbb{R}$ of real numbers. Recall that a group G is *determined by its endomorphism semigroup in the class of all groups* if G is isomorphic to H whenever H is a group such that the semigroup $\mathrm{End}(H)$ is isomorphic to the semigroup $\mathrm{End}(G)$. However, it is possible that an Abelian group G is not determined by its endomorphism semigroup in the class of all groups, there exists an Abelian group G^* such that G is a subgroup of G^* and G^* is determined by its endomorphism semigroup in the class of all groups [33].

Considering non-abelian groups, we have an information for some classes

of finite groups. Examples of non-abelian groups that are determined by their endomorphism semigroups in the class of all groups are for example generalized quaternion groups [35], finite symmetric groups [34], Sylow subgroups of finite symmetric groups [31], some wreath products groups [32, 24], some semidirect products of finite cyclic groups [25, 26] etc. There exist also a lot of examples of finite nonabelian groups that are not determined by their endomorphism semigroups in the class of all groups. We can present quite simple examples of those groups. For example, the semidirect products

$$G = \langle a,\, b \mid b^3 = a^{91} = 1,\ b^{-1}ab = a^{16} \rangle = \langle a \rangle \leftthreetimes \langle b \rangle$$

and

$$H = \langle c,\, d \mid d^3 = c^{91} = 1,\ d^{-1}cd = c^{9} \rangle = \langle c \rangle \leftthreetimes \langle d \rangle$$

of cyclic groups of orders 3 and 91 are non-isomorphic but their endomorphism semigroups are isomorphic [30]. Everything is known for all groups of orders less than 32. Namely, P. Puusemp [22, 23, 21] proved the following: if G is a group of order less than 32 and G^* is a group such that the endomorphism semigroups of G and G^* are isomorphic, then

1) if $G = \langle a,\, b \mid b^3 = 1,\ aba = bab \rangle$ (the binary tetrahedral group), then $G^* \cong G$ or G^* is isomorphic to the alternating group A_4 (the tetrahedral group);
2) if G is not isomorphic to the tetrahedral group or to the binary tetrahedral group, then $G^* \cong G$.

The result 2) inspired one of the main purposes of this dissertation – to detect which non-abelian groups of order $32 = 2^5$ are determined by their endomorphism semigroups in the class of all groups. All groups of order 32 were described by M. Jr. Hall and J. K. Senior [12]. There exist exactly 51 non-isomorphic groups of order 32. In [12], these groups are numbered by $1, 2, \ldots, 51$. We shall mark these groups by $G_1, G_2, \ldots, G_{51}$, respectively. The groups $G_1 - G_8$ are Abelian, and, therefore, are determined by their endomorphism semigroups in the class of all groups. The groups $G_9 - G_{51}$ are non-abelian. In this dissertation, the posed problem is solved for groups of order 32 which can be presented in the forms $G = (C_4 \times C_4) \leftthreetimes C_2$ and $G = (C_8 \times C_2) \leftthreetimes C_2$ where C_2, C_4 and C_8 are cyclic groups of orders 2, 4 and 8, respectively. To solve the problem for all groups of order 32, it occured to be too labor consuming for our dissertation. However, the method used by us is applicable for the rest of groups of this order. Groups $G = (C_4 \times C_4) \leftthreetimes C_2$ and $G = (C_8 \times C_2) \leftthreetimes C_2$ are partial cases of groups presentable in the forms $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$ $(n \geqslant 2)$ and $(C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$ $(n \geqslant 3, m \geqslant 1)$, respectively. Therefore, in the second part of the dissertation, the descriptions of these two classes 2-groups are given. In

addition, the class of finite 2-groups presentable in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$ $(n \geqslant 3)$ is described.

Outline of the thesis

This thesis consists of four chapters and appendices.

In Chapter 1, two classes of groups of order 32 are considered. In Section 1.1 of Chapter 1, it is proved that the groups, presentable in the form $G = (C_4 \times C_4) \leftthreetimes C_2$, can be determined by their endomorphism semigroups in the class of all groups. In Section 1.2 of Chapter 1, it is proved that the groups, presentable in the form $G = (C_8 \times C_2) \leftthreetimes C_2$, are determined by their endomorphism semigroups in the class of all groups.

In Chapter 2, all non-isomorphic groups of order 2^{2n+1}, presentable in the form $G = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2$ $(n \geqslant 3)$, are described. It turns out that there exist 17 different types of these groups. For one type of these groups, it is given for groups of this type their characterizations by endomorphism semigroups and shown that these groups are determined by their endomorphism semigroups in the class of all groups.

In Chapter 3, the groups presentable in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$ $(n \geqslant 3)$ are described by their generators and defining relations. These groups are divided into disjoint classes, where two groups of the same class are isomorphic. Unfortunately, the isomorphism problem for groups of different classes is still open.

In Chapter 4, similarly to Chapter 3, the groups presentable in the form $(C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$ $(n \geqslant 3,\ m \geqslant 1)$ are described by their generators and defining relations. Isomorphism problem for groups presentable in given form is not still solved.

Main novelties of the thesis

1. A method for characterizations finite groups by their endomorphism semigroups is presented. The method is applied to two classes of groups of order 32 and a class of 2-groups of order 2^{2n+1}.

2. All non-isomorphic groups of order 2^{2n+1}, presentable in the form $G = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2$, are described by their generators and defining relations $(n \geqslant 3)$.

3. All groups of order 2^{2n+2}, presentable in the form $G = (C_{2^n} \times C_{2^n}) \leftthreetimes C_4$, are described by their generators and defining relations $(n \geqslant 3)$. All these groups are divided into 36 (if $n = 3$) and 80 (if $n \geqslant 4$) disjoint classes, where two groups of the same class are isomorphic.

4. All groups of order 2^{2n+m+1}, presentable in the form $G = (C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$, are described by their generators and defining relations ($n \geqslant 3$, $m \geqslant 1$).

List of publications

The results of the thesis have been published in the following papers:

1. Gramušnjak, T., Puusemp, P. *A characterization of a class of groups of order* 32 *by their endomorphism semigroups.* Algebras, Groups and Geometries, 2005, **22**, no. 4, 387–412.

2. Gramushnjak, T., Puusemp, P. *Description of a Class of* 2*-Groups.* J. of Nonlinear Mathematical Physics, 2006, **13** (Supplement), 55–65.

3. Gramushnjak, T. *A characterization of a class of* 2*-groups by their defining relations.* J. of Generalized Lie Theory and Applications, 2008, **2** (3), 157–161.

4. Gramushnjak, T., Puusemp, P. *A Characterization of a Class of* 2*-Groups by Their Endomorphism Semigroups.* Ch. 14 in: S. Silvestrov et al. (eds.), *Generalized Lie Theory in Mathematics, Physics and Beyond.* Springer-Verlag, Berlin Heidelberg, 2009, pp. 151–159.

5. Tamberg, T. *Finding a class of* 2*-groups.* Proc. Estonian Acad. Sci., 2010, **59**, no. 4, 370–374.

Conference reports

The results of the thesis have been presented on the following conferences:

1. The 4th Baltic-Nordic Workshop on Algebra, Geometry, and Mathematical Physics, Tartu (Estonia), October 9–11, 2008. "A characterization of a class of 2-groups of order $2^{2(n+1)}$".

2. Workshop on Algebra and its Applications, Viinistu (Estonia), May 2–4, 2008. "A characterization of a class of 2-groups of order $2^{2(n+1)}$ by their defining relations".

3. The 3th Baltic-Nordic Workshop on Algebra, Geometry, and Mathematical Physics, Göteborg (Sweden), October 11-13, 2007. "A characterization of a class of 2-groups by their endomorphism semigroups".

4. Workshop on Algebra and its Applications, Ratnieki (Latvia), May 4–6, 2007. "A characterization of some groups of order 2^{2n+1} by their endomorphism semigroups".

5. The 2nd Baltic-Nordic Workshop on Algebra, Geometry, and Mathematical Physics, Lund (Sweden), October 12–14, 2006. "A characterization of a class of groups of order 32 by their endomorphism semigroups".

6. The 1st Baltic-Nordic Workshop on Algebra, Geometry, and Mathematical Physics, Tallinn (Estonia), October 8, 2005. "A class of 2-groups of order 2^{2n+1}".

7. Workshop on Algebra and its Applications, Nelijärve (Estonia), May 7–8, 2005. "(2×2)-matrices of order 2 over $\mathbb{Z}_{2^n}$".

Acknowledgements

I would like to thank my supervisor Prof. Peeter Puusemp for his patient, guidance and advice. My sincerest thanks belong to my colleagues in Tallinn University for supporting and encouraging me. I am deeply thankful to my husband Gert Tamberg for his help, support and love. I also would like to thank my mother and my father-in-law for sitting with my little son when I wrote this Thesis.

I gratefully acknowledge Tallinn University of Technology, especially its Department of Mathematics for financial support. The research was also partially supported by the Estonian Science Fund, grant ETF-5900.

Notations and preliminaries

We shall use the following notations:

G	a group
$a, b, c, ...$	the elements of G
G'	the derived group of G
$Z(G)$	the center of G
$o(g)$	the order of an element $g \in G$
x, y, z, u, v, w or $\alpha, \beta, \gamma, ...$	the maps
gx, $g\alpha$	the image of element $g \in G$ under maps x, α
$\mathrm{End}(G)$	the endomorphism semigroup of G
$\mathrm{Aut}(G)$	the group of all automorphisms of G
$\mathrm{Ker}\ x$	the kernel of x
$\mathrm{Im}\ x$	the image of x
C_n	the cyclic group of order n
$H \leftthreetimes K$	a semidirect product of a normal subgroup H and a subgroup K
$\widehat{g}$	the inner automorphism, generated by g ($h\widehat{g} = g^{-1}hg$)
$I(G)$	the set of all idempotents of $\mathrm{End}(G)$
$\mathbb{Z}_n$	the ring of residue classes modulo n
$\mathbb{Z}_n^*$	the set of all invertible elements of $\mathbb{Z}_n$
$\lvert A\rvert$	the number of elements of a set A

$Q_n = \langle a, b \mid a^{2^n} = 1,\ a^{2^{n-1}} = b^2,\ b^{-1}ab = a^{-1} \rangle$ the generalized quaternion group ($n \geqslant 2$)

$[g, h] = g^{-1}h^{-1}gh \quad (g, h \in G)$

$K(x) = \{\, z \in \mathrm{End}(G) \mid zx = xz = z \,\} \quad (x \in \mathrm{End}(G))$

$J(x) = \{\, z \in \mathrm{End}(G) \mid zx = xz = 0 \,\} \quad (x \in \mathrm{End}(G))$

$D(x) = \{u \in \mathrm{Aut}(G) \mid ux = xu = x\} \quad (x \in \mathrm{End}(G))$

$J_1(x) = \{\, z \in J(x) \mid$ there exist $v, w \in \mathrm{End}(G)$ such that $vx = v,\ vw = z \,\}$

$P(x) = \{\, z \in \mathrm{End}(G) \mid zx = xz = x \,\} \quad (x \in \mathrm{End}(G))$

$V(x) = \{\, z \in \mathrm{Aut}(G) \mid zx = x \,\} \quad (x \in \mathrm{End}(G))$

$W(x) = \{\, z \in \mathrm{End}(G) \mid xz = z \,\} \quad (x \in \mathrm{End}(G))$

$H(x) = \{\, z \in \mathrm{End}(G) \mid xz = z,\ zx = 0 \,\} \quad (x \in \mathrm{End}(G))$

Remark, that if $x \in I(G)$, then $K(x)$ forms semigroup with identity.

For convenience of reference, let us state some well known facts on the endomorphism semigroup $\mathrm{End}(G)$ of a group G.

Lemma 1 ([36], Lemma 1.1) *If $x \in I(G)$, then $G = \operatorname{Ker} x \leftthreetimes \operatorname{Im} x$ and $\operatorname{Im} x = \{\, g \in G \mid gx = g \,\}$.*

Lemma 2 ([11], Lemma 2) *If $y \in \operatorname{End}(G)$ and $\operatorname{Im} y$ is Abelian, then $\widehat{g} \in V(x)$ for each $g \in G$.*

Lemma 3 ([11], Lemma 3) *Let $x, y \in \operatorname{End}(G)$. Then $yx = x$ if and only if $g^{-1} \cdot gy \in \operatorname{Ker} x$ for each $g \in G$.*

Lemma 4 ([36], Lemma 1.6) *If $x \in I(G)$, then*

$$K(x) = \{\, y \in \operatorname{End}(G) \mid (\operatorname{Im} x)y \subset \operatorname{Im} x,\ (\operatorname{Ker} x)y = \langle 1 \rangle \,\}$$

and $K(x)$ is a subsemigroup with unity x of $\operatorname{End}(G)$ which is canonically isomorphic to $\operatorname{End}(\operatorname{Im} x)$. In this isomorphism element y of $K(x)$ corresponds to its restriction on the subgroup $\operatorname{Im} x$ of G.

Lemma 5 ([11], Lemma 5) *If $x \in I(G)$, then*

$$J(x) = \{\, y \in \operatorname{End}(G) \mid (\operatorname{Im} x)y = \langle 1 \rangle,\ (\operatorname{Ker} x)y \subset \operatorname{Ker} x \,\}.$$

Lemma 6 ([11], Lemma 6) *If $x \in I(G)$, then*

$$H(x) = \{\, y \in \operatorname{End}(G) \mid (\operatorname{Im} x)y \subset \operatorname{Ker} x,\ (\operatorname{Ker} x)y = \langle 1 \rangle \}.$$

Lemma 7 ([11], Lemma 7) *If $x \in I(G)$, then*

$$P(x) = \{\, y \in \operatorname{End}(G) \mid y|_{Im\, x} = 1_{Im\, x},\ (\operatorname{Ker} x)y \subset \operatorname{Ker} x \,\}.$$

Lemma 8 ([11], Lemma 8) *If $x \in I(G)$, then*

$$W(x) = \{\, y \in \operatorname{End}(G) \mid (\operatorname{Ker} x)y = \langle 1 \rangle \}.$$

Lemma 9 ([11], Lemma 9) *If $x, y \in \operatorname{End}(G)$ and $xy = yx$, then*

$$(\operatorname{Im} x)y \subset \operatorname{Im} x, \quad (\operatorname{Ker} x)y \subset \operatorname{Ker} x.$$

Lemma 10 ([36], Theorem 4.2) *Each finite Abelian group is determined by its endomorphism semigroup in the class of all groups.*

1 A characterization of two classes of 2-groups of order 32 by their endomorphism semigroups

There exist exactly 51 non-isomorphic groups of order 32 (see [12]). These groups (in [12]) are numbered by 1, 2, ..., 51. In this chapter we shall denote these groups by $G_1, G_2, \ldots, G_{51}$, respectively. The groups $G_1 - G_8$ are Abelian and, therefore, are determined by their endomorphism semigroups in the class of all groups (Lemma 10). The groups $G_9 - G_{51}$ are non-abelian. In this chapter it is proved that the groups of order 32, presentable in the forms $(C_4 \times C_4) \leftthreetimes C_2$ or $(C_8 \times C_2) \leftthreetimes C_2$, are determined by their endomorphism semigroups in the class of all groups.

1.1 The groups presentable in the form $(C_4 \times C_4) \leftthreetimes C_2$

The results presented in this section have been published in [11].

Denote by $\mathcal{G}$ the set of all groups G of order 32 such that G can be presented in the form $G = (C_4 \times C_4) \leftthreetimes C_2$. By [12],

$$\mathcal{G} = \{G_3, G_{14}, G_{16}, G_{31}, G_{34}, G_{39}, G_{41}\}.$$

The group G_3 is Abelian, i.e. $G_3 = (C_4 \times C_4) \times C_2$. Therefore, it is determined by its endomorphism semigroup in the class of all groups (Lemma 10). The group G_{14} splits into the direct product $G_{14} = C_4 \times D_4$, where D_4 is the dihedral group of order 8. The group D_4 is determined by its endomorphism semigroup in the class of all groups ([28], Corollary 3.7). On the other hand, if groups A and B are determined by their endomorphism semigroups in the class of all groups, so is their direct product $A \times B$ ([36], Theorem 1.13). Therefore, the group G_{14} also is determined by its endomorphism semigroup in the class of all groups.

In this section, we shall describe all groups of the class $\mathcal{G}$, except G_3 and G_{14}, by their endomorphism semigroups (Theorems 1.1, 1.3 and 1.5). It follows from these descriptions that each group of the class $\mathcal{G}$ is determined by its endomorphism semigroup in the class of all groups (Theorems 1.2, 1.4 and 1.6).

Let us recall some properties of groups G_{16}, G_{31}, G_{34}, G_{39}, G_{41}. All these properties are presented in [12]. These groups are given by generators and defining relations as follows:

$$G_{16} = \langle a, b, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ cb = bc,\ c^{-1}ac = ab^2 \rangle = \\ = (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2,$$

$$G_{31} = \langle a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = b \rangle = \\ = (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2,$$
$$G_{34} = \langle a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^{-1},\ c^{-1}bc = b^{-1} \rangle = \\ = (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2,$$
$$G_{39} = \langle a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = ab^2,\ c^{-1}bc = ba^2 \rangle = \\ = (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2,$$
$$G_{41} = \langle a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^{-1}b^2,\ c^{-1}bc = ba^2 \rangle = \\ = (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2.$$

The numbers of elements of given orders (i.e., order structure), the numbers of automorphisms and the derived groups for cited groups are presented in the following table.

Group	Order structure			Automorphisms	Derived group
	2	4	8		
G_{16}	7	24		2^8	$\langle b^2 \rangle \cong C_2$
G_{31}	7	16	8	2^5	$\langle a^{-1}b \rangle \cong C_4$
G_{34}	19	12		$2^9 \cdot 3$	$\langle a^2 \rangle \times \langle b^2 \rangle \cong C_2 \times C_2$
G_{39}	11	20		2^8	$\langle a^2 \rangle \times \langle b^2 \rangle \cong C_2 \times C_2$
G_{41}	7	24		$2^6 \cdot 3$	$\langle a^2 \rangle \times \langle b^2 \rangle \cong C_2 \times C_2$

Table 1. Order structure, the numbers of automorphisms and the derived groups for groups G_{16}, G_{31}, G_{34}, G_{39} and G_{41}.

In the next three subsections we shall characterize the groups G_{16}, G_{31}, G_{34}, G_{39} and G_{41} by their endomorphism semigroups.

1.1.1 The group G_{16}

In this subsection, we shall characterize the group

$$G_{16} = \langle\, a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ cb = bc,\ c^{-1}ac = ab^2 \,\rangle =$$

$$= (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2,$$

by its endomorphism semigroup. The derived group of G_{16} is $G'_{16} = \langle b^2 \rangle$ and

$$G_{16}/G'_{16} = \langle aG'_{16} \rangle \times \langle bG'_{16} \rangle \times \langle cG'_{16} \rangle \cong C_4 \times C_2 \times C_2.$$

Therefore,

$$G_{16} = \langle c,\, b \rangle \leftthreetimes \langle a \rangle = (\langle b \rangle \times \langle c \rangle) \leftthreetimes \langle a \rangle.$$

Theorem 1.1 *A finite group G is isomorphic to G_{16} if and only if $|\operatorname{Aut}(G)| = 2^8$ and there exist $x, y \in I(G)$ such that the following properties hold:*

1^0 $K(x) \cong \mathrm{End}(C_2)$;
2^0 $y \in I(G) \cap J(x)$ *and* $K(y) \cong \mathrm{End}(C_4)$;
3^0 $|J(x) \cap J(y)| = 2$;
4^0 $I(G) \cap J(x) \cap J(y) = \{0\}$;
5^0 $|\{z \in \mathrm{End}(G) \mid xz = z,\ zx = zy = 0\}| = 2$;
6^0 $|\{z \in \mathrm{End}(G) \mid yz = z,\ zx = zy = 0\}| = 4$;
7^0 $z \in V(x) \cap \left(\cap_{u \in J_1(x)} V(u)\right) \Longrightarrow z^2 = 1$;
8^0 $\cap_{z \in T} K(z) = \{0\}$, *where* $T = \{z \in I(G) \mid yz = z,\ zy = y,\ zx = 0\}$.

Proof. Necessity. Let $G = G_{16}$. Then $|\mathrm{Aut}(G)| = 2^8$. Denote by x and y the projections of G onto its subgroups $\langle c \rangle$ and $\langle a \rangle$, respectively. Then $x,\ y \in I(G)$ and $xy = yx = 0$, i.e., $y \in I(G) \cap J(x)$. We shall prove that x and y satisfy properties $1^0 - 8^0$.

Lemma 4 implies properties 1^0 and 2^0. Clearly, $\mathrm{Ker}\, x \cap \mathrm{Ker}\, y = \langle b \rangle$. Hence by Lemma 5, each $z \in J(x) \cap J(y)$ maps on the generators of G as follows

$$z:\ c \longmapsto 1,\ a \longmapsto 1,\ b \longmapsto b^i \tag{1.1}$$

for some $i \in \mathbb{Z}_4$. Map (1.1) preserves the defining relations of G and is an endomorphism of G if and only if $i \equiv 0 \pmod 2$. Hence $|J(x) \cap J(y)| = 2$. The map (1.1), where $i \equiv 0 \pmod 2$, is an idempotent of $\mathrm{End}(G)$ if and only if $i = 0$. Therefore, $I(G) \cap J(x) \cap J(y) = \{0\}$. Properties 3^0 and 4^0 are proved.

Assume that $z \in \{z \in \mathrm{End}(G) \mid xz = z,\ zx = zy = 0\}$. Then $az = bz = 1,\ cz \in \mathrm{Ker}\, x \cap \mathrm{Ker}\, y = \langle b \rangle$, i.e., $cz = b^i$ for some $i \in \mathbb{Z}_4$. Since $c^2 = 1$, we have $i \equiv 0 \pmod 2$. Each map z for which $az = bz = 1$ and $cz = b^i,\ i \equiv 0 \pmod 2$, preserves the defining relations of G and is an endomorphism of G such that $z \in \{z \in \mathrm{End}(G) \mid xz = z,\ zx = zy = 0\}$. There exist two endomorphisms of this type. Therefore, property 5^0 holds.

An endomorphism z of G belongs into $\mathcal{A} = \{z \in \mathrm{End}(G) \mid yz = z,\ zx = zy = 0\}$ if and only if $(\mathrm{Ker}\, y)z = \langle 1 \rangle$, $\mathrm{Im}\, z \subset \mathrm{Ker}\, x \cap \mathrm{Ker}\, y$. Hence

$$z:\ c \longmapsto 1,\ a \longmapsto b^i,\ b \longmapsto 1 \tag{1.2}$$

for some $i \in \mathbb{Z}_4$. Map (1.2) preserves the defining relations of G and is an endomorphism of G for each $i \in \mathbb{Z}_4$. Therefore, $|\mathcal{A}| = 4$ and property 6^0 holds.

In order to prove property 7^0, we find $V(x)$. If $z \in V(x)$, then, by Lemma 3,

$$z:\ \ c \longmapsto ca^s b^t,\ a \longmapsto a^p b^q,\ b \longmapsto a^m b^r \tag{1.3}$$

for some $s,\ t,\ p,\ q,\ m,\ r \in \mathbb{Z}_4$. It is easy to check that map (1.3) preserves the defining relations of G and is an endomorphism of G if and only if

$$s \equiv t \equiv m \equiv 0 \pmod 2,\quad p \equiv r \pmod 2.$$

Map (1.3) is an automorphism of G and belongs to $V(x)$ if and only if

$$s \equiv t \equiv m \equiv 0 \pmod 2, \quad p \equiv r \equiv 1 \pmod 2. \tag{1.4}$$

Let us find $J_1(x) \subset J(x)$. By Lemma 5, $J(x)$ consists of endomorphisms u of the form

$$u: \quad c \longmapsto 1,\ a \longmapsto a^i b^j,\ b \longmapsto a^k b^l. \tag{1.5}$$

Map (1.5) preserves the defining relations of G and belongs to $J(X)$ if and only if $k \equiv l \equiv 0 \pmod 2$. Let us find now under which conditions such u belongs to $J_1(x)$, i.e., there exist endomorphisms v, w of G such that $u = vw$ and $vx = v$. Clearly, $u = 0 \in J_1(x)$ (choose $v = w = 0$). The condition $vx = v$ is equivalent to the inclusion $\operatorname{Im} v \subset \operatorname{Im} x = \langle c \rangle$. It is easy to see that the case $cv = c$ is possible only if $u = 0$. Therefore, we have to consider three endomorphisms of G which are possible candidates for v:

$$\begin{aligned} v_1 &: \quad c \longmapsto 1,\ a \longmapsto c,\ b \longmapsto c, \\ v_2 &: \quad c \longmapsto 1,\ a \longmapsto c,\ b \longmapsto 1, \\ v_3 &: \quad c \longmapsto 1,\ a \longmapsto 1,\ b \longmapsto c. \end{aligned}$$

In the case of v_1 we have

$$a^i b^j = au = av_1 w = cw, \quad a^k b^l = bu = bv_1 w = cw,$$

which imply that $i = k,\ j = l$ and $k \equiv l \equiv 0 \pmod 2$. In the case of v_2 we have

$$a^i b^j = au = av_2 w = cw, \quad a^k b^l = bu = bv_2 w = 1w = 1,$$

which imply that $k = l = 0$ and $i \equiv j \equiv 0 \pmod 2$. In the case of v_3 we have

$$a^i b^j = au = av_3 w = 1w = 1, \quad a^k b^l = bu = bv_3 w = cw,$$

which imply that $i = j = 0$ and $k \equiv l \equiv 0 \pmod 2$. Consequently, if $u \in J_1(x)$, then u is an endomorphism of G which has one of the following forms (all these forms include $u = 0$):

$$\begin{aligned} u_1 &: \quad c \longmapsto 1,\ a \longmapsto a^{2f} b^{2g},\ b \longmapsto a^{2f} b^{2g}, \\ u_2 &: \quad c \longmapsto 1,\ a \longmapsto a^{2f} b^{2g},\ b \longmapsto 1, \\ u_3 &: \quad c \longmapsto 1,\ a \longmapsto 1,\ b \longmapsto a^{2f} b^{2g}, \end{aligned}$$

where $f,\ g \in \mathbb{Z}_2$. Conversely, each u_h $(h = 1, 2, 3)$ belongs to $J_1(x)$, because $v_h x = v_h$ and $u_h = v_h w$, where

$$w: \quad c \longmapsto a^{2f} b^{2g},\ a \longmapsto 1,\ b \longmapsto 1.$$

Choose $z \in V(x)$ such that $z \in \cap_{u \in J_1(x)} V(u) = \cap_{h \in \{1,2,3\}} V(u_h)$. Then z is given by (1.3), where s, t, p, q, r, m, r satisfy conditions (1.4), and $zu_h = u_h$, i.e.,

$$\begin{aligned} a^{2f}b^{2g} &= au_1 = azu_1 = (a^p b^q)\, u_1 = a^{2f(p+q)} b^{2g(p+q)}, \\ 1 &= au_3 = azu_3 = (a^p b^q)\, u_1 = a^{2fq} b^{2gq}. \end{aligned}$$

This implies $fq \equiv gq \equiv 0 \,(\mathrm{mod}\ 2)$ for each $f,\ g \in \mathbb{Z}_2$. Hence $q \equiv 0 \,(\mathrm{mod}\ 2)$ and

$$\begin{aligned} cz^2 &= (cz)z = \left(ca^s b^t\right) z = ca^{s(1+p)+mt} b^{t(1+r)+qs} = c, \\ az^2 &= (az)z = (a^p b^q)\, z = (a^p b^q)^p\, (a^m b^r)^q = a^{p^2+mq} b^{q(p+r)} = a, \\ bz^2 &= (bz)z = (a^m b^r)\, z = (a^p b^q)^m\, (a^m b^r)^r = a^{m(p+r)} b^{r^2+mq} = b, \end{aligned}$$

i.e., $z^2 = 1$. Therefore, property 7^0 holds.

To prove property 8^0, we find first the set T. Choose $z \in T$. Then

$$cz = c(yz) = 1,\ bz = b(yz) = 1,\ az \in \mathrm{Ker}\ x = \langle a \rangle \times \langle b \rangle$$

and $az = a^i b^j$ for some $i,\ j \in \mathbb{Z}_4$. Since $zy = y$, we have

$$a = ay = a(zy) = (a^i b^j) y = a^i, \quad i = 1,$$

$$z: \quad c \longmapsto 1,\ a \longmapsto ab^j,\ b \longmapsto 1. \tag{1.6}$$

Conversely, map (1.6) preserves the defining relations of G and is an endomorphism of G which satisfies equalities $z^2 = z,\ yz = z,\ zy = y$ and $zx = 0$. Therefore, the set T consists of maps (1.6), where $j \in \mathbb{Z}_4$. Denote map (1.6) by z_j. Then $T = \{ z_j \mid j \in \mathbb{Z}_4 \}$ and

$$\mathrm{Ker}\ z_j = \langle b,\, c \rangle\,,\ \mathrm{Im}\ z_j = \left\langle ab^j \right\rangle \cong C_4.$$

By Lemma 4, $K(z_j)$ consists of the following maps:

$$z_{ji}: \quad c \longmapsto 1,\ b \longmapsto 1,\ a \longmapsto (ab^j)^i = a^i b^{ij},$$

where $i \in \mathbb{Z}_4$. So

$$\cap_{z \in T} K(z) = \cap_{j \in \mathbb{Z}_4} K(z_j) = \{0\}.$$

Property 8^0 is proved. The necessity is proved.

Sufficiency. Let G be a finite group, $|\,\mathrm{Aut}(G)| = 2^8$, and let there exist $x,\ y \in I(G)$ which satisfy properties $1^0 - 8^0$. Our aim is to prove that $G \cong G_{16}$.

By Lemmas 1 and 4,

$$G = \operatorname{Ker} x \leftthreetimes \operatorname{Im} x, \quad K(x) \cong \operatorname{End}(\operatorname{Im} x).$$

As each finite Abelian group is determined by its endomorphism semigroup in the class of all groups, property 1^0 implies $\operatorname{Im} x \cong C_2$, i.e., $\operatorname{Im} x = \langle c \rangle$ for some element c of order 2. Similarly, by property 2^0, $G = \operatorname{Ker} y \leftthreetimes \operatorname{Im} y$ and $\operatorname{Im} y = \langle a \rangle$ for some element a of order 4. In view of Lemmas 1 and 9, we have

$$G = (M \leftthreetimes \langle a \rangle) \leftthreetimes \langle c \rangle, \ \ (M \leftthreetimes \langle c \rangle) \leftthreetimes \langle a \rangle,$$

where

$$M = \operatorname{Ker} x \cap \operatorname{Ker} y, \ \operatorname{Im} x = \langle c \rangle, \ \operatorname{Im} y = \langle a \rangle,$$

$$\operatorname{Ker} x = M \leftthreetimes \langle a \rangle, \ \operatorname{Ker} y = M \leftthreetimes \langle c \rangle.$$

Therefore, $G/M = \langle aM \rangle \times \langle cM \rangle$ and

$$G' \subset M. \tag{1.7}$$

Since $\operatorname{Aut}(G)$ is a 2-group, the group of inner automorphisms $\widehat{G} \cong G/Z(G)$ is also a 2-group and hence all $2'$-elements of G belong into its center $Z(G)$. Therefore, the group G splits into the direct product $G = G_{2'} \times G_2$ of its Hall $2'$-subgroup $G_{2'}$ and Sylow 2-subgroup G_2. Denote by z the projection of G onto its subgroup $G_{2'}$. Then $z \in I(G) \cap J(x) \cap J(y)$ and, by 4^0, $z = 0$. Hence G is 2-group.

Choose $z \in \operatorname{End}(G)$, such that $xz = z, \ zx = zy = 0$. Then $(cz)^2 = 1$ and

$$\operatorname{Ker} x \xrightarrow{z} \langle 1 \rangle, \ \operatorname{Im} x = \langle c \rangle \xrightarrow{z} \langle cz \rangle \in \operatorname{Ker} x \cap \operatorname{Ker} y = M.$$

Conversely, if $d \in M$ such that $d^2 = 1$, then we can define the endomorphism z of G by setting

$$\operatorname{Ker} x \xrightarrow{z} \langle 1 \rangle, \ \operatorname{Im} x = \langle c \rangle \xrightarrow{z} \langle d \rangle, \ cz = d.$$

This endomorphism satisfies equalities $xz = z, \ zx = zy = 0$. Together with property 5^0 it follows that the subgroup M of G has only one element of order two. By [38], Theorem 5.46, M is cyclic or generalized quaternion group. Similarly, by property 6^0, M has 4 elements d such that $d^4 = 1$. Since the number of elements d, $d^4 = 1$, is greater than 4 in each generalized quaternion group, the subgroup M is cyclic of order $2^n, \ n \geqslant 2$:

$$M = \langle b \rangle \cong C_{2^n}, \quad n \geqslant 2, \tag{1.8}$$

for some $b \in M$.

Choose $u \in J_1(x)$. By definition of $J_1(x)$, there exist $v,\, w \in \mathrm{End}(G)$ such that $vx = v,\ vw = u$. Hence by Lemma 1,

$$\mathrm{Im}\ v \subset \mathrm{Im}\ x = \langle c \rangle\,,\ \ \mathrm{Im}\ u = \mathrm{Im}\,(vw) \subset \langle cw \rangle\,,$$

and $\mathrm{Im}\ u$ is a cyclic group. Since $\mathrm{Im}\ x$ is also cyclic, then, due to Lemma 2, $\widehat{g} \in V(x) \cap \left(\cap_{u \in J_1(x)} V(u)\right)$ for each $g \in G$. Property 7^0 implies that

$$g^2 \in Z(G) \ \ \text{for each} \ \ g \in G.$$

Therefore, the factor-group $G/Z(G)$ is Abelian, $G' \subset Z(G)$ and

$$g^2 = 1 \ \ \text{for each} \ \ g \in G'. \tag{1.9}$$

Clearly, $G' \neq \langle 1 \rangle$, because otherwise $G = M \times \langle a \rangle \times \langle c \rangle$ and the projection z of G onto its subgroup M is non-zero element which belongs to $I(G) \cap J(x) \cap J(y)$. This contradicts 4^0. Therefore, by (1.7)–(1.9),

$$G' = \left\langle b^{2^{n-1}} \right\rangle$$

and the factor-group G/G' splits as follows:

$$G/G' = \left\langle cG' \right\rangle \times \left\langle aG' \right\rangle \times \left\langle bG' \right\rangle \cong C_2 \times C_4 \times C_{2^{n-1}}.$$

Let us consider the homomorphisms

$$G \xrightarrow{\ \varepsilon\ } G/G' \xrightarrow{\ \pi\ } \left\langle bG' \right\rangle \xrightarrow{\ \alpha_i\ } \langle b \rangle\,,$$

where ε is the natural homomorphism and π is the projection and $(bG')\alpha_i = b^{2i},\ i \in \mathbb{Z}_{2^{n-1}}$. The product $\varepsilon\pi\alpha_i$ is an endomorphism of G. The number of such endomorphisms is 2^{n-1} and each such endomorphism belongs to $J(x) \cap J(y)$. Property 3^0 implies that $n = 2$, i.e., $b^4 = 1$, $G' = \left\langle b^2 \right\rangle \cong C_2$ and G is a group of order 32.

Assume that $ab \neq ba$. Then

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

$$ab^i \cdot ab^i = a^2 \cdot a^{-1}b^i a \cdot b^i = a^2 \ \ (i \in \mathbb{Z}_4).$$

The set T consist of $z \in I(G)$ such that $yz = z,\ zy = y$ and $zx = 0$. Hence

$$\mathrm{Ker}\ z = \mathrm{Ker}\ y = \langle b,\, c \rangle\,,\ \mathrm{Im}\ z \cong \mathrm{Im}\ y = \langle a \rangle\,,$$

$$\mathrm{Im}\ z \subset \mathrm{Ker}\ x = \langle b,\, a \rangle = \langle b \rangle \leftthreetimes \langle a \rangle\,.$$

By Lemma 1, $\mathrm{Im}\ z \cap \mathrm{Ker}\ z = \langle 1 \rangle$. Therefore, $\mathrm{Im}\ z = \left\langle ab^i \right\rangle$ for some $i \in \mathbb{Z}_4$ and

$$G = \mathrm{Ker}\ z \leftthreetimes \mathrm{Im}\ z = \langle b,\, c \rangle \leftthreetimes \left\langle ab^i \right\rangle,$$

$$bz = cz = 1,\ az = (ab^i)z = ab^i. \tag{1.10}$$

Conversely, if $z : G \longrightarrow G$ is given by (1.10), where $i \in \mathbb{Z}_4$, then $z \in I(G),\ yz = z,\ zy = y$ and $zx = 0$, i.e., $z \in T$. If now z is an arbitrary element of T and z is given by (1.10), then the endomorphism u of G, where

$$bu = cu = 1,\ au = a^2,$$

satisfies the equalities $uz = zu = u$, i.e., $u \in K(z)$. This means that $u \in \cap_{z\in T} K(z)$. This contradicts property 8^0. Consequently,

$$ab = ba.$$

Let us consider now the commutators $[a, c]$ and $[b, c]$. Since $G' = \langle b^2 \rangle$, we have $a^{-1}c^{-1}ac \in \langle b^2 \rangle,\ b^{-1}c^{-1}bc \in \langle b^2 \rangle$, i.e.,

$$c^{-1}ac = ab^{2s},\quad c^{-1}bc = b^{\pm 1}$$

for some $s \in \mathbb{Z}_2$. Hence four cases are possible:

I $\quad c^{-1}ac = a,\quad c^{-1}bc = b;$
II $\quad c^{-1}ac = a,\quad c^{-1}bc = b^{-1};$
III $\quad c^{-1}ac = ab^2,\quad c^{-1}bc = b;$
IV $\quad c^{-1}ac = ab^2,\quad c^{-1}bc = b^{-1}.$

In the cases I, II and III we have $G \cong G_3,\ G \cong G_{14}$ and $G \cong G_{16}$, respectively. Let us now consider case IV. Then

$$c^{-1}bc = b^{-1},\quad c^{-1}(ab)c = ab^2b^{-1} = ab.$$

Replacing a by ab, we see that $G \cong G_{14}$. Since

$$|\operatorname{Aut}(G_3)| = 2^9 \cdot 3,\ |\operatorname{Aut}(G_{14})| = 2^7$$

and $|\operatorname{Aut}(G)| = 2^8$, we have $G \cong G_{16}$. The sufficiency is proved and so is Theorem 1.1. $\square$

Theorem 1.2 *The group G_{16} is determined by its endomorphism semigroup in the class of all groups.*

Proof. Let G^* be a group such that the endomorphism semigroups of G^* and G_{16} are isomorphic:

$$\operatorname{End}(G^*) \cong \operatorname{End}(G_{16}). \tag{1.11}$$

Denote by z^* the image of $z \in \operatorname{End}(G_{16})$ in isomorphism (1.11). Since $\operatorname{End}(G^*)$ is finite, so is G^* ([2], Theorem 2). By Theorem 1.1, $|\operatorname{Aut}(G_{16})| = 2^8$ and there exist $x, y \in I(G)$ satisfying properties $1^0 - 8^0$ of Theorem

1.1. These properties are formulated so that they are preserved in isomorphism (1.11). Therefore, $|\operatorname{Aut}(G^*)| = 2^8$ and the idempotents x^* and y^* of $\operatorname{End}(G^*)$ satisfy properties, similar to properties $1^0 - 8^0$ (it is necessary to change everywhere $z \in \operatorname{End}(G_{16})$ by $z^* \in \operatorname{End}(G^*)$). Using now Theorem 1.1 for G^*, it follows that G^* and G_{16} are isomorphic. Theorem 1.2 is proved. $\square$

1.1.2 The group G_{31}

In this subsection we characterize the group

$$G_{31} = \langle\, a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = b \rangle =$$

$$= (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2$$

by its endomorphism semigroup. Denote $d = a^{-1}b$. Then $c^{-1}dc = d^{-1}$, $c^{-1}ac = b = ad$ and, replacing the letter d by b, we get

$$G_{31} = \langle a,\, b,\, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}bc = b^{-1},\ c^{-1}ac = ab \rangle =$$

$$= (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (C_4 \times C_4) \leftthreetimes C_2 =$$

$$= (\langle b \rangle \leftthreetimes \langle c \rangle) \leftthreetimes \langle a \rangle = (C_4 \leftthreetimes C_2) \leftthreetimes C_4.$$

The derived group of G_{31} is $G'_{31} = \langle b \rangle \cong C_4$ and

$$G_{31}/G'_{31} = \langle aG'_{16} \rangle \times \langle cG'_{16} \rangle \cong C_4 \times C_2.$$

Theorem 1.3 *A finite group G is isomorphic to G_{31} if and only if $|\operatorname{Aut}(G)| = 2^5$ and there exist $x,\, y \in I(G)$ such that the following properties hold:*

1^0 $K(x) \cong \operatorname{End}(C_2)$;
2^0 $y \in I(G) \cap J(x)$ *and* $K(y) \cong \operatorname{End}(C_4)$;
3^0 $J(x) \cap J(y) = \{0\}$;
4^0 $|\{z \in \operatorname{End}(G) \mid xz = z,\ zx = zy = 0\}| = 2$;
5^0 $|\{z \in \operatorname{End}(G) \mid yz = z,\ zx = zy = 0\}| = 4$;
6^0 $|T| = 4$, *where* $T = \{\, z \in I(G) \mid yz = z,\ zy = y,\ zx = 0 \,\}$;
7^0 $\cap_{z \in T} K(z) = \{0\}$.

Proof. Necessity. Let $G = G_{31}$. Then $|\operatorname{Aut}(G)| = 2^5$. Denote by x and y the projections of G onto its subgroups $\langle c \rangle$ and $\langle a \rangle$, respectively. Then $x,\, y \in I(G)$ and $xy = yx = 0$, i.e., $y \in I(G) \cap J(x)$. We shall prove that x and y satisfy properties $1^0 - 7^0$. Lemma 4 implies properties 1^0 and 2^0. Clearly, $\operatorname{Ker} x \cap \operatorname{Ker} y = \langle b \rangle$. Hence by Lemma 5, each $z \in J(x) \cap J(y)$ maps on the generators of G as follows

$$z:\ a \longmapsto 1,\ c \longmapsto 1,\ b \longmapsto b^i \tag{1.12}$$

for some $i \in \mathbb{Z}_4$. Map (1.12) preserves the defining relations of G and is an endomorphism of G if and only if $i = 0$. Hence $z = 0$, i.e., $J(x) \cap J(y) = \{0\}$ and property 3^0 holds. The proofs of properties $4^0 - 7^0$ repeat exactly the proofs of properties $5^0 - 8^0$ in Theorem 1.1. The necessity is proved.

Sufficiency. Let G be a finite group, $|\operatorname{Aut}(G)| = 2^5$ and there exist $x, y \in I(G)$ which satisfy properties $1^0 - 7^0$. Our aim is to prove that $G \cong G_{31}$.

By Lemmas 1 and 4,

$$G = \operatorname{Ker} x \leftthreetimes \operatorname{Im} x, \quad K(x) \cong \operatorname{End}(\operatorname{Im} x).$$

As each finite Abelian group is determined by its endomorphism semigroup in the class of all groups, property 1^0 implies $\operatorname{Im} x \cong C_2$, i.e. $\operatorname{Im} x = \langle c \rangle$ for some element c of order 2. Similarly, by property 2^0, $G = \operatorname{Ker} y \leftthreetimes \operatorname{Im} y$ and $\operatorname{Im} y = \langle a \rangle$ for some element a of order 4. In view of Lemmas 1 and 9, we have

$$G = (M \leftthreetimes \langle a \rangle) \leftthreetimes \langle c \rangle = (M \leftthreetimes \langle c \rangle) \leftthreetimes \langle a \rangle,$$

where

$$M = \operatorname{Ker} x \cap \operatorname{Ker} y, \ \operatorname{Im} x = \langle c \rangle, \ \operatorname{Im} y = \langle a \rangle,$$

$$\operatorname{Ker} x = M \leftthreetimes \langle a \rangle, \ \operatorname{Ker} y = M \leftthreetimes \langle c \rangle.$$

Therefore, $G/M = \langle aM \rangle \times \langle cM \rangle$ and $G' \subset M$.

Since $\operatorname{Aut}(G)$ is 2-group, then the group of inner automorphisms $\widehat{G} \cong G/Z(G)$ is also 2-group. Hence all $2'$-elements of G belong to its center $Z(G)$. Therefore, the group G splits into the direct product $G = G_{2'} \times G_2$ of its Hall $2'$-subgroup $G_{2'}$ and Sylow 2-subgroup G_2. Denote by z the projection of G onto its subgroup $G_{2'}$. Then $z \in J(x) \cap J(y)$ and, by 3^0, $z = 0$. Hence G is 2-group.

Similarly to the proof of Theorem 1.1, properties 4^0 and 5^0 imply that

$$M = \langle b \rangle \cong C_{2^n}, \quad n \geqslant 2,$$

for some $b \in M$. Assume that $M \neq G'$. Then

$$G/G' = \langle bG' \rangle \times \langle aG' \rangle \times \langle cG' \rangle, \quad \langle bG' \rangle \ncong \langle 1 \rangle$$

and we can find a non-zero element $z \in J(x) \cap J(y)$:

$$G'z = \langle 1 \rangle, \quad az = cz = 1, \quad bz = b^{2^{n-1}}.$$

This contradicts property 3^0. Therefore,

$$M = G' = \langle b \rangle \cong C_{2^n}, \quad n \geqslant 2, \quad G/G' = \langle aG' \rangle \times \langle cG' \rangle. \tag{1.13}$$

Next we shall show that $n = 2$. In view of (1.13), $c^{-1}bc = b^t$ and $a^{-1}ba = b^s$ for some $t, s \equiv 1 (\mathrm{mod}\ 2)$. Hence $[b, c] = b^{t-1} \in \langle b^2 \rangle$ and $[b, a] = b^{s-1} \in \langle b^2 \rangle$. Since $G' = \langle b \rangle$,

$$a^{-1}c^{-1}ac = [a, c] = b^i$$

for some $i \equiv 1 (\mathrm{mod}\ 2)$. As $\langle b \rangle = \langle b^i \rangle$, we can assume that $i = 1$, i.e.,

$$c^{-1}ac = ab.$$

The element a is an element of order 4. Therefore, ab is also an element of order 4 and

$$ab \cdot ab = a^2 \cdot a^{-1}ba \cdot b = a^2 b^{s+1},$$

$$1 = (ab)^4 = a^2 b^{s+1} \cdot a^2 b^{s+1} = a^{-2} b^{s+1} a^2 \cdot b^{s+1} =$$

$$= a^{-1} b^{s(s+1)} a \cdot b^{s+1} = b^{s^2(s+1)+(s+1)} = b^{(s+1)(s^2+1)}. \qquad (1.14)$$

Choose an arbitrary $k \in \mathbb{Z}_{2^n}$. By (1.14), we have

$$ab^k \cdot ab^k = a^2 \cdot a^{-1} b^k a \cdot b^k = a^2 b^{k(s+1)},$$

$$(ab^k)^4 = a^2 b^{k(s+1)} \cdot a^2 b^{k(s+1)} = a^{-2} b^{k(s+1)} a^2 \cdot b^{k(s+1)} =$$

$$= b^{k(s^2+1)(s+1)} = 1.$$

It means that the group G splits into the semidirect product

$$G = \langle b, c \rangle \leftthreetimes \langle ab^k \rangle$$

for each $k \in \mathbb{Z}_{2^n}$. Denote by z_k the projection of G onto its subgroup $\langle ab^k \rangle \cong C_4$. Then $z_k \in I(G),\ yz_k = z_k,\ z_k y = y,\ z_k x = 0$, i.e., $z_k \in T$ and $|T| \geqslant 2^n$. Property 6^0 implies that $n = 2$ and

$$T = \{\, z_k \mid k \in \mathbb{Z}_4 \,\},\quad G' = \langle b \rangle = C_4.$$

Assume that $ab \neq ba$. Then

$$a^{-1}ba = b^{-1},\quad ab^k \cdot ab^k = a^2 \cdot a^{-1} b^k a \cdot b^k = a^2$$

and the endomorphism u of G, defined by

$$bu = cu = 1,\quad au = (ab^k)u = a^2 = (ab^k)^2,$$

is non-zero and satisfies equalities $uz_k = z_k u = u$, i.e., $u \in K(z_k)$. Hence $u \in \cap_{z \in T} K(z)$. This contradicts property 7^0. Hence $ab = ba$.

Since $c^{-1}bc = b^t$ for some $t \equiv 1 (\mathrm{mod}\ 2)$, then

$$c^{-1}bc = b^{-1} \quad \text{or} \quad c^{-1}bc = b.$$

If $c^{-1}bc = b$, then

$$a = c^{-2}ac^2 = c^{-1}(c^{-1}ac)c = c^{-1}abc = c^{-1}ac \cdot b = ab^2,$$

i.e., $b^2 = 1$. This contradicts the fact that the order of b is 4. Therefore, $c^{-1}bc = b^{-1}$ and $G = (\langle b\rangle \times \langle a\rangle) \leftthreetimes \langle c\rangle$, where

$$a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}bc = b^{-1},\ c^{-1}ac = ab.$$

This implies that $G \cong G_{31}$. The sufficiency is proved. Theorem 1.3 is proved. □

Theorem 1.4 *The group G_{31} is determined by its endomorphism semigroup in the class of all groups.*

The proof of Theorem 1.4 is similar to the proof of Theorem 1.2.

1.1.3 The groups G_{34}, G_{39}, G_{41}

In this subsection, we characterize the groups

$$G_{34} = \langle a, b, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^{-1},\ c^{-1}bc = b^{-1}\rangle = \\ = (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle = (C_4 \times C_4) \leftthreetimes C_2,$$

$$G_{39} = \langle a, b, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = ab^2,\ c^{-1}bc = ba^2\rangle = \\ = (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle = (C_4 \times C_4) \leftthreetimes C_2,$$

$$G_{41} = \langle a, b, c \mid a^4 = b^4 = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^{-1}b^2,\ c^{-1}bc = ba^2\rangle = \\ = (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle = (C_4 \times C_4) \leftthreetimes C_2$$

by their endomorphism semigroups.

Theorem 1.5 *A finite group G is isomorphic to a group from the class $\{G_{34},\ G_{39},\ G_{41}\}$ if and only if $|\operatorname{Aut}(G)| \in \{2^6 \cdot 3,\ 2^8,\ 2^9 \cdot 3\}$ and there exists $x \in I(G)$ such that the following properties hold:*

1^0 $K(x) \cong \operatorname{End}(C_2)$;
2^0 $|H(x)| = 4$;
3^0 $z^2 = 0$ *for each* $z \in J(x)$;
4^0 $|J_1(x)| = 10$;
5^0 *there exists* $y \in J_1(x)$ *such that* $V(x) \cap V(y)$ *is a 2-group;*
6^0 $z \in V(x) \cap \left(\cap_{y \in J_1(x)} V(y)\right) \Longrightarrow z^2 = 1$;
7^0 $|P(x)| \neq 48$;
8^0 $|W(x)| \in \{8,\ 12,\ 20\}$.

Moreover,

1) *if* $|\operatorname{Aut}(G)| = 2^9 \cdot 3$, *then* $G \cong G_{34}$,
2) *if* $|\operatorname{Aut}(G)| = 2^8$, *then* $G \cong G_{39}$,
3) *if* $|\operatorname{Aut}(G)| = 2^6 \cdot 3$, *then* $G \cong G_{41}$.

Proof. Necessity. Assume that $G \in \{G_{34},\, G_{39},\, G_{41}\}$. In the Table 1 (see the beginning of section 1.1) it was said that $|\operatorname{Aut}(G)| \in \{2^6 \cdot 3,\, 2^8,\, 2^9 \cdot 3\}$. Denote by x the projection of G onto its subgroup $\langle c\rangle$ of order two (see the equalities given in the beginning of this subsection). Then

$$\operatorname{Ker} x = \langle a,\, b\rangle = \langle a\rangle \times \langle b\rangle \cong C_4 \times C_4,\ \ \operatorname{Im} x = \langle c\rangle\,.$$

Prove that properties $1^0 - 8^0$ are satisfied for x.

Lemma 4 implies property 1^0.

By Lemma 6, $H(x)$ consists of endomorphisms y of G such that $(\operatorname{Im} x)y \subset \operatorname{Ker} x$ and $(\operatorname{Ker} x)y = \langle 1\rangle$, i.e., $ay = by = 1,\ cy \in \langle a\rangle \times \langle b\rangle$. As $\langle c\rangle \cong C_2$, there are exactly 4 endomorphisms y and property 2^0 holds.

Choose $y \in J(x)$. By Lemma 5,

$$cy = 1,\ \ ay = a^i b^j,\ \ by = a^k b^l \tag{1.15}$$

for some $i,\, j,\, k,\, l \in \mathbb{Z}_4$. Since y is an endomorphism of G, it preserves the defining relations of G. Map (1.15) preserves the defining relations of G if and only if

$$i \equiv j \equiv k \equiv l \equiv 0 \pmod 2. \tag{1.16}$$

Let us find y^2:

$$cy^2 = 1,\ ay^2 = (ay)y = (a^i b^j)y = (ay)^i (by)^j = a^{i^2+kj} b^{ij+lj} = 1,$$

$$by^2 = (by)y = (a^k b^l)y = (ay)^k (by)^l = a^{ik+lk} b^{jk+l^2} = 1,$$

i.e., $y^2 = 0$ and property 3^0 holds.

By definition, $J_1(x)$ consists of $y \in J(x)$ such that $vx = v$ and $vw = y$ for some $v,\, w \in \operatorname{End}(G)$. Each such y is given by (1.15) and (1.16). Due to Lemma 1, $\operatorname{Im} v \subset \operatorname{Im} x = \langle c\rangle \cong C_2$, i.e., $\operatorname{Im} y = \operatorname{Im}(vw) \subset \langle cw\rangle$ and

$$\operatorname{Im} y = \langle 1\rangle \quad \text{or} \quad \operatorname{Im} y \cong C_2. \tag{1.17}$$

Clearly, each $y \in J(x)$ which satisfies (1.17) belongs to $J_1(x)$. Map (1.15), where conditions (1.16) hold, satisfies conditions (1.17) if and only if

$$ay = 1,\ \langle by\rangle \cong C_2 \text{ or } \quad \langle ay\rangle \cong C_2,\ by = 1 \text{ or } ay = by.$$

The number of such maps is $3 + 3 + 4 = 10$, i.e., property 4^0 holds.

Let us prove property 5^0. Consider the following element y of $J_1(x)$:

$$cy = by = 1,\ ay = a^2.$$

If $G = G_{39}$, then $\operatorname{Aut}(G)$ is a 2-group, and property 5^0 holds. Therefore, assume that $G = G_{34}$ or $G = G_{41}$ and find $V(x) \cap V(y)$. Choose $z \in V(x)$. By Lemma 3, z maps on generators of G as follows

$$cz = ca^i b^j,\ \ az = a^k b^l,\ \ bz = a^m b^n \tag{1.18}$$

for some i, j, k, l, m, $n \in \mathbb{Z}_4$. If $G = G_{34}$, then map (1.18) preserves the generating relations of G and is an endomorphism for each values of parameters, but it is an automorphism, and therefore, an element of $V(x)$ if and only if

$$kn - ml \equiv 1 \pmod 2. \tag{1.19}$$

This z belongs to $V(y)$ if and only if $zy = y$, i.e.,

$$c(zy) = a^{2i} = cy = 1,\ a(zy) = a^{2k} = ay = a^2,\ b(zy) = a^{2m} = by = 1,$$

or, equivalently,

$$i \equiv m \equiv 0 \pmod 2,\ k \equiv 1 \pmod 2. \tag{1.20}$$

There exist 2^8 different values of i, j, k, l, m, n which satisfy conditions (1.19) and (1.20). Hence, if $G = G_{34}$, then $|V(x) \cap V(y)| = 2^8$ and in this case property 5^0 holds. If $G = G_{41}$, then map (1.18) preserves the generating relations of G and it is an endomorphism if and only if

$$i \equiv j \equiv 0 \pmod 2,\ l \equiv m \pmod 2,\ n \equiv l + k \pmod 2. \tag{1.21}$$

Endomorphism z is an automorphism and belongs to $V(x) \cap V(y)$ if and only if conditions (1.19) and (1.20) hold. There exist 2^6 different values of i, j, k, l, m, n which satisfy conditions (1.19)–(1.21). Hence, if $G = G_{41}$, then $|V(x) \cap V(y)| = 2^6$ and the property 5^0 holds. Property 5^0 is proved.

Let us prove now property 6^0. Choose the following elements u and v from $J_1(x)$:

$$u: \quad c \longmapsto 1,\ a \longmapsto a^2,\ b \longmapsto 1,$$

$$v: \quad c \longmapsto 1,\ a \longmapsto 1,\ b \longmapsto b^2.$$

Assume that $z \in V(x) \cap \big(\cap_{y \in J_1(x)} V(y)\big)$. Then z is given by (1.18) for some i, j, k, l, m, $n \in \mathbb{Z}_4$ and

$$c(zu) = a^{2i} = cu = 1,\ c(zv) = b^{2j} = cv = 1,\ a(zu) = a^{2k} = au = a^2,$$

$$b(zu) = a^{2m} = bu = 1,\ a(zv) = b^{2l} = av = 1,\ b(zv) = b^{2n} = bv = b^2,$$

i.e.,

$$i \equiv j \equiv m \equiv l \equiv 0 \pmod 2,\ k \equiv n \equiv 1 \pmod 2. \tag{1.22}$$

It is easy to check that under conditions (1.22) we have $z^2 = 1$. Property 6^0 is proved.

In order to prove property 7^0, we find elements of $P(x)$ for each three cases. By Lemma 7, $P(x)$ consists of maps y for which

$$y: \quad c \longmapsto c,\ a \longmapsto a^i b^j,\ b \longmapsto a^k b^l \tag{1.23}$$

for some i, j, k, $l \in \mathbb{Z}_4$. Map (1.23) is an endomorphism of G, and therefore, it is an element of $P(x)$ if and only if it preserves the generating relations of G. If $G = G_{34}$, then the map (1.23) preserves the generating relations of G for each i, j, k, $l \in \mathbb{Z}_4$ and in this case $|P(x)| = 4 \cdot 4 \cdot 4 \cdot 4 = 256$. If $G = G_{39}$, then the map (1.23) preserves the generating relations of G if and only if

$$j \equiv k \pmod 2, \quad i \equiv l \pmod 2,$$

and therefore, in this case $|P(x)| = 4 \cdot 2 \cdot 4 \cdot 2 = 64$. If $G = G_{41}$, then the map (1.23) preserves the generating relations of G if and only if

$$j \equiv k \pmod 2, \quad l \equiv i + j \pmod 2,$$

and in this case $|P(x)| = 4 \cdot 4 \cdot 2 \cdot 2 = 64$. Consequently, property 7^0 is true.

By Lemma 8, $W(x)$ consists of maps y for which $ay = by = 1$ and cy is an arbitrary element d of G such that $d^2 = 1$. Hence $|W(x)| = |\{\, d \in G \mid d^2 = 1 \,\}|$. The numbers of elements of order two are given in the Table 1 (see the beginning of section 1.1). For groups G_{34}, G_{39} and G_{41} they are 19, 11, 7. Therefore, $|W(x)| \in \{8, 12, 20\}$ and property 8^0 holds. The necessity is proved.

Sufficiency. Let G be a finite group such that $|\operatorname{Aut}(G)| \in \{2^6 \cdot 3, 2^8, 2^9 \cdot 3\}$. Assume that there exists $x \in I(G)$ which satisfies properties $1^0 - 8^0$. Our aim is to prove that G is isomorphic to a group from the class $\{G_{34}, G_{39}, G_{41}\}$.

As previously, property 1^0 implies the semidirect product

$$G = \operatorname{Ker} x \leftthreetimes \operatorname{Im} x, \quad \operatorname{Im} x = \langle c \rangle \cong C_2.$$

By Lemma 5, $J(x)$ consists of endomorphisms y of G such that $cy = 1$ and $(\operatorname{Ker} x)y \subset \operatorname{Ker} x$. We saw that y belongs to $J_1(x)$ if and only if it satisfies the condition (1.17), i.e.,

$$J_1(x) = \{\, y \in \operatorname{End}(G) \mid cy = 1,\ \operatorname{Ker} x \xrightarrow{y} \operatorname{Ker} x,\ \operatorname{Im} y = \langle d \rangle$$

$$\text{for some } d \in \operatorname{Ker} x \text{ such that } d^2 = 1 \,\}. \tag{1.24}$$

By property 5^0, there exists $y \in J_1(x)$ such that $V(x) \cap V(y)$ is a 2-group. In view of (1.24), $\operatorname{Im} y$ is Abelian. As $\operatorname{Im} x$ is Abelian as well, Lemma 2 implies that $G/Z(G) \cong \widehat{G} \subset V(x) \cap V(y)$. As $V(x) \cap V(y)$ is a 2-group, all $2'$-elements of G belong to $Z(G)$ and hence G splits into the direct product $G = G_{2'} \times G_2$ of its Hall $2'$-subgroup $G_{2'}$ and Sylow 2-subgroup G_2. Denote by z the projection of G onto its subgroup $G_{2'}$. Then $z \in I(G) \cap J(x)$ and, by 3^0, $z = 0$. Hence G is 2-group.

It was shown that Im x and Im y are Abelian for each $y \in J_1(x)$. Hence by Lemma 2, $G/Z(G) \cong \widehat{G} \subset V(x) \cap \left(\cap_{y \in J_1(x)} V(y)\right)$. Due to this and property 6^0, we have

$$g^2 \in Z(G) \quad \text{for each} \quad g \in G. \tag{1.25}$$

Therefore, $G/Z(G)$ is Abelian and

$$G' \subset Z(G), \quad g^2 = 1 \quad \text{for each} \quad g \in G'. \tag{1.26}$$

By Lemma 6, $|H(x)|$ is equal to the number of homomorphisms Im $x = \langle c \rangle \longrightarrow$ Ker x. Hence and by property 2^0, Ker x has three elements of order 2. Since Im x is Abelian, we have $G' \subset$ Ker x and, by (1.26),

$$G' = C_{2^n} \times C_{2^m}, \quad 0 \leq m, n \leq 1. \tag{1.27}$$

Property 4^0 and (1.24) imply that there exist $y, z \in J_1(x)$ and $a, b \in$ Ker x such that

$$\text{Ker } x/(\text{Ker } x \cap \text{Ker } y) = \langle a \cdot (\text{Ker } x \cap \text{Ker } y) \rangle \cong C_2,$$

$$\text{Ker } x/(\text{Ker } x \cap \text{Ker } z) = \langle b \cdot (\text{Ker } x \cap \text{Ker } z) \rangle \cong C_2,$$

$$a \in \text{Ker } x \cap \text{Ker } z, \quad b \in \text{Ker } x \cap \text{Ker } y.$$

Denote

$$N = \text{Ker } x \cap \text{Ker } y \cap \text{Ker } z.$$

It is obvious that under these conditions

$$G/N = \langle aN \rangle \times \langle bN \rangle \times \langle cN \rangle \cong C_2 \times C_2 \times C_2.$$

Note that $a^2 \neq 1$ because otherwise $G = \langle N, b, c \rangle \leftthreetimes \langle a \rangle$ and the projection of G onto $\langle a \rangle$ is non-zero element of $I(G) \cap J(x)$ which contradicts 3^0. Similarly, $b^2 \neq 1$ and $(ab)^2 \neq 1$.

Clearly, $G' \subset N$ because G/N is Abelian. It has been proved that Ker x has three elements of order two. As each 2-group has the non-trivial center, we can assume that these three elements are a_0, b_0 and $a_0 b_0$. Therefore, we can consider the following endomorphisms x_{ij}, y_{ij} and z_{ij} of G:

$$\langle c, b, N \rangle x_{ij} = \langle 1 \rangle, \ ax_{ij} = a_0^i b_0^j,$$

$$\langle c, a, N \rangle y_{ij} = \langle 1 \rangle, \ by_{ij} = a_0^i b_0^j,$$

$$\langle c, ab, N \rangle z_{ij} = \langle 1 \rangle, \ az_{ij} = bz_{ij} = a_0^i b_0^j,$$

where $i, j \in \mathbb{Z}_2$. All these endomorphisms belong to $J_1(x)$ and the number of them is 10. Hence, by 4^0,

$$J_1(x) = \{ x_{ij}, y_{ij}, z_{ij} \mid i, j \in \mathbb{Z}_2 \}. \tag{1.28}$$

As G/G' is Abelian, it splits into a direct product

$$G/G' = \left\langle a_1 G' \right\rangle \times \ldots \times \left\langle a_r G' \right\rangle \times \left\langle cG' \right\rangle, \ \left\langle a_k G' \right\rangle \cong C_{2^{n_k}},$$

where $n_k \geqslant 1;\ k = 1, \ldots, r$ and $r \geqslant 2$. Consider now the following endomorphisms $u_k \ \ (k = 1, \ldots, r)$ of G:

$$\left\langle G',\, c \right\rangle u_k = \langle 1 \rangle, \quad a_k u_k = \begin{cases} a_k^{2^{m_k - 1}} \text{ if } i = k, \\ 1 \text{ if } i \neq k, \end{cases}$$

where m_k is the order of a_k. Clearly, these endomorphisms belong to $J_1(x)$. In view of (1.28), $r = 2$ and we can assume that $a = a_1,\ b = a_2$, i.e.,

$$G/G' = \left\langle aG' \right\rangle \times \left\langle bG' \right\rangle \times \left\langle cG' \right\rangle. \tag{1.29}$$

By (1.25), (1.27) and (1.29), the map

$$z: \quad c \longmapsto 1,\ a \longmapsto a^2,\ b \longmapsto b^2,\ G' \longrightarrow \langle 1 \rangle,$$

can be extended to an endomorphism of G. This endomorphism belongs to $J(x)$. Therefore, by property 3^0, $z^2 = 0$, i.e.,

$$a^4 = b^4 = 1.$$

Remark that

$$a^2,\, b^2 \in G'.$$

Indeed, if $a^2 \notin G'$, then $G = \langle G',\, b,\, c \rangle \leftthreetimes \langle a \rangle$ and the projection of G onto its subgroup $\langle a \rangle$ is non-zero element of $I(G) \cap J(x)$. This contradicts property 3^0. Hence $a^2 \in G'$. Similarly, $b^2 \in G'$.

If $n = 0$ or $m = 0$, then $a^2 = b^2,\ G' = \left\langle a^2 \right\rangle$ and

$$(ab)^2 = abab = ab^2 \cdot b^{-1}ab = b^2a^2 \cdot a^{-1}b^{-1}ab = b^2a^2 \cdot [a,\, b] = [a,\, b].$$

Since $(ab)^2 \neq 1$, we have

$$(ab)^2 = [a,\, b] \neq 1, \quad [a,\, b] = a^2,$$

i.e., $b^{-1}ab = a^{-1}$ and Ker x is the quaternion group Q of order 8. This contradicts the fact that Ker x has three elements of order two. Therefore, $m = n = 1$ and

$$G' = C_2 \times C_2. \tag{1.30}$$

Assume that $b^2 = a^2$. Then $[a,\, b] \neq 1$ because otherwise $G = \langle G',\, b,\, c \rangle \leftthreetimes \left\langle a^{-1}b \right\rangle$ and the projection of G onto $\left\langle a^{-1}b \right\rangle$ is non-zero element of $I(G) \cap J(x)$ which contradicts 3^0. If $[a,\, b] \in \langle a \rangle$, then

$$[a,\, b] = a^2, \ \ a^{-1}b^{-1}ab = a^2, \ \ b^{-1}ab = a^{-1}$$

and we have

$$\langle a,\, b\rangle = Q,\ G = (Q \times \langle d\rangle) \leftthreetimes \langle c\rangle$$

(d is an element of order two, $d \in G'$). If $[a,\, b] \notin \langle a\rangle$, then $(ab)^2 = [a,\, b] \neq a^2$ and we can suppose from the beginning that $a^2 \neq b^2$ (otherwise we can change b to ab). Therefore, below we have to study two different cases:

I $G = (Q \times \langle d\rangle) \leftthreetimes \langle c\rangle$,
$Q = \langle a,\, b \mid a^4 = 1,\ a^2 = b^2,\ b^{-1}ab = a^{-1}\rangle$.
II $a^2 \neq b^2$.

Case I

In this case

$$c^{-1}ac = aa^{2i}d^j = a^{\pm 1}d^j,\ c^{-1}bc = bb^{2k}d^l = b^{\pm 1}d^l$$

for some $i,\, j,\, k,\, l \in \mathbb{Z}_2$ and, in view of $(ab)^2 = a^2$,

$$c^{-1}(ab)c = aba^{2i+2k}d^{j+l} = ab(ab)^{2i+2k}d^{j+l} = (ab)^{\pm 1}d^{j+l}.$$

If $j = l = 0$, then $G = \langle a,\, b,\, c\rangle \times \langle d\rangle$ and the projection of G onto $\langle d\rangle$ is non-zero element of $I(G) \cap J(x)$ which contradicts 3^0. If $j = l = 1$, then $c^{-1}(ab)c = (ab)^{\pm 1}$ and we can change a with ab. Therefore, we can assume that $j \neq l$. Suppose $j = 1,\ l = 0$ (the case $j = 0,\ l = 1$ can be studied similarly). Consequently,

$$c^{-1}ac = a^{\pm 1}d,\ c^{-1}bc = b^{\pm 1}$$

and we have to study four cases:

A. $c^{-1}ac = ad,\ c^{-1}bc = b$.
B. $c^{-1}ac = ad,\ c^{-1}bc = b^{-1}$.
C. $c^{-1}ac = a^{-1}d,\ c^{-1}bc = b$.
D. $c^{-1}ac = a^{-1}d,\ c^{-1}bc = b^{-1}$.

Our aim is to prove that these four cases are impossible, and therefore, the case I as well. We will use property 7^0. Choose $z \in P(x)$. By Lemma 7, z acts on generators of G as follows:

$$z: \quad c \longmapsto c,\ \ d \longmapsto d^i a^{2j},\ \ a \longmapsto a^k b^l d^m,\ \ b \longmapsto a^n b^r d^s \tag{1.31}$$

for some $i,\, j,\, m,\, s \in \mathbb{Z}_2$; $k,\, l,\, n,\, r \in \mathbb{Z}_4$. Since $a^2 = b^2$, we can assume that $l,\, r \in \{0,\, 1\}$. Map (1.31) is an endomorphism of G and belong to $P(x)$ if and only if it preserves the defining relations of G. Elementary calculations show that the map (1.31) preserves the defining relations of G only in the following cases:

$$A: \begin{cases} i = j = l = r = 0;\ n,\, k \in \{0,\, 2\},\ m,\, s \in \{0,\, 1\}; \\ i = r = 1;\ j = l = 0;\ n \in \{0,\, 2\},\ k \in \{1,\, 3\},\ m,\, s \in \{0,\, 1\}; \\ i = l = r = 1;\ j = 0;\ n \in \{0,\, 2\},\ k \in \{1,\, 3\},\ m,\, s \in \{0,\, 1\}; \end{cases}$$

$$B:\begin{cases} i=j=l=r=0;\ n,\,k\in\{0,\,2\},\ m,\,s\in\{0,\,1\};\\ i=r=1;\ j=l=0;\ n\in\{0,\,2\},\ k\in\{1,\,3\},\ m,\,s\in\{0,\,1\};\\ i=j=l=r=1;\ n\in\{0,\,2\},\ k\in\{1,\,3\},\ m,\,s\in\{0,\,1\};\end{cases}$$

$$C:\begin{cases} i=j=l=r=0;\ n,\,k\in\{0,\,2\},\ m,\,s\in\{0,\,1\};\\ i=r=1;\ j=l=0;\ n\in\{0,\,2\},\ k\in\{1,\,3\},\ m,\,s\in\{0,\,1\};\\ i=l=r=1;\ j=0;\ n\in\{0,\,2\},\ k\in\{1,\,3\},\ m,\,s\in\{0,\,1\};\end{cases}$$

$$D:\begin{cases} i=j=l=r=0;\ n,\,k\in\{0,\,2\},\ m,\,s\in\{0,\,1\};\\ i=r=1;\ j=l=0;\ n\in\{0,\,2\},\ k\in\{1,\,3\},\ m,\,s\in\{0,\,1\};\\ i=j=l=r=1;\ n\in\{0,\,2\},\ k\in\{1,\,3\},\ m,\,s\in\{0,\,1\}.\end{cases}$$

In all these four cases $|P(x)|=48$ which contradicts property 7^0. Consequently, case I cannot be possible, too, and we have case II, i.e.,

$$a^2\neq b^2$$

and, by (1.30),

$$G'=\left\langle a^2\right\rangle\times\left\langle b^2\right\rangle.$$

Since $(ab)^2=a^2b^2\cdot[a,\,b]$ and $(ab)^2\neq 1$, we have $[a,\,b]\neq a^2b^2$ and $[a,\,b]\in\{\,1,\,a^2,\,b^2\,\}$, i.e.,

$$ab=ba\ \text{ or }\ b^{-1}ab=a^{-1}\ \text{ or }\ a^{-1}ba=b^{-1}.$$

As the cases $b^{-1}ab=a^{-1}$ and $a^{-1}ba=b^{-1}$ are similar, below we have to study only the following two cases: $\mathcal{A})\ b^{-1}ab=a^{-1}$; $\mathcal{B})\ ab=ba$.

Case $\mathcal{A}$: $b^{-1}ab=a^{-1}$**.**

In this case, the group G is a group of order 32 in which the group

$$_{16}G_{10}=\left\langle a,\,b\mid a^4=b^4=1,\ b^{-1}ab=a^{-1}\right\rangle$$

of order 16 is a maximal subgroup (the subindex 16 shows the order of the given group and the subindex 10 shows the ordering number in the list of groups of order 16 given by Hall and Senior [12]). By [12], only 14 groups of order 32 have a maximal subgroup isomorphic to $_{16}G_{10}$. They are

$$G_{12},\,G_{14},\,G_{15},\,G_{16},\,G_{27},\,G_{28},\,G_{29},\,G_{30},\,G_{35},\,G_{36},\,G_{37},\,G_{38},\,G_{40},\,G_{41}. \tag{1.32}$$

Due to [12] again, the numbers of elements of order two in these groups are

$$7,\,11,\,3,\,7,\,11,\,3,\,3,\,3,\,3,\,15,\,7,\,11,\,3,\,7. \tag{1.33}$$

respectively. By Lemmas 1 and 8,

$$|W(x)|=|\mathrm{Hom}(\mathrm{Im}\ x,\,G)|=|\mathrm{Hom}(\langle c\rangle,\,G)|,$$

i.e., $|W(x)| - 1$ is the number of elements of order two in G. In view of property 8^0, the number of elements of order two of G is 7 or 11 or 19. Hence, by (1.32) and (1.33), G is one of following groups:

$$G_{12},\, G_{14},\, G_{16},\, G_{27},\, G_{37},\, G_{38},\, G_{41}. \tag{1.34}$$

By [12], the numbers of automorphisms of groups (1.34) are

$$2^9,\, 2^7,\, 2^8,\, 2^6,\, 2^7,\, 2^7,\, 2^6 \cdot 3$$

respectively. Therefore, $G \in \{G_{16},\, G_{41}\}$. Since $G'_{16} \cong C_2$, $G = G_{41}$. It means that case $\mathcal{A}$ is impossible.

Case $\mathcal{B}$: $ab = ba$**.** Assume that $ab = ba$. Then

$$G = (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle\,, \quad G' = \left\langle a^2\right\rangle \times \left\langle b^2\right\rangle \cong C_2 \times C_2.$$

By [12], only certain number of non-abelian groups of order 32 have a maximal subgroup isomorphic to $C_4 \times C_4$. These groups are

$$G_{14},\, G_{15},\, G_{16},\, G_{19},\, G_{21},\, G_{31},\, G_{34},\, G_{35},\, G_{39},\, G_{40},\, G_{41}. \tag{1.35}$$

Among groups (1.35) only 5 groups have a derived group isomorphic to $C_2 \times C_2$ and those groups are

$$G_{34},\, G_{35},\, G_{39},\, G_{40},\, G_{41}. \tag{1.36}$$

Among groups (1.36) only the groups G_{34}, G_{39} and G_{41} are isomorphic to a semidirect product $(C_4 \times C_4) \leftthreetimes C_2$. Therefore, G is one of the groups G_{34}, G_{39} and G_{41}. The sufficiency is proved and so is Theorem 1.5. □

Theorem 1.6 *The groups G_{34}, G_{39} and G_{41} are determined by their endomorphism semigroups in the class of all groups.*

The proof of Theorem 1.6 is similar to that of Theorem 1.2.

1.2 The groups presentable in the form $(C_8 \times C_2) \leftthreetimes C_2$

The results presented in this section have been published in [8].

By [12], the groups G of order 32 such that presentable in the form $G = (C_8 \times C_2) \leftthreetimes C_2$, are G_4, G_{17}, G_{20}, G_{26} and G_{27}, i.e., the groups

$$G_4 = C_8 \times C_2 \times C_2,$$

$$G_{17} = \left\langle a,\, b,\, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ ac = ca,\ c^{-1}bc = ba^4\right\rangle,$$

$$G_{20} = \langle a,\, b,\, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ bc = cb,\ c^{-1}ac = ab \rangle\,,$$
$$G_{26} = \langle a,\, b,\, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^{-1},\ c^{-1}bc = a^4b \rangle\,,$$
$$G_{27} = \langle a,\, b,\, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ bc = cb,\ c^{-1}ac = a^{-1}b \rangle\,.$$

The group G_4 is Abelian and, therefore, it is determined by its endomorphism semigroup in the class of all groups (Lemma 10). The group G_{26} can be presented in the form $G_{26} = \langle a,\, d\rangle \leftthreetimes \langle c\rangle$ and $\langle a,\, d\rangle \cong Q_3$, where $d = cba^6$ and Q_3 is a generalized quaternion group of order 16. Semidirect products $Q_n \leftthreetimes C_2,\ n \geqslant 3$, were investigated in [20]. It was proved that they are determined by their endomorphism semigroups in the class of all groups. In this section we shall describe the groups $G_{17},\ G_{20}$ and G_{27}, by their endomorphism semigroups (theorems 1.7, 1.9 and 1.11). From these descriptions follows that these groups also are determined by their endomorphism semigroups in the class of all groups (theorems 1.8, 1.10 and 1.12).

1.2.1 The group G_{17}

In this subsection, we shall characterize the group

$$G_{17} = \langle a,\, b,\, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ ac = ca,\ c^{-1}bc = ba^4 \rangle =$$
$$= (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle = (\langle a\rangle \times \langle c\rangle) \leftthreetimes \langle b\rangle$$

by its endomorphism semigroup.

Theorem 1.7 *A finite group G is isomorphic to the group G_{17} if and only if there exist $x,\, y \in I(G)$ which satisfy the following properties:*

1^0 $K(x) \cong K(y) \cong \mathrm{End}(C_2)$; 2^0 $xy = yx = 0$; 3^0 $V(x)$ *is a 2-group;*
4^0 $I(G) \cap J(x) \cap J(y) = \{0\}$; 5^0 $|J(x) \cap J(y)| = 4$;
6^0 $|\{\, z \in \mathrm{End}(G) \mid xz = z,\ zx = zy = 0\,\}| = 2$;
7^0 *there exists* $z \in J(x) \cap J(y)$ *such that* $z^2 \neq 0$ *and* $z^3 = 0$;
8^0 $\{\, z \in I(G) \mid zx = xz = x,\ zy = yz = y\,\} = \{1\}$.

Proof. Necessity. Let $G = G_{17}$. Denote by x and y the projections of G onto its subgroups $\langle c\rangle$ and $\langle b\rangle$. Then $x, y \in I\,(G)$, and, similarly to Theorems 1.1, 1.3 and 1.5, direct calculations show that x and y satisfy properties 1^0–8^0.

Sufficiency. Assume that G is a finite group and $x,\, y \in I(G)$ such that properties $1^0 - 8^0$ hold. By property 2^0, G splits up as follows

$$G = ((\mathrm{Ker}\ x \cap \mathrm{Ker}\ y) \leftthreetimes \mathrm{Im}\ x) \leftthreetimes \mathrm{Im}\ y = (\mathrm{Ker}\ x \cap \mathrm{Ker}\ y) \leftthreetimes \mathrm{Im}\ y) \leftthreetimes \mathrm{Im}\ x.$$

By property 1^0, $K(x) \cong \mathrm{End}(\mathrm{Im}\, x) \cong \mathrm{End}(C_2)$. Similarly, $\mathrm{End}(\mathrm{Im}\, y) \cong \mathrm{End}(C_2)$. As each finite Abelian group is determined by its endomorphism

semigroup in the class of all groups, we have $\mathrm{Im}\, x \cong \mathrm{Im}\, y \cong C_2$, i.e., $\mathrm{Im}\, x = \langle c \rangle$ and $\mathrm{Im}\, y = \langle b \rangle$ for some elements c, $b \in G$ of order 2. Hence

$$G = (M \leftthreetimes \langle c \rangle) \leftthreetimes \langle b \rangle = (M \leftthreetimes \langle b \rangle) \leftthreetimes \langle c \rangle ,$$

where $M = \mathrm{Ker}\, x \cap \mathrm{Ker}\, y$ and $c^2 = b^2 = 1$.

Assume that $g \in G$ is a $2'$-element of G. Then $g \in M$. Since $\mathrm{Im}\, x = \langle c \rangle$ is Abelian, $\widehat{g} \in V(x)$ and $\widehat{g}$ is a $2'$-element. Property 3^0 implies that $\widehat{g} = 1$, i.e., $g \in Z(G)$. Therefore, all $2'$-elements of G contain in the center $Z(G)$ of G and G splits up into the direct product $G = G_{2'} \times G_2$ of its Hall $2'$-subgroup $G_{2'}$ and Sylow 2-subgroup G_2. Denote by z the projection of G onto its subgroup $G_{2'}$. Clearly, $z \in I(G) \cap J(x) \cap J(y)$. Property 4^0 implies $z = 0$, i.e., $G_{2'} = \langle 1 \rangle$ and G is a 2-group.

Basing on property 7^0, subgroup M of G is non-trivial. Choose an element $d \in M$ of order 2. There exist two endomorphisms z_0 and z_1 of G such that $cz_i = d^i$ and $Mz_i = \langle 1 \rangle$, $bz_i = 1$. These endomorphisms satisfy equalities $xz_i = z_i$, $z_i x = z_i y = 0$. Therefore, by property 6^0, the subgroup M of G contains only one element of order 2 and hence is cyclic or a generalized quaternion group ([37], Theorem 5.3.6). Since a product of two proper endomorphisms of a generalized quaternion group is equal to 0 ([35], Theorem 14), property 7^0 implies that M is a cyclic subgroup of G, i.e., $M = \langle a \rangle \cong C_{2^n}$, and $n \geqslant 2$.

Let us show that $n = 3$. Clearly, $G' \subset M = \langle a \rangle$. Assume that $G' = \left\langle a^{2^m} \right\rangle$. Choose $z \in J(x) \cap J(y)$. Then $\mathrm{Im}\, z \subset \langle a \rangle$ and $\mathrm{Im}\, z$ is Abelian. Hence $G' \subset \mathrm{Ker}\, z$ and z can be presented as a product of following homomorphisms:

$$G \xrightarrow{\varepsilon} G/G' = \left\langle aG' \right\rangle \times \left\langle bG' \right\rangle \times \left\langle cG' \right\rangle \xrightarrow{\pi} \left\langle aG' \right\rangle \xrightarrow{\tau} \langle a \rangle ,$$

where ε is the natural homomorphism, π is a projection and $(aG')\tau = az$. Conversely, each such product of homomorphisms belongs to $J(x) \cap J(y)$. Hence property 5^0 implies $G' = \left\langle a^4 \right\rangle$ and $az = a^{i2^{n-2}}$ for some $i \in \mathbb{Z}_4$. By property 7^0, there exists $i \in \mathbb{Z}_4$ such that $z^2 \neq 0$ and $z^3 = 0$. For such z we have

$$az^2 = a^{i^2 2^{2n-4}} \neq 1, \quad az^3 = a^{i^3 2^{3n-6}} = 1.$$

This implies that $i \equiv 1 \,(\mathrm{mod}\, 2)$, $2n - 4 < n$ and $3n - 6 \geqslant n$, i.e., $n = 3$.

We have already proved that $M = \langle a \rangle \cong C_8$ and $G' = \left\langle a^4 \right\rangle \cong C_2$. Note that $bc \neq cb$. Indeed, if $bc = cb$, then the map $z : G \longrightarrow G$, where $bz = b$, $cz = c$ and $Mz = \langle 1 \rangle$, can be uniquely extended to an endomorphism of G such that $x = zx = x$, $zy = yz = y$ and $z \neq 1$. This contradicts property 8^0. Therefore, $bc \neq cb$ and $[b, c] = a^4$, i.e.,

$$c^{-1}bc = ba^4.$$

In order to prove that $G \cong G_{17}$, we consider two possible cases: $ab = ba$ or $ab \neq ba$.

Assume that $ab = ba$. If $ac = ca$, then the elements a, b, c satisfy the generating relations of G_{17} and, therefore, $G \cong G_{17}$. Suppose now that $ac \neq ca$. Then $[a, c] = a^4$, i.e., $c^{-1}ac = a^5$. Denote $\tilde{a} = ab$. Then $\tilde{a}$ is an element of order 8 of G, $G = \langle \tilde{a}, b, c \rangle$, $\tilde{a}b = b\tilde{a}$ and

$$c^{-1}\tilde{a}c = c^{-1}abc = c^{-1}ac \cdot c^{-1}bc = a^5ba^4 = ab = \tilde{a},\ \tilde{a}c = c\tilde{a}.$$

Hence the elements $\tilde{a}$, b, c satisfy the generating relations of G_{17} and $G \cong G_{17}$.

Assume now that $ab \neq ba$. Then $[a, b] = a^4$ and $b^{-1}ab = a^5$. Denote $\bar{a} = ac$. Then $\bar{a}^2 = acac = a^2[a, c] = a^2a^{4i}$ for some $i \in \mathbb{Z}_2$, $\bar{a}^4 = a^4$ and therefore, $\bar{a}$ is an element of order 8. In addition,

$$\bar{a}b = acb = a \cdot c^{-1}bc \cdot c = a \cdot ba^4 \cdot c = b \cdot b^{-1}ab \cdot a^4c = ba^5a^4c = bac = b\bar{a}.$$

Similarly to the case $ab = ba$ (take instead a the element $\bar{a}$), we obtain that $G \cong G_{17}$. Theorem 1.7 is proved. $\square$

Theorem 1.8 *The group G_{17} is determined by its endomorphism semigroup in the class of all groups.*

The proof of Theorem 1.8 is similar to that of Theorem 1.2.

1.2.2 The group G_{20}

In this subsection we shall characterize the group

$$G_{20} = \left\langle a, b, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ bc = cb,\ c^{-1}ac = ab \right\rangle =$$

$$= (\langle a \rangle \times \langle b \rangle) \leftthreetimes \langle c \rangle = (\langle b \rangle \times \langle c \rangle) \leftthreetimes \langle a \rangle ,$$

by its endomorphism semigroup.

Theorem 1.9 *A finite group G is isomorphic to the group G_{20} if and only if $\mathrm{Aut}(G)$ is a 2-group and there exist x, $y \in I(G)$ which satisfy the following properties:*

1^0 $K(x) \cong \mathrm{End}(C_2)$; 2^0 $K(y) \cong \mathrm{End}(C_8)$; 3^0 $xy = yx = 0$;
4^0 $J(x) \cap J(y) = \{0\}$; 5^0 $|\{\, z \in \mathrm{End}(G) \mid yz = z,\ zx = zy = 0 \,\}| = 2$.

Proof. Necessity. Let $G = G_{20}$. By [12], $|\mathrm{Aut}(G_{20})| = 2^6$. Denote by x and y the projections of G onto its subgroups $\langle c \rangle$ and $\langle a \rangle$, respectively. Then $x, y \in I(G)$, and, similarly to Theorems 1.1, 1.3 and 1.5, direct calculations show that x and y satisfy properties 1^0–5^0.

Sufficiency. Assume that G is a finite group, $\mathrm{Aut}(G)$ is a 2-group and $x,\, y \in I(G)$ such that properties $1^0 - 5^0$ hold. Similarly to the proof of theorem 1.7, properties $1^0 - 4^0$ imply that G is a 2-group such that

$$G = (M \leftthreetimes \langle c\rangle) \leftthreetimes \langle b\rangle = (M \leftthreetimes \langle b\rangle) \leftthreetimes \langle c\rangle\,,$$

where

$$M = \mathrm{Ker}\ x \cap \mathrm{Ker}\ y,\ \mathrm{Im}\ x = \langle c\rangle \cong C_2,\ \mathrm{Im}\ y = \langle a\rangle \cong C_8.$$

Hence $G/M = \langle aM\rangle \times \langle cM\rangle \cong C_8 \times C_2$ and an endomorphism z of G which satisfies equalities $yz = z$ and $zx = zy = 0$ is a product $z = \varepsilon\pi\tau$ of the natural homomorphism $G \xrightarrow{\varepsilon} G/M$, the projection $G/M \xrightarrow{\pi} \langle aM\rangle$ and a homomorphism $\langle aM\rangle \xrightarrow{\tau} M$. Conversely, for each homomorphism $\langle aM\rangle \xrightarrow{\tau} M$ the endomorphism $z = \varepsilon\pi\tau$ of G satisfies equalities $yz = z$ and $zx = zy = 0$. By property 5^0 it follows that the subgroup M of G has only one element of order 2 and does not contain an element of order 4. Therefore, by [37], Theorem 5.3.6, M is a cyclic group of order 2, i.e., $M = \langle b\rangle \cong C_2$ for an element b of G. Since M is an invariant subgroup of G, we have $ba = ab$ and $cb = bc$.

The elements a and b do not commute. Indeed, if $ac = ca$, then $G = \langle b\rangle \times \langle a\rangle \times \langle c\rangle$ and the projection z of G onto $\langle b\rangle$ belongs to $J(x) \cap J(y)$ which contradicts property 4^0. Therefore, $ac \neq ca$, $[c,\, a] = c^{-1}a^{-1}ca \in M = \langle b\rangle \cong C_2$, i.e., $c^{-1}a^{-1}ca = b$ and $c^{-1}ac = ab$. So it follows that the elements a, b and c of G satisfy the generating relations of the group G_{20}. Consequently, $G \cong G_{20}$. Theorem 1.9 is proved. $\square$

Theorem 1.10 *The group G_{20} is determined by its endomorphism semigroup in the class of all groups.*

The proof of Theorem 1.10 is similar to the proof of Theorem 1.2.

1.2.3 The group G_{27}

In this subsection, we shall characterize the group

$$G_{27} = \left\langle a,\, b,\, c \mid a^8 = b^2 = c^2 = 1,\ ab = ba,\ bc = cb,\ c^{-1}ac = a^{-1}b\right\rangle =$$

$$= (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle \cong (C_8 \times C_2) \leftthreetimes C_2$$

by its endomorphism semigroup.

Theorem 1.11 *A finite group G is isomorphic to the group G_{27} if and only if there exists $x \in I(G)$ which satisfies the following properties:*

1^0 $K(x) \cong \mathrm{End}(C_2)$; $\quad 2^0$ $J(x) \cap I(G) = \{0\}$; $\quad 3^0$ $|J(x)| = 8$;

4^0 $|H(x)| = 4$; 5^0 $V(x)$ *is a 2-group;*
6^0 $|\{y \in I(G) \mid xy = y,\ yx = x\}| = 8$;
7^0 *there exists* $z \in H(x)$ *such that* $z \cdot J(x) \neq \{0\}$;
8^0 *if* $z \in V(x)$, $v \in H(x)$ *and* $u \in \mathrm{End}(G)$ *such that* $xu = 0$ *and* $ux = u$, *then* $uvz = uv$.

Proof. Necessity. Let $G = G_{27}$. Denote by x the projection of G onto its subgroup $\langle c\rangle$. Then $x \in I(G)$ and direct calculations show that x satisfies properties 1^0–8^0.

Sufficiency. Assume that G is a finite group and $x \in I(G)$ such that properties $1^0 - 8^0$ hold. Similarly to the proof of theorem 1.7, properties 1^0, 2^0 and 5^0 imply that G is a 2-group such that

$$G = \mathrm{Ker}\ x \leftthreetimes \mathrm{Im}\ x,\ \mathrm{Im}\ x = \langle c\rangle \cong C_2.$$

By Lemma 6 there exists an one-to-one correspondence between $H(x)$ and $\mathrm{Hom}(\mathrm{Im}\, x, \mathrm{Ker}\ x)$. Hence by property 4^0, $\mathrm{Ker}(x)$ has 3 elements of order 2. Since G is a 2-group, one of these belongs to the center of G. Denote it by b_0. Let a_0 be an element of order 2 in $\mathrm{Ker}\ x$ different from b_0. Then b_0a_0 is the third element of order 2 in $\mathrm{Ker}\ x$.

Since $\mathrm{Im}\ x$ is Abelian and $J(x) \neq \{0\}$, we have $G' \subset \mathrm{Ker}\ x$ and

$$G/G' = \langle a_1G'\rangle \times \ldots \times \langle a_kG'\rangle \times \langle cG'\rangle$$

for some $k \geqslant 1$ ($a_i \in \mathrm{Ker}\ x \setminus G'$). Then $\varepsilon\pi\tau \in J(x)$, where $G \xrightarrow{\varepsilon} G/G'$ is the natural homomorphism, $G/G' \xrightarrow{\pi} \langle a_iG'\rangle$ is a projection and $(a_iG')\tau = a_0^s b_0^t$ ($s, t \in \mathbb{Z}_2$). By property 3^0, $k = 1$, i.e., $\mathrm{Ker}\ x/G' = \langle a_1G'\rangle$. Using again property 3^0 and elements a_0, b_0, it is easy to check that $\langle a_1G'\rangle \cong C_4$ and

$$z \in J(x) \Longrightarrow G' \subset \mathrm{Ker}\ z. \tag{1.37}$$

Therefore,

$$G/G' = \langle aG'\rangle \times \langle cG'\rangle \cong C_4 \times C_2$$

($a = a_1$). Note that $a^4 \neq 1$, because otherwise the product of the natural homomorphism $G \longrightarrow G/G'$, the projection $G/G' \longrightarrow \langle aG'\rangle$ and the isomorphism $\langle aG'\rangle \cong \langle a\rangle$ is a non-zero element in $J(x) \cap I(G)$ which contradicts property 2^0.

Property 7^0, Lemmas 6, 5 and condition (1.37) imply that $\mathrm{Ker}\ x \setminus G' = \langle a, G'\rangle \setminus G'$ contains an element of order 2. Denote this element by b. Therefore, $b \in \langle a, G'\rangle \setminus G'$, $b^2 = 1$, $b \in \{a_0, b_0, a_0b_0\}$. Since G' has an element of order 2 and $\mathrm{Ker}\ x$ has 3 elements of order 2, G' has only one element of order 2. Hence G' is cyclic or a generalized quaternion group. If G' is a generalized quaternion group, then it has at least 6 elements of order 4 and, therefore, we can construct more than 8 endomorphisms which

belong to $J(x)$. This contradicts property 3^0. Consequently, G' is a cyclic group and

$$G' = \langle d \rangle \cong C_{2^m},\ a^4 \in G',\ a^4 \neq 1.$$

Clearly, $a^4 \in \langle d^2 \rangle$, because otherwise $\langle a^4 \rangle = \langle d \rangle$, Ker $x = \langle a \rangle$ and this contradicts to the fact that Ker x has three elements of order 2. It follows also from here that $o(d) \geqslant 4$.

Let us prove that each element $h \in$ Ker x of order 2 belongs to the center $Z(G)$ of G. The maps u and v, where

$$cu = 1,\ G'u = \langle 1 \rangle,\ au = c,\ (\text{Ker } x)v = \langle 1 \rangle,\ cv = h,$$

can be extended to endomorphisms of G such that $v \in H(x)$, $xu = 0$ and $ux = u$. Denote $z = uv$. Choose an arbitrary element $g \in G$. Since Im x is Abelian, $\widehat{g} \in V(x)$. Hence z and $y = \widehat{g}$ satisfy to the conditions of property 8^0. Therefore, $zy = z$, $z\widehat{g} = z$. Since Im $z = \langle h \rangle$, we have $h\widehat{g} = h$, i.e., $hg = gh$ and $h \in Z(G)$. Particularly, $b \in Z(G)$ and $ab = ba$.

Due to $a^4 \neq 1$, we have $b \notin \langle a \rangle$ and hence

$$\langle a, b \rangle = \langle a \rangle \times \langle b \rangle.$$

Therefore, all 8 elements of $J(x)$ can be obtained as products $\varepsilon\pi\tau_{ij}$, where $G \xrightarrow{\varepsilon} G/G' = \langle aG' \rangle \times \langle cG' \rangle$ is the natural homomorphism, $G/G' \xrightarrow{\pi} \langle aG' \rangle$ is a projection and $(aG')\tau_{ij} = a^{i \cdot o(a)/4} b^j$ $(i \in \mathbb{Z}_4,\ j \in \mathbb{Z}_2)$.

Denote $N = \langle d^2 \rangle$ and $M = \langle a^2, N \rangle$. Then N and M are normal subgroups of G. Since $a^4 \in \langle d^2 \rangle$, we have Ker $x/N = \langle aN \rangle \times \langle dN \rangle \cong C_4 \times C_2$,

$$\text{Ker } x/M = \langle aM \rangle \times \langle dM \rangle \cong C_2 \times C_2,$$

$$G/M = (\langle aM \rangle \times \langle dM \rangle) \leftthreetimes \langle cM \rangle \cong (C_2 \times C_2) \leftthreetimes C_2.$$

If $cM \cdot aM = aM \cdot cM$, then we have $G/M = \langle aM \rangle \times \langle dM \rangle \times \langle cM \rangle$ and the endomorphism z of G defined by $Mz = \langle 1 \rangle$, $az = cz = 1$, $dz = b$, is an element of $J(x)$ which does not have the form showed above. Therefore, $cM \cdot aM \neq aM \cdot cM$, $[a, c] \notin M = \langle a^2, d^2 \rangle$, $\langle [a, c] \rangle = \langle d \rangle = G'$ and we can assume that $[a, c] = d$, i.e.,

$$c^{-1}ac = ad$$

and $a^{-1}ca = [a, c]c = dc$, $dc \cdot dc = a^{-1}c^2a = 1$, $c^{-1}dc = d^{-1}$. Hence for each integer i, the element cd^i of G is an element of order 2: $cd^i \cdot cd^i = c^{-1}d^ic \cdot d^i = d^{-i}d^i = 1$.

Let us define for each integer i an endomorphism z_i of G as follows:

$$(\text{Ker } x)z_i = \langle 1 \rangle,\quad cz_i = cd^i.$$

Define $z \in \text{End}(G)$ by $(\text{Ker } x)z = \langle 1 \rangle$, $cz = cb$. Then $z \neq z_i$ and

$$z,\ z_i \in \{y \in I(G) \mid xy = y,\ yx = x\}. \tag{1.38}$$

By property 6^0, $o(d) \geqslant 4$ and (1.38), we have $o(d) = 4$. Therefore, $|\operatorname{Ker} x| = 16$, $o(a) = 8$, $|\langle a\rangle \times \langle b\rangle| = 16$ and

$$\operatorname{Ker} x = \langle a\rangle \times \langle b\rangle \cong C_8 \times C_2.$$

Let us prove now that $G \cong G_{27}$. By construction, $b = a^2 d^i$ for some $i \in \mathbb{Z}_4$. Since $1 = b^2 = a^4 d^{2i} = d^2 d^{2i} = d^{2(i+1)}$, we have $i \equiv 1 \,(\mathrm{mod}\, 2)$, i.e., $i \in \{1, 3\}$. If $i = 1$, then $d = ba^{-2}$, $c^{-1}ac = ad = a^{-1}b$ and a, b, c satisfy the generating relations of the group G_{27}, i.e., $G \cong G_{27}$. If $i = 3$, then $b = a^2 d^3 = a^2 d^{-1}$, $d = a^2 b$, $c^{-1}ac = ad = a^{-1} \cdot a^4 b$ and the map $u : G_{27} = \langle a, b, c\rangle \longrightarrow G = \langle a, b, c\rangle$ defined by $cu = c$, $au = a$, $bu = a^4 b$, is an isomorphism, i.e., $G \cong G_{27}$. Theorem 1.11 is proved. $\square$

Theorem 1.12 *The group G_{27} is determined by its endomorphism semigroup in the class of all groups.*

The proof of Theorem 1.12 is similar to the proof of Theorem 1.2.

2 The groups presentable in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$

2.1 A characterization of groups presentable in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$ by their defining relations

The results presented in this section have been published in [10].

2.1.1 Main concepts

In this section we find all non-isomorphic groups of order 2^{2n+1} $(n \geqslant 3)$ which can be presented in the form $\mathcal{G} = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2$, i.e.,

$$\mathcal{G} = \left\langle a, b, c \mid a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^p b^q,\ c^{-1}bc = a^r b^s \right\rangle,$$

where p, q, r, $s \in \mathbb{Z}_{2^n}$. An element c induces an inner automorphism $\widehat{c}$ of order 1 or 2:

$$a\widehat{c} = c^{-1}ac = a^p b^q, \qquad b\widehat{c} = c^{-1}bc = a^r b^s,$$

and to find all groups in given form we have to find all automorphisms of the group $C_{2^n} \times C_{2^n} = \langle a \rangle \times \langle b \rangle$ of such kind.

It is clear that the map

$$\varphi : C_{2^n} \times C_{2^n} \longrightarrow C_{2^n} \times C_{2^n}, \quad a\varphi = a^p b^q, \quad b\varphi = a^r b^s \tag{2.1}$$

satisfies the defining relations of the group

$$C_{2^n} \times C_{2^n} = \left\langle a, b, c \mid a^{2^n} = b^{2^n} = 1,\ ab = ba \right\rangle$$

and it is an endomorphism of this group for every p, q, r, $s \in \mathbb{Z}_{2^n}$. An endomorphism (2.1) is an automorphism of $C_{2^n} \times C_{2^n}$ if and only if

$$ps - rq \equiv 1 \pmod 2, \tag{2.2}$$

i.e., if and only if the matrix $A = \left\| \begin{matrix} p & q \\ r & s \end{matrix} \right\|$ is invertible. Let us find, under which conditions an automorphism (2.1), (2.2) has order 1 or 2:

$$\begin{aligned} a &= (a)\,\varphi^2 = (a\varphi)\,\varphi = (a^p b^q)\,\varphi = (a^p b^q)^p\,(a^r b^s)^q = a^{p^2+rq} b^{q(p+s)}, \\ b &= (b)\,\varphi^2 = (b\varphi)\,\varphi = (a^r b^s)\,\varphi = (a^p b^q)^r\,(a^r b^s)^s = a^{r(p+s)} b^{qr+s^2}, \end{aligned}$$

i.e., it is an automorphism of order 1 or 2 if and only if the matrix $\left\| \begin{array}{cc} p & q \\ r & s \end{array} \right\|$ over $\mathbb{Z}_{2^n}$ satisfies condition (2.2) and the condition $A^2 = I$, where I is the identity matrix.

Recall that matrices $A_1 = \left\| \begin{array}{cc} p_1 & q_1 \\ r_1 & s_1 \end{array} \right\|$ and $A_2 = \left\| \begin{array}{cc} p_2 & q_2 \\ r_2 & s_2 \end{array} \right\|$ (over $\mathbb{Z}_{2^n}$) are conjugate if there exists a regular matrix g (over $\mathbb{Z}_{2^n}$) such that $g^{-1}A_2g \equiv A_1$.

It is obvious, that the relation "to be conjugate" is an equivalence relation on the set of all regular (2×2)-matrices over $\mathbb{Z}_{2^n}$. Let us denote the conditions $a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba$ by $(*)$.

Lemma 2.1 *If matrices A_1 and A_2 (over $\mathbb{Z}_{2^n}$) are conjugate, then the groups*

$$\mathcal{G}_1 = \left\langle a, b, c \mid (*),\ c^{-1}ac = a^{p_1}b^{q_1},\ c^{-1}bc = a^{r_1}b^{s_1} \right\rangle = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2$$

and

$$\mathcal{G}_2 = \left\langle a, b, c \mid (*),\ c^{-1}ac = a^{p_2}b^{q_2},\ c^{-1}bc = a^{r_2}b^{s_2} \right\rangle = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2,$$

corresponding matrices A_1 and A_2, are isomorphic.

Proof. Let matrices A_1 and A_2 (over $\mathbb{Z}_{2^n}$) be conjugate, i.e., there exists $g = \left\| \begin{array}{cc} x & y \\ z & w \end{array} \right\|$, $\det g \not\equiv 0 \,(\mathrm{mod}\, 2)$, such that $g^{-1}A_2g \equiv A_1$. It is easy to verify that the map

$$\varphi : \mathcal{G}_2 \longrightarrow \mathcal{G}_1, \qquad c\varphi = c,\ a\varphi = a^x b^y,\ b\varphi = a^z b^w.$$

is an isomorphism of the groups $\mathcal{G}_1$ and $\mathcal{G}_2$. Lemma 2.1 is proved. $\square$

To find all groups presentable in the form $\mathcal{G} = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2$, first of all we find all regular (2×2)-matrices A over $\mathbb{Z}_{2^n}$ such that $A^2 = I$. Next, by Lemma 2.1, we divide all obtained matrices into conjugacy classes. Finally, we decide under which conditions two groups corresponding to two matrices of different conjugacy classes are isomorphic.

2.1.2 Regular (2×2)-matrices over $\mathbb{Z}_{2^n}$ of order 1 or 2

The aim of this subsection is to find all matrices $A = \left\| \begin{array}{cc} a & b \\ c & d \end{array} \right\|$ (over $\mathbb{Z}_{2^n}$) which satisfy the conditions (2.2) and $A^2 = I$, i.e.,

$$ad - bc \not\equiv 0 \pmod 2 \tag{2.3}$$

and

$$a^2 \equiv 1 - bc,\ \ (a-d)\,(a+d) \equiv 0,\ \ b\,(a+d) \equiv 0,\ \ c\,(a+d) \equiv 0 \qquad (2.4)$$

modulo 2^n. Second congruence of (2.4) implies $a^2 \equiv d^2$, i.e., the numbers a and d are both even or odd.

Let us solve system (2.4) assuming (2.3). The sets of obtained solutions in the form of matrices are denoted by M_1, $M_2, \ldots, M_{36}$. The list of all sets M_i is given in Appendix B. Note that the sets M_i are pairwise disjoint. We consider two cases separately: i) at least one of the numbers b, c (or both) is odd and ii) both b and c are even.

Proposition 2.1 *Let at least one of the numbers b, c (or both) be odd. Then the solutions of system (2.4) belong to the sets M_1 and M_2. The number of matrices of these sets are*

$$|M_1| = 2^{2n-2},\ \ |M_2| = 2^{2n-1}.$$

Proof. Assume first that b and c be both odd numbers. Then the numbers a, d are both even and the first congruence of (2.4) implies $c \equiv \left(1-a^2\right) b^{-1} \pmod{2^n}$. The third congruence of (2.4) implies $d = -a$ and we get the set M_1. Let us find the number of elements of the set M_1. There is 2^{n-1} possibilities to choose odd number b, and 2^{n-1} possibilities to choose even number a. Hence $|M_1| = 2^{n-1}2^{n-1} = 2^{2n-2}$.

Let now only one of numbers b or c be odd. Then, by (2.3), a and d are odd numbers. The last two congruences of (2.4) imply again $d = -a$. The first congruence of (2.4) implies $c \equiv \left(1-a^2\right) b^{-1} \pmod{2^n}$ if b is odd and $b \equiv \left(1-a^2\right) c^{-1} \pmod{2^n}$ if c is odd. Hence we get the set M_2. It is $2^{n-1} \cdot 2^{n-1}$ possibilities to choose two odd numbers a and b (or c) and $|M_2| = 2^{n-1} \cdot 2^{n-1} \cdot 2 = 2^{2n-1}$. Proposition 2.1 is proved. □

Let now both b and c be even. We give without any proof the next well-known result:

Lemma 2.2 *Solutions of the congruence*

$$a^2 \equiv 1\,(mod\,2^n)$$

are $a \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$.

Lemma 2.2 gives us solutions of the first congruence of system (2.4) in the case $bc \equiv 0 \pmod{2^n}$. Let us solve now this congruence if $bc \not\equiv 0 \pmod{2^n}$.

Lemma 2.3 *Let numbers b, c be even and $bc \not\equiv 0\,(mod\,2^n)$. Then solutions of the congruence*

$$a^2 \equiv 1 - bc\,(mod\,2^n)$$

are triples

$$(a,b,c)=\left(\varepsilon+2^{t+s-1}p,2^tu,2^s\left(-\left(\varepsilon+2^{t+s-2}p\right)pu^{2^{n-s-t-1}-1}+2^{n-t-s}k\right)\right),$$

where

$$t,\ s\in\mathbb{Z}_n\setminus\{0\},\qquad n>t+s\geqslant 3,$$
$$\varepsilon=\pm1,\qquad u\in\mathbb{Z}^*_{2^{n-t}},\qquad p\in\mathbb{Z}^*_{2^{n-(t+s)+1}},\qquad k\in\mathbb{Z}_{2^t}.$$

The number of solutions is $|\{(a,b,c)\}|=2^{n+1}\left(3\cdot 2^{n-3}-n\right)$.

Proof. Let $b=2^tu,\ \ c=2^sv$, where $t,s\in\mathbb{Z}_n\setminus\{0\}$, $u\in\mathbb{Z}^*_{2^{n-t}}$, $v\in\mathbb{Z}^*_{2^{n-s}}$. Denote $s+t=m$. If our congruence has a solution then $1-bc\equiv 1\,(\mathrm{mod}8)$, i.e., $bc\equiv 0(\mathrm{mod}8)$ and $m\geqslant 3$. We can write our congruence in the form

$$(a-1)(a+1)\equiv -2^muv\ \ (\mathrm{mod}\ 2^n).$$

Thus

$$a-1=2^rp\ \text{ and }\ a+1=2^{m-r}q,$$

where $r\in\mathbb{Z}_m\setminus\{0\}$, $p\in\mathbb{Z}^*_{2^{n-r}}$, $q\in\mathbb{Z}^*_{2^{n-m+r}}$. Then

$$2^rp\cdot 2^{m-r}q\equiv -2^muv\,(\mathrm{mod}\ 2^n),$$

and, therefore,

$$pq\equiv -uv\left(\mathrm{mod}\ 2^{n-m}\right). \tag{2.5}$$

On the other hand,

$$a=1+2^rp\equiv -1+2^{m-r}q,$$

i.e., $2\left(1+2^{r-1}p\right)=2^{m-r}q$ and

$$1+2^{r-1}p\equiv 2^{m-r-1}q.$$

The last equation has a solution only in the cases $r=1$ and $r=m-1$.

In the case $r=1$ we have

$$p=-1+2^{m-2}q,$$

i.e., $p=-1+2^{m-2}q$. Therefore,

$$a=1+2\left(-1+2^{m-2}q\right)=-1+2^{m-1}q,\quad q\in\mathbb{Z}^*_{2^{n-m+1}}.$$

Analogously, in the case $r=m-1$ we have

$$q=1+2^{m-2}p,\ a=1+2^{m-1}p,\ \ p\in\mathbb{Z}^*_{2^{n-m+1}}.$$

Resume, that in both considered cases we can write

$$q = \varepsilon + 2^{m-2}p,\ a = \varepsilon + 2^{m-1}p,\quad p \in \mathbb{Z}^*_{2^{n-m+1}}.$$

where $\varepsilon = \pm 1$. By (2.5), we have

$$\left(\varepsilon + 2^{m-2}q\right) q \equiv -uv \left(\mathrm{mod}\ 2^{n-m}\right)$$

and

$$v = -\left(\varepsilon + 2^{m-2}q\right) qu^{-1} = -\left(\varepsilon + 2^{m-2}q\right) qu^{2^{n-m-1}-1} \left(\mathrm{mod}\ 2^{n-m}\right).$$

Since $0 < v < 2^{n-s}$, we have $2^{n-s}/2^{n-m} = 2^t$ different values modulo 2^n in the form $v_k = v + 2^{n-m}k$, where $k \in \mathbb{Z}_{2^t}$. We have obtained the first statement of Lemma 2.3.

Let us now determine the number of triples $(a,\ b,\ c)$, which satisfy the congruence $a^2 \equiv 1 - bc \left(\mathrm{mod}\ \ 2^n\right)$, where $bc \not\equiv 0 \left(\mathrm{mod}\ 2^n\right)$ and $b,\ c$ are both even numbers. Denote the number of such kind of triples by $\left|\{(a,b,c)\}\right|$. The triples $(a,\ b,\ c)$ are given by the parameters $s,\ t,\ \varepsilon,\ u,\ k,\ p$. The numbers of possible values of the parameters $\varepsilon,\ u,\ k,\ p$ are $2,\ 2^{n-t-1},\ 2^t,\ 2^{n-t-s}$, respectively. If we sum up over possible values of s and t, we get

$$\left|\{(a,b,c)\}\right| = 2\sum_{t=1}^{n-1} 2^{n-t-1} \sum_{s=1,\ s+t\geqslant 3}^{n-t-1} \left(2^t \cdot 2^{n-t-s}\right) = 2^{n+1}\left(3 \cdot 2^{n-3} - n\right).$$

Lemma 2.3 is proved. □

For even numbers $b,\ c$ we consider two cases: one of the numbers (or both) $b,\ c$ is zero and both numbers $b,\ c$ are nonzero even numbers.

Proposition 2.2 *Let one of numbers (or both) $b,\ c$ be zero. Then solutions of system (2.4) belong to the sets $M_3,\ M_4,\ M_5,\ M_6,\ M_7,\ M_8,\ M_9,\ M_{10},\ M_{11},\ M_{12},\ M_{13},\ M_{14},\ M_{15},\ M_{16},\ M_{17},\ M_{18},\ M_{19},\ M_{20},\ M_{21},\ M_{22}$. The number of elements of these sets are $|M_3| = |M_4| = |M_5| = |M_6| = 1,\ |M_i| = 2$ $(i = 7, 8, ..., 12, 15, 16, 17, 18)$, $|M_{19}| = |M_{20}| = 4$ and*

$$|M_{13}| = |M_{14}| = |M_{21}| = |M_{22}| = 4\left(2^{n-1} - 1\right).$$

Proof. By Lemma 2.2, the solution of the first congruence of system (2.4) is $a \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$.

I) If $b = c = 0$ then the third and fourth congruence of system (2.4) hold. In the second congruence, we have two possibilities: **1)** one of factors equals to zero (i.e., $a + d \equiv 0$ or $a - d \equiv 0$) and **2)** both factors are non-zero (i.e. $a + d \not\equiv 0$ and $a - d \not\equiv 0$).

In the case **1)** $d = \pm a$ and we get the sets $M_3,\ M_4, M_5,\ M_6, M_7,\ M_8$.

In the case **2)** we denote $a + d = 2^m x,\ a - d = 2^k y$ (where $m,\ k \in \mathbb{Z}_n \setminus \{0\}$, $x \in \mathbb{Z}^*_{2^{n-m}},\ y \in \mathbb{Z}^*_{2^{n-k}}$ and $m + k \geqslant n$). We have

$$a = 2^{m-1}x + 2^{k-1}y,\ d = 2^{m-1}x - 2^{k-1}y$$

modulo 2^{n-1} and

$$a = 2^{m-1}x + 2^{k-1}y + 2^{n-1}z,\ d = 2^{m-1}x - 2^{k-1}y + 2^{n-1}z \tag{2.6}$$

modulo 2^n, where $z = 0,\ 1$. As $a,\ d$ are odd, so one of the numbers $m - 1$ or $k - 1$ has to be zero (another has to be nonzero): **a)** $m - 1 = 0$, **b)** $k - 1 = 0$. Let us consider these two cases.

a) If $m = 1$ and $k > 1$, we have $k = n - 1,\ y = 1$, because $m + k \geqslant n$, and the solution of (2.6) is

$$a = x + 2^{n-2} + 2^{n-1}z,\ d = a + 2^{n-1},$$

where $x \in \mathbb{Z}^*_{2^{n-1}},\ z = 0,\ 1$.

b) Similarly, if $k = 1$ and $m > 1$, we get $m = n - 1,\ x = 1$ and the solution of (2.6) is

$$a = 2^{n-2} + y + 2^{n-1}z,\ d = 2^{n-1} - a,$$

where $y \in \mathbb{Z}^*_{2^{n-1}},\ z = 0,\ 1$.

Summarizing the case **2)**, we obtain $d = \pm a + 2^{n-1}$ and the values of number a which give us the sets $M_9,\ M_{10},\ M_{11},\ M_{12}$.

II) Let us now consider the case if $b = 0,\ c = 2^t u$ (or $c = 0,\ b = 2^t u$), where $t \in \mathbb{Z}_n \setminus \{0\},\ u \in \mathbb{Z}^*_{2^{n-t}}$. Then the fourth (or third) congruence of system (2.4) holds only if **1)** $a+d = 0$ or **2)** $a+d = 2^m x$ $(n-t \leqslant m \leqslant n-1$, $x \in \mathbb{Z}^*_{2^{n-m}})$.

1) If $a + d = 0$ we get the sets M_{13} and M_{14}. It is clear that for even number $2^t u \not\equiv 0$ there is $2^{n-1} - 1$ possibilities and $|M_{13}| = |M_{14}| = 4\left(2^{n-1} - 1\right)$.

2) If $a+d = 2^m x$ $(n-t \leqslant m \leqslant n-1,\ x \in \mathbb{Z}^*_{2^{n-m}})$, the second congruence of (2.4) implies **a)** $a - d = 0$ or **b)** $a - d = 2^k y$ (where $n - m \leqslant k \leqslant n - 1$, $y \in \mathbb{Z}^*_{2^{n-k}})$.

a) If $a - d = 0$, then $2^m x = a + d = 2a$ $(m \geqslant n - t,\ x \in \mathbb{Z}^*_{2^{n-m}})$ and $a = 2^{m-1}x$ is odd only if $m = 1$. Then $n-t \leqslant 1$, i.e., $t \geqslant n-1$ and $t = n-1$ (thus $u = 1$). We get the sets $M_{15},\ M_{16},\ M_{17},\ M_{18}$.

b) If $a - d = 2^k y$ (where $n - m \leqslant k \leqslant n - 1,\ y \in \mathbb{Z}^*_{2^{n-k}}$), then we get

$$a = 2^{m-1}x + 2^{k-1}y + 2^{n-1}z,\ d = 2^{m-1}x - 2^{k-1}y + 2^{n-1}z \tag{2.7}$$

modulo 2^n, where $z = 0,\ 1$. Since $a,\ d$ have to be odd numbers, one of the numbers $m - 1$ or $k - 1$ have to be zero: **i)** $m - 1 = 0$, **ii)** $k - 1 = 0$. Let us consider these two cases.

i) Case $m = 1$ and $k > 1$. Then $k = n-1$, $y = 1$ and $t \geqslant n-m = n-1$ i.e. $t = n-1$, $s = 1$. In this case we have $b = 0$, $c = 2^{n-1}$ (or $b = 2^{n-1}$, $c = 0$) and the solution of (2.7) is $a = x + 2^{n-2} + 2^{n-1}z$, $d = a + 2^{n-1}$, where $x \in \mathbb{Z}^*_{2^{n-1}}$, $z = 0, 1$. Since we already know all values of a, we get the sets M_{19}, M_{20}.

ii) Case $k = 1$ and $m > 1$. Then $m = n-1$, $x = 1$ and $t \geqslant n-m = 1$. In this case the solution of (2.7) is $a = 2^{n-2} + y + 2^{n-1}z$, $d = 2^{n-1} - a$, where $y \in \mathbb{Z}^*_{2^{n-1}}$, $z = 0, 1$. Since all values of a are already known, we get the sets M_{21}, M_{22}. It is clear, that $|M_{21}| = |M_{22}| = 4\left(2^{n-1} - 1\right)$. Proposition 2.2 is proved. □

Now let b and c both be nonzero even numbers.

Proposition 2.3 *Let b and c both be nonzero even numbers i.e. $b = 2^t u$, $c = 2^s v$, where $t, s \in \mathbb{Z}_n \setminus \{0\}$, $t + s \geqslant 3$, $u \in \mathbb{Z}^*_{2^{n-t}}$, $v \in \mathbb{Z}^*_{2^{n-s}}$. Then the solutions of system* (2.4) *belong to one of the sets M_{23}, M_{24}, M_{25}, M_{26}, M_{27}, M_{28}, M_{29}, M_{30}, M_{31}, M_{32}, M_{33}, M_{34}, M_{35}, M_{36}. Numbers of elements of these sets are $|M_{23}| = |M_{24}| = |M_{25}| = |M_{26}| = 1$, $|M_{31}| = |M_{32}| = 2$ and*

$$|M_{27}| = |M_{28}| = |M_{33}| = |M_{34}| = (n-2)\,2^n + 2,$$
$$|M_{29}| = |M_{30}| = |M_{35}| = |M_{36}| = 2^n\left(3 \cdot 2^{n-3} - n\right).$$

Proof. Considering the second congruence of system (2.4), the following three cases are possible: **I)** $a - d = 0$, **II)** $a + d = 0$, **III)** $a - d \not\equiv 0 \pmod{2^n}$, $a + d \not\equiv 0 \pmod{2^n}$.

I) If $a - d = 0$, then the third congruence implies $2^t u \cdot 2a = 2^{t+1}ua \equiv 0 \pmod{2^n}$ and the fourth congruence implies $2^s v \cdot 2a = 2^{s+1}va \equiv 0 \pmod{2^n}$, i.e., $t = s = n-1$. Since in this case $a^2 \equiv 1 \pmod{2^n}$, we get, by Lemma 2.2, the sets M_{23}, M_{24}, M_{25}, M_{26}.

II) If $a + d = 0$, then we have two possibilities: **1)** $t + s \geqslant n$ and **2)** $3 \leqslant t + s < n$.

1) If $t + s \geqslant n$, then $a^2 \equiv 1 \pmod{2^n}$ and, by Lemma 2.2, we get the sets M_{27}, M_{28}. Clearly, $|M_{27}| = |M_{28}|$ and

$$|M_{27} \cup M_{28}| = \left|\left\{(a, b, c) : a \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}, b = 2^t u,\ c = 2^s v\right\}\right|,$$

where $t, s \in \mathbb{Z}_n \setminus \{0\}$, $t + s \geqslant n$, $u \in \mathbb{Z}^*_{2^{n-t}}$, $v \in \mathbb{Z}^*_{2^{n-s}}$. We have four possibilities for the choice of a. The number of choices of (b, c) depends on t : there is 2^{n-t-1} possibilities for the choice of u and t possibilities for the choice of s; for every s we have 2^{n-s-1} possibilities for the choice of v. Hence

$$\begin{aligned} |M_{27}| &= |M_{28}| = \frac{1}{2}\,|M_{27} \cup M_{28}| = \\ &= \frac{1}{2} \cdot 4 \cdot \sum_{t=1}^{n-1} 2^{n-t-1} \left(\sum_{s=n-t}^{n-1} 2^{n-s-1} \right) = (n-2)\,2^n + 2. \end{aligned}$$

2) If $3 \leqslant t+s < n$, we use Lemma 2.3 and get the sets M_{29}, M_{30}. Clearly,

$$|M_{29}| = |M_{30}| = \frac{1}{2}\,|M_{29} \cup M_{30}| = \frac{1}{2}\,|\{(a,b,c)\}| = 2^n\left(3\cdot 2^{n-3} - n\right).$$

III) If $a+d = 2^m x$ ($m \in \mathbb{Z}_n \setminus \{0\}$, $x \in \mathbb{Z}^*_{2^{n-m}}$), the third and fourth congruences of system (2.4) imply $m+t \geqslant n$, $m+s \geqslant n$ and $a-d = 2^k y$ ($k \in \mathbb{Z}_n \setminus \{0\}$, $y \in \mathbb{Z}^*_{2^{n-k}}$, $k+m \geqslant n$). Then

$$a = 2^{m-1}x + 2^{k-1}y,\ d = 2^{m-1}x - 2^{k-1}y$$

modulo 2^{n-1} and, therefore, the solution is

$$a = 2^{m-1}x + 2^{k-1}y + 2^{n-1}z,\ d = 2^{m-1}x - 2^{k-1}y + 2^{n-1}z \tag{2.8}$$

modulo 2^n where $z = 0, 1$. Since a, d are odd, two cases are possible: **1)** $m = 1$, $k > 1$ and **2)** $k = 1$, $m > 1$.

1) In the case of $m = 1$ and $k > 1$ we have $k = s = t = n-1$, $y = u = v = 1$ and the solution of (2.8) is

$$b = c = 2^{n-1},\ a = x + 2^{n-2} + 2^{n-1}z,\ d = a + 2^{n-1},$$

where $x = 1, 3, ..., 2^{n-1}-1$, $z = 0, 1$. Since in this case $a^2 \equiv 1 \pmod{2^n}$, we get the sets M_{31}, M_{32}.

2) Assume $k = 1$ and $m > 1$. Then $m = n-1$, $x = 1$; $s, t \geqslant n-m = 1$ and the solution of (2.8) is

$$a = 2^{n-2} + y + 2^{n-1}z,\ d = 2^{n-1} - a,\ \text{where } y \in \mathbb{Z}^*_{2^{n-1}},\ z = 0, 1.$$

So, we have two possibilities for odd number a: **a)** $t+s \geqslant n$ and **b)** $3 \leqslant t+s < n$.

a) If $t+s \geqslant n$, then $a^2 \equiv 1 \pmod{2^n}$, and we get the sets M_{33}, M_{34}. Analogously to the sets M_{27}, M_{28}, the numbers of elements of the sets M_{33}, M_{34} are

$$|M_{33}| = |M_{34}| = \frac{1}{2}\,|M_{33} \cup M_{34}| = (n-2)\,2^n + 2.$$

b) If $3 \leqslant t+s < n$, then $a^2 \not\equiv 1 \pmod{2^n}$ and, by Lemma 2.3, we obtain the sets M_{35}, M_{36}. Similarly to the sets M_{29}, M_{30}, the numbers of elements of the sets M_{35}, M_{36} are

$$|M_{35}| = |M_{36}| = \frac{1}{2}\,|M_{35} \cup M_{36}| = \frac{1}{2}\,|\{(a,b,c)\}| = 2^n\left(3\cdot 2^{n-3} - n\right).$$

Proposition 2.3 is proved. □

From Propositions 2.1, 2.2 and 2.3 it follows that the following theorem is true:

Theorem 2.1 *There is exactly* $9 \cdot 4^{n-1} + 32$ *matrices over* Z_{2^n} *satisfying condition* (2.4) *i.e.,* $\left| \bigcup_{i=1}^{36} M_i \right| = 9 \cdot 4^{n-1} + 32$.

2.1.3 Conjugacy classes of regular (2×2)-matrices over $\mathbb{Z}_{2^n}$ of order 1 or 2

The aim of this subsection is to divide the set of regular (2×2)-matrices over $\mathbb{Z}_{2^n}$ of order 1 or 2 into conjugacy classes. This set was founded in subsection 2.1.2. Denote $A = \begin{Vmatrix} \alpha & \beta \\ \gamma & \delta \end{Vmatrix}$, $B = \begin{Vmatrix} a & b \\ c & d \end{Vmatrix}$ and $g = \begin{Vmatrix} x & y \\ z & w \end{Vmatrix}$.

It is clear that if A and B are conjugate, i.e., $g^{-1}Ag = B$, then $\det A = \det B$ and $\alpha + \delta = a + d$, i.e., $Tr\, A = Tr\, B$.

$TrA = a + d$	set M_i, where belongs matrix A
0	$M_1, M_2, M_7, M_8, M_{13}, M_{14}, M_{27}, M_{28}, M_{29}, M_{30}$
2^{n-1}	$M_{11}, M_{12}, M_{21}, M_{22}, M_{33}, M_{34}, M_{35}, M_{36}$
2	$M_3, M_5, M_{15}, M_{16}, M_{23}, M_{24}$
-2	$M_4, M_6, M_{17}, M_{18}, M_{25}, M_{26}$
$2 + 2^{n-1}$	M_9, M_{19}, M_{31}
$-2 + 2^{n-1}$	M_{10}, M_{20}, M_{32}

Table 2. Traces of matrices

Theorem 2.2 *For every* $n \geqslant 3$, *there is* 17 *conjugacy classes* K_i $(i = 1, 2, ..., 17)$ *of regular* (2×2)*-matrices* A *of order less or equal to* 2 *(over* $\mathbb{Z}_{2^n}$*):*

$$K_1 = M_3, \quad K_2 = M_5, \quad K_3 = M_{15} \cup M_{23}, \quad K_4 = M_{16} \cup M_{24},$$
$$K_5 = M_4, \quad K_6 = M_6, \quad K_7 = M_{17} \cup M_{25}, \quad K_8 = M_{18} \cup M_{26},$$
$$K_9 = M_{31}, \quad K_{10} = M_9 \cup M_{19}, \quad K_{11} = M_{32},$$
$$K_{12} = M_{10} \cup M_{20}, \quad K_{13} = M_{11} \cup M_{21} \cup M_{33} \cup M_{35},$$
$$K_{14} = M_{12} \cup M_{22} \cup M_{34} \cup M_{36}, \quad K_{15} = M_1 \cup M_2,$$
$$K_{16} = M_7 \cup M_{13} \cup M_{27} \cup M_{29}, \quad K_{17} = M_8 \cup M_{14} \cup M_{28} \cup M_{30}$$

and

$$|K_1| = |K_2| = |K_5| = |K_6| = 1, \quad |K_9| = |K_{11}| = 2,$$
$$|K_{13}| = |K_{14}| = |K_{16}| = |K_{17}| = 3 \cdot 2^{2n-3}, \quad |K_{15}| = 3 \cdot 2^{2n-2},$$
$$|K_3| = |K_4| = |K_7| = |K_8| = 3, \quad |K_{10}| = |K_{12}| = 6.$$

Remark. If $n = 3$ then $M_{29} = M_{30} = M_{35} = M_{36} = \emptyset$.

Proof. We have to solve the system $\begin{cases} gBg^{-1} \equiv A \,(\mathrm{mod}\, 2^n) \\ \det g \not\equiv 0 \,(\mathrm{mod}\, 2) \end{cases}$, i.e.,

$$gB \equiv Ag \,(\mathrm{mod}\, 2^n), \;\; \det g \not\equiv 0 \,(\mathrm{mod}\, 2), \tag{2.9}$$

where A, B are given and g is unknown. We choose the representatives A_i of classes K_i (see Appendix C).

I) Let us prove that these representatives are not conjugate to each other. By Table 2, we have to check only 18 conditions modulo 2^n:

$$\begin{array}{llll} gA_{15}g^{-1} \equiv A_{16}, & gA_{15}g^{-1} \equiv A_{17}, & gA_{16}g^{-1} \equiv A_{17}, & gA_{13}g^{-1} \equiv A_{14}, \\ gA_1g^{-1} \equiv A_2, & gA_1g^{-1} \equiv A_3, & gA_1g^{-1} \equiv A_4, & gA_2g^{-1} \equiv A_3, \\ gA_2g^{-1} \equiv A_4, & gA_3g^{-1} \equiv A_4, & gA_5g^{-1} \equiv A_6, & gA_5g^{-1} \equiv A_7, \\ gA_5g^{-1} \equiv A_8, & gA_6g^{-1} \equiv A_7, & gA_6g^{-1} \equiv A_8, & gA_7g^{-1} \equiv A_8, \\ gA_{10}g^{-1} \equiv A_9, & gA_{12}g^{-1} \equiv A_{11}, & & \end{array}$$

where $\det g \not\equiv 0 \,(\mathrm{mod}\, 2)$. It is easy to verify that all these congruences do not have a solution.

II) Let us prove that all other matrices of K_i are conjugate to representative A_i of this class. Note that if a matrix g is a solution of system (2.9) then the matrix

$$\left\| \begin{array}{cc} x + 2^{n-1}x_1 & y + 2^{n-1}y_1 \\ z + 2^{n-1}z_1 & w + 2^{n-1}w_1 \end{array} \right\|,$$

where $x_1, y_1, z_1, w_1 \in \mathbb{Z}_2$, is also a solution of the system (2.9). To prove that two matrices are conjugate we do not need to find all solutions of system (2.9); it is sufficient to give some solutions. Computations in this subsection are elementary. The solutions g for each form of matrices of the sets M_j ($j = 1, 2, ..., 36$) are presented in Appendix A.1 as well argumentations for the classes K_{13}, K_{14}, K_{16} and K_{17}. Theorem 2.2 is proved. □

2.1.4 Non-isomorphic groups $\mathcal{G}_i$

In this subsection we consider the groups $\mathcal{G}_i$ which correspond to the matrices A_i ($i = 1, ..., 17$) (see Appendix C) described in subsection 2.1.3. These groups are:

$$\begin{aligned} \mathcal{G}_1 &= \left\langle a, b, c \mid (*), c^{-1}ac = a, c^{-1}bc = b \right\rangle = (C_{2^n} \times C_{2^n}) \times C_2, \\ \mathcal{G}_2 &= \left\langle a, b, c \mid (*), c^{-1}ac = a^{1+2^{n-1}}, c^{-1}bc = b^{1+2^{n-1}} \right\rangle, \\ \mathcal{G}_3 &= \left\langle a, b, c \mid (*), c^{-1}ac = ab^{2^{n-1}}, c^{-1}bc = b \right\rangle, \\ \mathcal{G}_4 &= \left\langle a, b, c \mid (*), c^{-1}ac = a^{1+2^{n-1}}b^{2^{n-1}}, c^{-1}bc = b^{1+2^{n-1}} \right\rangle, \\ \mathcal{G}_5 &= \left\langle a, b, c \mid (*), c^{-1}ac = a^{-1}, c^{-1}bc = b^{-1} \right\rangle, \end{aligned}$$

$$\mathcal{G}_6 = \left\langle a,b,c \mid (*), c^{-1}ac = a^{-1+2^{n-1}}, c^{-1}bc = b^{-1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_7 = \left\langle a,b,c \mid (*), c^{-1}ac = a^{-1}b^{2^{n-1}}, c^{-1}bc = b^{-1} \right\rangle,$$
$$\mathcal{G}_8 = \left\langle a,b,c \mid (*), c^{-1}ac = a^{-1+2^{n-1}}b^{2^{n-1}}, c^{-1}bc = b^{-1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_9 = \left\langle a,b,c \mid (*), c^{-1}ac = ab^{2^{n-1}}, c^{-1}bc = a^{2^{n-1}}b^{1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_{10} = \left\langle a,b,c \mid (*), c^{-1}ac = a, c^{-1}bc = b^{1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_{11} = \left\langle a,b,c \mid (*), c^{-1}ac = a^{-1}b^{2^{n-1}}, c^{-1}bc = a^{2^{n-1}}b^{-1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_{12} = \left\langle a,b,c \mid (*), c^{-1}ac = a^{-1}, c^{-1}bc = b^{-1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_{13} = \left\langle a,b,c \mid (*), c^{-1}ac = a, c^{-1}bc = b^{-1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_{14} = \left\langle a,b,c \mid (*), c^{-1}ac = a^{-1}, c^{-1}bc = b^{1+2^{n-1}} \right\rangle,$$
$$\mathcal{G}_{15} = \left\langle a,b,c \mid (*), c^{-1}ac = b, c^{-1}bc = a \right\rangle,$$
$$\mathcal{G}_{16} = \left\langle a,b,c \mid (*), c^{-1}ac = a, c^{-1}bc = b^{-1} \right\rangle,$$
$$\mathcal{G}_{17} = \left\langle a,b,c \mid (*), c^{-1}ac = a^{1+2^{n-1}}, c^{-1}bc = b^{-1+2^{n-1}} \right\rangle,$$

where the conditions $a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba$ are denoted by $(*)$.

Let us prove next Theorem.

Theorem 2.3 *There is 17 non-isomorphic groups $\mathcal{G}_i$ $(i = 1, ..., 17)$ which can be presented in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$.*

Proof. To prove Theorem 2.3, we find first the derived subgroups $\mathcal{G}_i'$ and centers $Z(\mathcal{G}_i)$ of the groups $\mathcal{G}_i$. The obtained results are given in the Table 3.

derived subgroup $\mathcal{G}_i'$	center $Z(\mathcal{G}_i)$	group $\mathcal{G}_i$
C_{2^n}	C_{2^n}	$\mathcal{G}_{15}$
$\{1\}$	$C_{2^n} \times C_{2^n} \times C_{2^n}$	$\mathcal{G}_1$
$C_{2^{n-1}} \times C_{2^{n-1}}$	$C_2 \times C_2$	$\mathcal{G}_5, \mathcal{G}_6, \mathcal{G}_7, \mathcal{G}_8, \mathcal{G}_{11}, \mathcal{G}_{12}$
$C_2 \times C_2$	$C_{2^{n-1}} \times C_{2^{n-1}}$	$\mathcal{G}_2, \mathcal{G}_4, \mathcal{G}_9$
$C_{2^{n-1}}$	$C_2 \times C_{2^n}$	$\mathcal{G}_{13}, \mathcal{G}_{16}$
$C_2 \times C_{2^{n-1}}$	$C_{2^{n-1}} \times C_2$	$\mathcal{G}_{14}, \mathcal{G}_{17}$
C_2	$C_{2^n} \times C_{2^{n-1}}$	$\mathcal{G}_3, \mathcal{G}_{10}$

Table 3. Derived subgroups $\mathcal{G}_i'$ and centers $Z(\mathcal{G}_i)$ of groups $\mathcal{G}_i$.

If the derived subgroups $\mathcal{G}_i'$ (or centers $Z(\mathcal{G}_i)$) of two groups are different then these groups are non-isomorphic. Therefore, by Table 3, we have to check the problem of isomorphism **I)** for the groups $\mathcal{G}_5$, $\mathcal{G}_6$, $\mathcal{G}_7$, $\mathcal{G}_8$, $\mathcal{G}_{11}$, $\mathcal{G}_{12}$, **II)** for the groups $\mathcal{G}_2$, $\mathcal{G}_4$, $\mathcal{G}_9$, **III)** for the groups $\mathcal{G}_{13}$, $\mathcal{G}_{16}$, **IV)** for the groups $\mathcal{G}_{14}$, $\mathcal{G}_{17}$ and **V)** for the groups $\mathcal{G}_3$, $\mathcal{G}_{10}$. As follows, we determine the numbers of automorphisms of these groups. Obviously if the

numbers of automorphisms of two groups are different, then these groups are non-isomorphic. For example, we present the computations of the number of automorphisms of the group $\mathcal{G}_8$ (Appendix A.2.1). The numbers of automorphisms of the groups $\mathcal{G}_i$ $(i = 1, 2, ..., 17)$ are:

$$
\begin{array}{lll}
|\operatorname{Aut}(\mathcal{G}_1)| = 3 \cdot 2^{4n-1} & |\operatorname{Aut}(\mathcal{G}_2)| = 3 \cdot 2^{4n-1} & |\operatorname{Aut}(\mathcal{G}_3)| = 2^{4n} \\
|\operatorname{Aut}(\mathcal{G}_4)| = 2^{4n-1} & |\operatorname{Aut}(\mathcal{G}_5)| = 3 \cdot 2^{6n-3} & |\operatorname{Aut}(\mathcal{G}_6)| = 3 \cdot 2^{6n-5} \\
|\operatorname{Aut}(\mathcal{G}_7)| = 2^{6n-4} & |\operatorname{Aut}(\mathcal{G}_8)| = 2^{6n-5} & |\operatorname{Aut}(\mathcal{G}_9)| = 3 \cdot 2^{4n-2} \\
|\operatorname{Aut}(\mathcal{G}_{10})| = 2^{4n-1} & |\operatorname{Aut}(\mathcal{G}_{11})| = 3 \cdot 2^{6n-6} & |\operatorname{Aut}(\mathcal{G}_{12})| = 2^{6n-5} \\
|\operatorname{Aut}(\mathcal{G}_{13})| = 2^{3n} & |\operatorname{Aut}(\mathcal{G}_{14})| = 2^{3n+1} & |\operatorname{Aut}(\mathcal{G}_{15})| = 2^{3n-1} \\
|\operatorname{Aut}(\mathcal{G}_{16})| = 2^{3n+1} & |\operatorname{Aut}(\mathcal{G}_{17})| = 2^{3n} &
\end{array}
$$

Since $|\operatorname{Aut}(\mathcal{G}_8)| = |\operatorname{Aut}(\mathcal{G}_{12})|$, it is still necessary to check whether the groups $\mathcal{G}_8$ and $\mathcal{G}_{12}$ are non-isomorphic.

Let us determine the number of elements of order 2 in the groups $\mathcal{G}_8$ and $\mathcal{G}_{12}$. Consider an element $c^x a^i b^j \neq 1$ of $\mathcal{G}_8$ or $\mathcal{G}_{12}$. If $x = 0$, then in the both groups $1 = \left(a^i b^j\right)^2 = a^{2i} b^{2j}$ and we have $i \equiv j \equiv 0 \left(\operatorname{mod} 2^{n-1}\right)$ and there is 3 possibilities for (i, j) . If $x = 1$, then for $ca^i b^j \in \mathcal{G}_8$ we have

$$1 = \left(ca^i b^j\right)^2 = \left(c^{-1} a^i c\right) \left(c^{-1} b^j c\right) a^i b^j = a^{2^{n-1} i} b^{2^{n-1}(i+j)}$$

and, therefore, $i \equiv j \equiv 0 \,(\operatorname{mod} 2)$ and it is $2^{n-1} \cdot 2^{n-1} = 2^{2n-2}$ possibilities for (i, j) . Hence the number of elements of order 2 in the group $\mathcal{G}_8$ is $3 + 2^{2n-2}$. Similarly, for $ca^i b^j \in \mathcal{G}_{12}$ we have

$$1 = \left(ca^i b^j\right)^2 = \left(c^{-1} a^i c\right) \left(c^{-1} b^j c\right) a^i b^j = b^{2^{n-1} j}$$

and therefore, $j \equiv 0 \,(\operatorname{mod} 2)$, $i \in \mathbb{Z}_{2^n}$ and it is $2^n \cdot 2^{n-1} = 2^{2n-1}$ possibilities for (i, j) . Hence the number of elements of order 2 in group $\mathcal{G}_{12}$ is $3 + 2^{2n-1}$.

Since the numbers of elements of order two in groups $\mathcal{G}_8$ and $\mathcal{G}_{12}$ are different, the groups $\mathcal{G}_8$ and $\mathcal{G}_{12}$ are non-isomorphic. Theorem 2.3 is proved. □

2.2 A characterization of group $\mathcal{G}_{15}$ by its endomorphism semigroup

In this section we shall characterize the group

$$
\begin{aligned}
\mathcal{G}_{15} &= \left\langle a,\, b,\, c \mid a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1} a c = b,\ c^{-1} b c = a \right\rangle = \\
&= \left(\langle a \rangle \times \langle b \rangle\right) \leftthreetimes \langle c \rangle = \left(C_{2^n} \times C_{2^n}\right) \leftthreetimes C_2
\end{aligned}
$$

by its endomorphism semigroup.

Let us find the derived group of $\mathcal{G}_{15}$. The generating relations of $\mathcal{G}_{15}$ imply

$$c^{-t}a^m c^t = a^{\frac{1+(-1)^t}{2}m} b^{\frac{1-(-1)^t}{2}m},\ c^{-t}b^m c^t = a^{\frac{1-(-1)^t}{2}m} b^{\frac{1+(-1)^t}{2}m}.$$

Therefore,

$$\left[c^x a^i b^j, c^y a^k b^l\right] = b^{-j}a^{-i}c^{-x}b^{-l}a^{-k}c^{-y}c^x a^i b^j c^y a^k b^l =$$
$$= b^{-j}a^{-i}\left(c^{-x}b^{-l}c^x\right)\left(c^{-x}a^{-k}c^x\right)\left(c^{-y}a^i c^y\right)\left(c^{-y}b^j c^y\right)a^k b^l =$$
$$= \left(a^{-1}b\right)^{\frac{1-(-1)^y}{2}i - \frac{1-(-1)^y}{2}j - \frac{1-(-1)^x}{2}k + \frac{1-(-1)^x}{2}l},$$

i.e., $\mathcal{G}'_{15} = \left\langle a^{-1}b \right\rangle \cong C_{2^n}$. Denote $d = a^{-1}b$. Then $c^{-1}dc = d^{-1}$, $c^{-1}ac = b = ad$ and replacing the letter d by b, we get

$$\begin{aligned}
\mathcal{G}_{15} &= (\langle a\rangle \times \langle b\rangle) \leftthreetimes \langle c\rangle = (C_{2^n} \times C_{2^n}) \leftthreetimes C_2 = \\
&= \left\langle a,\, b,\, c \mid (*),\ ab = ba,\ c^{-1}ac = ab,\ c^{-1}bc = b^{-1}\right\rangle = \\
&= \left\langle a,\, b,\, c \mid (*),\ c^{-1}bc = b^{-1},\ a^{-1}ba = b,\ a^{-1}ca = cb^{-1}\right\rangle = \\
&= (\langle b\rangle \leftthreetimes \langle c\rangle) \leftthreetimes \langle a\rangle = (C_{2^n} \leftthreetimes C_2) \leftthreetimes C_{2^n},
\end{aligned}$$

where $(*)$ denotes the relations $a^{2^n} = b^{2^n} = c^2 = 1$. Using these notations, the derived group of $\mathcal{G}_{15}$ is $\mathcal{G}'_{15} = \langle b\rangle \cong C_{2^n}$ and

$$\mathcal{G}_{15}/\mathcal{G}'_{15} = \left\langle c\mathcal{G}'_{15}\right\rangle \times \left\langle a\mathcal{G}'_{15}\right\rangle \cong C_2 \times C_{2^n}.$$

The center of this group is $Z(\mathcal{G}_{15}) = \left\langle a^2 b\right\rangle$. Computations of the number of automorphisms of the group $\mathcal{G}_{15}$ are given in Appendix A.2.2.

Theorem 2.4 *A finite group $\mathcal{G}$ is isomorphic to $\mathcal{G}_{15}$ if and only if $|\mathrm{Aut}(\mathcal{G})| = 2^{3n-1}$ and there exist $x, y \in I(\mathcal{G})$ such that the following properties hold:*

1^0 $K(x) \cong \mathrm{End}(C_2)$;
2^0 $y \in J(x)$ *and* $K(y) \cong \mathrm{End}(C_{2^n})$;
3^0 $J(x) \cap J(y) = \{0\}$;
4^0 $|\{z \in \mathrm{End}(\mathcal{G}) \mid xz = z,\ zx = zy = 0\}| = 2$;
5^0 $\left|\left\{u^{n-2}S \mid u \in K(y), u^{n-1} \neq 0, u^n = 0\right\}\right| = 4$,
where $S = \{z \in \mathrm{End}(\mathcal{G}) \mid yz = z,\ zx = zy = 0\}$;
6^0 $|T| = 2^n$, *where* $T = \{z \in I(\mathcal{G}) \mid yz = z,\ zy = y,\ zx = 0\}$;
7^0 $u \in D(x), v \in D(y) \Longrightarrow u^{-1}vu \in D(y)$;
8^0 $|D(x)| = 2^{2n-1}$.

Proof. *Necessity.* Let $\mathcal{G} = \mathcal{G}_{15}$.

Denote by x and y the projections of $\mathcal{G}$ onto its subgroups $\langle c\rangle$ and $\langle a\rangle$, respectively:

$$x:\mathcal{G}\longrightarrow\langle c\rangle;\quad y:\mathcal{G}\longrightarrow\langle a\rangle.$$

Then $\operatorname{Ker}x=\langle a,b\rangle=\langle a\rangle\times\langle b\rangle$, $\operatorname{Ker}y=\langle b,c\rangle$ and $\operatorname{Ker}x\cap\operatorname{Ker}y=\langle b\rangle$. Clearly, $x,\ y\in I(\mathcal{G})$ and $xy=yx=0$, i.e., $y\in J(x)$. We shall prove that x and y satisfy properties 1^0–7^0.

Lemma 4 implies properties 1^0 and 2^0. By Lemma 5, $J(x)\cap J(y)$ consists of $z\in\operatorname{End}(\mathcal{G})$ such that $(\operatorname{Im}x)z=(\operatorname{Im}y)z=\langle 1\rangle$ and $(\operatorname{Ker}\ x)z\subset\operatorname{Ker}x$, $(\operatorname{Ker}\ y)z\subset\operatorname{Ker}y$, i.e.,

$$cz=az=1;\ bz=b^i,\ i\in\mathbb{Z}_{2^n}. \tag{2.10}$$

Map (2.10) preserves the defining relations of $\mathcal{G}$ and is an endomorphism of $\mathcal{G}$ if and only if $i=0$. Hence property 3^0 holds.

Choose $z\in\{z\in\operatorname{End}(\mathcal{G})\mid xz=z,\ zx=zy=0\}$. Then

$$az=a(xz)=(ax)z=1z=1,\quad bz=b(xz)=(bx)z=1z=1,$$
$$(cz)x=c(zx)=c\theta=1,\quad (cz)y=c(zy)=c\theta=1,$$

i.e., $cz\in\operatorname{Ker}x\cap\operatorname{Ker}y=\langle b\rangle$, and

$$z:\qquad c\longmapsto b^i,\ a\longmapsto 1,\ b\longmapsto 1\qquad (i\in\mathbb{Z}_{2^n}).$$

This map preserves the defining relations of $\mathcal{G}$ if and only if $i\in\{0,2^{n-1}\}$. Hence property 4^0 holds.

Choose $z\in S=\{z\in\operatorname{End}(\mathcal{G})\mid yz=z,\ zx=zy=0\}$. Then

$$cz=c(yz)=(cy)z=1z=1,\quad bz=b(yz)=(by)z=1z=1,$$
$$(az)x=a(zx)=a\theta=1,\quad (az)y=a(zy)=a\theta=1,$$

i.e., $az\in\operatorname{Ker}x\cap\operatorname{Ker}y=\langle b\rangle$ and

$$z:\qquad c\longmapsto 1,\ a\longmapsto b^j,\ b\longmapsto 1\qquad (j\in\mathbb{Z}_{2^n}).$$

This map preserves the defining relations of $\mathcal{G}$ and therefore, is an element of S for each $j\in\mathbb{Z}_{2^n}$. By Lemma 4, $K(y)$ consists of the following maps u:

$$u:\qquad c\longmapsto 1,\ a\longmapsto a^l,\ b\longmapsto 1\qquad (l\in\mathbb{Z}_{2^n}).$$

The map $u\in K(y)$ satisfies conditions $u^{n-1}\neq 0$, $u^n=0$ if and only if $l=2i$, $i\in\mathbb{Z}^*_{2^{n-1}}$. In this case

$$u^{n-2}:\qquad c\longmapsto 1,\ a\longmapsto a^{2^{n-2}i^{n-2}},\ b\longmapsto 1\qquad \left(i\in\mathbb{Z}^*_{2^{n-1}}\right)$$

and

$$u^{n-2}z:\qquad c\longmapsto 1,\ a\longmapsto b^{2^{n-2}i^{n-2}j},\ b\longmapsto 1\qquad \left(i\in\mathbb{Z}^*_{2^{n-1}},\ j\in\mathbb{Z}_{2^n}\right),$$

where $z \in S$ is given above. Since $2^{n-2}i^{n-2}j \in \left\{0;\, 2^{n-2};\, 2^{n-1};\, 3\cdot 2^{n-2}\right\}$, property 5^0 holds.

Denote $T = \{z \in I(\mathcal{G}) \mid yz = z,\ zy = y,\ zx = 0\}$ and choose $z \in T$. Then

$$cz = c(yz) = (cy)z = 1,\ bz = b(yz) = (by)z = 1,\ az \in \operatorname{Ker}\ x,$$

i.e., $az = a^j b^i$, where $i,\, j \in \mathbb{Z}_{2^n}$. By condition $y = zy$,

$$a = ay = a(zy) = (az)y = \left(a^j b^i\right) y = a^j,$$

i.e., $j = 1$ and

$$z: \quad c \longmapsto 1,\ b \longmapsto 1,\ a \longmapsto ab^i \qquad (i \in \mathbb{Z}_{2^n}).$$

This map preserves the defining relations of $\mathcal{G}$ and is an element of T for each $i \in \mathbb{Z}_{2^n}$. Hence $|T| = 2^n$. Property 6^0 is proved.

In order to prove properties 7^0 and 8^0 we find the set

$$D(x) = \{u \in \operatorname{Aut}(\mathcal{G}_{15}) \mid ux = xu = x\}.$$

By Lemma 7, $D(x)$ consists of automorphisms u of $\mathcal{G}_{15}$ such that $cu = c$ and $bu,\, au \in \operatorname{Ker}\ x$, i.e., $cu = c$, $au = a^i b^j$, $bu = a^k b^l$ for some $i,\, j,\, k,\, l \in \mathbb{Z}_{2^n}$. Therefore, by appendix A.2.2, $D(x)$ consists of maps

$$u:\ cu = c,\ au = a^i b^j,\ bu = b^l, \tag{2.11}$$

where

$$l = i - 2j,\ j \in \mathbb{Z}_{2^n},\ i \in \mathbb{Z}_{2^n}^*, \tag{2.12}$$

what means that $|D(x)| = 2^n \cdot 2^{n-1} = 2^{2n-1}$. Property 8^0 is proved. We need below the inverse u^{-1} of $u \in D(x)$:

$$u^{-1}:\ cu^{-1} = c,\ au^{-1} = a^{i^{-1}} b^{-jl^{-1}i^{-1}},\ bu^{-1} = b^{l^{-1}}. \tag{2.13}$$

Similarly,

$$D(y) = \{v \in \operatorname{Aut}(\mathcal{G}_{15}) \mid cv = cb^q, av = a, bv = b,\ q \in \mathbb{Z}_{2^n}\}. \tag{2.14}$$

Choose $u \in D(x)$, $v \in D(y)$ and compute $u^{-1}vu$. Using (2.11)–(2.14), we obtain

$$\begin{aligned}
c\left(u^{-1}vu\right) &= \left(cu^{-1}\right)(vu) = (cv)u = \left(cb^q\right)u = cb^{lq},\\
a\left(u^{-1}vu\right) &= \left(au^{-1}\right)(vu) = \left(a^{i^{-1}} b^{-jl^{-1}i^{-1}}\right) vu =\\
&= \left((av)^{i^{-1}} (bv)^{-jl^{-1}i^{-1}}\right) u = \left(a^{i^{-1}} b^{-jl^{-1}i^{-1}}\right) u =\\
&= (au)^{i^{-1}} (bu)^{-jl^{-1}i^{-1}} = \left(a^i b^j\right)^{i^{-1}} \left(b^l\right)^{-jl^{-1}i^{-1}} = a,\\
b\left(u^{-1}vu\right) &= \left(bu^{-1}\right)(vu) = \left(b^{l^{-1}}\right) vu = \left(b^{l^{-1}}\right) u = b^{l^{-1}l} = b.
\end{aligned}$$

Hence $u^{-1}vu \in D(y)$ and property 7^0 is proved.

Sufficiency. Let $\mathcal{G}$ be a finite group such that $|\mathrm{Aut}(\mathcal{G})| = 2^{3n-1}$ and there exist $x, y \in I(\mathcal{G})$ satisfying properties 1^0–8^0. We have to prove that $\mathcal{G} \cong \mathcal{G}_{15}$.

By Lemmas 1 and 4,

$$\begin{aligned} \mathcal{G} &= \mathrm{Ker}\, x \leftthreetimes \mathrm{Im}\, x,\ K(x) \cong \mathrm{End}(\mathrm{Im}\, x) \overset{1^0}{\cong} \mathrm{End}(C_2), \\ \mathcal{G} &= \mathrm{Ker}\, y \leftthreetimes \mathrm{Im}\, y,\ K(y) \cong \mathrm{End}(\mathrm{Im}\, y) \overset{2^0}{\cong} \mathrm{End}(C_{2^n}). \end{aligned}$$

Since each finite Abelian group is determined by its endomorphism semigroup in the class of all groups (Lemma 10), we have $\mathrm{Im}\, x \cong \langle c \rangle$ and $\mathrm{Im}\, y \cong \langle a \rangle$ for some $c, a \in \mathcal{G}$, $o(c) = 2$, $o(a) = 2^n$, i.e., $c^2 = 1$, $a^{2^n} = 1$. In view of Lemmas 1 and 9,

$$\mathcal{G} = (M \leftthreetimes \langle c \rangle) \leftthreetimes \langle a \rangle = (M \leftthreetimes \langle a \rangle) \leftthreetimes \langle c \rangle,$$

where

$$\begin{gathered} M = \mathrm{Ker}\, x \cap \mathrm{Ker}\, y,\ \ \mathrm{Im}\, x = \langle c \rangle,\ \ \mathrm{Im}\, y = \langle a \rangle, \\ \mathrm{Ker}\, x = M \leftthreetimes \langle a \rangle,\ \ \mathrm{Ker}\, y = M \leftthreetimes \langle c \rangle. \end{gathered}$$

Therefore, $\mathcal{G}/M = \langle aM \rangle \times \langle cM \rangle$ and $\mathcal{G}' \subset M$.

As $\mathrm{Aut}(\mathcal{G})$ is a 2-group, so the group of inner automorphism $\widehat{\mathcal{G}} \cong \mathcal{G}/Z(\mathcal{G})$ is also a 2-group. Hence all $2'$-elements of $\mathcal{G}$ belong to its center $Z(\mathcal{G})$. Therefore, the group $\mathcal{G}$ splits into the direct product $\mathcal{G} = \mathcal{G}_{2'} \times \mathcal{G}_2$ of its Hall $2'$-subgroup $\mathcal{G}_{2'}$ and Sylow 2-subgroup $\mathcal{G}_2$. Denote by z the projection of $\mathcal{G}$ onto its subgroup $\mathcal{G}_{2'}$. Then $z \in J(x) \cap J(y) \overset{3^0}{=} \{0\}$ and $z = 0$. Hence $\mathcal{G}$ is 2-group.

Choose $z \in \mathrm{End}(\mathcal{G})$ such that $xz = z$, $zx = zy = 0$. Then $(cz)^2 = 1$, $(\mathrm{Ker}\, x)\, z = (\mathrm{Ker}\, x)\, xz = \langle 1 \rangle\, z = \langle 1 \rangle$, $(\mathrm{Im}\, x)\, z = \langle c \rangle\, z = \langle cz \rangle \subset \mathrm{Ker}\, x \cap \mathrm{Ker}\, y = M$. Conversely, if $d \in M$ such that $d^2 = 1$, we can define $z \in \mathrm{End}(\mathcal{G})$ by setting

$$(\mathrm{Ker}\, x)\, z = \langle 1 \rangle,\ (\mathrm{Im}\, x)\, z = \langle d \rangle = \langle cz \rangle,\ \text{where } cz = d.$$

This endomorphism satisfies equalities $xz = z$, $zx = zy = 0$. Property 4^0 implies that the subgroup M of $\mathcal{G}$ has only one element of order 2. Therefore, M is cyclic or a generalized quaternion group ([38], Theorem 5.46). By property 5^0, M has 4 elements d such that $d^4 = 1$. Since the number of elements d, $d^4 = 1$, is greater than 4 in each generalized quaternion group, the subgroup M is cyclic of order 2^k, $k \geqslant 2$ and

$$M = \langle b \rangle \cong C_{2^k}, \quad k \geqslant 2$$

for some $b \in M$.

Assume that $M \neq \mathcal{G}'$. Then

$$\mathcal{G}/\mathcal{G}' = \left\langle a\mathcal{G}' \right\rangle \times \left\langle b\mathcal{G}' \right\rangle \times \left\langle c\mathcal{G}' \right\rangle, \quad \left\langle b\mathcal{G}' \right\rangle \ncong \langle 1 \rangle$$

and we can find a non-zero element $z \in J(x) \cap J(y)$:

$$\left(\mathcal{G}'\right) z = \langle 1 \rangle, \ az = cz = 1, \ bz = b^{2^{k-1}}.$$

This contradicts property 3^0. Therefore,

$$\mathcal{G}' = M = \langle b \rangle \cong C_{2^k} \quad (k \geqslant 2), \quad \mathcal{G}/\mathcal{G}' = \left\langle a\mathcal{G}' \right\rangle \times \left\langle c\mathcal{G}' \right\rangle. \tag{2.15}$$

In view of (2.15),

$$c^{-1}bc = b^t, \ a^{-1}ba = b^s$$

for some s, $t \equiv 1 \pmod 2$. Hence

$$\begin{aligned} b^{-1}c^{-1}bc &= [b, c] = b^{t-1} \in \left\langle b^2 \right\rangle, \\ b^{-1}a^{-1}ba &= [b, a] = b^{s-1} \in \left\langle b^2 \right\rangle. \end{aligned}$$

Since $\mathcal{G}' = \langle b \rangle$,

$$[a, c] = a^{-1}c^{-1}ac = b^i.$$

Here $i \equiv 1 \pmod 2$, because otherwise $[a, c] \in \left\langle b^2 \right\rangle$ and $\mathcal{G}' \subset \left\langle b^2 \right\rangle$ which is impossible. As $\left\langle b^i \right\rangle = \langle b \rangle$, we can assume that $i = 1$, i.e.,

$$c^{-1}ac = ab.$$

To find the value of t, we calculate

$$\begin{aligned} a &= c^{-2}ac^2 = c^{-1}\left(c^{-1}ac\right)c = c^{-1}abc = \\ &= \left(c^{-1}ac\right)\left(c^{-1}bc\right) = abb^t = ab^{t+1}. \end{aligned}$$

Hence $t = -1$ and

$$c^{-1}bc = b^{-1}.$$

Next we show that $k = n$. For this purpose, let us find $(ab^m)^{2^l}$ for each $1 \leqslant l \leqslant n$:

$$(ab^m)^2 = (ab^m)(ab^m) = a^2\left(a^{-1}b^m a\right)b^m = a^2 b^{m(s+1)},$$

$$(ab^m)^{2^2} = a^4\left(a^{-2}b^{m(s+1)}a^2\right)b^{m(s+1)} = a^4 b^{m\left(s^2+1\right)(s+1)},$$

and, using induction by l,

$$(ab^m)^{2^l} = a^{2^l} b^{m\left(s^{2^{l-1}}+1\right)\cdot\ldots\cdot\left(s^4+1\right)\left(s^2+1\right)(s+1)}. \tag{2.16}$$

The element a is an element of order 2^n. Therefore, ab $(= c^{-1}ac)$ is also an element of order 2^n and, by (2.16),

$$1 = (ab)^{2^n} = b^{\left(s^{2^{n-1}}+1\right)\cdot\ldots\cdot\left(s^4+1\right)\left(s^2+1\right)(s+1)}. \tag{2.17}$$

Equalities (2.16) and (2.17) imply

$$\begin{aligned}(ab^m)^{2^n} &= a^{2^n}b^{m\left(s^{2^{n-1}}+1\right)\cdot\ldots\cdot\left(s^4+1\right)\left(s^2+1\right)(s+1)} = \\ &= \left(b^{\left(s^{2^{n-1}}+1\right)\cdot\ldots\cdot\left(s^4+1\right)\left(s^2+1\right)(s+1)}\right)^m = 1\end{aligned}$$

for each $m \in \mathbb{Z}_{2^k}$, i.e., ab^m is also an element of order 2^n. This implies that the group $\mathcal{G}$ splits into the semidirect product

$$\mathcal{G} = \langle b, c\rangle \leftthreetimes \langle ab^m\rangle$$

for each $m \in \mathbb{Z}_{2^k}$. Denote by z_m the projection of $\mathcal{G}$ onto its subgroup $\langle ab^m\rangle \cong C_{2^n}$. Then $z_m \in I(\mathcal{G})$, $yz_m = z_m$, $z_m y = y$, $z_m x = \theta$, i.e., $z_m \in T$. On the other hand, assume that $z \in T$. Then $yz = z,\ zy = y,\ zx = 0$, and, therefore,

$$\text{Ker } z = \text{Ker } y = \langle b,\, c\rangle,\ \text{Im } z = \langle az\rangle \cong \text{Im } y \cong C_{2^n},$$

$$\text{Im } z \subset \text{Ker } x = \langle a,\, b\rangle.$$

It follows that $az = a^i b^j$ for some i, j, and $a = ay = a(zy) = (a^i b^j)y = a^i$, i.e., Im $z = \langle ab^j\rangle$. Hence $z = z_j$. Consequently, $T = \{z_m \mid m \in \mathbb{Z}_{2^k}\}$. Property 6^0 implies that $k = n$.

We have already proved that $\mathcal{G}' = \langle b\rangle \cong C_{2^n}$, $o(c) = 2$, $o(a) = o(b) = 2^n$ and

$$c^{-1}ac = ab,\ c^{-1}bc = b^{-1},\ a^{-1}ba = b^s$$

for some $s \in \mathbb{Z}_{2^n}^*$. Our aim is to prove that $s = 1$. In this case, $\mathcal{G} \cong \mathcal{G}_{15}$. Since $\mathcal{G}$ depends on the parameter s, we denote $\mathcal{G} = \mathcal{G}(s)$, i.e.,

$$\mathcal{G} = \mathcal{G}(s) = \left\langle a, b, c \mid (*),\ a^{-1}ba = b^s,\ c^{-1}bc = b^{-1},\ c^{-1}ac = ab\right\rangle,$$

where $(*)$ denotes the relations $a^{2^n} = b^{2^n} = c^2 = 1$. Note, that $\mathcal{G}(1) = \mathcal{G}_{15}$. The following equalities hold in the group $\mathcal{G}(s)$:

$$c^t = c^{-t},\quad c^{-1}b^r c = b^{-r},\quad b^r a^t = a^t b^{s^t r},\quad c^{-1}a^r c = a^r b^{1+s+\ldots+s^{r-1}}.$$

Next we shall find $D(x) = \{z \in \text{Aut}(\mathcal{G}(s)) \mid zx = xz = x\}$. By Lemma 7, $D(x)$ consists of maps $z \in \text{Aut}(\mathcal{G}(s))$ which are given on the generators as follows:

$$cz = c,\ az = a^i b^j,\ bz = a^k b^l \quad (i,\, j,\, k,\, l \in \mathbb{Z}_{2^n}).$$

The map z, given by last equalities, is an automorphism if and only if it preserves the defining relations of $\mathcal{G}(s)$ and is bijective.

The map z preserves the relation $c^{-1}ac = ab$ if and only if

$$\begin{aligned}(cz)^{-1}(az)(cz) &= \left(c^{-1}a^ic\right)\left(c^{-1}b^jc\right) = a^ib^{\left(1+s+...+s^{i-1}\right)-j} = \\ &= (az)(bz) = a^i\left(b^ja^k\right)b^l = a^{i+k}b^{s^kj+l},\end{aligned}$$

i.e.,

$$k = 0,\ l = -\left(1+s+...s^{i-1}\right) + 2j.$$

Since z preserves orders of elements and is invertible, it follows that

$$i \equiv l \equiv 1 \pmod 2.$$

By the last conditions, z preserves the relation $c^{-1}bc = b^{-1}$ trivially. The map z preserves the relation $a^{-1}ba = b^s$ if and only if

$$(az)^{-1}(bz)(az) = b^{-j}\left(a^{-i}b^la^i\right)b^j = b^{s^il} = (bz)^s = b^{ls},$$

i.e., $\left(s^i - s\right)l \equiv 0 \pmod{2^n}$ and hence

$$s^{i-1} \equiv 1 \pmod{2^n}.$$

Consequently, if $z \in D(x)$, then the parameters by which z is given, satisfy the following conditions:

$$k = 0,\ j \in \mathbb{Z}_{2^n},\ i \in \mathbb{Z}_{2^n}^*,\ s^{i-1} \equiv 1 \pmod{2^n},\ l = -\left(1+s+...s^{i-1}\right) + 2j. \tag{2.18}$$

The maximal possible number of values of parameters i, j, k, l, satisfying (2.18), is $2^n \cdot 2^{n-1} = 2^{2n-1}$. Therefore, $|D(x)| \leq 2^{2n-1}$. By property 8^0, $|D(x)| = 2^{2n-1}$, and hence the condition $s^{i-1} \equiv 1 \pmod{2^n}$ has to hold for every $i \in \mathbb{Z}_{2^n}^*$. It follows from here (take $i = 3$) that $s^2 \equiv 1 \pmod{2^n}$, i.e.,

$$s \in \left\{\pm 1,\ \pm 1 + 2^{n-1}\right\}.$$

The numbers of automorphisms of the groups $\mathcal{G}(-1)$, $\mathcal{G}\left(-1+2^{n-1}\right)$ and $\mathcal{G}\left(1+2^{n-1}\right)$ are calculated in Appendix A.2.3 and they are

$$\left|\mathrm{Aut}\left(\mathcal{G}(-1)\right)\right| = \left|\mathrm{Aut}\left(\mathcal{G}\left(-1+2^{n-1}\right)\right)\right| = 2^{3n},$$

$$\left|\mathrm{Aut}\left(\mathcal{G}\left(1+2^{n-1}\right)\right)\right| = 2^{3n-1} = \left|\mathrm{Aut}\left(\mathcal{G}(1)\right)\right|.$$

By assumptions of the theorem, $|\mathrm{Aut}(\mathcal{G})| = |\mathrm{Aut}(\mathcal{G}(s))| = 2^{3n-1}$. Hence $s = 1$ or $s = 1 + 2^{n-1}$. To eliminate the case $s = 1 + 2^{n-1}$, we use property 7^0.

Assume that $s = 1 + 2^{n-1}$ and consider property 7^0. By (2.18), the set $D(x)$ consists of automorphisms u of $\mathcal{G}\left(1 + 2^{n-1}\right)$ such that

$$cu = c, \;\; au = a^i b^j, \;\; bu = b^l$$

and

$$i \in \mathbb{Z}_{2^n}^*, \; j \in \mathbb{Z}_{2^n}, \;\; l \equiv -\left(i + 2^{n-2}(i-1)\right) + 2j \pmod{2^n}.$$

The inverse u^{-1} of this u is

$$cu^{-1} = c, \;\; au^{-1} = a^{i^{-1}} b^{-ji^{-1}l^{-1}}, \;\; bu^{-1} = b^{l^{-1}}.$$

Similarly to $D(x)$, we can find the subset $D(y)$ of $\mathrm{Aut}\left(\mathcal{G}(1 + 2^{n-1})\right)$. We obtain that $D(y)$ consists of maps v such that

$$cv = cb^w, \;\; av = a, \;\; bv = b^t$$

and

$$w \in \mathbb{Z}_{2^n}, \;\; t = 1 + 2^{n-1}w.$$

Let us compute $u^{-1}vu$ for these u and v. Since

$$\left(a^i b^j\right)^{i^{-1}} = ab^{i^{-1}j + 2^{n-2}\left(i^{-1}-1\right)j},$$

we have

$$\begin{aligned}
c\left(u^{-1}vu\right) &= \left(cu^{-1}\right)(vu) = (cv)\,u = \left(cb^w\right)u = cb^{lw}, \\
b\left(u^{-1}vu\right) &= \left(bu^{-1}\right)(vu) = \left(b^{l^{-1}}\right)vu = \left(b^{tl^{-1}}\right)u = b^{tl^{-1}l} = b^t, \\
a\left(u^{-1}vu\right) &= \left(au^{-1}\right)(vu) = \left(a^{i^{-1}} b^{-ji^{-1}l^{-1}}\right)vu = \\
&= \left((av)^{i^{-1}}(bv)^{-ji^{-1}l^{-1}}\right)u = \left(a^{i^{-1}} b^{-ji^{-1}l^{-1}t}\right)u = \\
&= (au)^{i^{-1}}(bu)^{-ji^{-1}l^{-1}t} = \left(a^i b^j\right)^{i^{-1}} b^{-ji^{-1}l^{-1}tl} = \\
&= ab^{i^{-1}j + 2^{n-2}\left(i^{-1}-1\right)j - ji^{-1}t} = ab^{i^{-1}j(1-t) + 2^{n-2}\left(i^{-1}-1\right)j} = \\
&= ab^{i^{-1}j2^{n-1}w + 2^{n-2}\left(i^{-1}-1\right)j} = ab^{2^{n-2}j\left[i^{-1}(2w+1)-1\right]}.
\end{aligned}$$

Therefore, choosing i, $j \in \mathbb{Z}_{2^n}^*$ so that $i \not\equiv 2w + 1 \pmod 4$ (it is possible to choose), we get $i^{-1}(2w+1) - 1 \not\equiv 0 \pmod 4$, $ab^{2^{n-2}j\left[i^{-1}(2w+1)-1\right]} \neq a$ and $u^{-1}vu \notin D(y)$. This contradicts property 7^0., i.e., the case $s = 1 + 2^{n-1}$ is impossible and, consequently, $s = 1$. This imlplies that $\mathcal{G} \cong \mathcal{G}_{15}$. The sufficiency is proved and so is Theorem 2.4. $\square$

Theorem 2.5 *The group $\mathcal{G}_{15}$ is determined by its endomorphism semigroup in the class of all groups.*

The proof of Theorem 2.5 is similar to the proof of Theorem 1.2.

3 The groups presentable in the form $\left(C_{2^n} \times C_{2^n}\right) \leftthreetimes C_4$

The results presented in this chapter (except section 3.5) have been published in [42].

3.1 Introduction

In this chapter we shall find all groups of order $2^{2(n+1)}$ $(n \geqslant 3)$ which can be presented in the form $\mathcal{G} = (C_{2^n} \times C_{2^n}) \leftthreetimes C_4$, i.e.,

$$\mathcal{G} = \left\langle a,\, b,\, c \mid a^{2^n} = b^{2^n} = c^4 = 1,\ ab = ba,\ c^{-1}ac = a^p b^q,\ c^{-1}bc = a^r b^s \right\rangle,$$

where $p,\, q,\, r,\, s \in \mathbb{Z}_{2^n}$. We shall describe all possible values of parameters $p,\, q,\, r,\, s$.The question when different quadruples of parameters imply isomorphic groups of this kind is not considered in this Theses.

An element c induces an inner automorphism $\widehat{c}$ such that $\widehat{c}^{\,4} = 1$:

$$a\widehat{c} = c^{-1}ac = a^p b^q, \qquad b\widehat{c} = c^{-1}bc = a^r b^s.$$

Consequently, we have to find all automorphisms φ of the group $C_{2^n} \times C_{2^n} = \langle a \rangle \times \langle b \rangle$ such that $\varphi^4 = 1$.

A map

$$\varphi : C_{2^n} \times C_{2^n} \longrightarrow C_{2^n} \times C_{2^n}, \quad a\varphi = a^p b^q, \quad b\varphi = a^r b^s \tag{3.1}$$

satisfies the defining relations of the group

$$C_{2^n} \times C_{2^n} = \left\langle a,\, b \mid a^{2^n} = b^{2^n} = 1,\ ab = ba \right\rangle$$

for every $p,\, q,\, r,\, s \in \mathbb{Z}_{2^n}$, and, therefore, is an endomorphism of this group:

$$\begin{aligned}
1 &= 1\varphi = \left(a^{2^n}\right)\varphi = (a\varphi)^{2^n} = (a^p b^q)^{2^n} = 1, \\
1 &= 1\varphi = \left(b^{2^n}\right)\varphi = (b\varphi)^{2^n} = (a^r b^s)^{2^n} = a^{2^n r} b^{2^n s} = a^{2^n r}, \\
(ab)\,\varphi &= a\varphi \cdot b\varphi = (a^p b^q)\,(a^r b^s) = a^{p+r} b^{q+s} = \\
&= a^{r+p} b^{s+q} = (a^r b^s)\,(a^p b^q) = b\varphi \cdot a\varphi = (ba)\,\varphi.
\end{aligned}$$

An endomorphism (3.1) is an automorphism of $C_{2^n} \times C_{2^n}$ if and only if

$$ps - rq \equiv 1 \pmod 2, \tag{3.2}$$

i.e., if and only if matrix $\{\{p,\,q\},\,\{r,\,s\}\}$ is invertible. Now let us decide under which conditions $\varphi^4 = 1$:

$$\begin{aligned} a &= (a)\,\varphi^4 = \left(a\varphi^2\right)\varphi^2 = \left(a^{p^2+rq}b^{q(p+s)}\right)\varphi^2 = \\ &= \left(a^{p^2+rq}b^{q(p+s)}\right)^{p^2+rq}\left(a^{r(p+s)}b^{qr+s^2}\right)^{q(p+s)} = \\ &= a^{\left(p^2+rq\right)^2+qr(p+s)^2}b^{q(p+s)\left(p^2+2qr+s^2\right)}, \\ b &= (b)\,\varphi^4 = \left(b\varphi^2\right)\varphi^2 = \left(a^{r(p+s)}b^{qr+s^2}\right)\varphi^2 = \\ &= \left(a^{p^2+rq}b^{q(p+s)}\right)^{r(p+s)}\left(a^{r(p+s)}b^{qr+s^2}\right)^{qr+s^2} = \\ &= a^{r(p+s)\left(p^2+2qr+s^2\right)}b^{\left(s^2+rq\right)^2+qr(p+s)^2}, \end{aligned}$$

i.e., φ is an automorphism satisfying $\varphi^4 = 1$ if and only if the matrix $\{\{p,\,q\},\,\{r,\,s\}\}$ satisfies condition (3.2) and the next system modulo 2^n

$$\begin{cases} \left(p^2+rq\right)^2 + qr\,(p+s)^2 \equiv 1, & q\,(p+s)\left(p^2+2qr+s^2\right) \equiv 0, \\ r\,(p+s)\left(p^2+2qr+s^2\right) \equiv 0, & \left(s^2+rq\right)^2 + qr\,(p+s)^2 \equiv 1. \end{cases} \tag{3.3}$$

3.2 Simplification of system (3.3)

System (3.3) is equivalent to the system

$$\begin{cases} \left(p^2+rq\right)^2 \equiv 1 - qr\,(p+s)^2 \\ q\,(p+s)\left(p^2+2qr+s^2\right) \equiv 0 \\ r\,(p+s)\left(p^2+2qr+s^2\right) \equiv 0 \\ (p-s)\,(p+s)\left(p^2+2qr+s^2\right) \equiv 0 \end{cases}. \tag{3.4}$$

Let us consider condition (3.2), i.e., condition $ps - rq \equiv 1 \pmod 2$. It is clear that the matrix $\{\{p,\,q\},\,\{r,\,s\}\}$ is congruent modulo 2 to one among of the next six matrices:

1) $\{\{1,\,1\},\,\{1,\,0\}\}$, 2) $\{\{0,\,1\},\,\{1,\,1\}\}$, 3) $\{\{0,\,1\},\,\{1,\,0\}\}$,
3) $\{\{1,\,1\},\,\{0,\,1\}\}$, 5) $\{\{1,\,0\},\,\{1,\,1\}\}$, 6) $\{\{1,\,0\},\,\{0,\,1\}\}$.

Consider two first cases, i.e., p and s are different modulo 2. Then the numbers $(p-s)\,(p+s) = p^2 - s^2$ and $p^2 + s^2$ are odd and the fourth congruence of (3.4) imply $p^2 + s^2 \equiv -2qr \pmod{2^n}$ which is impossible. Therefore, only the following four cases are possible:

$$\{\{0,\,1\},\,\{1,\,0\}\},\quad \{\{1,\,1\},\,\{0,\,1\}\},\quad \{\{1,\,0\},\,\{1,\,1\}\},\quad \{\{1,\,0\},\,\{0,\,1\}\}.$$

Let us consider now the expression $p^2 + 2qr + s^2$. If p and s are both even then q and r are both odd and $2 \mid p^2 + 2qr + s^2$, but $4 \nmid p^2 + 2qr + s^2$.

If p and s are both odd ($p = 2k+1$, $s = 2l+1$, where $k, l \in \mathbb{Z}$) then at least one of the numbers q or r is even ($2qr = 4m$, where $m \in \mathbb{Z}$) and

$$p^2 + 2qr + s^2 = (2k+1)^2 + 4m + (2l+1)^2 = 2 + 4\left(k^2 + l^2 + k + l + m\right),$$

i.e., $2 \mid p^2 + 2qr + s^2$, but $4 \nmid p^2 + 2qr + s^2$. Hence from the system (3.4) follows the system

$$\begin{cases} \left(p^2 + rq\right)^2 \equiv 1 - qr\,(p+s)^2 \pmod{2^n} \\ \begin{cases} q\,(p+s) \equiv 0 \\ r\,(p+s) \equiv 0 \\ (p-s)\,(p+s) \equiv 0 \end{cases} \left(\mathrm{mod} 2^{n-1}\right). \end{cases}$$

Since $q\,(p+s) \equiv 0$, $r\,(p+s) \equiv 0$ modulo 2^{n-1}, we have $qr\,(p+s)^2 \equiv 0 \,(\mathrm{mod}\ 2^n)$ and system (3.4) get the form

$$\begin{cases} \left(p^2 + rq\right)^2 \equiv 1 \pmod{2^n} \\ q\,(p+s) \equiv 0, \quad r\,(p+s) \equiv 0, \quad (p-s)\,(p+s) \equiv 0 \pmod{2^{n-1}}. \end{cases} \tag{3.5}$$

3.3 Automorphisms of order 4

Since all automorphisms of order 1 or 2 of the group $C_{2^n} \times C_{2^n}$ were found in subsection 2.1.2, we need now to find only its automorphisms of order four. In this section we prove

Theorem 3.1 *There are*

$$464 \text{ if } n = 3,$$
$$39 \cdot 4^{n-1} + 15 \cdot 2^5 \text{ if } n \geqslant 4$$

automorphisms of order 4 of group $C_{2^n} \times C_{2^n}$, and all these automorphisms are described in Propositions 3.1, 3.2, 3.3, 3.4, 3.5 and 3.6.

3.3.1 Case $n \geqslant 3$

Assume that $\{\{p, q\}, \{r, s\}\} \equiv \{\{0, 1\}, \{1, 0\}\} \,(\mathrm{mod}\ 2)$.

Proposition 3.1 *Let p, s be even. Then automorphisms of order four of the group $C_{2^n} \times C_{2^n}$ are given by matrices*

$$\begin{array}{lll} 1) & \{\{p, q\}, \{r, s\}\} & \equiv \left\{\{p, q\}, \left\{\left(1 - p^2\right) q^{-1}, -p + 2^{n-1}\right\}\right\}, \\ 2) & \{\{p, q\}, \{r, s\}\} & \equiv \left\{\{p, q\}, \left\{\left(a - p^2\right) q^{-1}, -p + 2^{n-1}k\right\}\right\}, \end{array}$$

where $q \in \mathbb{Z}_{2^n}^*$, $a \in \left\{\pm 1 + 2^{n-1}, -1\right\}$ and $k \in \mathbb{Z}_2$. The number of automorphisms 1) – 2) is $7 \cdot 2^{2n-2}$.

Proof. In this case by (3.5) $p+s \equiv 0 \pmod{2^{n-1}}$, i.e., $s = -p+2^{n-1}k$ and $p = 2u$, where $u \in \mathbb{Z}_{2^{n-1}}$ and $k \in \mathbb{Z}_2$. The first congruence of (3.5) implies

$$\begin{aligned} p^2 + rq &\in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}, \\ rq &\in \left\{\pm 1 - p^2, \pm 1 + 2^{n-1} - p^2\right\}, \\ r &\in \left\{\left(\pm 1 - p^2\right) q^{-1}, \left(\pm 1 + 2^{n-1} - p^2\right) q^{-1}\right\}. \end{aligned}$$

If $r = \left(1 - p^2\right) q^{-1}$ and $k = 0$ then automorphisms $\{\{p, q\}, \{r, s\}\}$ have order ≤ 2 (see Proposition 2.1). The first statement of the proposition is proved.

Let us find the number of automorphisms in forms 1)–2). There are 2^{n-1} possibilities for choosing odd number q and 2^{n-1} possibilities for choosing even number p. The number of choices of s depends on k, which have 2 possibilities in all cases 2) and 1 possibility in the case 1). In the case 2) we have also 3 possibilities for choice of number a. Thus the number of automorphisms in forms 1)–2) is $2^{n-1} \cdot 2^{n-1} \cdot (3 \cdot 2 + 1) = 7 \cdot 2^{2n-2}$. Proposition 3.1 is proved. □

Let us now consider next two cases:

$$\begin{aligned} \{\{p, q\}, \{r, s\}\} &\equiv \{\{1, 1\}, \{0, 1\}\} \pmod 2, \\ \{\{p, q\}, \{r, s\}\} &\equiv \{\{1, 0\}, \{1, 1\}\} \pmod 2. \end{aligned}$$

Proposition 3.2 *Let p, s and one of the numbers q, r be odd. Then the automorphisms of order four of the group $C_{2^n} \times C_{2^n}$ are given by matrices*

$$\begin{aligned} &1)\ \{\{p, q\}, \{r, s\}\} \equiv \left\{\{p, q\}, \left\{\left(1 - p^2\right) q^{-1}, -p + 2^{n-1}\right\}\right\}\ (q \in \mathbb{Z}_{2^n}^*), \\ &2)\ \{\{p, q\}, \{r, s\}\} \equiv \left\{\{p, q\}, \left\{\left(a - p^2\right) q^{-1}, -p + 2^{n-1}k\right\}\right\}\ (q \in \mathbb{Z}_{2^n}^*), \\ &3)\ \{\{p, q\}, \{r, s\}\} \equiv \left\{\left\{p, \left(1 - p^2\right) r^{-1}\right\}, \left\{r, -p + 2^{n-1}\right\}\right\}\ (r \in \mathbb{Z}_{2^n}^*), \\ &4)\ \{\{p, q\}, \{r, s\}\} \equiv \left\{\left\{p, \left(a - p^2\right) r^{-1}\right\}, \left\{r, -p + 2^{n-1}k\right\}\right\}\ (r \in \mathbb{Z}_{2^n}^*), \end{aligned}$$

where $p \in \mathbb{Z}_{2^n}^*$, $a \in \left\{\pm 1 + 2^{n-1}, -1\right\}$ and $k \in \mathbb{Z}_2$. The number of automorphisms 1) – 4) is $7 \cdot 2^{2n-1}$.

Proof. While by (3.5) $q(p+s) \equiv 0 \left(\mathrm{mod} 2^{n-1}\right)$, $r(p+s) \equiv 0 \left(\mathrm{mod} 2^{n-1}\right)$ and one of numbers q, r is odd, we have $p + s \equiv 0 \pmod{2^{n-1}}$, i.e., $s = -p+2^{n-1}k$, where $k \in \mathbb{Z}_2$ and $p \in \mathbb{Z}_{2^n}^*$. The first congruence of (3.5) implies

$$\begin{aligned} p^2 + rq &\in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}, \\ rq &\in \left\{\pm 1 - p^2, \pm 1 + 2^{n-1} - p^2\right\}. \end{aligned}$$

Hence

$$r \in \left\{\left(\pm 1 - p^2\right) q^{-1}, \left(\pm 1 + 2^{n-1} - p^2\right) q^{-1}\right\}, \quad \text{if } q \text{ is odd},$$

$$q \in \left\{ \left(\pm 1 - p^2\right) r^{-1},\, \left(\pm 1 + 2^{n-1} - p^2\right) r^{-1} \right\}, \quad \text{if } r \text{ is odd.}$$

It is easy to see that if if $rq = 1 - p^2$ and $k = 0$ then automorphisms $\{\{p,\, q\},\, \{r,\, s\}\}$ have order ≤ 2 (see Propositon 2.1). The first statement of the proposition is proved.

Let us calculate the number of all obtained solutions in forms 1)–2). There are 2^{n-1} possibilities for the choice of odd number q, and 2^{n-1} possibilities for the choice of odd number p. The number of choices of s depends on k which have 2 possibilities for forms 2) and only 1 possibility in form 1). For solutions in form 2) there are also 3 possibilities to choose the number a. Thus number of solutions in the forms 1)–4) is $2^{n-1} \cdot 2^{n-1} \cdot (2 \cdot 3 + 1) = 7 \cdot 2^{2n-2}$. Analogously the number of solutions in forms 3)–4) is $7 \cdot 2^{2n-2}$ and we get the second statement of the proposition. Proposition 3.2 is proved. $\square$

In order to investigate the last case

$$\{\{p,\, q\},\, \{r,\, s\}\} \equiv \{\{1,\, 0\},\, \{0,\, 1\}\} \pmod 2,$$

we need some lemmas. We shall consider the cases $n = 3$ and $n \geqslant 4$ separately.

3.3.2 The case $n = 3$

Assume that $n = 3$. Then both numbers r, q are even, i.e., $r = 2u$ and $q = 2v$, where $u, v \in \mathbb{Z}_4$. The first congruence of system (3.5) implies

$$\left(p^2 + rq\right)^2 = p^4 + 8p^2uv + 16u^2v^2 \equiv p^4 \pmod 8$$

and the system (3.5) takes the form

$$\begin{cases} p^4 \equiv 1 \pmod 8 \\ \{q\,(p+s) \equiv 0, \quad r\,(p+s) \equiv 0, \quad (p-s)\,(p+s) \equiv 0 \pmod 4. \end{cases} \tag{3.6}$$

Clearly, all four odd numbers $p \in \mathbb{Z}_8^*$ are solutions of the congruence $p^4 \equiv 1 \pmod 8$. We distinguish two cases: $p+s \equiv 0 \pmod 4$ and $p+s \not\equiv 0 \pmod 4$.

Proposition 3.3 *Let p, s be odd, q, r be even and $p + s \equiv 0 \pmod 4$. Then the automorphisms of order four of the group $C_8 \times C_8$ are given by the matrices $\{\{p,\, q\},\, \{r,\, s\}\} \equiv \{\{p,\, 2v\},\, \{2u,\, -p + 4k\}\}$, where $k \in \mathbb{Z}_2$ and u, $v \in \mathbb{Z}_{2^2}^*$. The number of those automorphisms is 2^5.*

Proof. Let q, r be even numbers and $p + s \equiv 0 \pmod 4$, i.e., $r = 2^f u$ or 0 and $q = 2^g v$ or 0, where f, $g \in \mathbb{Z}_3 \setminus \{0\}$ and $u \in \mathbb{Z}_{2^{3-f}}^*$, $v \in \mathbb{Z}_{2^{3-g}}^*$. Then $s = -p + 4k$, where $k \in \mathbb{Z}_2$, $p \in \mathbb{Z}_8^*$. We get all automorphisms of orders 1, 2 or 4. Computing the square of these automorphisms, we get

$$\{\{p,\, q\},\, \{r,\, s\}\}^2 \equiv \{\{1 + qr,\, 0\},\, \{0,\, 1 + qr\}\},$$

i.e., the automorphism $\{\{p,\,q\},\,\{r,\,s\}\}$ has order 4 if and only if $qr \not\equiv 0 \pmod 8$. The last condition is possible only if $f = g = 1$. The first statement of the proposition is proved.

Calculating the number of all obtained solutions, we get the second statement of the proposition. Proposition 3.3 is proved. □

Proposition 3.4 *Let p, s be odd, q, r be even and $p+s \not\equiv 0 \pmod 4$. Then the automorphisms of order four of the group $C_8 \times C_8$ are given by matrices*

1) $\{\{p,\,q\},\,\{r,\,s\}\} \equiv \{\{p,\,q\},\,\{r,\,p\}\}$,

2) $\{\{p,\,q\},\,\{r,\,s\}\} \equiv \{\{p,\,q\},\,\{r,\,p-4\}\}$,

where q, $r \in 2\mathbb{Z}_4$ and the condition $q \equiv r \equiv 0 \pmod 4$ is impossible. The number of those automorphisms is 96.

Proof. Let q, r be even numbers ($q,\, r \in 2\mathbb{Z}_4,\ r = 2^f u,\ q = 2^g v$) and $p + s = 2k$ ($k \in \mathbb{Z}^*_{2^2}$). Since $f,\, g \geqslant 1$ or one of the numbers (or both) r, q is zero, the second and third congruences of the system (3.6) hold. The fourth congruence of system (3.6) implies **a)** $p - s = 0$ or **b)** $p - s = 2^h l$ ($h \geqslant 1,\ l \in \mathbb{Z}^*_{2^{3-h}}$).

a) If $p - s = 0$, then $s = p \in \mathbb{Z}^*_8$ and we get the automorphisms in the form 1).

b) Let now $p - s = 2^h l$. Then

$$\begin{cases} p = k + 2^{h-1} l, \\ s = k - 2^{h-1} l = p - 2^h l. \end{cases}$$

Since p, s are odd, it follows that $h > 1$, i.e., $h = 2$ and $l = 1$. Hence $s = p - 4,\ p \in \mathbb{Z}^*_8$. We get automorphisms in the form 2).

Let us compute the square of the automorphisms in the forms 1) and 2). Since $q,\, r \in 2\mathbb{Z}_4$, we have

$$\{\{p,q\},\{r,p\}\}^2 \equiv \{\{p,q\},\{r,p-4k\}\}^2 \equiv \{\{1+qr,2qp\},\{2rp,1+qr\}\}.$$

This square is equal to the unity automorphism if and only if $q \equiv r \equiv 0 \pmod 4$. The first statement of the proposition is true.

Let us calculate the number of all obtained automorphisms of order 4. In the form 1) we have 48 automorphisms, because the numbers of possible values for s, p and $(q,\, r)$ are 1, 4 and $4 \cdot 4 - 4 = 12$, respectively. Similarly, in the form 2) we have 48 automorphisms. The second statement of the proposition is proved. Proposition 3.4 is proved. □

3.3.3 The case $n \geqslant 4$

Assume that $n \geqslant 4$. First of all we need to solve the congruence $\left(p^2 + rq\right)^2 \equiv 1 \pmod{2^n}$ in the cases $rq \equiv 0 \pmod{2^n}$ and $rq \not\equiv 0 \pmod{2^n}$.

Lemma 3.1 *Solutions of congruence*

$$p^4 \equiv 1 \pmod{2^n}$$

are $p \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$ *and* $p = \pm 1 + 2^{n-2}z$ *(where* $z \in \mathbb{Z}_4^*$*).*

We give 3.1 without any proof because it is well-known. Denote by p_1 a possible value of p given in Lemma 3.1.

Lemma 3.2 *Assume that* $rq \not\equiv 0 \pmod{2^n}$ *and both numbers* r, q *are even, i.e.,* $r = 2^f u$ *and* $q = 2^g v$*, where* f, $g \in \mathbb{Z}_n \setminus \{0\}$ *and* $u \in \mathbb{Z}^*_{2^{n-f}}$, $v \in \mathbb{Z}^*_{2^{n-g}}$*. Then the solutions of the congruence*

$$\left(p^2 + rq\right)^2 \equiv 1 \pmod{2^n},$$

are

a) $p = \varepsilon + 2^{f+g-1}x$, $r = 2^f u$,

$$q = 2^g\left(\left[2^{n-f-g-1}l - \left(\varepsilon + 2^{f+g-2}x\right)x\right]u^{2^{n-f-g-1}-1} + 2^{n-f-g}k\right),$$

where $\varepsilon = \pm 1$, $x \in \mathbb{Z}^*_{2^{n-f-g+1}}$, $k \in \mathbb{Z}_{2^f}$, *and*

$$(n-1 > f+g \geqslant 3,\ l \in \mathbb{Z}_2) \ \text{ or } (f+g = n-1,\ l = 0);$$

b) $p \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$, $r = 2^f u$, $q = 2^g v$, *where* $f + g = n - 1$.

Proof. The proof of Lemma 3.2 is similar to that of Lemma 2.3 and it is given in Appendix A.3. Lemma 3.2 is proved. □

Proposition 3.5 *Let* p, s *be odd,* $p + s \equiv 0 \left(\mathrm{mod}\ 2^{n-1}\right)$ *and* q, r *be even, i.e.,* $r = 2^f u$ *or* 0 *and* $q = 2^g v$ *or* 0*, where* f, $g \in \mathbb{Z}_n \setminus \{0\}$ *and* $u \in \mathbb{Z}^*_{2^{n-f}}$, $v \in \mathbb{Z}^*_{2^{n-g}}$*. Then automorphisms of order four of the group* $C_{2^n} \times C_{2^n}$ *are given by the matrices*

1) *if* $p = \pm 1 + 2^{n-2}z$, $z \in \mathbb{Z}_4^*$, *then*

$$\{\{p, q\}, \{r, s\}\} \equiv \left\{\{p, q\}, \left\{r, -p + 2^{n-1}k\right\}\right\},$$
where $(q, r) \in \left\{(0, 0), \left(0, 2^f u\right), (2^g v, 0)\right\}$;

$$\{\{p, q\}, \{r, s\}\} \equiv \left\{\{p, 2^g v\}, \left\{2^f u, -p + 2^{n-1}k\right\}\right\},$$
where $f + g \geqslant n$;

2) $\{\{p, q\}, \{r, s\}\} \equiv \left\{\left\{\varepsilon + 2^{f+g-1}x, 2^g v\right\}, \left\{2^f u, -p + 2^{n-1}k\right\}\right\}$,
where $v = \left[2^{n-f-g-1} - \left(\varepsilon + 2^{f+g-2}x\right)x\right]u^{2^{n-f-g-1}-1} + 2^{n-f-g}h$,
$\varepsilon = \pm 1$, $x \in \mathbb{Z}^*_{2^{n-f-g+1}}$, $h \in \mathbb{Z}_{2^f}$, $(n-1 > f+g \geqslant 3)$;

3) $\{\{p, q\}, \{r, s\}\} \equiv \left\{\{p, 2^g v\}, \left\{2^f u, -p + 2^{n-1}k\right\}\right\}$,
where $f + g = n - 1$ *and* $p \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$,

for each $k \in \mathbb{Z}_2$*. The number of automorphisms* 1)–3) *is* $3 \cdot 2^{2n-1}$.

Proof. Assume that the assumptions of the proposition hold. Then $s = -p + 2^{n-1}k$ for some $k \in \mathbb{Z}_2$. We need to solve only the first congruence of the system (3.5). We consider two cases: **I)** $rq \equiv 0 \pmod{2^n}$ and **II)** $rq \not\equiv 0 \pmod{2^n}$.

I) If $rq \equiv 0 \pmod{2^n}$ then at least one of the numbers q, r is zero or $f+g \geqslant n$. By Lemma 3.1, $p = p_1$. Let us compute square of automorphisms of this form. If $p_1 \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$, we have $p_1^2 \equiv 1 \pmod{2^n}$ and it is easy to check that we get an automorphism of order ≤ 2. Since $f, g \geqslant 1$, $2^{f+(n-1)} \equiv 2^{g+(n-1)} \equiv 0 \pmod{2^n}$ and we see that in this case automorphisms have order 2. An alternative variant for p_1 implies the automorphisms in the form 1).

II) If $rq \not\equiv 0 \pmod{2^n}$, then $f + g < n$ and we can use Lemma 3.2. By Proposition 2.3, if $l = 0$ then the corresponding automorphisms have order 1 or 2. An alternative variant for l gives the automorphisms of the forms 2)–3).

Let us determine the number automorphisms described in this proposition. For automorphisms in the form 1): s has 2 possible values and the number of possible values for $(q,\, r)$ is

$$\begin{cases} 1, \text{ if } (q,\, r) = (0,\, 0)\,, \\ \sum\limits_{f=1}^{n-1} 2^{n-f-1} = 2^{n-1} - 1, \text{ if } (q,\, r) = \left(0,\, 2^f u\right) \text{or } (q,\, r) = (2^g v,\, 0)\,, \\ \sum\limits_{f=1}^{n-1} 2^{n-f-1} \sum\limits_{g=n-f}^{n-1} 2^{n-g-1} = (n-2)\, 2^{n-1} + 1, \text{ if } (q,\, r) = \left(2^g v,\, 2^f u\right). \end{cases}$$

Thus for the choice of the triple $(s,\, q,\, r)$ we have

$$2\left[1 + 2\left(2^{n-1} - 1\right) + \left((n-2)\, 2^{n-1} + 1\right)\right] = 2^n n$$

possibilities. Since we have only 4 possible values for p, we state, that there is $2^{n+2}n$ automorphisms in the form 1).

The automorphisms of the form 2) are given by the parameters f, g, ε, h, x, u, k. The numbers of possible values of the parameters ε, h, x, u, k are 2, 2^f, 2^{n-f-g}, 2^{n-f-1}, 2, respectively. If we sum up over possible values of f and g, we get the number of automorphisms of the form 2):

$$2 \cdot 2 \cdot \sum_{f=1}^{n-3} 2^{n-f-1} \sum_{g=1,\ f+g\geqslant 3}^{n-f-2} \left(2^f \cdot 2^{n-f-g}\right) =$$

$$= 4 \left(2^{n-2} \cdot \sum_{g=2}^{n-3} 2^{n-g} + \sum_{f=2}^{n-3} 2^{n-f-1} \sum_{g=1}^{n-f-2} 2^{n-g}\right) =$$

$$= 2^{n+3}\left(3 \cdot 2^{n-4} - n + 1\right).$$

The automorphisms of the form 3) are given by the parameters p, k, f, u, v. The numbers of possible values of the parameters p, k, u, v are 4, 2, 2^{n-f-1}, $2^{n-g-1}=2^f$, respectively. Hence we have

$$8\sum_{f=1}^{n-2}2^{n-f-1}2^f = 8\sum_{f=1}^{n-2}2^{n-1} = (n-2)\,2^{n+2}$$

automorphisms of the form 3).

If we sum up the numbers of automorphisms in all cases we obtain $3\cdot 2^{2n-1}$. Proposition 3.5 is proved. $\square$

Proposition 3.6 *Let p, s be odd, q, r be even and $p+s\not\equiv 0\pmod{2^{n-1}}$. Then automorphisms of order four of the group $C_{2^n}\times C_{2^n}$ are given by the matrices*

1) $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\left\{p,\,2^{n-2}q'\right\},\left\{2^{n-2}r',\,p+2^{n-1}k\right\}\right\}$, *where* $k\in\mathbb{Z}_2$, $q',\,r'\in\mathbb{Z}_4$ *and*
   a) $p=\pm1+2^{n-2}z$, $z\in\mathbb{Z}_4^*$;
   b) $p\in\left\{\pm1,\,\pm1+2^{n-1}\right\}$, *condition* $q'\equiv r'\equiv 0\pmod 2$ *does not hold;*

2) *for every* $l\in\mathbb{Z}_4^*$ *and* $f,\,g\geqslant n-2$
   $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\{p_1,\,q\},\left\{r,\,p_1-2^{n-2}l\right\}\right\}$,
   where $(q,\,r)\in\left\{(0,\,0),\left(0,\,2^fu\right),(2^gv,\,0)\right\}$;
   $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\{p_1,\,2^gv\},\left\{2^fu,\,p_1-2^{n-2}l\right\}\right\}$;

3) *for* $l\in\mathbb{Z}_4^*$
   $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\{p_1,\,q\},\left\{r,\,-p+2^{n-2}l\right\}\right\}$,
   where $(q,\,r)\in\left\{(0,\,0),\left(0,\,2^fu\right),(2^gv,\,0)\right\}$,
   $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\{p_1,\,2^gv\},\left\{2^fu,\,-p+2^{n-2}l\right\}\right\}$ $(f+g\geqslant n)$;

4) *for* $l\in\mathbb{Z}_4^*$
   $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\left\{\varepsilon+2^{f+g-1}x,\,2^gv\right\},\left\{2^fu,\,-p+2^{n-2}l\right\}\right\}$,
   where $v=\left[2^{n-f-g-1}y-\left(\varepsilon+2^{f+g-2}x\right)x\right]u^{2^{n-f-g-1}-1}+2^{n-f-g}h$,
   $\varepsilon=\pm1$, $x\in\mathbb{Z}^*_{2^{n-f-g+1}}$, $h\in\mathbb{Z}_{2^f}$, $(n-1>f+g\geqslant 3$ *and* $y\in\mathbb{Z}_2)$
   or $(f+g=n-1$ *and* $y=0)$.

5) *for* $l\in\mathbb{Z}_4^*$ *and* $p\in\left\{\pm1,\,\pm1+2^{n-1}\right\}$
   $\{\{p,\,q\},\{r,\,s\}\}\equiv\left\{\{p,\,2^gv\},\left\{2^fu,\,-p+2^{n-2}l\right\}\right\}$,
   where $f+g=n-1$.

The number of automorphisms 1) – 5) *is* $3\cdot 2^{2n}+15\cdot 2^5$.

Proof. Let q, r be even numbers ($r=2^fu$ or 0 and $q=2^gv$ or 0 ($f,\,g\in\mathbb{Z}_n\setminus\{0\}$ and $u\in\mathbb{Z}^*_{2^{n-f}}$, $v\in\mathbb{Z}^*_{2^{n-g}}$)) and $p+s=2^ml$ $(m\in\mathbb{Z}_{n-1}\setminus\{0\}$, $l\in\mathbb{Z}^*_{2^{n-m}})$. Using the second, third and fourth congruence of system (3.5), we get $f,\,g\geqslant n-1-m$ and **I)** $p-s\equiv 0\left(\mathrm{mod}\ 2^{n-1}\right)$ or **II)** $p-s\not\equiv 0\left(\mathrm{mod}\ 2^{n-1}\right)$.

I) Let us consider the case $p - s \equiv 0 \pmod{2^{n-1}}$. Then $s = p + 2^{n-1}k$ and $p + s = 2\left(p + 2^{n-2}k\right)$. Second and third congruence of (3.5) imply that $r \equiv q \equiv 0 \pmod{2^{n-2}}$. Denote $r = 2^{n-2}r'$, $q = 2^{n-2}q'$ (where $q', r' \in \mathbb{Z}_4$). Since $n \geqslant 4$, we have $rq \equiv 2^n 2^{n-4} \equiv 0 \pmod{2^n}$, and, by Lemma 3.1, $p = p_1$. There are two possibilities: if $p_1 = \pm 1 + 2^{n-2}z$, then $p_1^2 \not\equiv 1 \pmod{2^n}$ and the corresponding automorphisms have order 4; if $p_1 \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$, then $p_1^2 \equiv 1 \pmod{2^n}$,

$$\{\{p, q\}, \{r, s\}\}^2 \equiv \left\{\left\{1, 2^{n-1}q'p_1\right\}, \left\{2^{n-1}r'p_1, 1\right\}\right\},$$

and the corresponding automorphisms have order 4 if and only if the condition $q' \equiv r' \equiv 0 \pmod 2$ does not hold. We get automorphisms in form 1).

II) Let us consider the case $p - s \not\equiv 0 \pmod{2^{n-1}}$, i.e., $p - s = 2^h l$ where $n - 2 \geqslant h \geqslant n - 1 - m$, $l \in \mathbb{Z}^*_{2^{n-h}}$. Then

$$\begin{cases} p = 2^{m-1}l + 2^{h-1}t, \\ s = 2^{m-1}l - 2^{h-1}t. \end{cases}$$

Since p, s are odd, it follows that **i)** $m = 1$, $h > 1$ or **ii)** $m > 1$, $h = 1$.

i) $m = 1$, $h > 1$. Then $s = p - 2^h t$, $t \in \mathbb{Z}^*_{2^{n-h}}$. Since f, g, $h \geqslant n-1-m = n-2$, we have $h = n-2$ and $rq \equiv 2^{2n-4} \equiv 0 \pmod{2^n}$. Hence the first congruence of (3.5) takes the form $p^4 \equiv 1 \pmod{2^n}$, which implies, by Lemma 3.1, that

$$p \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\} \text{ and } p = \pm 1 + 2^{n-2}z,\ z \in \mathbb{Z}^*_4,$$

and we obtained automorphisms 2).

ii) $m > 1$, $h = 1$. Condition $1 = h \geqslant n - 1 - m$ implies that $m \geqslant n - 2$. Since $m < n - 1$, we have $m = n - 2$ and f, $g \geqslant n - 1 - m = 1$. Thus we have $s = -p + 2^m l = -p + 2^{n-2}l$, $l \in \mathbb{Z}^*_{2^2}$. If $rq \equiv 0 \pmod{2^n}$ then the first congruence of (3.5) implies, by Lemma 3.1, that

$$p \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\},\ p = \pm 1 + 2^{n-2}z \ \ (\text{where } z \in \mathbb{Z}^*_4)$$

and we get automorphisms in the form 3). If $rq \not\equiv 0 \pmod{2^n}$ then the first congruence of (3.5) implies by Lemma 3.2 two possibilities:

a)
$$\begin{aligned} p &= \varepsilon + 2^{f+g-1}x,\ r = 2^f u, \\ q &= 2^g\left(\left[2^{n-f-g-1}y - \left(\varepsilon + 2^{f+g-2}x\right)x\right]u^{2^{n-f-g-1}-1} + 2^{n-f-g}k\right), \end{aligned}$$

where $\varepsilon = \pm 1$, $x \in \mathbb{Z}^*_{2^{n-f-g+1}}$, $k \in \mathbb{Z}_{2^f}$, and

$$(n - 1 > f + g \geqslant 3 \text{ and } y \in \mathbb{Z}_2) \ \text{ or } (f + g = n - 1 \text{ and } y = 0);$$

b) $p \in \left\{1, -1+2^{n-1}, 1+2^{n-1}, -1+2^n\right\}$, $r = 2^f u$, $q = 2^g v$, where $f+g = n-1$.
These possibilities give the automorphisms of the forms 4) and 5).

Let us determine the number of automorphisms described in this proposition.

For automorphisms in form 1a), we have 4 possibilities for p, 2 possibilities for s and for the pair $(r,\, q)$ $4 \cdot 4$ possibilities, i.e., there is $4 \cdot 2 \cdot 16 = 4 \cdot 2^5$ automorphisms in this form. We have for the automorphisms in the form 1b) 4 possibilities for p, 2 possibilities for s and for the pair $(r,\, q)$ $4 \cdot 4 - 4$ possibilities, i.e., there is $4 \cdot 2 \cdot 12 = 3 \cdot 2^5$ automorphisms in this form. Therefore, there is $7 \cdot 2^5$ automorphisms in form 1).

In form 2), we have 8 possibilities for p, 2 possibilities for s and for the pair $(r,\, q)$ one possibility if $(q,\, r) = (0,\, 0)$, $\sum\limits_{f=n-2}^{n-1} 2^{n-f-1} = 3$ possibilities if $(q,\, r) = \left(0,\, 2^f u\right)$ or $(q,\, r) = (2^g v,\, 0)$, and $\sum\limits_{f=n-2}^{n-1} 2^{n-f-1} \sum\limits_{g=n-2}^{n-1} 2^{n-g-1} = 9$ possibilities if $(q,\, r) = \left(2^g v,\, 2^f u\right)$. In conclusion, there are $8 \cdot 2\,[1 + 2 \cdot 3 + 9] = 2^8$ automorphisms in form 2).

In form 3), we have $8 \cdot 2$ possibilities for the pair $(p,\, s)$ and for the pair $(r,\, q)$ one possibility if $(q,\, r) = (0,\, 0)$, $\sum\limits_{f=1}^{n-1} 2^{n-f-1} = 2^{n-1} - 1$ possibilities if $(q,\, r) = \left(0,\, 2^f u\right)$ or $(q,\, r) = (2^g v,\, 0)$, and $\sum\limits_{f=1}^{n-1} 2^{n-f-1} \sum\limits_{g=n-f}^{n-1} 2^{n-g-1} = (n-2)\, 2^{n-1} + 1$ possibilities if $(q,\, r) = \left(2^g v,\, 2^f u\right)$. So, there are

$$16\left[1 + 2\left(2^{n-1} - 1\right) + \left((n-2)\, 2^{n-1} + 1\right)\right] = 2^{n+3} n$$

automorphisms in form 3).

In form 4), if $n - 1 > f + g \geqslant 3$ and $y \in \mathbb{Z}_2$, we have 2 possibilities for s and the choice of the triple $(p,\, q,\, r)$ depends on f : for odd number u we have 2^{n-f-1} possibilities; if $g = 1, 2, ..., n-f-2$ (where $n - 1 > f + g \geqslant 3$) is chosen, then for odd number v we have $2^f \cdot 2$ (since $y \in \mathbb{Z}_2$) possibilities and for p we have: $2^{n-(f+g)}$ possibilities for odd number x and 2 possibilities for number ε. Hence the number of automorphisms of this kind is

$$2 \cdot 2 \sum_{f=1}^{n-3} 2^{n-f-1} \sum_{g=1,\ f+g \geqslant 3}^{n-f-2} \left(2^{f+1} \cdot 2^{n-f-g}\right) =$$

$$= 4 \left(2^{n-2} \cdot \sum_{g=2}^{n-3} 2^{n-g+1} + \sum_{f=2}^{n-3} 2^{n-f-1} \sum_{g=1}^{n-f-2} 2^{n-g+1}\right) =$$

$$= 2^{n+4}\left(3 \cdot 2^{n-4} - n + 1\right).$$

In form 4), if $f+g=n-1$ and $y=0$, the automorphisms are given by the parameters s, u, h, x, ε. The numbers of possible values of these parameters are 2, 2^{n-f-1}, 2^f, 2, 2, respectively. Hence we have

$$4\cdot 2\sum_{f=1}^{n-2}2^{n-f-1}2^f=8\sum_{f=1}^{n-2}2^{n-1}=2^{n+2}\,(n-2)\,.$$

automorphisms of this form.

Resume, in the form 4) we have

$$2^{n+4}\left(3\cdot 2^{n-4}-n+1\right)+2^{n+2}\,(n-2)=2^{n+2}\left(3\cdot 2^{n-2}-3n+2\right)$$

automorphisms.

In form 5), we have $4\cdot 2$ possibilities for the pair $(p,\,s)$ and the choice of the pair $(q,\,r)$ depends on f : for odd number u we have 2^{n-f-1} possibilities; then we compute $g=n-f-1$ (since $f+g=n-1$) and for odd number v we have $2^{n-g-1}=2^f$ possibilities. Hence we have

$$8\sum_{f=1}^{n-2}2^{n-f-1}2^f=8\sum_{f=1}^{n-2}2^{n-1}=2^{n+2}\,(n-2)$$

automorphisms of form 5).

If we sum up the numbers of automorphisms in all cases we obtain $3\cdot 2^{2n}+15\cdot 2^5$. Proposition 3.6 is proved. $\square$

3.4 Main results

From Theorem 3.1 and Theorem 2.1 follows

Theorem 3.2 *There exist at most*

$$640\ (\textit{if } n=3),\qquad 12\cdot 4^n+512\ (\textit{if } n\geqslant 4)$$

groups of order $2^{2(n+1)}$ $(n\geqslant 3)$ *which can be presented in the form* $\mathcal{G}=(C_{2^n}\times C_{2^n})\leftthreetimes C_4$, *i.e.,*

$$\mathcal{G}=\langle a,\,b,\,c\mid a^{2^n}=b^{2^n}=c^4=1,\ ab=ba,\ c^{-1}ac=a^pb^q,\ c^{-1}bc=a^rb^s\rangle,$$

where $p,\,q,\,r,\,s\in\mathbb{Z}_{2^n}$, *and all possible values of* $\{\{p,\,q\},\{r,\,s\}\}$ *are described in Propositions 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, or* $\{\{p,\,q\},\{r,\,s\}\}\in M_i$ $(i=1,...,36)$ (*see Appendix B*).

3.5 Conjugacy classes of matrices of orders 1, 2 or 4

All (2×2)-matrices of order 1 or 2 over $\mathbb{Z}_{2^n}$ are already divided into conjugacy classes and representatives $A_1 - A_{17}$ of these classes are given in Appendix C. Similarly to subsubection 2.1.3, let us make now the same for (2×2)-matrices of order 4. We do not present elementary computations. Denote a conjugacy class of (2×2)-matrices (over $\mathbb{Z}_{2^n}$) of order 4 with a representative $\mathcal{A}_i$ by $\mathcal{K}_i$.

Theorem 3.3 *There are* 36 *conjugacy classes* K_i $(i = 1, 2, ..., 17)$, $\mathcal{K}_i$ $(i = 1, 2, ..., 7)$, $\mathcal{K}_i^3$ $(i = 8, 9, ..., 19)$ *if* $n = 3$ *and* 80 *conjugacy classes* K_i $(i = 1, 2, ..., 17)$, $\mathcal{K}_i$ $(i = 1, 2, ..., 63)$ *if* $n \geqslant 4$ *of regular* (2×2)*-matrices* (*over* $\mathbb{Z}_{2^n}$) *of orders* 1, 2 *or* 4.

Proof. To show that two given (2×2)-matrices A and B are conjugate, we have to solve the system

$$gBg^{-1} \equiv A \,(\mathrm{mod}\, 2^n), \qquad \det g \neq 0 \,(\mathrm{mod}\, 2),$$

where regular (2×2)-matrix g is unknown.

It is clear, that two matrices of different order could not be conjugate. Consequently, all matrices of orders 1 or 2 are already divided into conjugacy classes (see subsection 2.1.3 and Appendix A.1). However, we must divide into conjugacy classes matrices of order 4. We consider two cases: $n = 3$ and $n \geqslant 4$.

If $n = 3$, we consider matrices $\mathcal{A}_1 - \mathcal{A}_7$ and $\mathcal{A}_8^3 - \mathcal{A}_{19}^3$ (see Appendix E). It is easy to verify that they are not conjugate to each other. Each matrix B (described in Propositions 3.1, 3.2, 3.3, 3.4) of order 4 is conjugate to exactly one of the matrices $\mathcal{A}_i$ $(i = 1, 2, ..., 7)$ or matrix $\mathcal{A}_i^3$ $(i = 8, 9, ..., 19)$. Conditions under which this takes place, are given in tables of Appendix D.

If $n \geqslant 4$, we consider matrices $\mathcal{A}_1 - \mathcal{A}_{63}$ (see Appendix E). It is easy to verify that they are not conjugate to each other. Each matrix B (described in Propositions 3.1, 3.2, 3.5, 3.6) of order 4 is conjugate to exactly one of matrices $\mathcal{A}_i$ $(i = 1, 2, ..., 63)$. Conditions under which this takes place, are given in tables of Appendix D. Theorem 3.3 is proved. $\square$

4 The groups presentable in the form $\left(C_{2^{n+m}} \times C_{2^n}\right) \leftthreetimes C_2$

The results presented in this chapter have been published in [9].

4.1 Main concepts

In this chapter we find all groups of order 2^{2n+m+1} ($n \geqslant 3$, $m \geqslant 1$) which can be presented in the form $\mathcal{G} = \left(C_{2^{n+m}} \times C_{2^n}\right) \leftthreetimes C_2$, i.e.,

$$\mathcal{G} = \left\langle a, b, c \mid a^{2^{n+m}} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^p b^q,\ c^{-1}bc = a^r b^s \right\rangle,$$

where p, $r \in \mathbb{Z}_{2^{n+m}}$ and q, $s \in \mathbb{Z}_{2^n}$.

The inner automorphism $\widehat{c}$ induces an automorphism of $C_{2^{n+m}} \times C_{2^n} = \langle a,\, b\rangle$ of order 1 or 2:

$$a\widehat{c} = c^{-1}ac = a^p b^q, \quad b\widehat{c} = c^{-1}bc = a^r b^s,$$

and we have to find all possible automorphisms of this kind.

Consider a map

$$\begin{aligned} \varphi: \quad & C_{2^{n+m}} \times C_{2^n} \longrightarrow C_{2^{n+m}} \times C_{2^n}, \\ & a\varphi = a^p b^q, \quad b\varphi = a^r b^s, \end{aligned} \tag{4.1}$$

and decide under which conditions φ is an automorphism of order 1 or 2 of the group

$$C_{2^{n+m}} \times C_{2^n} = \left\langle a,\, b \mid a^{2^{n+m}} = b^{2^n} = 1,\ ab = ba \right\rangle.$$

To be an endomorphism, φ has to preserve the defining relations of $C_{2^{n+m}} \times C_{2^n}$. Clearly, the map φ preserves the relations $a^{2^{n+m}} = 1$ and $ab = ba$ for all values of parameters. Since $b^{2^n} = 1$, we have:

$$(b\varphi)^{2^n} = (a^r b^s)^{2^n} = a^{2^n r} b^{2^n s} = a^{2^n r} = 1.$$

Hence

$$2^n r \equiv 0 \left(\mathrm{mod}\ 2^{n+m}\right)$$

and

$$r \equiv 0 \left(\mathrm{mod}\ 2^m\right). \tag{4.2}$$

Consequently, φ is an endomorphism if and only if the condition (4.2) holds. This endomorphism is an automorphism if and only if

$$p \equiv s \equiv 1 \left(\mathrm{mod}\ 2\right). \tag{4.3}$$

The automorphism (4.1), (4.2), (4.3) has order 1 or 2 if and only if

$$\begin{aligned} a &= a\varphi^2 = (a\varphi)\,\varphi = (a^p b^q)\,\varphi = (a^p b^q)^p\,(a^r b^s)^q = a^{p^2+rq} b^{pq+sq}, \\ b &= b\varphi^2 = (b\varphi)\,\varphi = (a^r b^s)\,\varphi = (a^p b^q)^r\,(a^r b^s)^s = a^{pr+rs} b^{qr+s^2}, \end{aligned}$$

i.e.,

$$\begin{cases} p^2+rq \equiv 1, \quad pr+rs \equiv 0 & (\mathrm{mod}\ 2^{n+m}), \\ pq+sq \equiv 0, \quad qr+s^2 \equiv 1 & (\mathrm{mod}\ 2^{n}). \end{cases}$$

The last system is equivalent to the system

$$\begin{cases} \begin{cases} p^2+rq \equiv 1, \quad pq+sq \equiv 0 \\ pr+rs \equiv 0, \quad qr+s^2 \equiv 1 \end{cases} & (\mathrm{mod}\ 2^{n}), \\ p^2+rq \equiv 1, \quad pr+rs \equiv 0 & (\mathrm{mod}\ 2^{n+m}). \end{cases} \tag{4.4}$$

The subsystem modulo 2^n of (4.4) is already solved for $n \geqslant 3$ in subsection 2.1.2. Let $\{\{p,\, q\},\{r,\, s\}\} = \{\{a,\, q\},\{c,\, s\}\}$ be a solution of this subsystem modulo 2^n where in addition condition (4.3), i.e., $a \equiv s \equiv 1\,(\mathrm{mod}2)$, holds. Let

$$p = a + 2^n x, \qquad r = c + 2^n y, \tag{4.5}$$

where

$$x,\, y \in \mathbb{Z}_{2^m}. \tag{4.6}$$

Hence system (4.4) with conditions (4.2), (4.3) is equivalent to the following system with unknown $x,\, y \in \mathbb{Z}_{2^m}$:

$$\begin{cases} (a+2^n x)^2 + (c+2^n y)\, q \equiv 1 \\ (c+2^n y)\,(a+2^n x+s) \equiv 0 \end{cases} \quad \left(\mathrm{mod}\ 2^{n+m}\right), \tag{4.7}$$

$$c + 2^n y \equiv 0\,(\mathrm{mod}\ 2^m), \tag{4.8}$$

where $\{\{a,q\},\{c,s\}\} \in M_i$ $(i = 1, ..., 36)$ (see subsection 2.1.2 and Appendix B).

4.2 Automorphisms of order 1 or 2 of $C_{2^{n+m}} \times C_{2^n}$

To find the automorphisms of order 1 or 2 of $C_{2^{n+m}} \times C_{2^n}$, we have to solve system (4.7), (4.8) under assumptions (4.2), (4.3).

By (4.8), there are three possible alternative cases: **1)** $c \equiv 0\,(\mathrm{mod}\ 2^m)$, $m < n$; **2)** $c = 0,\ \ m = n$; **3)** $y \equiv 0\,(\mathrm{mod}\ 2^{m-n})$, $c = 0,\ m > n$. Let us consider these three cases separately.

4.2.1 The case $m < n$

In this case system (4.7), (4.8) takes the form

$$\begin{cases} a^2 + 2^{n+1}ax + (c + 2^n y)\, q \equiv 1 \\ (c + 2^n y)\,(a + s) + 2^n xc \equiv 0 \end{cases} \pmod{2^{n+m}}, \tag{4.9}$$

$$c \equiv 0 \pmod{2^m}. \tag{4.10}$$

Proposition 4.1 *If q is odd then the automorphisms of order equal or less than 2 of the group $C_{2^{n+m}} \times C_{2^n}$ are*

$$\{\{(s_0 + 2^m k) + 2^n x, q\}, \{c + 2^n y, -(s_0 + 2^m k)\}\}$$

for each $k \in \mathbb{Z}_{2^{n-m}}$ and $x \in \mathbb{Z}_{2^m}$, where

$$y \equiv \left(\frac{\left(1 - (s_0 + 2^m k)^2 - cq\right)}{2^n} - 2\,(s_0 + 2^m k)\, x \right) q^{-1} \pmod{2^m},$$

and

$$\begin{aligned} s_0 &\in \left\{1, -1 + 2^m, \pm 1 + 2^{m-1}\right\}, \text{ if } m \geqslant 3, \\ s_0 &\in \left\{1, -1 + 2^m\right\}, \text{ if } m = 2, \\ s_0 &= 1, \text{ if } m = 1. \end{aligned}$$

The number of these automorphisms is: 2^{2n+1}, if $m \geqslant 3$; 2^{2n}, if $m = 2$, and 2^{2n-1}, if $m = 1$.

Proof. The matrices of the set M_1 do not satisfy condition (4.3). Let us consider the matrices of the second possible set M_2. In this set, only the matrices of the form $\left\| \begin{matrix} s & q \\ (1 - s^2)\, q^{-1} & -s \end{matrix} \right\|$, where $q, s \in \mathbb{Z}_{2^n}^*$, $s^2 \equiv 1 \pmod{2^m}$, satisfy conditions (4.10). The last condition implies $s = s_0 + 2^m k$, where $k \in \mathbb{Z}_{2^{n-m}}$, and: $s_0 \in \left\{1, -1 + 2^m, \pm 1 + 2^{m-1}\right\}$, if $m \geqslant 3$; $s_0 \in \{1, -1 + 2^m\}$, if $m = 2$; $s_0 = 1$, if $m = 1$.

Since $a + s = 2^n$, the second congruence of (4.9) implies

$$\begin{aligned} 2^n\,(c + 2^n y) + 2^n xc &\equiv 0 \pmod{2^{n+m}}, \\ c\,(x + 1) &\equiv 0 \pmod{2^m}, \end{aligned}$$

which holds by (4.10) for every $x, y \in \mathbb{Z}_{2^m}$.

Let us consider the first congruence of (4.9). We have

$$\begin{aligned} s^2 + 2^{n+1}sx + cq + 2^n yq &\equiv 1 \pmod{2^{n+m}}, \\ 2^n yq &\equiv \left(1 - s^2 - cq\right) - 2^{n+1}sx \pmod{2^{n+m}}, \\ y &\equiv \left(\frac{\left(1 - s^2 - cq\right)}{2^n} - 2sx \right) q^{-1} \pmod{2^m}. \end{aligned}$$

Next we find the number of obtained automorphisms. We have 2^{n-m} choices for k, 2^{n-1} choices for odd number q, 2^m choices for x and z choices for s_0, where $z = 4$, if $m \geqslant 3$; $z = 2$, if $m = 2$; $z = 1$, if $m = 1$. This implies that we have $z \cdot 2^{n-m}$ choices for s and the number of automorphisms of the given form is equal to the number of triples $(s,\, q,\, x)$ and $|\{(s,\, q,\, x)\}| = z \cdot 2^{n-m} \cdot 2^{n-1} \cdot 2^m = z \cdot 2^{2n-1}$. Proposition 4.1 is proved. $\square$

To solve the first congruence of (4.9), we need two lemmas.

Lemma 4.1 *Let $s \in \left\{1,\, \pm 1 + 2^{n-1},\, -1 + 2^n\right\}$ and $2^n q \equiv 0 \ (mod\ 2^{n+m})$, i.e., $q = 0$ or $q = 2^t u$, where $1 \leqslant m \leqslant t < n$, $u \in \mathbb{Z}^*_{2^{n-t}}$. Then the congruence*

$$\left(s^2 - 1\right) + 2^{n+1} sx + 2^n yq \equiv 0 \qquad \left(mod\ 2^{n+m}\right),$$

has solutions if and only if $s \in \{1,\, -1 + 2^n\}$ and these solutions are: $y \in \mathbb{Z}_{2^m}$ and

1) $x \in \left\{0,\, 2^{m-1}\right\}$, *if* $s = 1$;
2) $x \in \left\{-1 + 2^{m-1},\, -1 + 2^m\right\}$, *if* $s = -1 + 2^n$.

Proof. 1) If $s = 1$, then $s^2 - 1 = 0$ and $x \equiv 0 \left(\mathrm{mod}\ 2^{m-1}\right)$, (if $m = 1$, then the congruence holds for every $x \in \mathbb{Z}_2$).

2) If $s = -1 + 2^n$, then $s^2 - 1 = -2^{n+1}$ and $x \equiv -1 \left(\mathrm{mod}\ 2^{m-1}\right)$ (if $m = 1$, then the congruence holds for every $x \in \mathbb{Z}_2$).

3) If $s = \pm 1 + 2^{n-1}$, then $s^2 - 1 = 2^{2n-2} \pm 2^n$ and the congruence implies

$$\begin{aligned} 2^{2n-2} \pm 2^n + 2^{n+1} sx &\equiv 0 \ \left(\mathrm{mod}\ 2^{n+m}\right), \\ 2^{n-2} \pm 1 + 2sx &\equiv 0 \ \left(\mathrm{mod}\ 2^{n+m}\right), \end{aligned}$$

which is impossible.

Note that if $m = 1$, we have $x \in \left\{0,\, 2^{m-1}\right\} = \{0,\, 1\} = \mathbb{Z}_2$ in the case 1), and $x \in \left\{-1 + 2^{m-1},\, -1 + 2^m\right\} = \{-1 + 1,\, -1 + 2\} = \{0,\, 1\} = \mathbb{Z}_2$ in the case 2). Lemma 4.1 is proved. $\square$

Lemma 4.2 *Let $s \in \left\{1,\, \pm 1 + 2^{n-1},\, -1 + 2^n\right\}$ and $2^n q \not\equiv 0 \ (mod\ 2^{n+m})$, i.e., $q = 2^t u$, where $1 \leqslant t < m$ $(1 < m < n)$, $u \in \mathbb{Z}^*_{2^{n-t}}$. Then the congruence*

$$\left(s^2 - 1\right) + 2^{n+1} sx + 2^n yq \equiv 0 \ \left(mod\ 2^{n+m}\right)$$

has solutions if and only if $s \in \{1, -1 + 2^n\}$, and these solutions are: $y \in \mathbb{Z}_{2^m}$ and

1) $x \equiv -2^{t-1} uy \ \left(mod\ 2^{m-1}\right)$, *if* $s = 1$;
2) $x \equiv 2^{t-1} uy - 1 \ \left(mod\ 2^{m-1}\right)$, *if* $s = -1$.

Proof. The congruence takes now the form

$$\left(s^2-1\right)+2^{n+1}sx+2^{n+t}yu\equiv 0 \pmod{2^{n+m}}.$$

1) If $s=1$, we have $s^2-1=0$ and $x\equiv -2^{t-1}uy \pmod{2^{m-1}}$.
2) If $s=-1+2^n$, then $s^2-1=-2^{n+1}$ and $x\equiv 2^{t-1}uy-1 \pmod{2^{m-1}}$.
3) If $s=\pm 1+2^{n-1}$, then $s^2-1=2^{2n-2}\pm 2^n$ and

$$\begin{aligned}\left(2^{2n-2}\pm 2^n\right)+2^{n+1}sx+2^{n+t}yu &\equiv 0 \pmod{2^{n+m}},\\ 2^{n-2}\pm 1+2sx+2^tyu &\equiv 0 \pmod{2^m},\end{aligned}$$

which is impossible. Lemma 4.2 is proved. □

Denote by x_1 the solutions from Lemma 4.1 and by x_2 the solutions from Lemma 4.2.

Proposition 4.2 *Let q or c be equal to 0 and both numbers be even. Then automorphisms of order 1 or 2 of the group $C_{2^{n+m}}\times C_{2^n}$ exist only in the case $s\in\{1,\,-1+2^n\}$ and these automorphisms are:*

1) $\left\{\left\{s+2^nx_1,\,0\right\},\left\{2^ny_2,\,s+2^{n-1}k\right\}\right\}$ $(k\in\mathbb{Z}_2)$,
2) $\left\{\left\{s+2^nx_1,\,0\right\},\left\{2^ny_1,\,-s\right\}\right\}$,
3) $\left\{\left\{s+2^nx_1,\,0\right\},\left\{2^ny_1,\,-s+2^{n-1}\right\}\right\}$,
4) $\left\{\left\{s+2^nx_1,\,0\right\},\left\{2^tu+2^ny_1,\,-s\right\}\right\}$ $(t\in\mathbb{Z}_n\setminus\mathbb{Z}_m)$,
5) $\left\{\left\{s+2^nx_1,\,2^tu\right\},\left\{2^ny_1,\,-s\right\}\right\}$ $(t\in\mathbb{Z}_n\setminus\mathbb{Z}_m)$,
6) $\left\{\left\{s+2^nx_2,\,2^tu\right\},\left\{2^ny_1,\,-s\right\}\right\}$ $(t\in\mathbb{Z}_m\setminus\{0\})$,
7) $\left\{\left\{s+2^nx_1,\,2^{n-1}\right\},\left\{2^ny_2,\,s+2^{n-1}k\right\}\right\}$ $(k\in\mathbb{Z}_2)$,
8) $\left\{\left\{s+2^nx_1,\,2^tu+2^ny_1\right\},\left\{0,\,-s+2^{n-1}\right\}\right\}$ $(t\in\mathbb{Z}_n\setminus\mathbb{Z}_m)$,
9) $\left\{\left\{s+2^nx_2,\,2^tu+2^ny_1\right\},\left\{0,\,-s+2^{n-1}\right\}\right\}$ $(t\in\mathbb{Z}_m\setminus\{0\})$,
10) $\left\{\left\{s+2^nx_1,\,0\right\},\left\{2^tu+2^ny_1,-s+2^{n-1}\right\}\right\}$ $(t\in\mathbb{Z}_n\setminus\mathbb{Z}_{m+1})$

for each $y_1\in\mathbb{Z}_{2^m}$ and $y_2\in\left\{0,\,2^{m-1}\right\}$. The number of automorphisms of this form is $16+7\cdot 2^{n+1}$, if $m=1$, and $32-2^{m+3}+3\cdot 2^{n+1}+2^{n+m+2}$, if $m\geqslant 2$.

Remark. If $m=1$, then: **a**) there are no automorphisms in the forms 6) and 9); **b**) $y_1,\,y_2,\,x_1\in\mathbb{Z}_2$.

Proof. If q or c is equal to 0, then the matrices considered belong to the sets M_3–M_{22}. We have to consider all these cases like in the proof of Proposition 4.1. It is done in Appendix A.4. Proposition 4.2 is proved. □

Proposition 4.3 *Let q and c be both nonzero even numbers, $k\in\{0,\,1\}$ and $s\in\left\{1,\,\pm 1+2^{n-1},\,-1+2^n\right\}$. Then automorphisms of order 1 or 2 of the group $C_{2^{n+m}}\times C_{2^n}$ are:*

1) $\left\{\left\{s+2^n x,\, 2^t u\right\},\left\{2^r v+2^n y,\, -s+2^{n-1}k\right\}\right\}$, *where* $r \in \mathbb{Z}_n \setminus \mathbb{Z}_{m+k}$, $t+r>n$, $s \in \{1, -1+2^n\}$ *and, if* $m>1$,

$$x \equiv \begin{cases} -2^{r+t-n-1}\left(v+2^{n-r}y\right)u \ \left(mod 2^{m-1}\right), & \text{if } s=1, \\ -1+2^{r+t-n-1}\left(v+2^{n-r}y\right)u \ \left(mod 2^{m-1}\right), & \text{if } s=-1+2^n, \end{cases}$$

2) $\left\{\left\{s+2^n x,\, 2^t u\right\},\left\{2^r v+2^n y,\, -s+2^{n-1}k\right\}\right\}$, *where* $r \in \mathbb{Z}_n \setminus \mathbb{Z}_{m+k}$, $t+r=n$, $s=\pm 1+2^{n-1}$ *and, if* $m>1$,

$$x \equiv \left(\frac{\mp\left(v+2^{n-r}y\right)u-1}{2} \mp 2^{n-3}\right) \ \left(mod\ 2^{m-1}\right)$$

for each $y \in \mathbb{Z}_{2^m}$ (*and for each* $x \in \mathbb{Z}_2$, *if* $m=1$). *There exist* $(2n-2m-1)\,2^{n+m+1}-3\cdot 2^{n+1}+2^{m+3}$ *automorphisms of this form.*

Proof. Only the matrices of the sets M_i, $i = 23, 24, 25, 26, 27, 28, 31, 32, 33, 34$, satisfy the conditions of the proposition. We have to consider all these cases. It is done in Appendix A.5. Proposition 4.3 is proved. □

Proposition 4.4 *Let* $q=2^t u$ *and* $c=2^r v$ *be both nonzero even numbers, number* $s \notin \left\{1, \pm 1+2^{n-1}, -1+2^n\right\}$ *be odd* (*i.e,* $s=\varepsilon+2^{t+r-1}p$, $p \in \mathbb{Z}^*_{2^{n-t-r+1}}$, $\varepsilon=\pm 1$) *and* $k \in \{0,1\}$. *Then the automorphisms of order* 1 *or* 2 *of the group* $C_{2^{n+m}} \times C_{2^n}$ *exist if and only if*

$$\begin{aligned} r &\in \mathbb{Z}_n \setminus \mathbb{Z}_{m+k},\ 3 \leqslant t+r<n, \\ v &= -\left(\varepsilon+2^{t+r-2}p\right)pu^{2^{n-t-r}-1}+2^{n-t-r+1}l \quad \left(l \in \mathbb{Z}_{2^{t-1}}\right), \end{aligned}$$

and these automorphisms are

$$\left\{\left\{s+2^n x, 2^t u\right\},\left\{2^r v+2^n y, -s+2^{n-1}k\right\}\right\},$$

where $y \in \mathbb{Z}_{2^m}$ *and*

$$x \in \mathbb{Z}_2, \ \text{if } m=1,$$

$$x \equiv s^{-1}\left(-\frac{\left(\varepsilon p+uv+2^{t+r-2}p^2\right)}{2^{n+1-t-r}}-2^{t-1}yu\right)\left(mod 2^{m-1}\right), \ \text{if } m>1.$$

The number of automorphisms of this form is $2^{n+2}\left(5\cdot 2^{n-3}-2n+1\right)$, *if* $m=1$, *and* $3\cdot 2^{2n}-2^{n+m+1}(2n-2m+1)$, *if* $m>1$.

Proof. Only the matrices of the sets M_{29}, M_{30} and M_{35}, M_{36} satisfy the conditions of the proposition. We have to consider all these cases. It is done in Appendix A.6. Proposition 4.4 is proved. □

Propositions 4.1,4.2,4.3 and 4.4 imply the following theorem:

Theorem 4.1 *If $n \geqslant 3$, $n > m \geqslant 1$, then there exist at most*

$$\begin{aligned} &3 \cdot 4^n + 32, \ \textit{if } m = 1, \\ &4 \cdot 4^n + 32, \ \textit{if } m = 2, \\ &5 \cdot 4^n + 32, \ \textit{if } m \geqslant 3, \end{aligned}$$

groups of order 2^{2n+m+1} presentable in the form $\mathcal{G} = (C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$, i.e.,

$$\mathcal{G} = \left\langle a, b, c \mid a^{2^{n+m}} = b^{2^n} = c^2 = 1, \ ab = ba, \ c^{-1}ac = a^p b^q, \ c^{-1}bc = a^r b^s \right\rangle,$$

where p, $r \in \mathbb{Z}_{2^{n+m}}$; q, $s \in \mathbb{Z}_{2^n}$, and all possible values of $\{\{p, q\}, \{r, s\}\}$ are described in Propositions 4.1, 4.2, 4.3 and 4.4.

4.2.2 The case $m = n$

In this subsection, it is assumed that $m = n$. Then system (4.7), (4.8) is

$$a^2 + 2^{n+1}ax + 2^n yq \equiv 1, \quad 2^n y\,(a + s) \equiv 0 \pmod{2^{2n}}, \tag{4.11}$$

$$c = 0. \tag{4.12}$$

Proposition 4.5 *If q is odd and $c = 0$, then the automorphisms of order 1 or 2 of the group $C_{2^{2n}} \times C_{2^n}$ are*

$$\{\{s + 2^n x,\, q\},\, \{2^n y,\, -s\}\},$$

for each $s \in \left\{1, \pm 1 + 2^{n-1}, -1 + 2^n\right\}$ and $x \in \mathbb{Z}_{2^n}$, where

$$\begin{aligned} y &\equiv -2xq^{-1}\,(mod\ 2^n), \ \textit{if } s = 1, \\ y &\equiv 2\,(1 + x)\,q^{-1}\,(mod\ 2^n), \ \textit{if } s = -1 + 2^n, \\ y &\equiv -\left(2^{n-2} \pm 1 \pm 2x\right) q^{-1}\,(mod\ 2^n), \ \textit{if } s = \pm 1 + 2^{n-1}. \end{aligned}$$

There are 2^{2n+1} automorphisms of such kind.

Proof. The matrices of the set M_1 do not satisfy assumptions of the proposition and, therefore, we need to consider only the matrices of the set M_2. In this set, only matrices $\left\| \begin{array}{cc} s & q \\ \left(1 - s^2\right) q^{-1} & -s \end{array} \right\|$, where q, $s \in \mathbb{Z}_{2^n}^*$, $s^2 \equiv 1 \pmod{2^n}$, satisfy conditions (4.12). Hence $s \in \left\{1, \pm 1 + 2^{n-1}, -1 + 2^n\right\}$. Since $(a + s) = 2^n$, the second congruence of (4.11) holds for every $y \in \mathbb{Z}_{2^n}$. Let us solve the first congruence of (4.11). If $s = 1$, then $s^2 - 1 = 0$ and the first congruence of (4.11) implies $y \equiv -2xq^{-1} \pmod{2^n}$. If $s = -1 = -1 + 2^n$, then $s^2 - 1 = -2^{n+1}$ and the first congruence of (4.11) implies $-2^{n+1}x + 2^n yq \equiv 2^{n+1} \pmod{2^{2n}}$, i.e., $y \equiv 2\,(1 + x)\,q^{-1} \pmod{2^n}$.

If $s = \pm 1 + 2^{n-1}$, then $s^2 - 1 = 2^{2n-2} \pm 2^n$ and the first congruence of (4.11) implies $2^{2n-2} \pm 2^n \pm 2^{n+1}x + 2^n yq \equiv 0 \pmod{2^{2n}}$, and therefore, $y \equiv -\left(2^{n-2} \pm 1 \pm 2x\right) q^{-1} \pmod{2^n}$.

Let us calculate the number of solutions of this form. The numbers of choices of parameters q, s, x are 2^{n-1}, 4, 2^n, respectively. Hence we have $4 \cdot 2^{n-1} \cdot 2^n = 2^{2n+1}$ solutions. Proposition 4.5 is proved. □

We need some simple lemmas.

Lemma 4.3 *Let $s \in \left\{1, \pm 1 + 2^{n-1}, -1 + 2^n\right\}$. Then the congruence*

$$\left(s^2 - 1\right) + 2^{n+1}sx \equiv 0 \pmod{2^{2n}}$$

has solutions if and only if $s \in \{1, -1 + 2^n\}$. These solutions are

1) $x \in \left\{0, 2^{n-1}\right\}$, *if* $s = 1$;
2) $x \in \left\{-1 + 2^{n-1}, -1 + 2^n\right\}$, *if* $s = -1 + 2^n$.

Proof. 1) If $s = 1$, then $s^2 - 1 = 0$ and $x \equiv 0 \pmod{2^{n-1}}$. 2) If $s = -1 + 2^n$, then $s^2 - 1 = -2^{n+1}$ and $x \equiv -1 \pmod{2^{n-1}}$. 3) If $s = \pm 1 + 2^{n-1}$, then $s^2 - 1 = 2^{2n-2} \pm 2^n$ and the congruence implies

$$2^{2n-2} \pm 2^n + 2^{n+1}sx \equiv 0 \pmod{2^{2n}},$$
$$2^{n-2} \pm 1 + 2sx \equiv 0 \pmod{2^n},$$

which is impossible. Lemma 4.3 is proved. □

Lemma 4.4 *Let $s \in \left\{1, \pm 1 + 2^{n-1}, -1 + 2^n\right\}$ and $q = 2^t u$, where $1 \leqslant t < n$, $u \in \mathbb{Z}^*_{2^{n-t}}$. Then the congruence*

$$\left(s^2 - 1\right) + 2^{n+1}sx + 2^n yq \equiv 0 \pmod{2^{2n}}$$

has solutions if and only only if $s \in \{1, -1 + 2^n\}$. These solutions are: $y \in \mathbb{Z}_{2^n}$ and

1) $x \equiv -2^{t-1}uy \pmod{2^{n-1}}$, *if* $s = 1$;
2) $x \equiv 2^{t-1}uy - 1 \pmod{2^{n-1}}$, *if* $s = -1 + 2^n$.

Proof. By assumptions, the congruence takes the form

$$\left(s^2 - 1\right) + 2^{n+1}sx + 2^{n+t}yu \equiv 0 \pmod{2^{2n}}.$$

1) If $s = 1$, we have $s^2 - 1 = 0$ and $x \equiv -2^{t-1}uy \pmod{2^{n-1}}$. 2) If $s = -1 + 2^n$, then $s^2 - 1 = -2^{n+1}$ and $x \equiv 2^{t-1}uy - 1 \pmod{2^{m-1}}$. 3) If $s = \pm 1 + 2^{n-1}$, then $s^2 - 1 = 2^{2n-2} \pm 2^n$ and

$$\left(2^{2n-2} \pm 2^n\right) + 2^{n+1}sx + 2^{n+t}yu \equiv 0 \pmod{2^{2n}},$$
$$2^{n-2} \pm 1 + 2sx + 2^t yu \equiv 0 \pmod{2^n},$$

which is impossible. Lemma 4.4 is proved. □

Denote by x_1 solutions from Lemma 4.3 and by x_2 solutions from Lemma 4.4.

Proposition 4.6 *Let q be even and $c = 0$. Then the automorphisms of order 1 or 2 of the group $C_{2^{2n}} \times C_{2^n}$ exist if and only if $s \in \{1, -1 + 2^n\}$. These automorphisms are:*

$$1)\ \left\{\{s + 2^n x_1,\, 0\},\, \left\{2^n y_2,\, s + 2^{n-1} i\right\}\right\},\quad 2)\ \left\{\{s + 2^n x_1,\, 0\},\, \{2^n y_1,\, -s\}\right\},$$
$$3)\ \left\{\{s + 2^n x_1,\, 0\},\, \left\{2^n y,\, -s + 2^{n-1}\right\}\right\},\ \textit{where } y \in 2\mathbb{Z}_{2^{n-1}},$$
$$4)\ \left\{\left\{s + 2^n x_1,\, 2^t u\right\},\, \{2^n y,\, -s\}\right\},\ \textit{where } y = z,$$
$$5)\ \left\{\left\{s + 2^n x_2,\, 2^t u\right\},\, \{2^n y_1,\, -s\}\right\},\ \textit{where } y = j + z,\ j \in \mathbb{Z}_{2^{n-t}} \setminus \{0\},$$
$$6)\ \left\{\left\{s + 2^n x_1,\, 2^{n-1}\right\},\, \left\{2^n y_2,\, s + 2^{n-1} i\right\}\right\},$$
$$7)\ \left\{\left\{s + 2^n x_1,\, 2^t u\right\},\, \left\{2^n y,\, -s + 2^{n-1}\right\}\right\},\ \textit{where } y = z,$$
$$8)\ \left\{\left\{s + 2^n x_2,\, 2^t u\right\},\, \left\{2^n y,\, -s + 2^{n-1}\right\}\right\},\ \textit{where } t \leqslant n-2,\ y = j + z,\ j \in 2\mathbb{Z}_{2^{n-t-1}} \setminus \{0\},$$

where $y_1 \in \mathbb{Z}_{2^n}$, $y_2 \in \left\{0, 2^{n-1}\right\}$, $z = 2^{n-t}k$, $k \in \mathbb{Z}_{2^t}$, $i \in \mathbb{Z}_2$. There exist $32 + 3 \cdot 4^n$ automorphisms of such kind.

Proof. Only the matrices of the sets M_3–M_{22} satisfy the conditions of the proposition. We have to consider all these cases. It is done in Appendix A.7. Proposition 4.6 is proved. □

Matrices of sets M_i, $i = 23, 24, \ldots, 35, 36$ do not satisfy condition (4.12). Propositions 4.5 and 4.6 imply

Theorem 4.2 *If $n \geqslant 3$, then there exist at most*

$$5 \cdot 4^n + 32$$

groups of order 2^{3n+1} presentable in the form $\mathcal{G} = (C_{2^{2n}} \times C_{2^n}) \leftthreetimes C_2$, i.e.,

$$\mathcal{G} = \left\langle a, b, c \mid a^{2^{2n}} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^p b^q,\ c^{-1}bc = a^r b^s \right\rangle,$$

where $p, r \in \mathbb{Z}_{2^{2n}}$ and $q, s \in \mathbb{Z}_{2^n}$. All possible values of $\{\{p, q\}, \{r, s\}\}$ are described in Propositions 4.5 and 4.6.

4.2.3 The case $m > n$

In this subsection it is assumed that $m > n$. Condition (4.8) implies $c = 0$ and $y \equiv 0 \pmod{2^{m-n}}$, i.e., y is even, $y = 2^{m-n}z$, $z \in \mathbb{Z}_{2^n}$, where $z = 0$ or z is non-zero number. Let us denote

$$z = 2^k w,$$

where

$$k \in \mathbb{Z}_n \quad \text{and} \quad w \in \mathbb{Z}^*_{2^{n-k}}$$

(if $k = 0$, then z is odd; if $k > 1$, then z is nonzero even number). System (4.7) takes now the form

$$(s + 2^n x)^2 + 2^m zq \equiv 1, \quad 2^m z\,(a + s) \equiv 0 \pmod{2^{n+m}}. \tag{4.13}$$

Lemma 4.5 *Let $s \in \{1, \pm 1 + 2^{n-1}, -1 + 2^n\}$. Then the congruence*

$$(s + 2^n x)^2 \equiv 1 \pmod{2^{n+m}}$$

has solutions if and only if $s \in \{1, -1 + 2^n\}$, and these solutions are

1) $x \in \{0, 2^{m-1}\}$, *if* $s = 1$;
2) $x \in \{-1 + 2^{m-1}, -1 + 2^m\}$, *if* $s = -1$.

Proof. It is clear that

$$s + 2^n x \in \{1, -1 + 2^{n+m}, 1 + 2^{n+m-1}, -1 + 2^{n+m-1}\},$$
$$2^n x \in \{1 - s, -1 - s + 2^{n+m}, 1 - s + 2^{n+m-1}, -1 - s + 2^{n+m-1}\}.$$

Consequently,

1) if $s = 1$, then $2^n x \in \{0, 2^{n+m-1}\}$ and hence $x \in \{0, 2^{m-1}\}$;

2) if $s = -1 + 2^n$, then $2^n x \in \{-2^n + 2^{n+m}, -2^n + 2^{n+m-1}\}$ and hence $x \in \{-1 + 2^m, -1 + 2^{m-1}\}$;

3) If $s = \pm 1 + 2^{n-1}$, then $x \in \varnothing$.

Lemma 4.5 is proved. □

Lemma 4.6 *Let $s \in \{1, \pm 1 + 2^{n-1}, -1 + 2^n\}$, $q = 2^t u$, $z = 2^k w$ $(k, t \in \mathbb{Z}_n$, $u \in \mathbb{Z}^*_{2^{n-t}}$, $w \in \mathbb{Z}^*_{2^{n-k}})$ and $zq \not\equiv 0 \,(mod\, 2^n)$ (i.e., $0 \leqslant t + k < n$). Then the congruence*

$$(s + 2^n x)^2 \equiv 1 - 2^m zq \pmod{2^{n+m}},$$

has solutions if and only if $s \in \{1, -1 + 2^n\}$ and these solutions (x, z) are

$$\left(2^{m-n+k+t-1} p + \frac{\varepsilon - 1}{2}, 2^k \left(-\left(\varepsilon + 2^{m+k+t-2} p\right) p u^{2^{n-k-t-1}-1} + 2^{n-k-t} i\right)\right),$$

where $p \in \mathbb{Z}^*_{2^{n-k-t+1}}$, $i \in \mathbb{Z}_{2^t}$ and

$$\varepsilon = \begin{cases} 1, & \text{if } s = 1, \\ -1, & \text{if } s = -1 + 2^n. \end{cases}$$

Remark. 1) the condition $k+t \geqslant 3$ is not needed now; **2)** if $t=0$, then $i \in \mathbb{Z}_{2^0} = \{0\}$, i.e., $i=0$; **3)** if $t+k>0$ or $m>n+1$, then $2^{m+k+t-2} \equiv 0 \pmod{2^{n-k-t}}$ and

$$z = 2^k \left(-\varepsilon p u^{2^{n-k-t-1}-1} + 2^{n-k-t} i\right).$$

Proof. Proof of Lemma 4.6 is similar to that of Lemma 2.3 and the whole proof is given in Appendix A.8. Lemma 4.6 is proved. □

Denote by x_1 solutions from Lemma 4.5 and by x_2, z_2 solutions from Lemma 4.6.

Proposition 4.7 *Automorphisms of order* 2 *of the group* $C_{2^{n+m}} \times C_{2^n}$ *in the case if number* q *is odd (i.e.,* $t=0$, $q=u \in \mathbb{Z}^*_{2^{n-t}} = \mathbb{Z}^*_{2^n}$*) and* $c=0$, *are*

$$1)\ \{\{s+2^n x_2,\, q\},\, \{2^m z_2,\, -s\}\}, \qquad 2)\ \{\{s+2^n x_1,\, q\},\, \{0,\, -s\}\},$$

where $s \in \{1,\, -1+2^n\}$. *There is* 2^{2n+1} *automorphisms in these forms.*

Proof. The matrices of the set M_1 do not satisfy the condition of the proposition and therefore, we need to consider only the matrices of the set M_2. In this set only matrices $\left\| \begin{array}{cc} s & q \\ \left(1-s^2\right) q^{-1} & -s \end{array} \right\|$, where $q,\, s \in \mathbb{Z}^*_{2^n}$, $s^2 \equiv 1 \,(\mathrm{mod} 2^n)$, satisfy the condition $c=0$. Hence $s \in \left\{1,\, -1+2^n,\, \pm 1+2^{n-1}\right\}$. Since $(a+s)=2^n$, the second congruence of (4.13) holds for every $z \in \mathbb{Z}_{2^n}$. Let us consider two possible cases for z : **1)** $z=2^k w$ $(k \in \mathbb{Z}_n,\ w \in \mathbb{Z}^*_{2^{n-k}})$ and **2)** $z=0$ (i.e., $y=0$).

1) Consider the first congruence of (4.13). It is solved in Lemma 4.6, where $k \in \mathbb{Z}_n$, $t=0$, $q=u \in \mathbb{Z}^*_{2^{n-t}}$ and $i=0$ (see Remark 2)). We have $x=x_2$, $z=z_2$. Let us determine the number of such kind of automorphisms. The numbers of choices of s and odd number q are 2 and 2^{n-1}, respectively. If k is fixed $(k=0, ..., n-1)$, then we have 2^{n-k} possibilities for odd number $p \in \mathbb{Z}^*_{2^{n-k+1}}$, and the number of automorphisms in this form is $2 \cdot 2^{n-1} \sum\limits_{k=0}^{n-1} 2^{n-k} = 2^{n+1}\left(2^n-1\right)$.

2) If $y=0$ then all solutions are given in Lemma 4.5. Let us determine the number of such kind of automorphisms. The numbers of choices of x, s, q are 2, 2, 2^{n-1}, respectively. Therefore, there is 2^{n+1} automorphisms of this form.

If we sum up all the numbers of automorphisms of considered two cases, we get $2^{n+1}\left(2^n-1\right)+2^{n+1}=2^{2n+1}$. Proposition 4.7 is proved. □

Proposition 4.8 *Let number* q *be even* ($q=0$ *or* $q=2^t u$, *where* $t \in \mathbb{Z}_n \setminus \{0\}$, $u \in \mathbb{Z}^*_{2^{n-t}}$) *and* $c=0$. *Then automorphisms of order* 1 *or* 2 *of*

the group $C_{2^{n+m}} \times C_{2^n}$ *exists if and only only* $s \in \{1, -1+2^n\}$*, and these automorphisms are:*

$$1)\ \left\{\{s+2^n x_1,\, 0\},\, \left\{2^m z_0,\, s+2^{n-1}j\right\}\right\},\ \textit{where } j \in \mathbb{Z}_2,$$
$$2)\ \{\{s+2^n x_1,\, 0\},\, \{2^m z,\, -s\}\},\ \textit{where } z \in \mathbb{Z}_{2^n},$$
$$3)\ \left\{\{s+2^n x_1,\, 0\},\, \left\{2^m z,\, -s+2^{n-1}\right\}\right\},\ \textit{where } z \in 2\mathbb{Z}_{2^{n-1}},$$
$$4)\ \left\{\left\{s+2^n x_1,\, 2^t u\right\},\, \left\{2^{m+n-t} l,\, -s\right\}\right\},\ \textit{where } l \in \mathbb{Z}_{2^t},$$
$$5)\ \left\{\left\{s+2^n x_2,\, 2^t u\right\},\, \{2^m z_2,\, -s\}\right\},\ \textit{where } k \in \mathbb{Z}_{n-t},$$
$$6)\ \left\{\left\{s+2^n x_1,\, 2^{n-1}\right\},\, \left\{2^m z_0,\, s+2^{n-1}j\right\}\right\},\ \textit{where } j \in \mathbb{Z}_2,$$
$$7)\ \left\{\left\{s+2^n x_1,\, 2^t u\right\},\, \left\{2^{m+n-t} l,\, -s+2^{n-1}\right\}\right\},\ \textit{where } l \in \mathbb{Z}_{2^t},$$
$$8)\ \left\{\left\{s+2^n x_2,\, 2^t u\right\},\, \left\{2^m z_2,\, -s+2^{n-1}\right\}\right\},\ \textit{where } k \in \mathbb{Z}_{n-t} \setminus \{0\},$$

where $z_0 \in \left\{0,\, 2^{n-1}\right\}$*. There exists* $3 \cdot 4^n + 32$ *automorphisms of this form.*

Proof. The only matrices satisfying the assumptions of the proposition are of the sets M_3–M_{22}. We have to consider all these cases. It is done in Appendix A.9. Proposition 4.8 is proved. □

Matrices of the sets M_i, $i = 23, 24, \ldots, 35, 36$ do not satisfy the condition $c = 0$. Propositions 4.7 and 4.8 imply

Theorem 4.3 *If* $m > n \geqslant 3$*, then there exist at most*

$$5 \cdot 4^n + 32$$

groups of order 2^{2n+m+1} *which can be presented in the form* $\mathcal{G} = (C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$*, i.e.,*

$$\mathcal{G} = \left\langle a,\, b,\, c \mid a^{2^{n+m}} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1}ac = a^p b^q,\ c^{-1}bc = a^r b^s \right\rangle,$$

where $p,\, r \in \mathbb{Z}_{2^{n+m}}$ *and* $q,\, s \in \mathbb{Z}_{2^n}$*. All possible values of* $\{\{p,\, q\},\, \{r,\, s\}\}$ *are described in Propositions 4.7 and 4.8.*

Kokkuvõte

MÕNEDEST LÕPLIKE 2-RÜHMADE KLASSIDEST JA NENDE ENDOMORFISMIPOOLRÜHMADEST

Käesolevas töös uuritakse mõningaid lõplike 2-rühmade klasse. On ilmne, et kui kaks rühma on isomorfsed, siis on isomorfsed ka nende endomorfismipoolrühmad. Vastupidine väide üldjuhul ei kehti. Töös on uuritud kahe 32-ndat järku rühmade klassi korral nendesse klassidesse kuuluvate rühmade määratavust oma endomorfismipoolrühmadega kõikide rühmade klassis. Tõestatakse, et kõik 32-ndat järku rühmad, mis on esitatavad kujul $(C_4 \times C_4) \leftthreetimes C_2$ või $(C_8 \times C_2) \leftthreetimes C_2$, on määratud oma endomorfismipoolrühmadega kõikide rühmade klassis. Üldistamaks juhtu $(C_4 \times C_4) \leftthreetimes C_2$, leitakse kõik mitteisomorfsed 2-rühmad, mis on esitatavad kujul $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$ (kus $n \geqslant 3$), ning kirjeldatakse üks leitud rühmadest tema endomorfismipoolrühma kaudu. Samuti antakse juhtudele $(C_4 \times C_4) \leftthreetimes C_2$ ja $(C_8 \times C_2) \leftthreetimes C_2$ üldistused: kirjeldatakse moodustajate ja määravate seoste abil kõik 2-rühmad, mis on esitatavad kas kujul $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$ või kujul $(C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$ (kus $n \geqslant 3$ ning $m \geqslant 1$). Kahjuks pole viimane kirjeldus antud isomorfismi täpsuseni.

Abstract

SOME CLASSES OF FINITE 2-GROUPS AND THEIR ENDOMORPHISM SEMIGROUPS

In this Thesis, we study some classes of finite 2-groups. It is clear that if two groups are isomorphic then so are their endomorphism semigroups. In general, the inverse statement does not take place. We decide for two classes of groups of order 32 whether they are determined by endomorphism semigroups in the class of all groups. We prove that all groups of order 32 which can be represented in the form $(C_4 \times C_4) \leftthreetimes C_2$ or $(C_8 \times C_2) \leftthreetimes C_2$ are determined by their endomorphism semigroups in the class of all groups. We generalize the case of groups presentable in the form $(C_4 \times C_4) \leftthreetimes C_2$ and find all non-isomorphic groups which can be represented in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$ (where $n \geqslant 3$) and characterize one of these groups by its endomorphism semigroup. We also give two more generalizations of the cases $(C_4 \times C_4) \leftthreetimes C_2$ and $(C_8 \times C_2) \leftthreetimes C_2$. Namely, we describe all possible 2-groups which can be represented in the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$ or in the form $(C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$ (where $n \geqslant 3$ and $m \geqslant 1$) by generators and defining relations. Unfortunately, we could not answered the question which groups among obtained groups are non-isomorphic.

References

[1] Adams, M., Bulman-Fleming, S. D., Gould, M. *Endomorphism properties of algebraic structures.* Proceedings of the Tennessee Topology Conference, World Scientific, 1997, pp. 1–17.

[2] Alperin, J.L. *Groups with finitely many automorphisms.* Pacific J. Math., 1962, **12**, No 1, 1–5.

[3] Baer, R. *Automorphism rings of primary Abelian operator groups.* Ann. of Math., 1943, **44**, 192–227.

[4] Clifford, A. H. *Semigroups admitting relative inverses.* Annals of Mathematics, Second Series, 1941, **42**, No. 4 , 1037–1049.

[5] Corner, A. L. *Everey countable reduced torsion-free ring is an endomorphism ring.* Proc. London Math. Soc., 1963, **13**, no. 52, 687–710.

[6] Demlová, M., Koubek, V. *Endomorphism monoids of bands.* Semigroup Forum, 1989, **38**, 305–329.

[7] Gilbert, N. D., Samman, M. *Clifford semigroups and seminear-rings of endomorphisms.* Intern. Electronic J. of Algebra, 2010, **7**, 110–119.

[8] Gramushnjak, T., Puusemp, P. *A Characterization of a Class of* 2*-Groups by Their Endomorphism Semigroups.* Ch. 14 in: S. Silvestrov et al. (eds.), *Generalized Lie Theory in Mathematics, Physics and Beyond.* Springer-Verlag, Berlin Heidelberg, 2009, pp. 151–159.

[9] Gramushnjak, T. *A characterization of a class of* 2*-groups by their defining relations.* J. of Generalized Lie Theory and Applications, 2008, **2** (3), 157–161.

[10] Gramushnjak, T., Puusemp, P. *Description of a Class of* 2*-Groups.* J. of Nonlinear Mathematical Physics, **13** (Supplement), 2006, 55–65.

[11] Gramušnjak, T., Puusemp, P. *A characterization of a class of groups of order* 32 *by their endomorphism semigroups.* Algebras, Groups and Geometries, 2005, **22**, no. 4, 387–412.

[12] Hall, M., Jr., Senior, J.K. *The groups of order* 2^n, $n \leq 6$. Macmillan, New York; Collier-Macmillan, London, 1964.

[13] Hedrlin, Z., Lambek, J. *How comprehensive is the category of semigroups?* J. Algebra, 1969, **11**, 195–212.

[14] Kaplansky, I. *Some results on abelian groups.* Proc. Nat. Acad. USA, 1952, **38**, 538–540.

[15] Krylov, P. A., Mikhalev, A. V., Tuganbaev, A. A. *Endomorphism Rings of Abelian Groups.* Kluwer Academic Publisher, 2003.

[16] Krylov, P. A., Mikhalev, A. V., Tuganbaev, A. A. *Properties of endomorphism rings of abelian groups, II.* J. Math. Sci. (New York), 2002, **113**, no. 1, 1–174.

[17] Krylov, P. A., Mikhalev, A. V., Tuganbaev, A. A. *Properties of endomorphism rings of abelian groups, I.* J. Math. Sci. (New York), 2002, **112**, no. 6, 4598–4735.

[18] Magill, K. D. *The semigroup of endomorphisms of a Boolean ring.* Semigroup Forum, 1972, **4**, 411–416.

[19] Maxson, C. J. *On semigroups of Boolean ring endomorphisms.* Semigroup Forum, 1972, **4**, 78–82.

[20] Puusemp, P. *Semidirect products of generalized quaternion groups by a cyclic group.* Silvestrov, S.; Paal, E.; Abramov, V.; Stolin, A. (Ed.). Generalized Lie Theory in Mathematics, Physics and Beyond (141 - 149). Springer, 2009

[21] Puusemp P. *Groups of Order Less Than* 32 *and Their Endomorphism Semigroups.* J. of Nonlinear Mathematical Physics, 2006, **13**, Supplement, 93–101.

[22] Puusemp, P. *Non-abelian groups of order* 16 *and their endomorphism semigroups.* J. of Mathematical Sciences, 2005, **131**, no 6, 6098–6111.

[23] Puusemp, P. *Groups of order* 24 *and their endomorphism semigroups.* Fundamentalnaya i Prikladnaya Matematika, 2005, **11**, no. 3, 155–172.

[24] Puusemp, P. *A standart wreath product of groups and its endomorphism semigroup.* Algebras, Groups and Geometries, 2003, **20**, 101–116.

[25] Puusemp, P. *Characterization of a semidirect product of groups by its endomorphism semigroup.* Smith, Paula (ed.) et al., Semigroups. Proc. of the Intern. Conference, Braga, Portugal, June 18–23, 1999. Singapore: World Scientific, 2000, 161–170.

[26] Puusemp, P. *Characterization of a semidirect product of cyclic groups by its endomorphism semigroup.* Algebras, Groups and Geometries, 2000, **17**, 479–498.

[27] Puusemp, P. *A characterization of divisible and torsion Abelian groups by their endomorphism semigroups.* Algebras, Groups and Geometries, 1999, **16**, 183–193.

[28] Puusemp, P. *On endomorphism semigroups of dihedral* 2*-groups and alternating group* A_4. Algebras, Groups and Geometries, 1999, **16**, 487–500.

[29] Puusemp, P. *On the torsion subgroups and endomorphism semigroups of abelian groups.* Algebras, Groups and Geometries, 1997, **14**, 407–422.

[30] Puusemp, P. *A characterization of the semidirect product of cyclic groups by its endomorphism semigroup.* Proc. Estonian Acad. Sci. Phys. Math., 1996, **45**, no. 2/3, 134–144.

[31] Puusemp, P. *Connection between Sylow subgroups of symmetric group and their semigroups of endomorphisms.* Proc. Estonian Acad. Sci. Phys. Math., 1993, **42**, no. 2, 144–156 (in Russian).

[32] Puusemp, P. *On the determinity of standart wreath product by its semigroup of endomorphisms.* Proc. Estonian Acad. Sci. Phys. Math., 1992, **41**, no. 4, 241–247.

[33] Puusemp, P. *On a theorem of May.* Proc. Estonian Acad. Sci. Phys. Math., 1989, **38**, no. 2, 139–145 (in Russian).

[34] Puusemp, P. *Semigroups of endomorphisms of symmetric groups.* Acta et Comment. Univ. Tartuensis, 1985, **700**, 42–49 (in Russian).

[35] Puusemp, P. *Endomorphism semigroups of generalized quaternion groups.* Acta et Comment. Univ. Tartuensis, 1976, **390**, 84–103 (in Russian).

[36] Puusemp, P. *Idempotents of the endomorphism semigroups of groups.* Acta et Comment. Univ. Tartuensis, 1975, **366**, 76–104 (in Russian).

[37] Robinson, D.J.S. *A Course in the Theory of Groups.* Springer-Verlag, GTM 80, New York, Inc., 1996.

[38] Rotman, J.J. *An Introduction to the Theory of Groups.* Springer-Verlag, New York, Inc., 1994.

[39] Samman, M., Meldrum, J. D. P. *On endomorphisms of semilattices of groups.* Algebra Colloq., 2005, **12**, no. 1, 93–100.

[40] Schein, B. M. *Bands with isomorphic endomorphism semigroups.* J. Algebra, 1985, **96**, 548–565.

[41] Schein, B. M. *Ordered sets, semilattices, distributive lattices and Boolean algebras with homomorphic endomorphism semigroups.* Fund. Math., 1970, **68**, 31–50.

[42] Tamberg, T. *Finding a class of* 2*-groups.* Proc. Estonian Acad. Sci., 2010, **59** no. 4, 370–374.

[43] Worawiset, S. *On endomorphisms of Clifford semigroups.* In: Semigroups, acts and categories with applications to graphs. Math. Stud. (Tartu), 3, Est. Math. Soc., Tartu, 2008, 143–150.

APPENDICES

A Proofs

A.1 Dividing matrices of order 1 or 2 into conjugacy classes

In this appendix, it is proved that all matrices of K_i are conjugate to the representative A_i of K_i ($i = 1, 2, \ldots, 36$).

1) Classes K_1, K_2, K_5 and K_6 contain only one matrix and therefore, the statement holds.

2) Classes K_3, K_4, K_7 and K_8. Denote $g = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\|$, $h = \left\| \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right\|$. Then $K_i = \{A_i,\ g^{-1}A_i g,\ h^{-1}A_i h\}$, where $i \in \{3, 4, 7, 8\}$.

3) Classes K_9 and K_{11}. Clearly, $K_9 = \{A_9,\ g^{-1}A_9 g\}$ and $K_{11} = \{A_{11},\ g^{-1}A_{11}g\}$, where $g = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\|$.

4) Classes K_{10} and K_{12}. Denote $g_1 = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\|$, $g_2 = \left\| \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right\|$, $g_3 = \left\| \begin{array}{cc} 1 & 0 \\ 1 & 1 \end{array} \right\|$, $g_4 = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 1 \end{array} \right\|$ and $g_5 = \left\| \begin{array}{cc} 1 & 1 \\ 1 & 0 \end{array} \right\|$. Then

$$K_i = \{A_i,\ g_1^{-1}A_i g_1,\ g_2^{-1}A_i g_2,\ g_3^{-1}A_i g_3,\ g_4^{-1}A_i g_4,\ g_5^{-1}A_i g_5\},$$

where $i \in \{10, 12\}$.

5) Classes K_{13} and K_{14}.

a) Denote in K_{13} (in K_{14}, respectively) the second matrix of M_{11} (of M_{12}, respectively) by B, in M_{21} (in M_{22}, respectively) the first, second, third and fourth matrices by C, D, F and G, respectively. Let $g_B = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\|$ and

$$g_C = \left\| \begin{array}{cc} 1 & 0 \\ -2^{t-1}u\left(\varepsilon + 2^{n-2}\right) & 1 \end{array} \right\|, \quad g_D = \left\| \begin{array}{cc} 1 & -2^{t-1}u\left(-\varepsilon + 2^{n-2}\right) \\ 0 & 1 \end{array} \right\|,$$

$$g_F = \left\| \begin{array}{cc} -2^{t-1}u\left(-\varepsilon + 2^{n-2}\right) & 1 \\ 1 & 0 \end{array} \right\|, \quad g_G = \left\| \begin{array}{cc} 0 & 1 \\ 1 & -2^{t-1}u\left(\varepsilon + 2^{n-2}\right) \end{array} \right\|,$$

where $\varepsilon = 1$ in the case of the class K_{13} and $\varepsilon = -1$ in the case of the class K_{14}. Then $g_B^{-1}A_i g_B = B \in K_i$, $g_C^{-1}A_i g_C = C \in K_i$, $g_D^{-1}A_i g_D = D \in K_i$, $g_F^{-1}A_i g_F = F \in K_i$, $g_G^{-1}A_i g_G = G \in K_i$, where $i \in \{13, 14\}$.

b) Denote in the subset M_{33} (M_{34}, respectively) of the class K_{13} (of K_{14}, respectively) the first, second, third and fourth matrices by H, I, J and K, respectively, i.e.,

$$H = \left\| \begin{array}{cc} 1 & 2^t u \\ 2^s v & -1 + 2^{n-1} \end{array} \right\|, \quad I = \left\| \begin{array}{cc} -1 + 2^{n-1} & 2^t u \\ 2^s v & 1 \end{array} \right\|,$$

$$J = \left\| \begin{array}{cc} 1+2^{n-1} & 2^t u \\ 2^s v & -1 \end{array} \right\|, \quad K = \left\| \begin{array}{cc} -1 & 2^t u \\ 2^s v & 1+2^{n-1} \end{array} \right\|.$$

Let us consider matrices in the form $H \in K_{13}$. System (2.9) (choose there $A = A_{13}$, $B = H$) takes the form

$$\left\{ \begin{array}{c} 2^{s-1} v\ y \equiv 0,\ 2^{t-1} u\ x - \left(1+2^{n-2}\right)\ y \equiv 0, \\ \left(1+2^{n-2}\right)\ z + 2^{s-1} v\ w \equiv 0,\ 2^{t-1} u\ z \equiv 0, \\ xw - yz \not\equiv 0 \,(\mathrm{mod}\ 2) \end{array} \right.$$

modulo 2^{n-1}. By the second and third congruences we have

$$\left\{ \begin{array}{l} y \equiv 2^{t-1} u \left(1+2^{n-2}\right)\ x \\ z \equiv -2^{n-t-1} v \left(1+2^{n-2}\right)\ w \end{array} \right. \qquad (x \equiv w \equiv 1 \,(\mathrm{mod}\ 2)).$$

Hence $g = g_H = \left\| \begin{array}{cc} 1 & 2^{t-1} u \left(1+2^{n-2}\right) \\ -2^{s-1} v \left(1+2^{n-2}\right) & 1 \end{array} \right\|$.

Since $t + s > n$, i.e., $t + s \geqslant n + 1$, the first congruence of the system is true:

$$2^{s-1} v\ y \equiv 2^{s-1} v 2^{t-1} u \left(1+2^{n-2}\right)\ x \equiv 2^{t+s-2} uv \left(1+2^{n-2}\right)\ x \equiv 0,$$

modulo 2^{n-1}. Analogously, the fourth congruence is valid as well.

Consider now matrices in the form $H \in K_{14}$. Then $t + s = n$ and system (2.9) (choose there $A = A_{14}$, $B = H$) takes the form

$$\left\{ \begin{array}{c} x + 2^{n-t-1} v\ y \equiv 0,\ 2^{t-1} u\ x + 2^{n-2}\ y \equiv 0, \\ 2^{n-2}\ z + 2^{n-t-1} v\ w \equiv 0,\ 2^{t-1} u\ z - w \equiv 0, \\ xw - yz \not\equiv 0 \,(\mathrm{mod}\ 2) \end{array} \right.$$

modulo 2^{n-1}. By the first and fourth congruences, we have

$$\left\{ \begin{array}{l} x \equiv -2^{n-t-1} v\ y \\ w \equiv 2^{t-1} u\ z \end{array} \right. \qquad (y \equiv z \equiv 1 \,(\mathrm{mod}\ 2))$$

modulo 2^{n-1}, i.e., $g = g_H = \left\| \begin{array}{cc} -2^{n-t-1} v & 1 \\ 1 & 2^{t-1} u \end{array} \right\|$.

Let us check the validity of the second and third congruences of the system for obtained values of x, w. Since the number $-uv + 1$ is even, i.e., $-uv + 1 = 2l$, the second congruence is true:

$$\begin{array}{rcl} 2^{t-1} u\ x + 2^{n-2}\ y & \equiv & 2^{t-1} u\ \left(-2^{n-t-1} v\ y\right) + 2^{n-2}\ y \equiv \\ & = & 2^{n-2}\ y\,(-uv+1) \equiv 2^{n-2}\ y\,(2l) \equiv 0 \end{array}$$

modulo 2^{n-1}. Similarly, the third congruence is true.

Analogously, the solutions of the system (2.9) for I, J, $K \in K_{13}$ and I, J, $K \in K_{14}$ are

$$\begin{aligned} g_I &= \left\| \begin{array}{cc} 2^{s-1}v\left(1+2^{n-2}\right) & 1 \\ 1 & -2^{t-1}u\left(1+2^{n-2}\right) \end{array} \right\|, \\ g_J &= \left\| \begin{array}{cc} 1 & 2^{t-1}u \\ -2^{n-t-1}v & 1 \end{array} \right\|, \; g_K = \left\| \begin{array}{cc} 2^{n-t-1}v & 1 \\ 1 & -2^{t-1}u \end{array} \right\| \end{aligned}$$

and

$$\begin{aligned} g_I &= \left\| \begin{array}{cc} 1 & -2^{t-1}u \\ 2^{n-t-1}v & 1 \end{array} \right\|, \\ g_J &= \left\| \begin{array}{cc} -2^{s-1}v\left(1+2^{n-2}\right) & 1 \\ 1 & 2^{t-1}u\left(1+2^{n-2}\right) \end{array} \right\|, \\ g_K &= \left\| \begin{array}{cc} 1 & -2^{t-1}u\left(1+2^{n-2}\right) \\ 2^{s-1}v\left(1+2^{n-2}\right) & 1 \end{array} \right\|, \end{aligned}$$

respectively.

c) Denote in the subset M_{35} (M_{36}, respectively) of the class K_{13} (of K_{14}, respectively) the first and second matrices by L and N, respectively, i.e.,

$$\begin{aligned} L &= \left\| \begin{array}{cc} 1+2^{t+s-1}p & 2^t u \\ 2^s v & -1-2^{t+s-1}p+2^{n-1} \end{array} \right\|, \\ N &= \left\| \begin{array}{cc} -1+2^{t+s-1}p & 2^t u \\ 2^s v & 1-2^{t+s-1}p+2^{n-1} \end{array} \right\|. \end{aligned}$$

Consider the matrix $L \in K_{13}$. System (2.9) (choose there $A = A_{13}$, $B = L$) takes the form

$$\left\{ \begin{array}{c} 2^{t+s-2}p\; x + 2^{s-1}v\; y \equiv 0,\; 2^{t-1}u\; x - \left(1+2^{n-2}+2^{t+s-2}p\right)\; y \equiv 0, \\ \left(1+2^{n-2}+2^{t+s-2}p\right)\; z + 2^{s-1}v\; w \equiv 0,\; 2^{t-1}u\; z - 2^{t+s-2}p\; w \equiv 0, \\ xw - yz \not\equiv 0 \,(\mathrm{mod}\; 2) \end{array} \right.$$

modulo 2^{n-1}. The second and third congruences of the system imply

$$\left\{ \begin{array}{l} y \equiv 2^{t-1}u\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\; x \\ z \equiv -2^{s-1}v\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\; w \end{array} \right. \qquad (x \equiv w \equiv 1 \,(\mathrm{mod}\; 2))$$

modulo 2^{n-1}. Hence $g = g_L = \left\| \begin{array}{cc} 1 & 2^{t-1}uq^{-1} \\ -2^{s-1}vq^{-1} & 1 \end{array} \right\|$, where q^{-1} is the inverse of $q = 1 + 2^{n-2} + 2^{t+s-2}p$ modulo 2^{n-1}.

Let us check whether the first and fourth congruences of the system are valid. Replacing the obtained values of y, z into the first and fourth congruences we have

$$\begin{cases} 2^{t+s-2}p\ x + 2^{s-1}v\ 2^{t-1}u\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\ x \equiv 0, \\ 2^{t-1}u\ \left(-2^{s-1}v\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\ w\right) - 2^{t+s-2}p\ w \equiv 0 \end{cases}$$

modulo 2^{n-1}. Multiplying the first and second congruences of this system by $x^{-1}\left(1+2^{n-2}+2^{t+s-2}p\right)$ and $-w^{-1}\left(1+2^{n-2}+2^{t+s-2}p\right)$ respectively, we get

$$\begin{cases} p\left(1+2^{n-2}+2^{t+s-2}p\right)+vu \equiv 0 \\ uv + p\left(1+2^{n-2}+2^{t+s-2}p\right) \equiv 0 \end{cases} \pmod{2^{n-t-s+1}}. \tag{A.1}$$

Using the condition for $L \in K_{13}$, namely

$$p\left(1+2^{t+s-2}p\right)+uv \equiv 0 \pmod{2^{n-t-s+1}},$$

the both congruences of (A.1) take the form

$$2^{n-2}p \equiv 0 \pmod{2^{n-t-s+1}}.$$

It is true since $t+s \geqslant 3$ and $2^{n-2} \equiv 0 \pmod{2^{n-t-s+1}}$.

Consider the matrix $L \in K_{14}$. System (2.9) (choose there $A = A_{14}$, $B = L$) takes the form

$$\begin{cases} \left(1+2^{t+s-2}p\right)\ x + 2^{s-1}v\ y \equiv 0,\ \ 2^{t-1}u\ x - \left(2^{n-2}+2^{t+s-2}p\right)\ y \equiv 0, \\ \left(2^{n-2}+2^{t+s-2}p\right)\ z + 2^{s-1}v\ w \equiv 0,\ \ 2^{t-1}u\ z - \left(1+2^{t+s-2}p\right)\ w \equiv 0, \\ xw - yz \not\equiv 0 \pmod 2 \end{cases}$$

modulo 2^{n-1}. The first and fourth congruences of the system imply

$$\begin{cases} x \equiv -2^{s-1}v\left(1+2^{t+s-2}p\right)^{-1}\ y \\ w \equiv 2^{t-1}u\left(1+2^{t+s-2}p\right)^{-1}\ z \end{cases} \qquad (y \equiv z \equiv 1 \pmod 2)$$

modulo 2^{n-1}. Hence

$$g = g_L = \left\| \begin{array}{cc} -2^{s-1}v\left(1+2^{t+s-2}p\right)^{-1} & 1 \\ 1 & 2^{t-1}u\left(1+2^{t+s-2}p\right)^{-1} \end{array} \right\|,$$

where $\left(1+2^{t+s-2}p\right)^{-1}$ is the inverse of $\left(1+2^{t+s-2}p\right)$ modulo 2^{n-1}.

Let us check whether the second and third congruences of the system are valid. Replacing the obtained values of x, w into the second and third congruences, we have

$$\begin{cases} 2^{t-1}u\ \left(-2^{s-1}v\left(1+2^{t+s-2}p\right)^{-1}\ y\right) - \left(2^{n-2}+2^{t+s-2}p\right)\ y \equiv 0, \\ \left(2^{n-2}+2^{t+s-2}p\right)\ z + 2^{s-1}v\ 2^{t-1}u\left(1+2^{t+s-2}p\right)^{-1}\ z \equiv 0 \end{cases}$$

modulo 2^{n-1}. Multiplying the first and second congruences of this system by $-y^{-1}\left(1+2^{t+s-2}p\right)$ and $z^{-1}\left(1+2^{t+s-2}p\right)$ respectively, we get

$$\begin{cases} vu+\left(2^{n-t-s}+p\right)\left(1+2^{t+s-2}p\right)\equiv 0 \\ \left(2^{n-t-s}+p\right)\left(1+2^{t+s-2}p\right)+uv\equiv 0 \end{cases} \pmod{2^{n-t-s+1}}. \qquad (A.2)$$

Using the condition for $L\in K_{14}$, namely

$$p\left(1+2^{t+s-2}p\right)+uv\equiv 2^{n-t-s}\pmod{2^{n-t-s+1}},$$

we have that both congruences of (A.2) are expressed in the form

$$2^{n-t-s}\left(1+2^{t+s-2}p\right)+2^{n-t-s}\equiv 0\pmod{2^{n-t-s+1}}.$$

It is obviously true.

Analogously, for the matrix $N\in K_{13}$ we have

$$g_N=\left\| \begin{array}{cc} -2^{s-1}v\left(-1+2^{t+s-2}p\right)^{-1} & 1 \\ 1 & 2^{t-1}u\left(-1+2^{t+s-2}p\right)^{-1} \end{array} \right\|,$$

where $\left(-1+2^{t+s-2}p\right)^{-1}$ is the inverse of $-1+2^{t+s-2}p$ modulo 2^{n-1}, and for the matrix $N\in K_{14}$ we have

$$g_N=\left\| \begin{array}{cc} 1 & 2^{t-1}uq^{-1} \\ -2^{s-1}vq^{-1} & 1 \end{array} \right\|,$$

where q^{-1} is the inverse of $q=-1+2^{n-2}+2^{t+s-2}p$ modulo 2^{n-1}.

6) Class K_{15}. Denote

$$B=\left\| \begin{array}{cc} 0 & b \\ b^{-1} & 0 \end{array} \right\|\in M_1, \qquad C=\left\| \begin{array}{cc} 2^tu & b \\ \left(1-\left(2^tu\right)^2\right)b^{-1} & -2^ku \end{array} \right\|\in M_1,$$

$$D=\left\| \begin{array}{cc} a & b \\ \left(1-a^2\right)b^{-1} & -a \end{array} \right\|\in M_2, \qquad F=\left\| \begin{array}{cc} a & \left(1-a^2\right)c^{-1} \\ c & -a \end{array} \right\|\in M_2.$$

Then

$$g_B=\left\| \begin{array}{cc} b^{-1}w & bz \\ z & w \end{array} \right\|,\ g_C=\left\| \begin{array}{cc} \left(1-2^{2t}u^2\right)b^{-1}w+2^tuz & bz-2^tuw \\ z & w \end{array} \right\|,$$

where $z\not\equiv w\pmod 2$,

$$g_D=\left\| \begin{array}{cc} \left(1-a^2\right)b^{-1}w+az & bz-aw \\ z & w \end{array} \right\|,\ \text{where } z\not\equiv 0\pmod 2,$$

$$g_F=\left\| \begin{array}{cc} az+cw & \left(1-a^2\right)c^{-1}z-aw \\ z & w \end{array} \right\|,\ \text{where } w\not\equiv 0\pmod 2.$$

7) Classes K_{16} and K_{17}.

a) Denote in K_{16} (in K_{17}, respectively) the second matrix of M_7 (of M_8, respectively) by B, in M_{13} (in M_{14}, respectively) the first, second, third and fourth matrices by C, D, F and G, respectively. Let $g_B = \begin{Vmatrix} 0 & 1 \\ 1 & 0 \end{Vmatrix}$, $g_C = \begin{Vmatrix} 1 & 0 \\ -2^{t-1}u & 1 \end{Vmatrix}$, $g_D = \begin{Vmatrix} 1 & 2^{t-1}u \\ 0 & 1 \end{Vmatrix}$, $g_F = \begin{Vmatrix} 2^{t-1}u & 1 \\ 1 & 0 \end{Vmatrix}$ and $g_G = \begin{Vmatrix} 0 & 1 \\ 1 & -2^{t-1}u \end{Vmatrix}$. Then $g_B^{-1}A_ig_B = B \in K_i$, $g_C^{-1}A_ig_C = C \in K_i$, $g_D^{-1}A_ig_D = D \in K_i$, $g_F^{-1}A_ig_F = F \in K_i$, $g_G^{-1}A_ig_G = G \in K_i$, where $i \in \{16, 17\}$.

b) Denote in the subset M_{27} (M_{28}, respectively) of the class K_{16} (of K_{17}, respectively) the first, second, third and fourth matrices by H, I, J and K, respectively, i.e., $H = \begin{Vmatrix} 1 & 2^tu \\ 2^sv & -1 \end{Vmatrix}$, $I = \begin{Vmatrix} -1 & 2^tu \\ 2^sv & 1 \end{Vmatrix}$, $J = \begin{Vmatrix} 1+2^{n-1} & 2^tu \\ 2^sv & -1+2^{n-1} \end{Vmatrix}$, $K = \begin{Vmatrix} -1+2^{n-1} & 2^tu \\ 2^sv & 1+2^{n-1} \end{Vmatrix}$.

Consider $H \in K_{16}$. Then $t+s > n$ and system (2.9) (choose there $A = A_{16}$ and $B = H$) takes the form

$$\begin{cases} 2^{s-1}vy \equiv 0,\ 2^{t-1}ux - y \equiv 0,\ z + 2^{s-1}vw \equiv 0,\ 2^{t-1}uz \equiv 0 \pmod{2^{n-1}}, \\ xw - yz \not\equiv 0 \pmod 2. \end{cases}$$

The second and third congruences imply

$$y \equiv 2^{t-1}u\ x,\ z \equiv -2^{s-1}v\ w \pmod{2^{n-1}}, \text{ where } x \equiv w \equiv 1 \pmod 2.$$

Since $t+s > n$, i.e., $t+s \geqslant n+1$, we have

$$2^{s-1}vy = 2^{s-1}v2^{t-1}ux = 2^{t+s-2}uvx \equiv 0 \pmod{2^{n-1}},$$

and therefore, the first congruence of the system holds. Similarly, the fourth congruence holds. Hence $g = g_H = \begin{Vmatrix} 1 & 2^{t-1}u \\ -2^{s-1}v & 1 \end{Vmatrix}$.

Consider $H \in K_{17}$. Then $t+s = n$. The system (2.9) takes the form

$$\begin{cases} 2^{n-2}x + 2^{n-t-1}vy \equiv 0,\ \ 2^{t-1}ux - \left(1+2^{n-2}\right)y \equiv 0, \\ \left(1+2^{n-2}\right)z + 2^{n-t-1}vw \equiv 0,\ \ 2^{t-1}uz + 2^{n-2}w \equiv 0 \\ xw - yz \not\equiv 0 \pmod 2 \end{cases}$$

modulo 2^{n-1}. The second and third congruences of the system imply

$$y \equiv 2^{t-1}u\left(1+2^{n-2}\right)x,\ z \equiv -2^{n-t-1}v\left(1+2^{n-2}\right)w\ \ (x \equiv w \equiv 1 \pmod 2)$$

modulo 2^{n-1}. Since the number $1 + vu\left(1+2^{n-2}\right)$ is even, i.e., $1 + vu\left(1+2^{n-2}\right) = 2l$, we have:

$$2^{n-2}x + 2^{n-t-1}vy \equiv 2^{n-2}x + 2^{n-t-1}v2^{t-1}u\left(1+2^{n-2}\right)x \equiv$$
$$\equiv 2^{n-2}x\left[1 + vu\left(1+2^{n-2}\right)\right] \equiv 2^{n-2}x2l \equiv 2^{n-1}xl \equiv 0$$

modulo 2^{n-1}. Thus the first congruence holds. Similarly, the fourth congruence holds. Hence $g = g_H = \left\| \begin{array}{cc} 1 & 2^{t-1}u\left(1+2^{n-2}\right) \\ -2^{n-t-1}v\left(1+2^{n-2}\right) & 1 \end{array} \right\|$.

Analogously, for I, J, $K \in K_{16}$ we have

$$\begin{aligned} g_I &= \left\| \begin{array}{cc} 2^{s-1}v & 1 \\ 1 & -2^{t-1}u \end{array} \right\|, \\ g_J &= \left\| \begin{array}{cc} 1 & 2^{t-1}u\left(1+2^{n-2}\right) \\ -2^{n-t-1}v\left(1+2^{n-2}\right) & 1 \end{array} \right\|, \\ g_K &= \left\| \begin{array}{cc} 2^{n-t-1}v\left(1+2^{n-2}\right) & 1 \\ 1 & -2^{t-1}u\left(1+2^{n-2}\right) \end{array} \right\|, \end{aligned}$$

and for I, J, $K \in K_{17}$ we have

$$\begin{aligned} g_I &= \left\| \begin{array}{cc} 2^{n-t-1}v\left(1+2^{n-2}\right) & 1 \\ 1 & -2^{t-1}u\left(1+2^{n-2}\right) \end{array} \right\|, \\ g_J &= \left\| \begin{array}{cc} 1 & 2^{t-1}u \\ -2^{s-1}v & 1 \end{array} \right\|, \quad g_K = \left\| \begin{array}{cc} 2^{s-1}v & 1 \\ 1 & -2^{t-1}u \end{array} \right\|. \end{aligned}$$

c) Denote in the subset M_{29} (M_{30}, respectively) of the class K_{16} (of K_{17}, respectively) the first and second matrices by L and N, respectively.

Consider $L \in K_{16}$. The system (2.9) (choose there $A = A_{16}$ and $B = L$) takes the form

$$\left\{ \begin{array}{c} 2^{t+s-2}p\ x + 2^{s-1}v\ y \equiv 0,\ \ 2^{t-1}u\ x - \left(1+2^{t+s-2}p\right)\ y \equiv 0, \\ \left(1+2^{t+s-2}p\right)\ z + 2^{s-1}v\ w \equiv 0,\ 2^{t-1}u\ z - 2^{t+s-2}p\ w \equiv 0, \\ xw - yz \not\equiv 0 \,(\mathrm{mod}\ 2)\,. \end{array} \right.$$

modulo 2^{n-1}. The second and third congruences of the system imply

$$y \equiv 2^{t-1}u\left(1+2^{t+s-2}p\right)^{-1}\ x, \quad z \equiv -2^{s-1}v\left(1+2^{t+s-2}p\right)^{-1}\ w$$

modulo 2^{n-1}, where $x \equiv w \equiv 1 \,(\mathrm{mod}\ 2)$. Hence

$$g = g_L = \left\| \begin{array}{cc} 1 & 2^{t-1}u\left(1+2^{t+s-2}p\right)^{-1} \\ -2^{s-1}v\left(1+2^{t+s-2}p\right)^{-1} & 1 \end{array} \right\|,$$

where $\left(1+2^{t+s-2}p\right)^{-1}$ is the inverse of $1+2^{t+s-2}p$ modulo 2^{n-1}.

Let us show that the first and fourth congruences are valid. Replacing y, z in the first and fourth congruences by obtained values, we have

$$\left\{ \begin{array}{l} 2^{t+s-2}p\ x + 2^{s-1}v\ 2^{t-1}u\left(1+2^{t+s-2}p\right)^{-1}\ x \equiv 0 \\ 2^{t-1}u\ \left(-2^{s-1}v\left(1+2^{t+s-2}p\right)^{-1}\ w\right) - 2^{t+s-2}p\ w \equiv 0 \end{array} \right. \left(\mathrm{mod}\ 2^{n-1}\right)$$

and, multiplying the first congruence of this system by $x^{-1}\left(1+2^{t+s-2}p\right)$, second congruence of this system by $-w^{-1}\left(1+2^{t+s-2}p\right)$, we get

$$p\left(1+2^{t+s-2}p\right)+uv\equiv 0\left(\mathrm{mod}2^{n-t-s+1}\right),$$

but this congruence holds for the matrices of M_{29}.

Consider $L\in K_{17}$. The system (2.9) (choose there $A=A_{17}$ and $B=L$) takes the form

$$\begin{cases} \left(2^{n-2}+2^{t+s-2}p\right)\ x+2^{s-1}v\ y\equiv 0, \\ 2^{t-1}u\ x-\left(1+2^{n-2}+2^{t+s-2}p\right)\ y\equiv 0 \\ \left(1+2^{n-2}+2^{t+s-2}p\right)\ z+2^{s-1}v\ w\equiv 0, \\ 2^{t-1}u\ z-\left(2^{n-2}+2^{t+s-2}p\right)\ w\equiv 0 \\ xw-yz\neq 0\,(\mathrm{mod}2) \end{cases}$$

modulo 2^{n-1}. The second and third congruences of the system imply

$$\begin{cases} y\equiv 2^{t-1}u\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\ x \\ z\equiv -2^{s-1}v\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\ w \end{cases} \qquad (x\equiv w\equiv 1\,(\mathrm{mod}2))$$

modulo 2^{n-1}. Hence $g=g_L=\left\| \begin{array}{cc} 1 & 2^{t-1}uq^{-1} \\ -2^{s-1}vq^{-1} & 1 \end{array} \right\|$, where q^{-1} is the inverse of $q=1+2^{n-2}+2^{t+s-2}p$ modulo 2^{n-1}.

Let us check whether the thirst and fourth congruency are valid. Replacing y, z in the first and fourth congruences by obtained values, we have

$$\begin{cases} \left(2^{n-2}+2^{t+s-2}p\right)\ x+2^{s-1}v\ 2^{t-1}u\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\ x\equiv 0 \\ 2^{t-1}u\ \left(-2^{s-1}v\left(1+2^{n-2}+2^{t+s-2}p\right)^{-1}\ w\right)-\left(2^{n-2}+2^{t+s-2}p\right)\ w\equiv 0 \end{cases}$$

modulo 2^{n-1}. Multiplying the first congruence of this system by $x^{-1}\left(1+2^{n-2}+2^{t+s-2}p\right)$ and the second congruence of this system by $-w^{-1}\left(1+2^{n-2}+2^{t+s-2}p\right)$, we get

$$\begin{cases} \left(2^{n-s-t}+p\right)\left(1+2^{n-2}+2^{t+s-2}p\right)+vu\equiv 0 \\ uv+\left(2^{n-s-t}+p\right)\left(1+2^{n-2}+2^{t+s-2}p\right)\equiv 0 \end{cases} \left(\mathrm{mod}\ 2^{n-t-s+1}\right).$$

Using the condition for $L\in K_{17}$, namely

$$p\left(1+2^{t+s-2}p\right)+uv\equiv 2^{n-t-s}\left(\mathrm{mod}\ 2^{n-t-s+1}\right),$$

we have that both congruences are in form $0\equiv 0$.

Analogously, for $N\in K_{16}$ we get

$$g_N=\left\| \begin{array}{cc} -2^{s-1}v\left(-1+2^{t+s-2}p\right)^{-1} & 1 \\ 1 & 2^{t-1}u\left(-1+2^{t+s-2}p\right)^{-1} \end{array} \right\|,$$

where $\left(-1+2^{t+s-2}p\right)^{-1}$ is the inverse of $\left(-1+2^{t+s-2}p\right)$ modulo 2^{n-1}, and for $N\in K_{17}$ we get $g_N=\left\| \begin{array}{cc} -2^{s-1}vq^{-1} & 1 \\ 1 & 2^{t-1}uq^{-1} \end{array} \right\|$, where q^{-1} is the inverse of $q=-1+2^{n-2}+2^{t+s-2}p$ modulo 2^{n-1}.

A.2 Computations of the number of automorphisms of some groups

The groups $\mathcal{G}_t = \langle a,\, b,\, c\rangle$ $(t = 1,\, 2, \ldots,\, 17)$ were defined in subsection 2.1.4. The map $\varphi : \mathcal{G}_t \longrightarrow \mathcal{G}_t$, given by

$$\begin{gathered} c\varphi = c^x a^i b^j, \quad a\varphi = c^y a^k b^l, \quad b\varphi = c^z a^p b^q, \\ x,\, y,\, z \in \mathbb{Z}_2, \quad i,\, j,\, k,\, l,\, p,\, q \in \mathbb{Z}_{2^n}, \end{gathered} \tag{A.3}$$

is an endomorphism of $\mathcal{G}$, if it preserves the defining relations of this group, and the endomorphism φ is an automorphism, if φ is bijective.

A.2.1 Group $\mathcal{G}_8$

Let us determine the number of automorphisms of the group

$$\begin{aligned} \mathcal{G}_8 \;=\; \Big\langle a,\, b,\, c \mid\, & a^{2^n} = b^{2^n} = c^2 = 1,\; ab = ba, \\ & c^{-1}ac = a^{-1+2^{n-1}} b^{2^{n-1}}, c^{-1}bc = b^{-1+2^{n-1}} \Big\rangle . \end{aligned}$$

We shall use the formulas

$$c^m = c^{-m}, \quad c^{-m}ac^m = a^{(-1)^m + 2^{n-1}m} b^{2^{n-1}m}, \quad c^{-m}bc^m = b^{(-1)^m + 2^{n-1}m}$$

$(m = 0,\, 1)$ and

$$(c^t a^u b^v)^2 = \begin{cases} a^{2u} b^{2v}, \text{ if } t = 0, \\ a^{u2^{n-1}} b^{(u+v)2^{n-1}}, \text{ if } t = 1, \end{cases}$$

which hold in this group.

Consider a map (A.3) $(t = 8)$ and decide under which conditions the map φ is an endomorphism of $\mathcal{G}_8$, i.e., under which conditions φ preserves the defining relations of the group $\mathcal{G}_8$.

The map φ preserves the relations $a^{2^n} = b^{2^n} = 1$, i.e., $(a\varphi)^{2^n} = (b\varphi)^{2^n} = 1$. Indeed,

$$(a\varphi)^{2^n} = (c^y a^k b^l)^{2^n} = ((c^y a^k b^l)^2)^{2^{n-1}} =$$

$$= \begin{cases} (a^{2k} b^{2l})^{2^{n-1}}, \text{ if } y = 0, \\ (a^{k2^{n-1}} b^{(k+l)2^{n-1}})^{2^{n-1}}, \text{ if } y = 1 \end{cases} = 1,$$

and, similarly, $(b\varphi)^{2^n} = 1$. The map φ preserves the relation $c^2 = 1$, i.e., $(c\varphi)^2 = (c^x a^i b^j)^2 = 1$, if and only if

$$(1 + (-1)^x)\, i + 2^{n-1} xi \equiv 0, \quad (1 + (-1)^x)\, j + 2^{n-1} x\, (i + j) \equiv 0 \tag{A.4}$$

modulo 2^n.

The map φ preserves last three defining relations of $\mathcal{G}_8$ if and only if

$$\begin{aligned}
(a\varphi)(b\varphi) &= \left(c^y a^k b^l\right)\left(c^z a^p b^q\right) = c^{y+z}\left(c^{-z} a^k c^z\right)\left(c^{-z} b^l c^z\right) a^p b^q = \\
&= c^{z+y} a^{p+(-1)^z k+2^{n-1} z k} b^{q+(-1)^z l+2^{n-1} z(k+l)} = \\
&= (b\varphi)(a\varphi) = \\
&= \left(c^z a^p b^q\right)\left(c^y a^k b^l\right) = c^{z+y}\left(c^{-y} a^p c^y\right)\left(c^{-y} b^q c^y\right) a^k b^l = \\
&= c^{z+y} a^{k+(-1)^y p+2^{n-1} y p} b^{l+(-1)^y q+2^{n-1} y(p+q)},
\end{aligned}$$

$$\begin{aligned}
(c\varphi)^{-1}(a\varphi)(c\varphi) &= b^{-j} a^{-i} c^{-x} c^y a^k b^l c^x a^i b^j = \\
&= \left(c^y c^{-y}\right) b^{-j}\left(c^y c^{-y}\right) a^{-i} c^y c^{-x} a^k\left(c^x c^{-x}\right) b^l c^x a^i b^j = \\
&= c^y a^{(1-(-1)^y) i+(-1)^x k+2^{n-1}(y i+x k)} \cdot \\
&\quad \cdot b^{(1-(-1)^y) j+(-1)^x l+2^{n-1}(y j+y i+x k+x l)} = \\
&= (a\varphi)^{-1+2^{n-1}} (b\varphi)^{2^{n-1}} = \\
&= \left(c^y a^k b^l\right)^{-1}\left(c^y a^k b^l\right)^{2^{n-1}} \left(c^z a^p b^q\right)^{2^{n-1}} = \\
&= \left(c^y a^k b^l\right)^{-1}\left(c^y a^k b^l c^y a^k b^l\right)^{2^{n-2}} \left(c^z a^p b^q c^z a^p b^q\right)^{2^{n-2}} = \\
&= c^y a^{-(-1)^y k+2^{n-1} y k+2^{n-2}(1+(-1)^y) k+2^{n-2}(1+(-1)^z) p} \cdot \\
&\quad \cdot b^{-(-1)^y l+2^{n-1} y(l+k)+2^{n-2}(1+(-1)^y) l+2^{n-2}(1+(-1)^z) q},
\end{aligned}$$

$$\begin{aligned}
(c\varphi)^{-1}(b\varphi)(c\varphi) &= b^{-j} a^{-i} c^{-x} c^z a^p b^q c^x a^i b^j = \\
&= \left(c^z c^{-z}\right) b^{-j}\left(c^z c^{-z}\right) a^{-i} c^z c^{-x} a^p\left(c^x c^{-x}\right) b^q c^x a^i b^j = \\
&= c^z a^{(1-(-1)^z) i+2^{n-1}(z i+x p)+(-1)^x p} \cdot \\
&\quad \cdot b^{(1-(-1)^z) j+2^{n-1}(z j+z i+x p+x q)+(-1)^x q} = \\
&= (b\varphi)^{-1+2^{n-1}} = \left(c^z a^p b^q\right)^{-1}\left(c^z a^p b^q\right)^{2^{n-1}} = \\
&= c^z c^{-z} b^{-q} c^z c^{-z} a^{-p} c^z\left(a^{2^{n-2}(1+(-1)^z) p} b^{2^{n-2}(1+(-1)^z) q}\right) = \\
&= c^z a^{-(-1)^z p+2^{n-1} z p+2^{n-2}(1+(-1)^z) p} \cdot \\
&\quad \cdot b^{-(-1)^z q+2^{n-1} z(q+p)+2^{n-2}(1+(-1)^z) q}.
\end{aligned}$$

Let us decide under which conditions the obtained endomorphism φ of $\mathcal{G}_8$ is an automorphism, i.e., when it preserves the orders of all elements of $\mathcal{G}_8$.

1) If $x = i = j = 0$, then $o(c\varphi) < 2 = o(c)$.

2) If a) $y = 1$ $(k, l \in \mathbb{Z}_{2^n})$ or b) $y = 0$, $k \equiv l \equiv 0 \,(\mathrm{mod}\, 2)$, then $o(a\varphi) < 2^n = o(a)$.

3) If a) $z = 1$ $(p, q \in \mathbb{Z}_{2^n})$ or b) $z = 0$, $p \equiv q \equiv 0 \,(\mathrm{mod}\, 2)$, then $o(b\varphi) < 2^n = o(b)$.

Hence $y = z = 0$ and therefore, it follows from relations $(a\varphi)(b\varphi) = (b\varphi)(a\varphi)$, $(c\varphi)^{-1}(a\varphi)(c\varphi) = (a\varphi)^{-1+2^{n-1}}(b\varphi)^{2^{n-1}}$ and $(c\varphi)^{-1}(b\varphi)(c\varphi) = (b\varphi)^{-1+2^{n-1}}$ that

$$\begin{cases} -k\left[1+(-1)^x\right] + 2^{n-1}(k+p) \equiv 2^{n-1}xk, \\ -l\left[1+(-1)^x\right] + 2^{n-1}(l+q) \equiv 2^{n-1}x(k+l), \\ -p\left[1+(-1)^x\right] + 2^{n-1}p \equiv 2^{n-1}xp, \\ -q\left[1+(-1)^x\right] + 2^{n-1}q \equiv 2^{n-1}x(p+q) \end{cases} \tag{A.5}$$

modulo 2^n. If $x = 0$, then (A.5) implies $k \equiv l \equiv p \equiv q \equiv 0 \left(\mathrm{mod}\ 2^{n-1}\right)$ and φ is not an automorphism, since the orders of elements $a\varphi$ and $b\varphi$ are less than 2^n. Hence $x = 1$ and the solution of system (A.5) is

$$k \equiv q,\ p \equiv 0 \,(\mathrm{mod}\ 2)\,.$$

The solution of system (A.4) is now

$$i \equiv j \equiv 0 \,(\mathrm{mod}\ 2)\,.$$

Therefore, we get endomorphisms

$$\begin{aligned} \varphi \ :\ & c\varphi = cb^i a^j, \quad b\varphi = b^k a^l, \quad a\varphi = b^p a^q, \\ & i,\, j,\, p \in 2\mathbb{Z}_{2^{n-1}}, \quad k,\, l,\, q \in \mathbb{Z}_{2^n}, \quad k \equiv q \,(\mathrm{mod}\ 2) \end{aligned}$$

which are candidates of automorphisms of $\mathcal{G}_8$. Clearly, this endomorphism is an automorphism of $\mathcal{G}_8$ if and only if $kq - lp \equiv 1 \,(\mathrm{mod}\ 2)$, i.e., $k \equiv q \equiv 1 \,(\mathrm{mod}\ 2)$.

For the choice of pair $(i,\, j)$ we have $2^{n-1} \cdot 2^{n-1} = 2^{2n-2}$ possibilities, for the choice of $(k,\, l,\, p,\, q)$ we have $2^{n-1} \cdot 2^n \cdot 2^{n-1} \cdot 2^{n-1} = 2^{4n-3}$ possibilities and hence the number of automorphisms of $\mathcal{G}_8$ is

$$|\mathrm{Aut}\,(\mathcal{G}_8)| = 2^{2n-2} \cdot 2^{4n-3} = 2^{6n-5}.$$

A.2.2 Group $\mathcal{G}_{15}$

Let us find all automorphisms of the group

$$\mathcal{G}_{15} = \left\langle a, b, c \mid a^{2^n} = b^{2^n} = c^2 = 1,\ ab = ba,\ c^{-1}ac = ab,\ c^{-1}bc = b^{-1} \right\rangle.$$

We shall use formulas

$$c^t = c^{-t}, \qquad c^{-t}a^r c^t = a^r b^{\frac{\left(1-(-1)^t\right)}{2}r}, \qquad c^{-t}b^r c^t = b^{(-1)^t r}$$

that hold in this group. Consider map (A.3) ($t = 15$) and check under which conditions it is an endomorphism of $\mathcal{G}_{15}$, i.e., under which conditions φ preserves the defining relations of $\mathcal{G}_8$.

Since $c^2 = 1$, we have

$$\begin{aligned} 1 &= 1\varphi = c^2\varphi = (c\varphi)^2 = \left(c^x a^i b^j\right)^2 = \left(c^{-x} a^i c^x\right)\left(c^{-x} b^j c^x\right) a^i b^j = \\ &= a^i b^{\frac{(1-(-1)^x)}{2} i} b^{(-1)^x j} a^i b^j = a^{2i} b^{(1+(-1)^x) j + \frac{(1-(-1)^x)}{2} i}, \end{aligned}$$

$$2i \equiv 0, \;\; (1+(-1)^x)\, j + \frac{(1-(-1)^x)}{2} i \equiv 0 \pmod{2^n},$$

i.e.,

$$\begin{array}{l} \text{if } x \text{ is even, then } i \equiv j \equiv 0 \pmod{2^{n-1}}, \\ \text{if } x \text{ is odd, then } i = 0, \;\; j \in \mathbb{Z}_{2^n}. \end{array} \tag{A.6}$$

Analogously, in view of $a^{2^n} = b^{2^n} = 1$,

$$\begin{aligned} 1 &= 1\varphi = \left(a^{2^n}\right)\varphi = (a\varphi)^{2^n} = \left(c^y a^k b^l\right)^{2^n} = \left[\left(c^y a^k b^l\right)\left(c^y a^k b^l\right)\right]^{2^{n-1}} = \\ &= \left[\left(c^{-y} a^k c^y\right)\left(c^{-y} b^l c^y\right) a^k b^l\right]^{2^{n-1}} = \left[a^{2k} b^{(1+(-1)^y) l + \frac{(1-(-1)^y)}{2} k}\right]^{2^{n-1}} = \\ &= b^{(1+(-1)^y) 2^{n-1} l + (1-(-1)^y) 2^{n-2} k}, \end{aligned}$$

$$\begin{aligned} 1 &= 1\varphi = \left(b^{2^n}\right)\varphi = (b\varphi)^{2^n} = (c^z a^p b^q)^{2^n} = \left[(c^z a^p b^q)\,(c^z a^p b^q)\right]^{2^{n-1}} = \\ &= \left[\left(c^{-z} a^p c^z\right)\left(c^{-z} b^q c^z\right) a^p b^q\right]^{2^{n-1}} = \left[a^{2p} b^{\frac{(1-(-1)^z)}{2} p + (1+(-1)^z) q}\right]^{2^{n-1}} = \\ &= b^{(1+(-1)^z) 2^{n-1} q + (1-(-1)^z) 2^{n-2} p}, \end{aligned}$$

$$\begin{cases} (1+(-1)^y)\, 2^{n-1} l + (1-(-1)^y)\, 2^{n-2} k \equiv 0 \\ (1+(-1)^z)\, 2^{n-1} q + (1-(-1)^z)\, 2^{n-2} p \equiv 0 \end{cases} \pmod{2^n},$$

i.e.,

$$\begin{array}{l} \text{if } y \text{ is even, then } k, \, l \in \mathbb{Z}_{2^n}, \\ \text{if } y \text{ is odd, then } k \equiv 0 \pmod{2}, \;\; l \in \mathbb{Z}_{2^n}, \end{array} \tag{A.7}$$

and

$$\begin{array}{l} \text{if } z \text{ is even, then } p, \, q \in \mathbb{Z}_{2^n}, \\ \text{if } z \text{ is odd, then } p \equiv 0 \pmod{2}, \, q \in \mathbb{Z}_{2^n}. \end{array} \tag{A.8}$$

Since $ab = ba$, we have

$$\begin{aligned} (a\varphi)(b\varphi) &= \left(c^y a^k b^l\right)(c^z a^p b^q) = c^{y+z}\left(c^{-z} a^k c^z\right)\left(c^{-z} b^l c^z\right) a^p b^q = \\ &= c^{y+z} a^{p+k} b^{(-1)^z l + \frac{(1-(-1)^z)}{2} k + q} = \\ &= (b\varphi)(a\varphi) = (c^z a^p b^q)\left(c^y a^k b^l\right) = \\ &= c^{z+y}\left(c^{-y} a^p c^y\right)\left(c^{-y} b^q c^y\right) a^k b^l = c^{z+y} a^{k+p} b^{(-1)^y q + \frac{(1-(-1)^y)}{2} p + l}, \end{aligned}$$

$$(-1)^z\, l + \frac{(1-(-1)^z)}{2} k + q \equiv (-1)^y\, q + \frac{(1-(-1)^y)}{2} p + l \,(\mathrm{mod}\, 2^n),$$

i.e.,

$$\begin{array}{l} \text{if } y = z = 0, \text{ then } k,\, l,\, q,\, p \in \mathbb{Z}_{2^n}, \\ \text{if } y = 0,\, z = 1, \text{ then } 2l - k \equiv 0 \pmod{2^n}, \\ \text{if } y = 1,\, z = 0, \text{ then } 2q - p \equiv 0 \pmod{2^n}, \\ \text{if } y = z = 1, \text{ then } 2l - k \equiv 2q - p \pmod{2^n}. \end{array} \tag{A.9}$$

The relation $c^{-1}bc = b^{-1}$ implies

$$\begin{aligned} (b\varphi)^{-1} &= (c^z a^p b^q)^{-1} = b^{-q} a^{-p} c^{-z} = \\ &= c^z \left(c^{-z} b^{-q} c^z\right) \left(c^{-z} a^{-p} c^z\right) = c^z a^{-p} b^{-\frac{(1-(-1)^z)}{2} p - (-1)^z q} = \\ &= (c\varphi)^{-1} (b\varphi) (c\varphi) = \\ &= b^{-j} a^{-i} c^{-x} c^z a^p b^q c^x a^i b^j = \\ &= c^z \left(c^{-z} b^{-j} c^z\right) \left(c^{-z} a^{-i} c^z\right) \left(c^{-x} a^p c^x\right) \left(c^{-x} b^q c^x\right) a^i b^j = \\ &= c^z a^p b^{-\frac{(1-(-1)^z)}{2} i + \frac{(1-(-1)^x)}{2} p + (1-(-1)^z) j + (-1)^x q}. \end{aligned}$$

Hence $2p \equiv 0 \pmod{2^n}$, $p \equiv 0 \pmod{2^{n-1}}$ and

$$\begin{aligned} -\frac{(1-(-1)^z)}{2} i + \frac{(1-(-1)^x)}{2} p + (1-(-1)^z)\, j + (-1)^x\, q \equiv \\ \equiv -\frac{(1-(-1)^z)}{2} p - (-1)^z\, q \pmod{2^n}, \end{aligned}$$

i.e.,

$$\begin{array}{l} \text{if } z = x = 0, \text{ then } p \equiv q \equiv 0 \pmod{2^{n-1}}, \\ \text{if } z = 0,\, x = 1, \text{ then } p \equiv 0 \pmod{2^n}, \\ \text{if } z = 1,\, x = 0, \text{ then } p \equiv 0 \pmod{2^{n-1}},\ i - 2j \equiv p \pmod{2^n}, \\ \text{if } z = x = 1, \text{ then } p \equiv 0 \pmod{2^{n-1}},\ 2j - i \equiv 2q \pmod{2^n}. \end{array} \tag{A.10}$$

The relation $c^{-1}ac = ab$ implies

$$\begin{aligned} (a\varphi)(b\varphi) &= c^{y+z} \left(c^{-z} a^k c^z\right) \left(c^{-z} b^l c^z\right) a^p b^q = \\ &= c^{y+z} a^{p+k} b^{(-1)^z l + \frac{(1-(-1)^z)}{2} k + q} = \\ &= (c\varphi)^{-1} (a\varphi) (c\varphi) = \\ &= b^{-j} a^{-i} c^{-x} c^y a^k b^l c^x a^i b^j = \\ &= c^y \left(c^{-y} b^{-j} c^y\right) \left(c^{-y} a^{-i} c^y\right) \left(c^{-x} a^k c^x\right) \left(c^{-x} b^l c^x\right) a^i b^j = \\ &= c^y a^k b^{-\frac{(1-(-1)^y)}{2} i + \frac{(1-(-1)^x)}{2} k + (1-(-1)^y) j + (-1)^x l}, \end{aligned}$$

i.e.,

$$z = 0, \quad p = 0, \tag{A.11}$$

and, using (A.11),

$$-\frac{(1-(-1)^y)}{2}i+\frac{(1-(-1)^x)}{2}k+(1-(-1)^y)\,j+(-1)^x\,l\equiv l+q\,(\mathrm{mod}\,2^n),$$

which implies

$$\begin{array}{l}\text{if } y=x=0, \text{ then } q=0, \quad i,\,j,\,k,\,l\in\mathbb{Z}_{2^n},\\ \text{if } y=0,\ x=1, \text{ then } q\equiv k-2l\,(\mathrm{mod}\ 2^n)\,,\ k,\,l,\,i,\,j\in\mathbb{Z}_{2^n},\\ \text{if } y=1,\ x=0, \text{ then } q\equiv 2j-i\,(\mathrm{mod}\ 2^n)\,,\ i,\,j,\,k,\,l\in\mathbb{Z}_{2^n},\\ \text{if } y=x=1, \text{ then } q\equiv (k-2l)-(i-2j)\,(\mathrm{mod}\ 2^n)\,.\end{array} \tag{A.12}$$

In conclusion, we have proved that φ is an endomorphism of $\mathcal{G}_{15}$ if and only if it satisfies conditions (A.6)–(A.12). By (A.11), $b\varphi=b^q$. If φ is an automorphism, then $x=1$ and $y=0$, because otherwise, in view of (A.9) and (A.10), $q\equiv 0\,(\mathrm{mod}\,2^{n-1})$ and $o(b\varphi)<2^n=o(b)$. Under conditions $x=1$, $y=0$ and $z=p=0$, the solutions of system (A.6)–(A.12) are

$$q\equiv k-2l\ \ (\mathrm{mod}\ 2^n)\,,\ \ i=0,\ \ j,\,k,\,l\in\mathbb{Z}_{2^n},$$

i.e., we get the following endomorphisms

$$\varphi:\qquad c\varphi=cb^j,\quad a\varphi=a^kb^l,\quad b\varphi=b^{k-2l},$$

where $j,\,k,\,l\in\mathbb{Z}_{2^n}$. This map φ is invertible if and only if $k\equiv 1\ \ (\mathrm{mod}\ 2)$. Therefore,

$$\begin{array}{rcl}\mathrm{Aut}(\mathcal{G}_{15}) & = & \{\varphi\mid c\varphi=cb^j,\ a\varphi=a^kb^l,\ b\varphi=b^{k-2l};\\ & & \qquad j,\,k,\,l\in\mathbb{Z}_{2^n};\ k\equiv 1\,(\mathrm{mod}\,2)\}\end{array}$$

and

$$|\mathrm{Aut}\,(\mathcal{G}_{15})|=|\{(j,\,k,\,l)\}|=2^n\cdot 2^{n-1}\cdot 2^n=2^{3n-1}.$$

A.2.3 Auxiliary groups $\mathcal{G}\,(-1)$ and $\mathcal{G}\left(\pm 1+2^{n-1}\right)$

Let us find the numbers of automorphisms of the groups $\mathcal{G}\,(-1)$ and $\mathcal{G}\left(\pm 1+2^{n-1}\right)$, where

$$\mathcal{G}\,(s)=\left\langle a,b,c\mid(*),\ a^{-1}ba=b^s,\ c^{-1}bc=b^{-1},\ c^{-1}ac=ab\right\rangle$$

and $(*)$ denotes the relations $a^{2^n}=b^{2^n}=c^2=1$. Each automorphism φ of $\mathcal{G}\,(s)$ is given by (A.3) for some values of parameters. Remark, that if $x=y=z=0$, then the map φ is not an automorphism.

Auxiliary group $\mathcal{G}(-1)$

For the group

$$\mathcal{G}(-1) = \left\langle a,b,c \mid a^{2^n} = b^{2^n} = c^2 = 1,\ a^{-1}ba = b^{-1},\ c^{-1}ac = ab,\ c^{-1}bc = b^{-1} \right\rangle,$$

we have

$$c^t = c^{-t},\ \ c^{-1}b^r c = b^{-r},\ b^r a^t = a^t b^{(-1)^t r},\ c^{-1}a^r c = a^r b^{\frac{(1-(-1)^r)}{2}},$$
$$\left(a^f b^g\right)^{2^m} = a^{2^m f} b^{2^{m-1}\left(1+(-1)^f\right)g},\ \ m \geqslant 1.$$

Consider the map φ given by (A.3) and find the conditions under which φ is an automorphism of $\mathcal{G}(-1)$.

If $y = 1$, then

$$\begin{aligned}
(a\varphi)^2 &= \left(ca^k b^l\right)^2 = \left(c^{-1}a^k c\right)\left(c^{-1}b^l c\right)a^k b^l = a^k b^{\frac{\left(1-(-1)^k\right)}{2}} b^{-l} a^k b^l = \\
&= a^k \left(b^{\frac{\left(1-(-1)^k\right)}{2}-l} a^k\right) b^l = a^{2k} b^{\frac{\left(1-(-1)^k\right)}{2}(2l-1)}, \\
(a\varphi)^{2^r} &= \left((a\varphi)^2\right)^{2^{r-1}} = \left(a^{2k} b^{\frac{\left(1-(-1)^k\right)}{2}(2l-1)}\right)^{2^{r-1}} = \\
&= a^{2^r k} b^{2^{r-2}\left(1+(-1)^{2k}\right)\frac{\left(1-(-1)^k\right)}{2}(2l-1)} = a^{2^r k} b^{2^{r-1}\frac{\left(1-(-1)^k\right)}{2}(2l-1)} = \\
&= \begin{cases} a^{2^r k} b^{2^{r-1}(2l-1)}, & \text{if } k \text{ is odd}, \\ a^{2^r k}, & \text{if } k \text{ is even}, \end{cases}
\end{aligned}$$

i.e., $o(a\varphi) > 2^n = o(a)$, if k is odd, and $o(a\varphi) < o(a)$, if k is even. Both cases are impossible, because φ is an automorphism. Therefore, $y = 0$. Similarly, $z = 0$.

So we have to find the conditions under which the map

$$c\varphi = ca^i b^j, \quad a\varphi = a^k b^l, \quad b\varphi = a^p b^q$$

is an automorphism of $\mathcal{G}(-1)$, i.e., it preserves the defining relations of this group and is invertible.

Since $c^2 = 1$, we have

$$\begin{aligned}
1 &= (c\varphi)^2 = \left(ca^i b^j\right)^2 = \left(c^{-1}a^i c\right)\left(c^{-1}b^j c\right)a^i b^j = \\
&= a^i b^{\frac{\left(1-(-1)^i\right)}{2}} b^{-j} a^i b^j = a^i \left(b^{\frac{\left(1-(-1)^i\right)}{2}-j} a^i\right) b^j = \\
&= a^{2i} b^{(-1)^i\left(\frac{\left(1-(-1)^i\right)}{2}-j\right)+j} = a^{2i} b^{\frac{\left(1-(-1)^i\right)}{2}(2j-1)}
\end{aligned}$$

and

$$2i \equiv 0, \quad \frac{\left(1-(-1)^i\right)}{2}(2j-1) \equiv 0 \pmod{2^n},$$

i.e.,

$$i \equiv 0 \pmod{2^{n-1}}, \ j \in \mathbb{Z}_{2^n}. \tag{A.13}$$

The map φ preserves the relations $a^{2^n} = b^{2^n} = 1$:

$$\begin{aligned}(a\varphi)^{2^n} &= \left(a^k b^l\right)^{2^n} = a^{2^n k} b^{2^{n-1}\left(1+(-1)^k\right)l} = 1,\\ (b\varphi)^{2^n} &= \left(a^p b^q\right)^{2^n} = a^{2^n p} b^{2^{n-1}(1+(-1)^p)q} = 1.\end{aligned}$$

Since $a^{-1}ba = b^{-1}$, we have

$$\begin{aligned}(b\varphi)^{-1} &= (a^p b^q)^{-1} = b^{-q}a^{-p} = a^{-p}b^{-(-1)^p q} =\\ &= (a\varphi)^{-1}(b\varphi)(a\varphi) = \left(a^k b^l\right)^{-1}\left(a^p b^q\right)\left(a^k b^l\right) =\\ &= b^{-l}a^{-k}a^p\left(b^q a^k\right)b^l = b^{-l}a^{p-k}\left(a^k b^{(-1)^k q}\right)b^l =\\ &= \left(b^{-l}a^p\right)b^{(-1)^k q + l} = a^p b^{-(-1)^p l + (-1)^k q + l},\end{aligned}$$

which implies

$$\begin{gathered}p \equiv -p, \quad -(-1)^p l + (-1)^k q + l \equiv -(-1)^p q \pmod{2^n},\\ p \equiv 0 \pmod{2^{n-1}}, \ (-1)^k q \equiv -q \pmod{2^n},\end{gathered}$$

i.e.,

$$p \equiv 0 \pmod{2^{n-1}} \tag{A.14}$$

and

$$\begin{gathered}\text{if } k \equiv 0 \pmod 2, \text{ then } q \equiv 0 \pmod{2^{n-1}}, \ l \in \mathbb{Z}_{2^n},\\ \text{if } k \equiv 1 \pmod 2, \text{ then } q,\ l \in \mathbb{Z}_{2^n},\end{gathered} \tag{A.15}$$

By (A.13) and (A.14), the map preserves the relation $c^{-1}bc = b^{-1}$:

$$\begin{aligned}(b\varphi)^{-1} &= (a^p b^q)^{-1} = b^{-q}a^{-p} = a^{-p}b^{-(-1)^p q} = a^{-p}b^{-q} = a^p b^{-q},\\ (c\varphi)^{-1}(b\varphi)(c\varphi) &= \left(ca^i b^j\right)^{-1}\left(a^p b^q\right)\left(ca^i b^j\right) =\\ &= b^{-j}a^{-i}\left(c^{-1}a^p c\right)\left(c^{-1}b^q c\right)a^i b^j =\\ &= b^{-j}a^{-i}\left(a^p b^{\frac{(1-(-1)^p)}{2}}\right)\left(b^{-q}\right)a^i b^j =\\ &= b^{-j}a^{p-i}\left(b^{-q}a^i\right)b^j = b^{-j}a^{p-i}\left(a^i b^{-(-1)^i q}\right)b^j =\\ &= \left(b^{-j}a^p\right)b^{j-q} = \left(a^p b^{-(-1)^p j}\right)b^{j-q} = a^p b^{-q} = (b\varphi)^{-1}.\end{aligned}$$

By (A.13), (A.14) and $c^{-1}ac = ab$, we have

$$\begin{aligned}
(c\varphi)^{-1}(a\varphi)(c\varphi) &= \left(ca^ib^j\right)^{-1}\left(a^kb^l\right)\left(ca^ib^j\right) = \\
&= b^{-j}a^{-i}\left(c^{-1}a^kc\right)\left(c^{-1}b^lc\right)a^ib^j = \\
&= b^{-j}a^{-i}\left(a^kb^{\frac{\left(1-(-1)^k\right)}{2}}\right)\left(b^{-l}\right)a^ib^j = \\
&= b^{-j}a^{k-i}\left(b^{\frac{\left(1-(-1)^k\right)}{2}-l}a^i\right)b^j = b^{-j}a^{k-i}a^ib^{\frac{\left(1-(-1)^k\right)}{2}-l}b^j = \\
&= \left(b^{-j}a^k\right)b^{\frac{\left(1-(-1)^k\right)}{2}-l+j} = \left(a^kb^{-(-1)^kj}\right)b^{\frac{\left(1-(-1)^k\right)}{2}-l+j} = \\
&= a^kb^{-(-1)^kj+\frac{\left(1-(-1)^k\right)}{2}-l+j} = a^kb^{\frac{\left(1-(-1)^k\right)}{2}(2j+1)-l} = \\
&= (a\varphi)(b\varphi) = a^k\left(b^la^p\right)b^q = a^k\left(a^pb^l\right)b^q = a^{k+p}b^{l+q}
\end{aligned}$$

and

$$p = 0, \quad \frac{\left(1-(-1)^k\right)}{2}(2j+1) - l \equiv l + q \pmod{2^n},$$

which implies

$$p = 0, \quad \text{and} \quad \begin{array}{l} \text{if } k \equiv 0 \pmod 2, \text{ then } q \equiv -2l \pmod{2^n}, \\ \text{if } k \equiv 1 \pmod 2, \text{ then } q \equiv 1 + 2j - 2l \pmod{2^n}. \end{array} \tag{A.16}$$

We have obtained that the map φ is an endomorphism of $\mathcal{G}(-1)$ if and only if it satisfies conditions (A.13)–(A.16). By (A.16), if $k \equiv 0 \pmod 2$, then $q \equiv 0 \pmod 2$, $o(b\varphi) = o(b^q) < 2^n = o(b)$ and φ does not be an automorphism. Therefore, $k \equiv 1 \pmod 2$. In this case $q \equiv 1 \pmod 2$, $\langle b^q\rangle = \langle b\rangle$, $\mathcal{G}(-1) = \langle a, b, c\rangle = \langle a^kb^l, b^q, ca^ib^j\rangle = \langle a\varphi, b\varphi, c\varphi\rangle$ and φ is an automorphism. Consequently, $\mathrm{Aut}(\mathcal{G}(-1))$ consists of maps

$$c\varphi = ca^ib^j, \quad a\varphi = a^kb^l, \quad b\varphi = b^q,$$

where

$$q \equiv 1 + 2j - 2l \pmod{2^n}, \ i = 0 \pmod{2^{n-1}}, \ k \equiv 1 \pmod 2, \ j, l \in \mathbb{Z}_{2^n}.$$

Hence

$$|\mathrm{Aut}(\mathcal{G}(-1))| = |\{(i, j, k, l)\}| = 2 \cdot 2^n \cdot 2^{n-1} \cdot 2^n = 2^{3n}.$$

Auxiliary group $\mathcal{G}\left(-1+2^{n-1}\right)$

For the group

$$\mathcal{G}\left(-1+2^{n-1}\right) = \left\langle a,b,c \mid a^{2^n}=b^{2^n}=c^2=1,\ a^{-1}ba=b^{-1+2^{n-1}},\right.$$
$$\left. c^{-1}ac=ab,\ c^{-1}bc=b^{-1}\right\rangle,$$

we have

$$c^t=c^{-t},\quad c^{-1}b^rc=b^{-r},\quad b^ra^t=a^tb^{\left((-1)^t+2^{n-1}t\right)r},$$
$$c^{-1}a^rc=a^rb^{\frac{(1-(-1)^r)}{2}\left(1-2^{n-2}\right)+2^{n-2}r},$$
$$\left(a^fb^g\right)^{2^m}=a^{2^mf}b^{2^{m-1}\left(1+(-1)^f+2^{n-1}f\right)g},\ \ m\geqslant 1.$$

Consider the map φ given by (A.3) and find the conditions under which φ is an automorphism of $\mathcal{G}\left(-1+2^{n-1}\right)$.

If $y=1$, then

$$\begin{aligned}(a\varphi)^2 &= \left(ca^kb^l\right)^2=\left(c^{-1}a^kc\right)\left(c^{-1}b^lc\right)a^kb^l=\\ &= a^k\left(b^{\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l}a^k\right)b^l=\\ &= a^{2k}b^{\left((-1)^k+2^{n-1}k\right)\left(\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l\right)+l}=a^{2k}b^m,\end{aligned}$$

where

$$m=\left((-1)^k+2^{n-1}k\right)\left(\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l\right)+l,$$

and

$$(a\varphi)^{2^r} = \left(a^{2k}b^m\right)^{2^{r-1}}=a^{2^rk}b^{2^{r-2}\left(1+(-1)^{2k}+2^{n-1}\cdot 2k\right)m}=a^{2^rk}b^{2^{r-1}m}$$

i.e., $o(a\varphi)>2^n=o(a)$, if k is odd (because then $m\equiv 1\,(\mathrm{mod}\,2)$), and $o(a\varphi)<o(a)$, if k is even. Both cases are impossible, because φ is an automorphism. Therefore, $y=0$. Similarly, $z=0$.

Hence we have to find the conditions under which the map

$$c\varphi=ca^ib^j,\quad a\varphi=a^kb^l,\quad b\varphi=a^pb^q$$

is an automorphism of $\mathcal{G}\left(-1+2^{n-1}\right)$, i.e., it preserves the defining relations of this group and is invertible.

Since $c^2 = 1$, we have

$$\begin{aligned}
1 &= (c\varphi)^2 = \left(ca^ib^j\right)^2 = \left(c^{-1}a^ic\right)\left(c^{-1}b^jc\right)a^ib^j = \\
&= a^ib^{\frac{\left(1-(-1)^i\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}i}b^{-j}a^ib^j = \\
&= a^i\left(b^{\frac{\left(1-(-1)^i\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}i-j}a^i\right)b^j = \\
&= a^i\left(a^ib^{\left((-1)^i+2^{n-1}i\right)\left(\frac{\left(1-(-1)^i\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}i-j\right)}\right)b^j = \\
&= a^{2i}b^{\left((-1)^i+2^{n-1}i\right)\left(\frac{\left(1-(-1)^i\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}i-j\right)+j}
\end{aligned}$$

and

$$2i \equiv 0,\ \left((-1)^i + 2^{n-1}i\right)\left(\frac{\left(1-(-1)^i\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}i-j\right)+j \equiv 0$$

modulo 2^n, i.e.,

$$i \equiv 0 \pmod{2^{n-1}},\ j \in \mathbb{Z}_{2^n}. \tag{A.17}$$

The map φ preserves the relations $a^{2^n} = b^{2^n} = 1$:

$$\begin{aligned}
(a\varphi)^{2^n} &= \left(a^kb^l\right)^{2^n} = a^{2^nk}b^{2^{n-1}\left(1+(-1)^k+2^{n-1}k\right)l} = 1, \\
(b\varphi)^{2^n} &= \left(a^pb^q\right)^{2^n} = a^{2^np}b^{2^{n-1}\left(1+(-1)^p+2^{n-1}p\right)q} = 1.
\end{aligned}$$

Since $a^{-1}ba = b^{-1+2^{n-1}}$, we have

$$\begin{aligned}
(b\varphi)^{-1+2^{n-1}} &= \left(a^pb^q\right)^{-1+2^{n-1}} = \left(a^pb^q\right)^{-1}\left(a^pb^q\right)^{2^{n-1}} = \\
&= \left(b^{-q}a^{-p}\right)\left(a^{2^{n-1}p}b^{2^{n-2}\left(1+(-1)^p+2^{n-1}p\right)q}\right) = \\
&= \left(b^{-q}a^{\left(-1+2^{n-1}\right)p}\right)b^{2^{n-2}\left(1+(-1)^p+2^{n-1}p\right)q} = \\
&= \left(a^{\left(-1+2^{n-1}\right)p}b^{-\left((-1)^p+2^{n-1}p\right)q}\right)b^{2^{n-2}\left(1+(-1)^p+2^{n-1}p\right)q} = \\
&= a^{\left(-1+2^{n-1}\right)p}b^{-\left((-1)^p+2^{n-1}p\right)q+2^{n-2}(1+(-1)^p)q} = \\
&= (a\varphi)^{-1}(b\varphi)(a\varphi) = \left(a^kb^l\right)^{-1}\left(a^pb^q\right)\left(a^kb^l\right) = \\
&= b^{-l}a^{-k}a^p\left(b^qa^k\right)b^l = b^{-l}a^{p-k}\left(a^kb^{\left((-1)^k+2^{n-1}k\right)q}\right)b^l = \\
&= \left(b^{-l}a^p\right)b^{\left((-1)^k+2^{n-1}k\right)q+l} = \\
&= \left(a^pb^{-\left((-1)^p+2^{n-1}p\right)l}\right)b^{\left((-1)^k+2^{n-1}k\right)q+l} = \\
&= a^pb^{-\left((-1)^p+2^{n-1}p\right)l+\left((-1)^k+2^{n-1}k\right)q+l}
\end{aligned}$$

which implies

$$\begin{cases} p \equiv \left(-1+2^{n-1}\right) p \\ -\left((-1)^p + 2^{n-1}p\right) l + \left((-1)^k + 2^{n-1}k\right) q + l \equiv \\ \qquad\qquad \equiv -\left((-1)^p + 2^{n-1}p\right) q + 2^{n-2}\left(1+(-1)^p\right) q \end{cases} \pmod{2^n}.$$

Simplifying, we get

$$p \equiv 0 \pmod{2^{n-1}}, \tag{A.18}$$

and $\left((-1)^k + 2^{n-1}k\right) q \equiv 2^{n-1}q - q \pmod{2^n}$, i.e.,

$$\begin{array}{l} \text{if } k \equiv 0 \pmod 2, \text{ then } q \equiv 0 \pmod{2^{n-1}},\ l \in \mathbb{Z}_{2^n} \\ \text{if } k \equiv 1 \pmod 2, \text{ then } q,\ l \in \mathbb{Z}_{2^n}. \end{array} \tag{A.19}$$

By (A.17) and (A.18), the map preserves the relation $c^{-1}bc = b^{-1}$:

$$\begin{aligned} (b\varphi)^{-1} &= (a^p b^q)^{-1} = b^{-q}a^{-p} = a^{-p}b^{-\left((-1)^p + 2^{n-1}p\right)q} = a^{-p}b^{-q}, \\ (c\varphi)^{-1}(b\varphi)(c\varphi) &= \left(ca^ib^j\right)^{-1}\left(a^pb^q\right)\left(ca^ib^j\right) = \\ &= b^{-j}a^{-i}\left(c^{-1}a^pc\right)\left(c^{-1}b^qc\right)a^ib^j = \\ &= b^{-j}a^{-i}\left(a^pb^{\frac{\left(1-(-1)^p\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}p}\right)\left(b^{-q}\right)a^ib^j = \\ &= b^{-j}a^{p-i}b^{2^{n-2}p-q}a^ib^j = a^pb^{2^{n-2}p-q} = a^{-p}b^{-q}. \end{aligned}$$

By (A.17), (A.18) and $c^{-1}ac = ab$, we have

$$\begin{aligned} (c\varphi)^{-1}(a\varphi)(c\varphi) &= \left(ca^ib^j\right)^{-1}\left(a^kb^l\right)\left(ca^ib^j\right) = \\ &= b^{-j}a^{-i}\left(c^{-1}a^kc\right)\left(c^{-1}b^lc\right)a^ib^j = \\ &= b^{-j}a^{-i}\left(a^kb^{\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k}\right)b^{-l}a^ib^j = \\ &= b^{-j}a^{k-i}\left(b^{\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l}a^i\right)b^j = \\ &= b^{-j}a^{k-i}\left(a^ib^{\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l}\right)b^j = \\ &= \left(b^{-j}a^k\right)b^{\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l+j} = \\ &= \left(a^kb^{-\left((-1)^k+2^{n-1}k\right)j}\right)b^{\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l+j} = \\ &= a^kb^{-\left((-1)^k+2^{n-1}k\right)j+\frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right)+2^{n-2}k-l+j} = \\ &= (a\varphi)(b\varphi) = a^k\left(b^la^p\right)b^q = \\ &= a^k\left(a^pb^{\left((-1)^p+2^{n-1}p\right)l}\right)b^q = a^{k+p}b^{l+q}, \end{aligned}$$

i.e.,

$$p = 0 \tag{A.20}$$

and

$$-\left((-1)^k + 2^{n-1}k\right) j + \frac{\left(1-(-1)^k\right)}{2}\left(1-2^{n-2}\right) + 2^{n-2}k - l + j \equiv l + q,$$

modulo 2^n which implies

$$\begin{array}{l} \text{if } k \equiv 0 \pmod 2, \text{ then } q \equiv 2^{n-2}k - 2l \pmod{2^n}, \\ \text{if } k \equiv 1 \pmod 2, \text{ then } q \equiv w \pmod{2^n}, \end{array} \tag{A.21}$$

where $w = 1 + 2\left(1 + 2^{n-2}\right) j + 2^{n-2}(k-1) - 2l$.

We have obtained that the map φ is an endomorphism of $\mathcal{G}(-1+2^{n-1})$ if and only if it satisfies conditions (A.17)–(A.21). By (A.21), if $k \equiv 0 \pmod 2$, then $q \equiv 0 \pmod 2$, $o(b\varphi) = o(b^q) < 2^n = o(b)$ and φ cannot be an automorphism. Therefore, $k \equiv 1 \pmod 2$. In this case $q \equiv 1 \pmod 2$, $\langle b^q\rangle = \langle b\rangle$, $\mathcal{G}(-1) = \langle a, b, c\rangle = \langle a^k b^l, b^q, ca^i b^j\rangle = \langle a\varphi, b\varphi, c\varphi\rangle$ and φ is an automorphism. Consequently, $\mathrm{Aut}(\mathcal{G}(-1+2^{n-1}))$ consists of maps

$$c\varphi = ca^i b^j, \quad a\varphi = a^k b^l, \quad b\varphi = b^q,$$

where

$$\begin{array}{rcl} q & \equiv & 1 + 2\left(1 + 2^{n-2}\right) j + 2^{n-2}(k-1) - 2l \pmod{2^n}, \\ i & \equiv & 0 \pmod{2^{n-1}}, \ k \equiv 1 \pmod 2, \ j, l \in \mathbb{Z}_{2^n}. \end{array}$$

Hence

$$\left|\mathrm{Aut}\left(\mathcal{G}\left(-1+2^{n-1}\right)\right)\right| = |\{(i, j, k, l)\}| = 2 \cdot 2^n \cdot 2^{n-1} \cdot 2^n = 2^{3n}.$$

Auxiliary group $\mathcal{G}\left(1+2^{n-1}\right)$

For the group

$$\begin{array}{rcl} \mathcal{G}\left(1+2^{n-1}\right) & = & \Big\langle a, b, c \mid a^{2^n} = b^{2^n} = c^2 = 1, \ a^{-1}ba = b^{1+2^{n-1}}, \\ & & \qquad\qquad c^{-1}ac = ab, \ c^{-1}bc = b^{-1}\Big\rangle, \end{array}$$

we have

$$\begin{array}{rcl} c^t & = & c^{-t}, \ \ c^{-1}b^r c = b^{-r}, \ \ b^r a^t = a^t b^{r+2^{n-1}rt}, \\ c^{-1}a^r c & = & a^r b^{r+2^{n-2}\left(r-\frac{(1-(-1)^r)}{2}\right)}, \ \ \left(a^f b^g\right)^{2^m} = a^{2^m f} b^{2^m g}, \ \ m \geqslant 2. \end{array}$$

Consider the map φ given by (A.3) and find the conditions under which φ is an automorphism of $\mathcal{G}\left(1+2^{n-1}\right)$.

If $z = 1$ then φ does not preserve the relation $c^{-1}ac = ab$. Hence $z = 0$. If $x = 0$, then it follows from the relation $(c\varphi)^2 = 1$ that $i \equiv j \equiv 0 \pmod{2^{n-1}}$ and the condition $(c\varphi)^{-1}(b\varphi)(c\varphi) = (b\varphi)^{-1}$ implies $p \equiv q \equiv 0 \pmod{2^{n-1}}$, i.e., $o(b\varphi) = o(a^p b^q) < 2^n$. This is impossible, because φ is an automorphism. Therefore, $x = 1$. Assume that $y = 1$. By $(c\varphi)^2 = 1$ and (A.22), $i = 0$ and the relation $(a\varphi)^{2^n} = 1$ implies $k \equiv 0 \pmod 2$. The condition $(c\varphi)^{-1}(b\varphi)(c\varphi) = (b\varphi)^{-1}$ implies $p = 0$, i.e., $b\varphi = b^q$. It follows from $(c\varphi)^{-1}(a\varphi)(c\varphi) = (a\varphi)(b\varphi)$ that q is even and, therefore, $o(b\varphi) < 2^n = o(b)$. This is impossible, because φ is an automorphism. Consequently, $x = 1$, $y = z = 0$.

Consider now the map (A.3) in the case $x = 1$, $y = z = 0$, and find the conditions under which φ is an automorphism of $\mathcal{G}\left(1 + 2^{n-1}\right)$, i.e., φ preserves the generating relations of this group and is invertible.

Since $c^2 = 1$, we have

$$\begin{aligned}(c\varphi)^2 &= \left(ca^i b^j\right)^2 = \left(c^{-1}a^i c\right)\left(c^{-1}b^j c\right)a^i b^j = \\ &= a^{2i} b^{i+2^{n-2}\left(i-\frac{\left(1-(-1)^i\right)}{2}\right)+2^{n-1}i(i-j)} = 1\end{aligned}$$

and

$$2i \equiv 0,\ i + 2^{n-2}\left(i - \frac{\left(1-(-1)^i\right)}{2}\right) + 2^{n-1}i\,(i-j) \equiv 0 \pmod{2^n}.$$

Hence

$$i = 0,\ j \in \mathbb{Z}_{2^n}. \tag{A.22}$$

The map φ preserves the relations $a^{2^n} = b^{2^n} = 1$:

$$\begin{aligned}(a\varphi)^{2^n} &= \left(a^k b^l\right)^{2^n} = a^{2^n k} b^{2^n l} = 1, \\ (b\varphi)^{2^n} &= (a^p b^q)^{2^n} = a^{2^n p} b^{2^n q} = 1.\end{aligned}$$

Since $a^{-1}ba = b^{1+2^{n-1}}$, we have

$$\begin{aligned}(a\varphi)^{-1}(b\varphi)(a\varphi) &= \left(a^k b^l\right)^{-1}(a^p b^q)\left(a^k b^l\right) = b^{-l}a^{-k}a^p\left(b^q a^k\right)b^l = \\ &= b^{-l}a^{p-k}\left(a^k b^{q+2^{n-1}kq}\right)b^l = \left(b^{-l}a^p\right)b^{q+2^{n-1}kq+l} = \\ &= \left(a^p b^{-l+2^{n-1}pl}\right)b^{q+2^{n-1}kq+l} = a^p b^{q+2^{n-1}(pl+kq)} = \\ &= (b\varphi)^{1+2^{n-1}} = (a^p b^q)^{1+2^{n-1}} = (a^p b^q)^1 (a^p b^q)^{2^{n-1}} = \\ &= a^p b^q a^{2^{n-1}p} b^{2^{n-1}q} = a^{\left(1+2^{n-1}\right)p} b^{\left(1+2^{n-1}\right)q}\end{aligned}$$

which implies

$$\begin{cases} p \equiv \left(1+2^{n-1}\right) p \\ q + 2^{n-1}\left(pl+kq\right) \equiv \left(1+2^{n-1}\right) q \end{cases} \pmod{2^n},$$

i.e.,

$$p \equiv 0 \pmod 2,\ q\left(k-1\right) \equiv 0 \pmod 2.$$

If $q \equiv 0 \pmod 2$, then $o(b\varphi) = o(a^p b^q) < 2^n = o(b)$ and φ cannot be an automorphism. Hence we get conditions

$$p \equiv 0 \pmod 2,\ k \equiv q \equiv 1 \pmod 2,\ l \in \mathbb{Z}_{2^n}. \tag{A.23}$$

By (A.22) and (A.23), the relation $c^{-1}bc = b^{-1}$ implies

$$\begin{aligned} \left(c\varphi\right)^{-1}\left(b\varphi\right)\left(c\varphi\right) &= \left(cb^j\right)^{-1}\left(a^p b^q\right)\left(cb^j\right) = \\ &= b^{-j}\left(c^{-1}a^p c\right)\left(c^{-1}b^q c\right)b^j = \\ &= b^{-j}\left(a^p b^{p+2^{n-2}\left(p-\frac{\left(1-(-1)^p\right)}{2}\right)}\right)\left(b^{-q}\right)b^j = \\ &= \left(b^{-j}a^p\right)b^{p+2^{n-2}p-q+j} = a^p b^{p+2^{n-2}p-q} = \\ &= \left(b\varphi\right)^{-1} = \left(a^p b^q\right)^{-1} = b^{-q}a^{-p} = a^{-p}b^{-q}. \end{aligned}$$

It follows from here that

$$2p \equiv 0,\ p + 2^{n-2}p - q \equiv -q \pmod{2^n},$$

i.e.,

$$p = 0;\quad q,\, j \in \mathbb{Z}_{2^n}. \tag{A.24}$$

By (A.22), (A.23) and (A.24), the relation $c^{-1}ac = ab$ implies

$$\begin{aligned} \left(c\varphi\right)^{-1}\left(a\varphi\right)\left(c\varphi\right) &= \left(cb^j\right)^{-1}\left(a^k b^l\right)\left(cb^j\right) = \\ &= b^{-j}\left(c^{-1}a^k c\right)\left(c^{-1}b^l c\right)b^j = \\ &= b^{-j}\left(a^k b^{k+2^{n-2}\left(k-\frac{\left(1-(-1)^k\right)}{2}\right)}\right)b^{-l}b^j = \\ &= \left(b^{-j}a^k\right)b^{k+2^{n-2}(k-1)-l+j} = \\ &= a^k b^{-j+2^{n-1}j}b^{k+2^{n-2}(k-1)-l+j} = \\ &= a^k b^{k+2^{n-2}(k-1)+2^{n-1}j-l} = \\ &= \left(a\varphi\right)\left(b\varphi\right) = a^k b^l b^q = a^k b^{l+q}, \end{aligned}$$

Therefore,

$$k + 2^{n-2}(k-1) + 2^{n-1}j - l \equiv l + q \pmod{2^n},$$

and hence

$$q \equiv k + 2^{n-2}(k-1) + 2^{n-1}j - 2l \pmod{2^n}, \tag{A.25}$$

If conditions (A.22)–(A.25) hold, then $\langle a, b, c\rangle = \langle a\varphi, b\varphi, c\varphi\rangle$ and φ is an automorphism.

We have obtained that $\mathrm{Aut}(\mathcal{G}(1+2^{n-1}))$ consists of maps

$$c\varphi = cb^j, \quad a\varphi = a^k b^l, \quad b\varphi = b^q,$$

where

$$q \equiv k + 2^{n-2}(k-1) + 2^{n-1}j - 2l \pmod{2^n},\ k \equiv 1 \pmod 2,\ j, l \in \mathbb{Z}_{2^n}.$$

Hence

$$\left|\mathrm{Aut}\left(\mathcal{G}\left(1+2^{n-1}\right)\right)\right| = |\{(j, k, l)\}| = 2^n \cdot 2^{n-1} \cdot 2^n = 2^{3n-1}.$$

A.3 The proof of Lemma 3.2

The congruence $(p^2+rq)^2 \equiv 1 \pmod{2^n}$ implies

$$p^2 + 2^{f+g}uv \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\},$$

$$p^2 = a \in \left\{\pm 1 - 2^{f+g}uv,\ \pm 1 + 2^{n-1} - 2^{f+g}uv\right\}.$$

Since $a \equiv 1 \pmod 8$, we have **I)** $a = 1 - 2^{f+g}uv$ or **II)** $a = 1 + 2^{n-1} - 2^{f+g}uv$.

I) If $a = 1 - 2^{f+g}uv$ we have by Lemma 2.3,

$$\begin{aligned} p &= \varepsilon + 2^{f+g-1}x,\ r = 2^f u, \\ q &= 2^g\left(-\left(\varepsilon + 2^{f+g-2}x\right)xu^{2^{n-f-g-1}-1} + 2^{n-f-g}k\right), \end{aligned}$$

where $n > f+g \geqslant 3$, $\varepsilon = \pm 1$, $x \in \mathbb{Z}^*_{2^{n-f-g+1}}$, $k \in \mathbb{Z}_{2^f}$. We have obtained the solution a), where $l = 0$.

II) If $a = 1 + 2^{n-1} - 2^{f+g}uv = 1 + 2^{f+g}\left(2^{n-f-g-1} - uv\right)$, we have two possibilities: **1)** $f+g = n-1$ or **2)** $3 \leqslant f+g < n-1$.

1) If $f+g = n-1$, then (since $1-uv$ is even) $a = 1 + 2^{n-1}(1-uv) \equiv 1 \pmod{2^n}$ and the congruence of the lemma has the form $p^2 \equiv 1 \pmod{2^n}$,

i.e., by Lemma 3.2, $p \in \left\{1, \pm 1 + 2^{n-1}, -1 + 2^n\right\}$ and we have obtained solutions b).

2) If $3 \leqslant f + g < n - 1$, then $a = 1 + 2^{f+g}\left(2^{n-f-g-1} - uv\right)$, where $2^{n-f-g-1} - uv$ is odd. Denote $f + g = m$. Then the congruence takes the form

$$(p-1)(p+1) \equiv 2^m\left(2^{n-m-1} - uv\right) \pmod{2^n}.$$

Denote

$$p - 1 = 2^w y \quad \text{and} \quad p + 1 = 2^{m-w} z,$$

where

$$w \in \mathbb{Z}_m \setminus \{0\}, \ y \in \mathbb{Z}^*_{2^{n-w}}, \ z \in \mathbb{Z}^*_{2^{n+w-m}}.$$

Then

$$2^w y \cdot 2^{m-w} z \equiv 2^m\left(2^{n-m-1} - uv\right) \pmod{2^n}$$

and

$$yz \equiv 2^{n-m-1} - uv \pmod{2^{n-m}}. \tag{A.26}$$

On the other side,

$$p = 1 + 2^w y = -1 + 2^{m-w} z,$$

i.e., $2\left(1 + 2^{w-1} y\right) = 2^{m-w} z$ and

$$1 + 2^{w-1} y = 2^{m-w-1} z.$$

The last equation has a solution only in the cases **i)** $w = 1$ and **ii)** $w = m - 1$.

i) In the case $w = 1$, we have

$$y = -1 + 2^{m-2} z, \quad p = -1 + 2^{m-1} z, \quad z \in \mathbb{Z}^*_{2^{n-m+1}}.$$

ii) Analogously, in the case $w = m - 1$, we have

$$z = 1 + 2^{m-2} y, \ p = 1 + 2^{m-1} y, \quad y \in \mathbb{Z}^*_{2^{n-m+1}}.$$

Note that for both considered cases **i)** and **ii)**, we can write

$$yz = \left(\varepsilon + 2^{m-2} x\right) x, \ p = \varepsilon + 2^{m-1} x, \quad x \in \mathbb{Z}^*_{2^{n-m+1}},$$

where $\varepsilon = \pm 1$. Then, by (A.26), we have

$$uv \equiv 2^{n-m-1} - \left(\varepsilon + 2^{m-2} x\right) x \pmod{2^{n-m}}$$

and

$$\begin{aligned} v &\equiv \left[2^{n-m-1} - \left(\varepsilon + 2^{m-2} x\right) x\right] u^{-1} = \\ &= \left[2^{n-m-1} - \left(\varepsilon + 2^{m-2} x\right) x\right] u^{2^{n-m-1}-1} \pmod{2^{n-m}}. \end{aligned}$$

Since $0 < v < 2^{n-g}$, we have $2^{n-g}/2^{n-m} = 2^f$ different values modulo 2^n for v in the form $v_k = v + 2^{n-m}k$, where $k \in \mathbb{Z}_{2^f}$. Therefore, the solution of the congruence

$$p^2 \equiv 1 + 2^{f+g}\left(2^{n-f-g-1} - uv\right) \pmod{2^n},$$

where $3 \leqslant f + g < n - 1$, is

$$\begin{aligned} p &= \varepsilon + 2^{f+g-1}x,\ r = 2^f u, \\ q &= 2^g\left(\left[2^{n-f-g-1} - \left(\varepsilon + 2^{f+g-2}x\right)x\right]u^{2^{n-f-g-1}-1} + 2^{n-f-g}k\right), \end{aligned}$$

where

$$\varepsilon = \pm 1,\ x \in \mathbb{Z}^*_{2^{n-f-g+1}},\ k \in \mathbb{Z}_{2^f}.$$

This gives solution a), where $l = 1$.

A.4 Proof of Proposition 4.2

If q or c is equal to 0, then the considered matrices belong to the sets M_3–M_{22}. We have to consider all these cases like in the proof of Proposition 4.1.

Let us begin from the sets M_3, M_4, M_5, M_6 and M_9, M_{10}. Matrices of this sets have the form $\left\| \begin{array}{cc} s & 0 \\ 0 & s + 2^{n-1}k \end{array} \right\|$, where $k \in \mathbb{Z}_2$. Since $a + s = 2s + 2^{n-1}k \not\equiv 0 \pmod{2^{n-1}}$, it follows from system (4.9)

$$s^2 + 2^{n+1}sx \equiv 1, \quad 2^{n+1}y\left(s + 2^{n-2}k\right) \equiv 0 \pmod{2^{n+m}}.$$

The second congruence implies that $y \in \mathbb{Z}_2$ if $m = 1$ and $y \equiv 0 \pmod{2^{m-1}}$ if $m > 1$. The first congruence is solved in Lemma 4.1 and we get the automorphisms 1) of the proposition.

Now consider the sets M_7 and M_8. Matrices of these sets have the form $\left\| \begin{array}{cc} s & 0 \\ 0 & -s \end{array} \right\|$. Since $a + s = 2^n \equiv 0 \pmod{2^{n-1}}$, system (4.9) implies

$$s^2 + 2^{n+1}sx \equiv 1,\ 2^{2n}y \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $y \in \mathbb{Z}_{2^m}$ and the first congruence is solved in Lemma 4.1. Thus we have the automorphisms 2) of the proposition.

Consider the sets M_{11} and M_{12}. Matrices of this sets have the form $\left\| \begin{array}{cc} s & 0 \\ 0 & -s + 2^{n-1} \end{array} \right\|$. Since $a + s \equiv 0 \pmod{2^{n-1}}$, it follows from system (4.9)

$$s^2 + 2^{n+1}sx \equiv 1, \quad 2^n y \cdot 2^{n-1} \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $y \in \mathbb{Z}_{2^m}$ and the first congruence is solved in Lemma 4.1. Thus we have the automorphisms 3) of the proposition.

Let us consider the sets M_{13} and M_{14}. Matrices of these sets have the forms $\left\| \begin{array}{cc} s & 0 \\ 2^t u & -s \end{array} \right\|$ and $\left\| \begin{array}{cc} s & 2^t u \\ 0 & -s \end{array} \right\|$. For both forms of matrices, $a + s = 2^n \equiv 0 \pmod{2^{n-1}}$. For the first form, by (4.10), $t = m, ..., n-1$ and it follows from system (4.9)

$$s^2 + 2^{n+1} sx \equiv 1, \quad 2^n \left(2^t u + 2^n y\right) + 2^{n+t} xu \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $x, y \in \mathbb{Z}_{2^m}$ and the first congruence is solved in Lemma 4.1. Thus we get the automorphisms 4) of the proposition. For the second form, (4.9) implies

$$s^2 + 2^{n+1} sx + 2^{n+t} yu \equiv 1, \quad 2^{2n} y \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $x, y \in \mathbb{Z}_{2^m}$. For the first congruence we consider two cases: if $t = m, ..., n-1$, then it is solved in Lemma 4.1 (we get the automorphisms 5) of the proposition), and, if $t = 1, ..., m-1$ (this case it not possible if $m = 1$), then it is solved in Lemma 4.2 (we get the automorphisms 6) of the proposition).

Now consider the sets M_{15}, M_{16}, M_{17}, M_{18} and M_{19}, M_{20}. Matrices of these sets have forms $\left\| \begin{array}{cc} s & 2^{n-1} \\ 0 & s + 2^{n-1} k \end{array} \right\|$ and $\left\| \begin{array}{cc} s & 0 \\ 2^{n-1} & s + 2^{n-1} k \end{array} \right\|$, where $k \in \mathbb{Z}_2$. For both forms of matrices, $a + s = 2s + 2^{n-1} k \not\equiv 0 \pmod{2^{n-1}}$. For the first form, system (4.9) implies

$$s^2 + 2^{n+1} sx \equiv 1, \quad 2^{n+1} y \left(s + 2^{n-2} k\right) \equiv 0 \pmod{2^{n+m}}.$$

The second congruence implies that $y \in \mathbb{Z}_2$ if $m = 1$ and $y \equiv 0 \pmod{2^{m-1}}$ if $m > 1$. The first congruence is solved in Lemma 4.1 and we get the automorphisms 7) of the proposition. The case of second form, by (4.10), is possible only if $m = n - 1$ and it follows from system (4.9) that

$$s^2 + 2^{n+1} sx \equiv 1, \quad 2^n (1 + 2y) \left(s + 2^{n-2} k\right) \equiv 0 \pmod{2^{2n-1}}.$$

The second congruence implies $1 + 2y \equiv 0 \pmod{2^{n-1}}$ which is impossible.

Let us consider the sets M_{21} and M_{22}. Matrices of these sets have the forms $\left\| \begin{array}{cc} s & 2^t u \\ 0 & -s + 2^{n-1} \end{array} \right\|$ and $\left\| \begin{array}{cc} s & 0 \\ 2^t u & -s + 2^{n-1} \end{array} \right\|$. For the both form of matrices, $a + s = 2^{n-1} \equiv 0 \pmod{2^{n-1}}$. For the first form, by system (4.9),

$$s^2 + 2^{n+1} sx + 2^{n+t} yu \equiv 1, \quad 2^{n-1} 2^n y \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $y \in \mathbb{Z}_{2^m}$. The first congruence is solved **i**) in the case of $m \leqslant t < n$ in Lemma 4.1 (so we get the automorphisms 8) of the proposition) and **ii**) in the case of $1 \leqslant t < m$ (this case is possible only if $m > 1$) in Lemma 4.2 (so we get the automorphisms 9) of the proposition). By (4.10), the second form is possible only if $t = m, ..., n-1$ and system (4.9) implies

$$s^2 + 2^{n+1}sx \equiv 1, \quad 2^{n-1}\left(2^t u + 2^n y\right) \equiv 0 \pmod{2^{n+m}}.$$

The second congruence has a solution only if $t > m$; the first congruence is solved in Lemma 4.1 (so we get the automorphisms 10) of the proposition).

Let us now find the number of automorphisms described in the proposition (it is equal to the number of choices of $(s,\, 2^t u,\, x,\, y)$). For $(s,\, x,\, y)$ we have $2 \cdot 2 \cdot 2^m = 2^{m+2}$ choices if $a + s \equiv 0 \pmod{2^{n-1}}$, i.e., if $y \in \mathbb{Z}_{2^m}$, and $2 \cdot 2 \cdot 2 = 8$ choices if $a + s \neq 0 \pmod{2^{n-1}}$, i.e., if $y \equiv 0 \pmod{2^{m-1}}$. Hence there is 16 automorphisms of forms 1) and 7), 2^{m+2} automorphisms of forms 2) and 3), $2^{m+2}\sum\limits_{t=m}^{n-1} 2^{n-t-1} = 2^{m+2}\left(2^{n-m} - 1\right)$ automorphisms of forms 4), 5) and 8), $2^{m+2}\sum\limits_{t=1}^{m-1} 2^{n-t-1} = 2^{n+m+1} - 2^{n+2}$ automorphisms of forms 6) and 9) (note, that if $m = 1$, then there is $2^{n+m+1} - 2^{n+2} = 0$ automorphisms of forms 6) and 9)), $2^{m+2}\sum\limits_{t=m+1}^{n-1} 2^{n-t-1} = 2^{m+2}\left(2^{n-m-1} - 1\right)$ automorphisms of form 10). Hence if $m \geqslant 1$ then the number of automorphisms is $32 - 2^{m+3} + 3 \cdot 2^{n+1} + 2^{n+m+2}$.

A.5 Proof of Proposition 4.3

Conditions of Proposition satisfy matrices of the sets M_i, $i = 23, 24, \ldots, 28$, and $i = 31, 32, 33, 34$.

Let us start from the sets M_{23}, M_{24}, M_{25}, M_{26} and M_{31}, M_{32}. Matrices of these sets have the form $\left\| \begin{matrix} s & 2^{n-1} \\ 2^{n-1} & s + 2^{n-1}k \end{matrix} \right\|$, where $k \in \mathbb{Z}_2$. By (4.10), $c = 2^{n-1} \equiv 0 \pmod{2^m}$ which is possible only if $m = n - 1$. The second congruence of system (4.9) takes the form $2^n(1 + 2y) \equiv 0 \pmod{2^{2n-1}}$, and it has no solution.

Let us consider the sets M_{27}, M_{28} and M_{33}, M_{34}. Matrices of these sets have the form $\left\| \begin{matrix} s & 2^t u \\ 2^r v & -s + 2^{n-1}k \end{matrix} \right\|$, where $t \geqslant n - r$ and $k \in \mathbb{Z}_2$. In view of (4.10), we have $c = 2^r v \equiv 0 \pmod{2^m}$ which is possible only if $r \geqslant m$. System (4.9) implies

$$\begin{cases} s^2 + 2^{n+1}sx + (2^r v + 2^n y)\, 2^t u \equiv 1 \\ \left(2^n + 2^{n-1}k\right)(2^r v + 2^n y) + 2^n x 2^r v \equiv 0 \end{cases} \pmod{2^{n+m}},$$

If $k = 0$ (the sets M_{27}, M_{28}), then the second congruence holds for every $r \geqslant m$, and if $k = 1$ (the sets M_{33}, M_{34}), then it holds if $r \geqslant m + 1$. The first congruence implies: **1)** if $s = \pm 1$ and $r + t = n$, then the congruence has no solution; if $s = \pm 1$, $r + t > n$ and $m = 1$, then solution is x, $y \in \mathbb{Z}_2$; if $s = \pm 1$, $r + t > n$ and $m > 1$, then

$$\begin{aligned} x &\equiv -2^{r+t-n-1}\left(v + 2^{n-r}y\right)u \pmod{2^{m-1}}, \qquad \text{if } s = 1, \\ x &\equiv -1 + 2^{r+t-n-1}\left(v + 2^{n-r}y\right)u \pmod{2^{m-1}}, \qquad \text{if } s = -1 + 2^n, \end{aligned}$$

(we get the automorphisms 1) of the proposition); **2)** if $s = \pm 1 + 2^{n-1}$ and $r + t > n$, then the congruence has no solution; if $s = \pm 1 + 2^{n-1}$, $r + t = n$ and $m = 1$, then the solution is x, $y \in \mathbb{Z}_2$; if $s = \pm 1 + 2^{n-1}$, $r + t = n$ and $m > 1$, then

$$x \equiv \frac{\mp\left(v + 2^{n-r}y\right)u - 1}{2} \mp 2^{n-3} \pmod{2^{m-1}},$$

(we get the automorphisms 2) of the proposition).

Let us now determine the number of automorphisms of these forms (for every m and $k = 0, 1$). For every form of matrices, the numbers of possible values of s, x and y are 2, 2 and 2^m, respectively. If the number r ($r = m + k, ..., n - 1$) is fixed, then there is 2^{n-r-1} possible values of v. Since $t + r \geqslant n$, we have $t = n - r, n - r + 1, ..., n - 1$. If t is fixed, we have 2^{n-t-1} possible values for odd number u. Hence the number of automorphisms is

$$\sum_{k=0}^{1} 2^{m+2} \sum_{r=m+k}^{n-1} 2^{n-r-1} \sum_{t=n-r}^{n-1} 2^{n-t-1} = (2n - 2m - 1)\, 2^{n+m+1} - 3 \cdot 2^{n+1} + 2^{m+3}.$$

A.6 Proof of Proposition 4.4

Only matrices of the sets M_{29}, M_{30} and M_{35}, M_{36} satisfy to the conditions of Proposition 4.4.

Matrices of these sets have the form $\left\| \begin{array}{cc} s & 2^t u \\ 2^r v & -s + 2^{n-1}k \end{array} \right\|$, where $3 \leqslant t + r < n$. By (4.10), we have $c = 2^r v \equiv 0 \pmod{2^m}$ and, therefore, $r \geqslant m$. System (4.9) implies

$$\begin{cases} s^2 + 2^{n+1}sx + \left(2^r v + 2^n y\right)2^t u \equiv 1 \\ \left(2^n + 2^{n-1}k\right)\left(2^r v + 2^n y\right) + 2^n x 2^r v \equiv 0 \end{cases} \pmod{2^{n+m}}.$$

The second congruence holds for every $r \geqslant m$ if $k = 0$ (the sets M_{29}, M_{30}) and for every $r \geqslant m + 1$ if $k = 1$ (the sets M_{35}, M_{36}). Since $s^2 - 1 =$

$2^{t+r}p\varepsilon + 2^{2(t+r-1)}p^2$, the first congruence implies

$$2^{t+r}p\varepsilon + 2^{2(t+r-1)}p^2 + 2^{n+1}sx + 2^{t+r}\left(v + 2^{n-r}y\right)u \equiv 0 \pmod{2^{n+m}},$$
$$2^{n+1-t-r}sx + 2^{n-t}yu + \left(p\left(\varepsilon + 2^{t+r-2}p\right) + uv\right) \equiv 0 \pmod{2^{n+m-t-r}}$$

and it has solutions if and only if

$$p\left(\varepsilon + 2^{t+r-2}p\right) + uv \equiv 0 \pmod{2^{n+1-t-r}}. \tag{A.27}$$

If $m = 1$, then the solutions are $x, y \in \mathbb{Z}_2$. If $m > 1$, then

$$x \equiv s^{-1}\left(-\frac{p\left(\varepsilon + 2^{t+r-2}p\right) + uv}{2^{n+1-t-r}} - 2^{t-1}yu\right) \pmod{2^{m-1}}.$$

Consider condition (A.27) and note that in the proof of Lemma 2.3 we get a similar condition for u, v and p : $vu \equiv -\left(\varepsilon + 2^{t+r-2}p\right)p \pmod{2^{n-t-r}}$, but this condition follows from (A.27). Hence like in the proof of Lemma 2.3,

$$v \equiv -\left(\varepsilon + 2^{t+r-2}p\right)pu^{-1} \pmod{2^{n+1-t-r}},$$

where u^{-1} is the inverse of odd number u modulo $2^{n+1-t-r}$, i.e., $u^{-1} = u^{2^{n-t-r}-1}$. Since $v \in \mathbb{Z}^*_{2^{n-r}}$, we have $\frac{2^{n-r}}{2^{n+1-t-r}} = 2^{t-1}$ values for v modulo 2^{n-r} in the form

$$v = -\left(\varepsilon + 2^{t+r-2}p\right)pu^{2^{n-t-r}-1} + 2^{n-t-r+1}l,$$

where $l \in \mathbb{Z}_{2^{t-1}}$.

Let us determine the number of automorphisms of the form considered. The choice of triples $(s,\, q,\, c)$ depends on t : for odd number u we have 2^{n-t-1} possibilities; if $r = m + k, ..., n - t - 1$ (where $n > t + r \geqslant 3$) is chosen (note, that this is possible only if $n - t - 1 \geqslant m + k$, i.e., $t = 1, ..., n - m - k - 1$), then for odd number u we have 2^{t-1} possibilities and for number s we have: $2^{n-(t+r)}$ possibilities for odd number p and 2 possibilities for number ε. Hence

$$\begin{aligned}|\{(s,\, q,\, c)\}| &= \sum_{k=0}^{1}\left(2\sum_{t=1}^{n-m-k-1}2^{n-t-1}\sum_{r=m+k,\ r+t\geqslant 3}^{n-t-1}\left(2^{t-1}\cdot 2^{n-t-r}\right)\right) = \\ &= \sum_{k=0}^{1}\left(\sum_{t=1}^{n-m-k-1}2^{n-t}\sum_{r=m+k,\ r+t\geqslant 3}^{n-t-1}2^{n-r-1}\right).\end{aligned}$$

If $m = 1$, then

$$|\{(s,\, q,\, c)\}| = 2^n\left(5\cdot 2^{n-3} - 2n + 1\right).$$

If $m > 1$, then the condition $r + t \geqslant 3$ holds for every t, r, k and

$$|\{(s, q, c)\}| = 2^n \left(3 \cdot 2^{n-m-1} - 2n + 2m - 1\right).$$

For choosing the pair (x, y), we have 4 possibilities if $m = 1$ and 2^{m+1} possibilities if $m > 1$. Therefore, the number of obtained automorphisms is $2^{n+2}\left(5 \cdot 2^{n-3} - 2n + 1\right)$ if $m = 1$ and

$$2^{n+m+1}\left(3 \cdot 2^{n-m-1} - 2n + 2m - 1\right) = 3 \cdot 2^{2n} - 2^{n+m+1}(2n - 2m + 1)$$

automorphisms if $m > 1$.

A.7 Proof of Proposition 4.6

Conditions of Proposition are satisfied only by matrices of the sets M_3, $M_4, \ldots, M_{22}$.

Let us consider the sets M_3, M_4, M_5, M_6 and M_9, M_{10}. Matrices of these sets have the form $\begin{Vmatrix} s & 0 \\ 0 & s + 2^{n-1}i \end{Vmatrix}$, where $i \in \mathbb{Z}_2$. Since $a + s = 2s + 2^{n-1}i$, system (4.11) implies

$$s^2 + 2^{n+1}sx \equiv 1, \quad 2^{n+1}y\left(s + 2^{n-2}i\right) \equiv 0 \pmod{2^{2n}}.$$

The second congruence implies that $y \equiv 0 \pmod{2^{n-1}}$. By Lemma 4.3, the first congruence implies that $x = x_1$. Thus we have obtained automorphisms 1). For choosing pairs (s, i) and (x, y) we have 4 and 4 possibilities, respectively, and hence the number of these automorphisms is 16.

Consider the sets M_7, M_8. Matrices of these sets have the form $\begin{Vmatrix} s & 0 \\ 0 & -s \end{Vmatrix}$, where $a + s = 2^n$, and system (4.11) implies

$$s^2 + 2^{n+1}sx \equiv 1, \quad 2^n y 2^n \equiv 0 \pmod{2^{2n}}.$$

The second congruence holds for every $y \in \mathbb{Z}_{2^n}$ and the first congruence is solved in Lemma 4.3. Thus we have got automorphisms 2). For choosing s and a pair (x, y) we have 2 and $2 \cdot 2^n$ possibilities, respectively. Hence the number of these automorphisms is $2 \cdot 2 \cdot 2^n = 2^{n+2}$.

Now consider the sets M_{11}, M_{12}. Matrices of these sets have the form $\begin{Vmatrix} s & 0 \\ 0 & -s + 2^{n-1} \end{Vmatrix}$. Since $a + s = 2^{n-1}$, system (4.11) implies

$$s^2 + 2^{n+1}sx \equiv 1, \quad 2^n y \cdot 2^{n-1} \equiv 0 \pmod{2^{2n}}.$$

The second congruence holds for every $y \equiv 0 \pmod 2$ and the first congruence is solved in Lemma 4.3. Thus we have automorphisms 3). For choosing

s and a pair $(x,\, y)$ we have 2 and $2 \cdot 2^{n-1}$ possibilities, respectively. Hence the number of these automorphisms is $2 \cdot 2 \cdot 2^{n-1} = 2^{n+1}$.

Let us consider the sets M_{13}, M_{14}. Matrices of these sets, satisfying condition (4.12), have the form $\left\| \begin{array}{cc} s & 2^t u \\ 0 & -s \end{array} \right\|$, where $a + s = 0$. The second congruence of system (4.11) holds for every $x,\, y \in \mathbb{Z}_{2^n}$ and the first congruence

$$s^2 + 2^{n+1} sx + 2^n y 2^t u \equiv 1 \pmod{2^{2n}}$$

is solved in Lemma 4.3 (if $y \equiv 0 \pmod{2^{n-t}}$; we get automorphisms 4)) and in Lemma 4.4 (if $y \not\equiv 0 \pmod{2^{n-t}}$; we get automorphisms 5)). For automorphisms 4) we can write y in the form $y = 2^{n-t}k$, where $k \in \mathbb{Z}_{2^t}$, $t = 1, ..., n-1$, and for the choosing of parameters s, u, y, x we have 2, 2^{n-t-1}, 2^t, 2 possibilities, respectively. Hence the number of these automorphisms is $2 \sum\limits_{t=1}^{n-1} 2^{n-t-1} \cdot 2^t \cdot 2 = 2^{n+1} \sum\limits_{t=1}^{n-1} 1 = 2^{n+1}\,(n-1)$. For automorphisms 5) we can write y in the form $y = j + 2^{n-t}k$, where $j \in \mathbb{Z}_{2^{n-t}} \setminus \{0\}$, $k \in \mathbb{Z}_{2^t}$, $t = 1, ..., n-1$, and choosing parameters s, u, k, j, x we have 2, 2^{n-t-1}, 2^t, $2^{n-t} - 1$, 2 possibilities, respectively. Hence the number of these automorphisms is

$$2 \sum_{t=1}^{n-1} 2^{n-t-1} \cdot 2^t \cdot \left(2^{n-t} - 1\right) \cdot 2 = 2^{2n+1} - 2^{n+1}\,(n+1)\,.$$

Consider the sets M_{15}, M_{16}, M_{17}, M_{18} and M_{19}, M_{20}. Matrices of these sets satisfying condition (4.12), have the form $\left\| \begin{array}{cc} s & 2^{n-1} \\ 0 & s + 2^{n-1} i \end{array} \right\|$, where $i \in \mathbb{Z}_2$. Since $a + s = 2s + 2^{n-1} i$, system (4.11) implies

$$s^2 + 2^{n+1} sx + 2^n y 2^{n-1} \equiv 1, \quad 2^{n+1} y \left(s + 2^{n-2} i\right) \equiv 0 \pmod{2^{2n}}\,.$$

The second congruence implies that $y \equiv 0 \pmod{2^{n-1}}$. The first congruence is solved (in view of $2^n y 2^{n-1} \equiv 0 \pmod{2^{2n}}$) in Lemma 4.3. Thus we have automorphisms 6). For choosing the pairs $(s,\, i)$ and $(x,\, y)$ we have 4 and 4 possibilities, respectively. Hence the number of these automorphisms is 16.

Let us consider now the sets M_{21}, M_{22}. Matrices of these sets satisfying condition (4.12), have the form $\left\| \begin{array}{cc} s & 2^t u \\ 0 & -s + 2^{n-1} \end{array} \right\|$. Since $a + s = 2^{n-1}$, system (4.11) implies

$$s^2 + 2^{n+1} sx + 2^n y 2^t u \equiv 1, \quad 2^n y 2^{n-1} \equiv 0 \pmod{2^{2n}}\,.$$

The second congruence holds for every $y \equiv 0 \pmod 2$. The first congruence is solved in Lemma 4.3 (if $y \equiv 0 \pmod{2^{n-t}}$; we get automorphisms 7)) and in Lemma 4.4 (if $y \not\equiv 0 \pmod{2^{n-t}}$; we get automorphisms 8)). For automorphisms 7) we can write y in the form $y = 2^{n-t}k$,

where $k \in \mathbb{Z}_{2^t}$, $t = 1, ..., n-1$, and for the choice of parameters s, u, y, x we have 2, 2^{n-t-1}, 2^t, 2 possibilities, respectively. Hence the number of these automorphisms is $2\sum\limits_{t=1}^{n-1} 2^{n-t-1} \cdot 2^t \cdot 2 = 2^{n+1}\sum\limits_{t=1}^{n-1} 1 = 2^{n+1}(n-1)$. For automorphisms 8) we can write y in the form $y = j + 2^{n-t}k$, $k \in \mathbb{Z}_{2^t}$, $t = 1, ..., n-2$, $j \in 2\mathbb{Z}_{2^{n-t-1}} \setminus \{0\}$ (the last condition implies $n-t-1 \geqslant 1$, i.e., $t \leqslant n-2$), and for the choosing of parameters s, u, k, j, x we have 2, 2^{n-t-1}, 2^t, $2^{n-t-1}-1$, 2 possibilities, respectively. Hence the number of these automorphisms is

$$2\sum_{t=1}^{n-2} 2^{n-t-1} \cdot 2^t \cdot \left(2^{n-t-1}-1\right) \cdot 2 = 2^{2n} - 2^{n+1}n.$$

Conclude, that there are $32 + 3 \cdot 4^n$ automorphisms in forms 1)–8).

A.8 Proof of Lemma 4.6

Let us denote $s + 2^n x = a$, $t + k = l$. Then the congruence takes the form $a^2 - 1 \equiv -2^{m+l}uw \pmod{2^{n+m}}$ and first at all we solve this congruence (similarly to the proof of Lemma 2.3). Since $m > n \geqslant 3$, a solution of the congruence exists for every l $(0 \leqslant l < n)$. We have

$$(a-1)(a+1) \equiv -2^{m+l}uw \pmod{2^{n+m}}.$$

Denote $a - 1 = 2^r p$ and $a + 1 = 2^{m+l-r}q$, where

$$r \in \mathbb{Z}_{2^{m+l}} \setminus \{0\},\ p \in \mathbb{Z}^*_{2^{n+m-r}},\ q \in \mathbb{Z}^*_{2^{n+r-l}}.$$

Then $2^r p \cdot 2^{m+l-r}q \equiv -2^{m+l}uw \pmod{2^{n+m}}$ and therefore,

$$pq \equiv -uw \pmod{2^{n-l}}. \tag{A.28}$$

By the other side,

$$a = 1 + 2^r p = -1 + 2^{m+l-r}q,$$

i.e., $2\left(1 + 2^{r-1}p\right) = 2^{m+l-r}q$ and thus

$$1 + 2^{r-1}p = 2^{m+l-r-1}q. \tag{A.29}$$

The last equation has a solution only in the cases $r = 1$ and $r = m+l-1$.

If $r = 1$ then (A.29) implies $q \in \mathbb{Z}^*_{2^{n-l+1}}$ and

$$p = -1 + 2^{m+l-2}q,\ a = 1 + 2\left(-1 + 2^{m+l-2}q\right) = -1 + 2^{m+l-1}q. \tag{A.30}$$

Analogously, if $r = m + l - 1$ then (A.29) implies $p \in \mathbb{Z}^*_{2^{n-l+1}}$ and

$$q = 1 + 2^{m+l-2}p,\ a = 1 + 2^{m+l-1}p. \tag{A.31}$$

Conditions (A.30) and (A.31) are presentable as follows:

$$q = \varepsilon + 2^{m+l-2}p,\ a = \varepsilon + 2^{m+l-1}p,\ p \in \mathbb{Z}^*_{2^{n-l+1}},\ \varepsilon = \pm 1.$$

By (A.28), we have

$$\left(\varepsilon + 2^{m+l-2}p\right) p \equiv -uw \left(\mathrm{mod}\ 2^{n-l}\right)$$

and

$$w \equiv -\left(\varepsilon + 2^{m+l-2}p\right) pu^{-1} \equiv -\left(\varepsilon + 2^{m+l-2}p\right) pu^{2^{n-l-1}-1} \left(\mathrm{mod}\ 2^{n-l}\right).$$

Since $0 < w < 2^{n-k}$, the element w has $2^{n-k}/2^{n-l} = 2^t$ different values modulo 2^n in the form $w_k = w + 2^{n-l}i$, where $i = 0, 1, ..., 2^t - 1$.

Thus we have obtained that the solution of the congruence

$$a^2 \equiv 1 - 2^m zq \left(\mathrm{mod}\ 2^{n+m}\right),$$

where $zq \not\equiv 0 \left(\mathrm{mod}\ 2^n\right)$, is $a = \varepsilon + 2^{m+l-1}p$ and

$$q = 2^t u,\ z = 2^k \left(-\left(\varepsilon + 2^{m+t+k-2}p\right) pu^{2^{n-t-k-1}-1} + 2^{n-t-k}i\right),$$

where $\varepsilon = \pm 1,\ u \in \mathbb{Z}^*_{2^{n-t}},\ p \in \mathbb{Z}^*_{2^{n-l+1}},\ i \in \mathbb{Z}_{2^t}$ and $0 \leqslant t + k < n$.

Now let us find x from $a = s + 2^n x = \varepsilon + 2^{m+l-1}p$. We have: **1)** if $s = 1$, then $x = 2^{m-n+l-1}p$, $\varepsilon = 1$; **2)** if $s = -1 + 2^n$, then $x = 2^{m-n+l-1}p - 1$, $\varepsilon = -1$; **3)** if $s = \pm 1 + 2^{n-1}$, then $x \in \varnothing$.

A.9 Proof of Proposition 4.8

Conditions of the proposition satisfy only matrices of the sets M_3–M_{22}.

Let us consider the sets M_3, M_4, M_5, M_6 and M_9, M_{10}. Matrices of these sets have the form $\left\| \begin{matrix} s & 0 \\ 0 & s + 2^{n-1}j \end{matrix} \right\|$, where $j \in \mathbb{Z}_2$. Since $a + s = 2s + 2^{n-1}j$, system (4.13) implies

$$(s + 2^n x)^2 \equiv 1, \quad 2^{m+1}z \equiv 0 \quad \left(\mathrm{mod}\ 2^{n+m}\right).$$

The second congruence implies $z \equiv 0 \left(\mathrm{mod}\ 2^{n-1}\right)$, i.e., $z \in \left\{0, 2^{n-1}\right\}$. The first congruence is solved in Lemma 4.5. Thus we have got automorphisms 1). There is 16 automorphisms in this form.

Now consider the sets M_7, M_8. Matrices of these sets have the form $\begin{Vmatrix} s & 0 \\ 0 & -s \end{Vmatrix}$. Since $a + s = 2^n$, system (4.13) implies

$$(s + 2^n x)^2 \equiv 1, \quad 2^m z 2^n \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $z \in \mathbb{Z}_{2^n}$ and the first congruence is solved in Lemma 4.5. Thus we have got automorphisms 2). There is 2^{n+2} automorphisms in this form.

Now consider the sets M_{11}, M_{12}. Matrices of these sets have the form $\begin{Vmatrix} s & 0 \\ 0 & -s + 2^{n-1} \end{Vmatrix}$, $a + s = 2^{n-1}$, and system (4.13) implies

$$(s + 2^n x)^2 \equiv 1, \quad 2^m z 2^{n-1} \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $z \equiv 0 \pmod 2$ and the first congruence is solved in Lemma 4.5. Thus we have got automorphisms 3). Let us determine the number of automorphisms of this form. The numbers of possible values of the parameters s, x and z are 2, 2 and 2^{n-1}, respectively. Hence the number of automorphisms of this form is 2^{n+1}.

Let us consider the sets M_{13}, M_{14}. Matrices of these sets, which satisfy the condition $c = 0$, have the form $\begin{Vmatrix} s & 2^t u \\ 0 & -s \end{Vmatrix}$. Since $a + s = 2^n$, system (4.13) implies

$$(s + 2^n x)^2 + 2^m z q \equiv 1, \quad 2^m z 2^n \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $z \in \mathbb{Z}_{2^n}$. The first congruence is solved in Lemma 4.5 (if $z \equiv 0 \pmod{2^{n-t}}$, i.e., if $z = 2^{n-t} l$, where $l \in \mathbb{Z}_{2^t}$; we get automorphisms 4)) and in Lemma 4.6 (if $z \not\equiv 0 \pmod{2^{n-t}}$, i.e., $z = 2^k w$, where $k + t < n$; we get automorphisms 5)). Let us determine the number of solutions in these forms. For form 4), we have 2 choices for s and 2 choices for x, too. If $t = 1, \ldots, n-1$ is fixed, we have 2^t choices for z and 2^{n-t-1} choices for odd number u. The number of automorphisms of this form is $2 \cdot 2 \left(\sum_{t=1}^{n-1} 2^t 2^{n-t-1} \right) = 2^{n+1} (n-1)$. For form 5), we have 2 choices for s and, if $t \in \mathbb{Z}_n \setminus \{0\}$ is fixed, we have 2^{n-t-1} choices for odd number u. Since $k + t < n$, we have $k = 0, 1, \ldots, n-t-1$ ($k \in \mathbb{Z}_{n-t}$) and, if k is fixed, we have 2^t choices for odd number w and 2^{n-k-t} choices for odd number p. Hence the number of automorphisms in this form is $2 \sum_{t=1}^{n-1} 2^{n-t-1} \sum_{k=0}^{n-t-1} 2^t 2^{n-k-t} = 2^{2n+1} - 2^{n+1} (n+1)$.

Now consider the sets $M_{15}, M_{16}, M_{17}, M_{18}$ and M_{19}, M_{20}. Condition $c = 0$ satisfying matrices of these sets have the form $\begin{Vmatrix} s & 2^{n-1} \\ 0 & s + 2^{n-1} j \end{Vmatrix}$, where

$j \in \mathbb{Z}_2$. Since $a + s = 2s + 2^{n-1}j$, system (4.13) implies

$$(s + 2^n x)^2 + 2^m zq \equiv 1, \quad 2^{m+1} z \equiv 0 \pmod{2^{n+m}}.$$

The second congruence implies that $z \equiv 0 \pmod{2^{n-1}}$. Then $zq = z2^{n-1} \equiv 0 \pmod{2^n}$ and the first congruence is solved in Lemma 4.5. Hence we get automorphisms 6). There is 16 automorphisms in this form.

Finally, let us now consider the sets M_{21}, M_{22}. Condition $c = 0$ satisfying matrices of these sets have the form $\begin{Vmatrix} s & 2^t u \\ 0 & -s + 2^{n-1} \end{Vmatrix}$. Since $a + s = 2^{n-1}$, system (4.13) implies

$$(s + 2^n x)^2 + 2^m zq \equiv 1, \quad 2^m z 2^{n-1} \equiv 0 \pmod{2^{n+m}}.$$

The second congruence holds for every $z \equiv 0 \pmod 2$. The first congruence is solved in Lemma 4.5 (if $z \equiv 0 \pmod{2^{n-t}}$, i.e., $z = 2^{n-t} l$, where $l \in \mathbb{Z}_{2^t}$; we get automorphisms 7)) and in Lemma 4.6 (if $z \not\equiv 0 \pmod{2^{n-t}}$, i.e., $z = 2^k w$, where $k + t < n$; we get automorphisms 8)). Let us determine the number of automorphisms of these forms. For form 7), we have 2 choices for s and 2 choices for x, as well. If t is fixed, we have 2^{n-t-1} choices for odd number u and 2^t choices for z. The number of automorphisms of this form is $2 \cdot 2 \sum_{t=1}^{n-1} 2^{n-t-1} 2^t = 2^{n+1}(n-1)$. For form 8), we have 2 choices for s and if t is fixed, we have 2^{n-t-1} choices for odd number u. Since $z \equiv 0 \pmod 2$, we have $k = 1, \ldots, n-t-1$, i.e., $k \in \mathbb{Z}_{n-t} \setminus \{0\}$ (it is possible, if $n - t - 1 \geqslant 1$, i.e., $t \leqslant n-2$) and, if k is fixed, we have 2^t choices for odd number w and 2^{n-k-t} choices for odd number p. The number of automorphisms of this form is $2 \sum_{t=1}^{n-2} 2^{n-t-1} \sum_{k=1}^{n-t-1} 2^t 2^{n-k-t} = 2^{2n} - 2^{n+1} n$.

In conclusion, that the number of automorphisms described in this proposition is $3 \cdot 4^n + 32$.

B Matrices over $\mathbb{Z}_{2^n}$ of order 1 or 2

In this appendix all (2×2)-matrices over $\mathbb{Z}_{2^n}$ of order 1 or 2 are listed. These matrices form the set $\cup_{i=1}^{36} M_i$, where M_1, $M_2, \ldots, M_{36}$ are given below. In the description of these sets

$$t, s \in \mathbb{Z}_n \setminus \{0\}\,,\ u \in \mathbb{Z}^*_{2^{n-t}},\ v \in \mathbb{Z}^*_{2^{n-s}}.$$

By necessity, some supplementary conditions for the numbers t, s, u, v are given. For the sets M_{29}, M_{30} and M_{35}, M_{36}, it is denoted

$$x = p\left(\varepsilon + 2^{t+s-2}p\right) + uv, \qquad y = 2^{n-s-t}$$

and used the supplementary conditions

$$\begin{aligned} 3 &\leqslant t+s<n, \quad p \in \mathbb{Z}^*_{2^{n-(t+s)+1}}, \quad k \in \mathbb{Z}_{2^t}, \\ v &= -\left(\varepsilon + 2^{t+s-2}p\right) p u^{2^{n-s-t-1}-1} + 2^{n-t-s}k. \end{aligned}$$

$$M_1 = \left\{ \begin{Vmatrix} a & b \\ \left(1-a^2\right)b^{-1} & -a \end{Vmatrix} : \ a \in 2\mathbb{Z}_{2^{n-1}},\ b \in \mathbb{Z}^*_{2^n} \right\}$$

$$M_2 = \left\{ \begin{Vmatrix} a & b \\ \left(1-a^2\right)b^{-1} & -a \end{Vmatrix}, \begin{Vmatrix} a & \left(1-a^2\right)c^{-1} \\ c & -a \end{Vmatrix} : a,b,c \in \mathbb{Z}^*_{2^n} \right\}$$

$$M_3 = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix} \right\},$$

$$M_4 = \left\{ \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix} \right\},$$

$$M_5 = \left\{ \begin{Vmatrix} 1+2^{n-1} & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix} \right\},$$

$$M_6 = \left\{ \begin{Vmatrix} -1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix} \right\},$$

$$M_7 = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}, \begin{Vmatrix} -1 & 0 \\ 0 & 1 \end{Vmatrix} \right\},$$

$$M_8 = \left\{ \begin{Vmatrix} 1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix}, \begin{Vmatrix} -1+2^{n-1} & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix} \right\},$$

$$M_9 = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix}, \begin{Vmatrix} 1+2^{n-1} & 0 \\ 0 & 1 \end{Vmatrix} \right\},$$

$$M_{10} = \left\{ \begin{Vmatrix} -1 & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix}, \begin{Vmatrix} -1+2^{n-1} & 0 \\ 0 & -1 \end{Vmatrix} \right\},$$

$$M_{11} = \left\{ \begin{Vmatrix} 1 & 0 \\ 0 & -1+2^{n-1} \end{Vmatrix}, \begin{Vmatrix} -1+2^{n-1} & 0 \\ 0 & 1 \end{Vmatrix} \right\},$$

$$M_{12} = \left\{ \begin{Vmatrix} -1 & 0 \\ 0 & 1+2^{n-1} \end{Vmatrix}, \begin{Vmatrix} 1+2^{n-1} & 0 \\ 0 & -1 \end{Vmatrix} \right\},$$

$$M_{13} = \left\{ \left\| \begin{matrix} 1 & 0 \\ 2^t u & -1 \end{matrix} \right\|, \left\| \begin{matrix} 1 & 2^t u \\ 0 & -1 \end{matrix} \right\|, \left\| \begin{matrix} -1 & 0 \\ 2^t u & 1 \end{matrix} \right\|, \left\| \begin{matrix} -1 & 2^t u \\ 0 & 1 \end{matrix} \right\| \right\},$$

$$M_{14} = \left\{ \left\| \begin{matrix} 1+2^{n-1} & 0 \\ 2^t u & -1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 2^t u \\ 0 & -1+2^{n-1} \end{matrix} \right\| \right\} \cup$$
$$\cup \left\{ \left\| \begin{matrix} -1+2^{n-1} & 0 \\ 2^t u & 1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} -1+2^{n-1} & 2^t u \\ 0 & 1+2^{n-1} \end{matrix} \right\| \right\},$$

$$M_{15} = \left\{ \left\| \begin{matrix} 1 & 2^{n-1} \\ 0 & 1 \end{matrix} \right\|, \left\| \begin{matrix} 1 & 0 \\ 2^{n-1} & 1 \end{matrix} \right\| \right\},$$

$$M_{16} = \left\{ \left\| \begin{matrix} 1+2^{n-1} & 2^{n-1} \\ 0 & 1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 0 \\ 2^{n-1} & 1+2^{n-1} \end{matrix} \right\| \right\},$$

$$M_{17} = \left\{ \left\| \begin{matrix} -1 & 2^{n-1} \\ 0 & -1 \end{matrix} \right\|, \left\| \begin{matrix} -1 & 0 \\ 2^{n-1} & -1 \end{matrix} \right\| \right\},$$

$$M_{18} = \left\{ \left\| \begin{matrix} -1+2^{n-1} & 2^{n-1} \\ 0 & -1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} -1+2^{n-1} & 0 \\ 2^{n-1} & -1+2^{n-1} \end{matrix} \right\| \right\},$$

$$M_{19} = \left\{ \left\| \begin{matrix} 1 & 2^{n-1} \\ 0 & 1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} 1 & 0 \\ 2^{n-1} & 1+2^{n-1} \end{matrix} \right\| \right\} \cup$$
$$\cup \left\{ \left\| \begin{matrix} 1+2^{n-1} & 2^{n-1} \\ 0 & 1 \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 0 \\ 2^{n-1} & 1 \end{matrix} \right\| \right\},$$

$$M_{20} = \left\{ \left\| \begin{matrix} -1 & 2^{n-1} \\ 0 & -1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} -1 & 0 \\ 2^{n-1} & -1+2^{n-1} \end{matrix} \right\| \right\} \cup$$
$$\cup \left\{ \left\| \begin{matrix} -1+2^{n-1} & 2^{n-1} \\ 0 & -1 \end{matrix} \right\|, \left\| \begin{matrix} -1+2^{n-1} & 0 \\ 2^{n-1} & -1 \end{matrix} \right\| \right\},$$

$$M_{21} = \left\{ \left\| \begin{matrix} 1 & 0 \\ 2^t u & -1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} 1 & 2^t u \\ 0 & -1+2^{n-1} \end{matrix} \right\| \right\} \cup$$
$$\cup \left\{ \left\| \begin{matrix} -1+2^{n-1} & 0 \\ 2^t u & 1 \end{matrix} \right\|, \left\| \begin{matrix} -1+2^{n-1} & 2^t u \\ 0 & 1 \end{matrix} \right\| \right\},$$

$$M_{22} = \left\{ \left\| \begin{matrix} -1 & 0 \\ 2^t u & 1+2^{n-1} \end{matrix} \right\|, \left\| \begin{matrix} -1 & 2^t u \\ 0 & 1+2^{n-1} \end{matrix} \right\| \right\} \cup$$
$$\cup \left\{ \left\| \begin{matrix} 1+2^{n-1} & 0 \\ 2^t u & -1 \end{matrix} \right\|, \left\| \begin{matrix} 1+2^{n-1} & 2^t u \\ 0 & -1 \end{matrix} \right\| \right\},$$

$$M_{23} = \left\{ \left\| \begin{matrix} 1+2^{n-1} & 2^{n-1} \\ 2^{n-1} & 1+2^{n-1} \end{matrix} \right\| \right\},$$

$$M_{24} = \left\{ \left\| \begin{matrix} 1 & 2^{n-1} \\ 2^{n-1} & 1 \end{matrix} \right\| \right\},$$

$$M_{25} = \left\{ \left\| \begin{matrix} -1+2^{n-1} & 2^{n-1} \\ 2^{n-1} & -1+2^{n-1} \end{matrix} \right\| \right\},$$

$$M_{26} = \left\{ \left\| \begin{matrix} -1 & 2^{n-1} \\ 2^{n-1} & -1 \end{matrix} \right\| \right\},$$

$$M_{27} = \left\{ \left\| \begin{matrix} 1 & 2^t u \\ 2^s v & -1 \end{matrix} \right\|, \left\| \begin{matrix} -1 & 2^t u \\ 2^s v & 1 \end{matrix} \right\| : s+t > n \right\} \cup$$

$$\cup\left\{\left\|\begin{array}{cc}1+2^{n-1} & 2^t u\\ 2^s v & -1+2^{n-1}\end{array}\right\|,\left\|\begin{array}{cc}-1+2^{n-1} & 2^t u\\ 2^s v & 1+2^{n-1}\end{array}\right\| : s+t=n\right\},$$

$$M_{28}=\left\{\left\|\begin{array}{cc}1 & 2^t u\\ 2^s v & -1\end{array}\right\|,\left\|\begin{array}{cc}-1 & 2^t u\\ 2^s v & 1\end{array}\right\| : s+t=n\right\}\cup$$

$$\cup\left\{\left\|\begin{array}{cc}1+2^{n-1} & 2^t u\\ 2^s v & -1+2^{n-1}\end{array}\right\|,\left\|\begin{array}{cc}-1+2^{n-1} & 2^t u\\ 2^s v & 1+2^{n-1}\end{array}\right\| : s+t>n\right\},$$

$$M_{29}=\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)\end{array}\right\| : x\equiv 0(\mathrm{mod}\ 2y),\ \varepsilon=1\right\}\cup$$

$$\cup\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)\end{array}\right\| : x\equiv 0(\mathrm{mod}\ 2y),\ \varepsilon=-1\right\},$$

$$M_{30}=\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)\end{array}\right\| : x\equiv y(\mathrm{mod}\ 2y),\ \varepsilon=1\right\}\cup$$

$$\cup\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)\end{array}\right\| : x\equiv y(\mathrm{mod}\ 2y),\ \varepsilon=-1\right\},$$

$$M_{31}=\left\{\left\|\begin{array}{cc}1 & 2^{n-1}\\ 2^{n-1} & 1+2^{n-1}\end{array}\right\|,\left\|\begin{array}{cc}1+2^{n-1} & 2^{n-1}\\ 2^{n-1} & 1\end{array}\right\|\right\},$$

$$M_{32}=\left\{\left\|\begin{array}{cc}-1 & 2^{n-1}\\ 2^{n-1} & -1+2^{n-1}\end{array}\right\|,\left\|\begin{array}{cc}-1+2^{n-1} & 2^{n-1}\\ 2^{n-1} & -1\end{array}\right\|\right\},$$

$$M_{33}=\left\{\left\|\begin{array}{cc}1 & 2^t u\\ 2^s v & -1+2^{n-1}\end{array}\right\|,\left\|\begin{array}{cc}-1+2^{n-1} & 2^t u\\ 2^s v & 1\end{array}\right\| : s+t>n\right\}\cup$$

$$\cup\left\{\left\|\begin{array}{cc}1+2^{n-1} & 2^t u\\ 2^s v & -1\end{array}\right\|,\left\|\begin{array}{cc}-1 & 2^t u\\ 2^s v & 1+2^{n-1}\end{array}\right\| : s+t=n\right\},$$

$$M_{34}=\left\{\left\|\begin{array}{cc}1 & 2^t u\\ 2^s v & -1+2^{n-1}\end{array}\right\|,\left\|\begin{array}{cc}-1+2^{n-1} & 2^t u\\ 2^s v & 1\end{array}\right\| : s+t=n\right\}\cup$$

$$\cup\left\{\left\|\begin{array}{cc}1+2^{n-1} & 2^t u\\ 2^s v & -1\end{array}\right\|,\left\|\begin{array}{cc}-1 & 2^t u\\ 2^s v & 1+2^{n-1}\end{array}\right\| : s+t>n\right\},$$

$$M_{35}=\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)+2^{n-1}\end{array}\right\| : x\equiv 0(\mathrm{mod}\ 2y),\ \varepsilon=1\right\}$$

$$\cup\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)+2^{n-1}\end{array}\right\| : x\equiv y(\mathrm{mod}\ 2y),\ \varepsilon=-1\right\},$$

$$M_{36}=\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)+2^{n-1}\end{array}\right\| : x\equiv y(\mathrm{mod}\ 2y),\ \varepsilon=1\right\}$$

$$\cup\left\{\left\|\begin{array}{cc}\varepsilon+2^{t+s-1}p & 2^t u\\ 2^s v & -\left(\varepsilon+2^{t+s-1}p\right)+2^{n-1}\end{array}\right\| : x\equiv 0(\mathrm{mod}\ 2y),\ \varepsilon=-1\right\}.$$

C Representatives of conjugacy classes of matrices over $\mathbb{Z}_{2^n}$ of order 1 or 2

$$A_1 = \left\| \begin{array}{cc} 1 & 0 \\ 0 & 1 \end{array} \right\| \in M_3, \qquad A_2 = \left\| \begin{array}{cc} 1+2^{n-1} & 0 \\ 0 & 1+2^{n-1} \end{array} \right\| \in M_5,$$

$$A_3 = \left\| \begin{array}{cc} 1 & 2^{n-1} \\ 0 & 1 \end{array} \right\| \in M_{15}, \qquad A_4 = \left\| \begin{array}{cc} 1+2^{n-1} & 2^{n-1} \\ 0 & 1+2^{n-1} \end{array} \right\| \in M_{16},$$

$$A_5 = \left\| \begin{array}{cc} -1+2^{n} & 0 \\ 0 & -1+2^{n} \end{array} \right\| \in M_4,$$

$$A_6 = \left\| \begin{array}{cc} -1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{array} \right\| \in M_6,$$

$$A_7 = \left\| \begin{array}{cc} -1+2^{n} & 2^{n-1} \\ 0 & -1+2^{n} \end{array} \right\| \in M_{17},$$

$$A_8 = \left\| \begin{array}{cc} -1+2^{n-1} & 2^{n-1} \\ 0 & -1+2^{n-1} \end{array} \right\| \in M_{18},$$

$$A_9 = \left\| \begin{array}{cc} 1 & 2^{n-1} \\ 2^{n-1} & 1+2^{n-1} \end{array} \right\| \in M_{31}, \qquad A_{10} = \left\| \begin{array}{cc} 1 & 0 \\ 0 & 1+2^{n-1} \end{array} \right\| \in M_9,$$

$$A_{11} = \left\| \begin{array}{cc} -1+2^{n} & 2^{n-1} \\ 2^{n-1} & -1+2^{n-1} \end{array} \right\| \in M_{32},$$

$$A_{12} = \left\| \begin{array}{cc} -1+2^{n} & 0 \\ 0 & -1+2^{n-1} \end{array} \right\| \in M_{10},$$

$$A_{13} = \left\| \begin{array}{cc} 1 & 0 \\ 0 & -1+2^{n-1} \end{array} \right\| \in M_{11},$$

$$A_{14} = \left\| \begin{array}{cc} -1+2^{n} & 0 \\ 0 & 1+2^{n-1} \end{array} \right\| \in M_{12},$$

$$A_{15} = \left\| \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\| \in M_1, \qquad A_{16} = \left\| \begin{array}{cc} 1 & 0 \\ 0 & -1+2^{n} \end{array} \right\| \in M_7,$$

$$A_{17} = \left\| \begin{array}{cc} 1+2^{n-1} & 0 \\ 0 & -1+2^{n-1} \end{array} \right\| \in M_8.$$

D Conjugacy classes of matrices of order 4

In this appendix we shall use the following abbreviations:

Cl = Class, F = Form, NoE = Number of Elements, R = Row

and notations:

$$
\begin{array}{ll}
M = 2^{n-(f+g)} & n3 = 2^{n+1}\left(3\cdot 2^{n-4} - n + 1\right), \\
n1 = 2\left(2^n - 1\right), & n4 = (n-2)\,2^n, \\
n2 = (n-2)\,2^n + 2, & n5 = 2^{n-1}\left(3\cdot 2^{n-2} - 3n + 2\right), \\
n6 = 2^{n-1}\,(n-2)\,. &
\end{array}
$$

Conjugacy classes are $\mathcal{K}_1 - \mathcal{K}_7,\ \mathcal{K}_8^3 - \mathcal{K}_{19}^3$, if $n = 3$, and $\mathcal{K}_1 - \mathcal{K}_7,\ \mathcal{K}_8 - \mathcal{K}_{63}$, if $n \geqslant 4$.

Cl	Prop.	F	Condition	NoE
$\mathcal{K}_1$	3.1	2	$k=0,\ \ a=-1+2^{n-1}$	2^{2n-2}
	3.2	2	$k=0,\ \ a=-1+2^{n-1}$	2^{2n-2}
	3.2	4	$k=0,\ \ a=-1+2^{n-1}$	2^{2n-2}
$\mathcal{K}_2$	3.1	2	$k=0,\ \ a=1+2^{n-1}$	2^{2n-2}
	3.2	2	$k=0,\ \ a=1+2^{n-1}$	2^{2n-2}
	3.2	4	$k=0,\ \ a=1+2^{n-1}$	2^{2n-2}
$\mathcal{K}_3$	3.1	2	$k=0,\ \ a=-1+2^{n}$	2^{2n-2}
	3.2	2	$k=0,\ \ a=-1+2^{n}$	2^{2n-2}
	3.2	4	$k=0,\ \ a=-1+2^{n}$	2^{2n-2}
$\mathcal{K}_4$	3.1	1		2^{2n-2}
	3.2	2	$k=1,\ \ a=1+2^{n-1}$	2^{2n-2}
	3.2	4	$k=1,\ \ a=1+2^{n-1}$	2^{2n-2}
$\mathcal{K}_5$	3.1	2	$k=1,\ \ a=-1+2^{n-1}$	2^{2n-2}
	3.2	2	$k=1,\ \ a=-1+2^{n}$	2^{2n-2}
	3.2	4	$k=1,\ \ a=-1+2^{n}$	2^{2n-2}
$\mathcal{K}_6$	3.1	2	$k=1,\ \ a=1+2^{n-1}$	2^{2n-2}
	3.2	1		2^{2n-2}
	3.2	3		2^{2n-2}
$\mathcal{K}_7$	3.1	2	$k=1,\ \ a=-1+2^{n}$	2^{2n-2}
	3.2	2	$k=1,\ \ a=-1+2^{n-1}$	2^{2n-2}
	3.2	4	$k=1,\ \ a=-1+2^{n-1}$	2^{2n-2}

Table 4. Matrices from Propositions 3.1 and 3.2, $n \geqslant 3$

Cl	Condition	NoE
$\mathcal{K}_8^3$	$k=0,\ p\in\{1,7\},\ uv\equiv 1(\text{mod } 4)$	8
	$k=0,\ p\in\{3,5\},\ uv\equiv 3(\text{mod } 4)$	
$\mathcal{K}_9^3$	$k=0,\ p\in\{1,7\},\ uv\equiv 3(\text{mod } 4)$	8
	$k=0,\ p\in\{3,5\},\ uv\equiv 1(\text{mod } 4)$	
$\mathcal{K}_{10}^3$	$k=1,\ p\in\{1,3\},\ uv\equiv 1(\text{mod } 4)$	8
	$k=1,\ p\in\{5,7\},\ uv\equiv 3(\text{mod } 4)$	
$\mathcal{K}_{11}^3$	$k=1,\ p\in\{1,3\},\ uv\equiv 3(\text{mod } 4)$	8
	$k=1,\ p\in\{5,7\},\ uv\equiv 1(\text{mod } 4)$	

Table 5. Matrices from Proposition 3.3, $n=3$

Cl	F	Condition	NoE
$\mathcal{K}_{12}^3$	1	$p\in\{1,5\},\ uv\equiv 0\ (\text{mod } 4)$	8
	2	$p\in\{3,7\},\ uv\equiv 3\ (\text{mod } 4)$	4
$\mathcal{K}_{13}^3$	1	$p\in\{1,5\},\ uv\equiv 1\ (\text{mod } 4)$	4
	2	$p\in\{3,7\},\ uv\equiv 0\ (\text{mod } 4)$	8
$\mathcal{K}_{14}^3$	1	$p\in\{1,5\},\ uv\equiv 2\ (\text{mod } 4)$	8
	2	$p\in\{3,7\},\ uv\equiv 1\ (\text{mod } 4)$	4
$\mathcal{K}_{15}^3$	1	$p\in\{1,5\},\ uv\equiv 3\ (\text{mod } 4)$	4
	2	$p\in\{3,7\},\ uv\equiv 2\ (\text{mod } 4)$	8
$\mathcal{K}_{16}^3$	1	$p\in\{3,7\},\ uv\equiv 0\ (\text{mod } 4)$	8
	2	$p\in\{1,5\},\ uv\equiv 3\ (\text{mod } 4)$	4
$\mathcal{K}_{17}^3$	1	$p\in\{3,7\},\ uv\equiv 1\ (\text{mod } 4)$	4
	2	$p\in\{1,5\},\ uv\equiv 0\ (\text{mod } 4)$	8
$\mathcal{K}_{18}^3$	1	$p\in\{3,7\},\ uv\equiv 2\ (\text{mod } 4)$	8
	2	$p\in\{1,5\},\ uv\equiv 1\ (\text{mod } 4)$	4
$\mathcal{K}_{19}^3$	1	$p\in\{3,7\},\ uv\equiv 3\ (\text{mod } 4)$	4
	2	$p\in\{1,5\},\ uv\equiv 2\ (\text{mod } 4)$	8

Table 6. Matrices from Proposition 3.4, $n=3$

Let us denote for two next tables $uv - 2^{n-(f+g)-1} + \left(\varepsilon + 2^{f+g-2}p\right) p$ by d.

Cl	F	R	Condition	NoE
$\mathcal{K}_8$	1	1	$p \in \left\{-1+2^{n-2}, 1+3\cdot 2^{n-2}\right\}$	$n1$
		2	$p \in \left\{-1+2^{n-2}, 1+3\cdot 2^{n-2}\right\}$, $f+g>n$	$n2$
			$p \in \left\{1+2^{n-2}, -1+3\cdot 2^{n-2}\right\}$, $f+g=n$	
	2		$d \equiv 2^{n-(f+g)} \pmod{2^{n-(f+g)+1}}$	$n3$
	3		$p \in \{1, -1+2^n\}$, $uv \equiv -1+2^{n-3} \pmod 4$	$n4$
			$p \in \left\{\pm 1+2^{n-1}\right\}$, $uv \equiv 1+2^{n-3} \pmod 4$	
$\mathcal{K}_9$	1	1	$p \in \left\{1+2^{n-2}, -1+3\cdot 2^{n-2}\right\}$	$n1$
		2	$p \in \left\{1+2^{n-2}, -1+3\cdot 2^{n-2}\right\}$, $f+g>n$	$n2$
			$p \in \left\{-1+2^{n-2}, 1+3\cdot 2^{n-2}\right\}$, $f+g=n$	
	2		$d \equiv 0 \pmod{2^{n-(f+g)+1}}$	$n3$
	3		$p \in \{1, -1+2^n\}$, $uv \equiv 1+2^{n-3} \pmod 4$	$n4$
			$p \in \left\{\pm 1+2^{n-1}\right\}$, $uv \equiv -1+2^{n-3} \pmod 4$	

Table 7. Matrices from Proposition 3.5, $k = 0$, $n \geqslant 4$

Cl	F	R	Condition	NoE
$\mathcal{K}_{10}$	1	1	$p = \pm 1+2^{n-2}$	$n1$
		2	$p = \pm 1+2^{n-2}$, $f+g>n$	$n2$
			$p = \pm 1+3\cdot 2^{n-2}$, $f+g=n$	
	2		$d \equiv \left(\frac{1-\varepsilon}{2}\right) 2^{n-(f+g)} \pmod{2^{n-(f+g)+1}}$	$n3$
	3		$p \in \left\{1, -1+2^{n-1}\right\}$, $uv \equiv 1-2^{n-3} \pmod 4$	$n4$
			$p \in \left\{\pm 1+2^{n-1}\right\}$, $uv \equiv -1-2^{n-3} \pmod 4$	
$\mathcal{K}_{11}$	1	1	$p = \pm 1+3\cdot 2^{n-2}$	$n1$
		2	$p = \pm 1+3\cdot 2^{n-2}$, $f+g>n$	$n2$
			$p = \pm 1+2^{n-2}$, $f+g=n$	
	2		$d \equiv \left(\frac{\varepsilon+1}{2}\right) 2^{n-(f+g)} \pmod{2^{n-(f+g)+1}}$	$n3$
	3		$p \in \left\{1, -1+2^{n-1}\right\}$, $uv \equiv -1-2^{n-3} \pmod 4$	$n4$
			$p \in \left\{\pm 1+2^{n-1}\right\}$, $uv \equiv 1-2^{n-3} \pmod 4$	

Table 8. Matrices from Proposition 3.5, $k = 1$, $n \geqslant 4$

Cl	Matrix or conditions	NoE
$\mathcal{K}_{12}$	$\left\{\left\{-1+2^{n-2},0\right\},\left\{0,-1+2^{n-2}\right\}\right\}=\mathcal{A}_{12}$	1
$\mathcal{K}_{13}$	$k=1$, $p=-1+2^{n-2}z$, $(q',r')\in\{(0,0);(2,0);(0,2)\}$	6
$\mathcal{K}_{14}$	$\left\{\left\{1+2^{n-2},0\right\},\left\{0,1+2^{n-2}\right\}\right\}=\mathcal{A}_{14}$	1
$\mathcal{K}_{15}$	$k=1$, $p=1+2^{n-2}z$, $(q',r')\in\{(0,0);(2,0);(0,2)\}$	6
$\mathcal{K}_{16}$	$\left\{\left\{-1+3\cdot 2^{n-2},0\right\},\left\{0,-1+3\cdot 2^{n-2}\right\}\right\}=\mathcal{A}_{16}$	1
$\mathcal{K}_{17}$	$\left\{\left\{1+3\cdot 2^{n-2},0\right\},\left\{0,1+3\cdot 2^{n-2}\right\}\right\}=\mathcal{A}_{17}$	1
$\mathcal{K}_{18}$	$k=0$, $p=-1+2^{n-2}z$, $\begin{cases} q'r'\equiv 0\,(\mathrm{mod}\,4)\\ q'\neq r'\,(\mathrm{mod}\,2)\end{cases}$	12
	$k=1$, $p\in\left\{-1+2^{n-1},-1+2^{n}\right\}$, $q'r'\equiv 3\,(\mathrm{mod}\,4)$	
$\mathcal{K}_{19}$	$k=1$, $p=-1+2^{n-2}z$, $\begin{cases} q'r'\equiv 0\,(\mathrm{mod}\,4)\\ q'\neq r'\,(\mathrm{mod}\,2)\end{cases}$	12
	$k=0$, $p\in\left\{-1+2^{n-1},-1+2^{n}\right\}$, $q'r'\equiv 1\,(\mathrm{mod}\,4)$	
$\mathcal{K}_{20}$	$k=0$, $p=1+2^{n-2}z$, $\begin{cases} q'r'\equiv 0\,(\mathrm{mod}\,4)\\ q'\neq r'\,(\mathrm{mod}\,2)\end{cases}$	12
	$k=1$, $p\in\left\{1,1+2^{n-1}\right\}$, $q'r'\equiv 3\,(\mathrm{mod}\,4)$	
$\mathcal{K}_{21}$	$k=1$, $p=1+2^{n-2}z$, $\begin{cases} q'r'\equiv 0\,(\mathrm{mod}\,4)\\ q'\neq r'\,(\mathrm{mod}\,2)\end{cases}$	12
	$k=0$, $p\in\left\{1,1+2^{n-1}\right\}$, $q'r'\equiv 1\,(\mathrm{mod}\,4)$	
$\mathcal{K}_{22}$	$k=0$, $p=-1+2^{n-2}$, $(q',r')\in\{(2,0);(0,2)\}$	3
	$k=0$, $p=-1+3\cdot 2^{n-2}$, $q'=r'=2$	
$\mathcal{K}_{23}$	$k=0$, $p=1+2^{n-2}$, $(q',r')\in\{(2,0);(0,2)\}$	3
	$k=0$, $p=1+3\cdot 2^{n-2}$, $q'=r'=2$	
$\mathcal{K}_{24}$	$k=0$, $p=-1+3\cdot 2^{n-2}$, $(q',r')\in\{(2,0);(0,2)\}$	3
	$k=0$, $p=-1+2^{n-2}$, $q'=r'=2$	
$\mathcal{K}_{25}$	$k=0$, $p=1+3\cdot 2^{n-2}$, $(q',r')\in\{(2,0);(0,2)\}$	3
	$k=0$, $p=1+2^{n-2}$, $q'=r'=2$	

Table 9. Matrices from Proposition 3.6, form 1), $n\geqslant 4$

Cl	Matrix or conditions	NoE
$\mathcal{K}_{26}$	$k=0,\ p=-1+2^{n-2}z,\ q'r'\equiv 1\,(\mathrm{mod}\ 4)$	12
	$k=1,\ p\in\left\{-1+2^{n-1},-1+2^{n}\right\},\ \begin{cases} q'r'\equiv 0\,(\mathrm{mod}\ 4)\\ q'\neq r'\,(\mathrm{mod}\ 2)\end{cases}$	
$\mathcal{K}_{27}$	$k=1,\ p=-1+2^{n-2}z,\ q'r'\equiv 1\,(\mathrm{mod}\ 4)$	12
	$k=0,\ p\in\left\{-1+2^{n-1},-1+2^{n}\right\},\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{28}$	$k=0,\ p=1+2^{n-2}z,\ q'r'\equiv 1\,(\mathrm{mod}\ 4)$	12
	$k=1,\ p\in\left\{1,1+2^{n-1}\right\},\ \begin{cases} q'r'\equiv 0\,(\mathrm{mod}\ 4)\\ q'\neq r'\,(\mathrm{mod}\ 2)\end{cases}$	
$\mathcal{K}_{29}$	$k=1,\ p=1+2^{n-2}z,\ q'r'\equiv 1\,(\mathrm{mod}\ 4)$	12
	$k=0,\ p\in\left\{1,1+2^{n-1}\right\},\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{30}$	$k=0,\ p=-1+2^{n-2}z,\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	12
	$k=1,\ p\in\left\{-1+2^{n-1},-1+2^{n}\right\},\ q'r'\equiv 1\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{31}$	$k=1,\ p=-1+2^{n-2}z,\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	12
	$k=0,\ p\in\left\{-1+2^{n-1},-1+2^{n}\right\},\ q'r'\equiv 3\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{32}$	$k=0,\ p=1+2^{n-2}z,\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	12
	$k=1,\ p\in\left\{1,1+2^{n-1}\right\},\ q'r'\equiv 1\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{33}$	$k=1,\ p=1+2^{n-2}z,\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	12
	$k=0,\ p\in\left\{1,1+2^{n-1}\right\},\ q'r'\equiv 3\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{34}$	$k=0,\ p=-1+2^{n-2}z,\ q'r'\equiv 3\,(\mathrm{mod}\ 4)$	12
	$k=1,\ p\in\left\{-1+2^{n-1},-1+2^{n}\right\},\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{35}$	$k=1,\ p=-1+2^{n-2}z,\ q'r'\equiv 3\,(\mathrm{mod}\ 4)$	12
	$k=0,\ p\in\left\{-1+2^{n-1},-1+2^{n}\right\},\ \begin{cases} q'r'\equiv 0\,(\mathrm{mod}\ 4)\\ q'\neq r'\,(\mathrm{mod}\ 2)\end{cases}$	
$\mathcal{K}_{36}$	$k=0,\ p=1+2^{n-2}z,\ q'r'\equiv 3\,(\mathrm{mod}\ 4)$	12
	$k=1,\ p\in\left\{1,1+2^{n-1}\right\},\ q'r'\equiv 2\,(\mathrm{mod}\ 4)$	
$\mathcal{K}_{37}$	$k=1,\ p=1+2^{n-2}z,\ q'r'\equiv 3\,(\mathrm{mod}\ 4)$	12
	$k=0,\ p\in\left\{1,1+2^{n-1}\right\},\ \begin{cases} q'r'\equiv 0\,(\mathrm{mod}\ 4)\\ q'\neq r'\,(\mathrm{mod}\ 2)\end{cases}$	
$\mathcal{K}_{38}$	$k=1,\ p=-1+2^{n-2}z,\ q'=r'=2$	2
$\mathcal{K}_{39}$	$k=1,\ p=1+2^{n-2}z,\ q'=r'=2$	2

Table 9 (continued). Matrices from Proposition 3.6, form 1), $n\geqslant 4$

Cl	R	condition	NoE
$\mathcal{K}_{40}$	1	$(l,p) \in \left\{(1,1), \left(3, 1+3\cdot 2^{n-2}\right)\right\}$	14
	2	$l=1,\ p=1,\ f+g=2n-2$	10
		$l=1,\ p=1+2^{n-1},\ f+g=2n-3$	
		$l=3,\ p=1+2^{n-2},\ f+g=2n-3$	
		$l=3,\ p=1+3\cdot 2^{n-2},\ f+g=2n-2$	
$\mathcal{K}_{41}$	2	$f+g=2n-4,\ uv\equiv 1 \pmod 4,$ $(l,p) \in \left\{(1,1), \left(3, 1+3\cdot 2^{n-2}\right)\right\}$	8
		$f+g=2n-4,\ uv\equiv 3 \pmod 4,$ $(l,p) \in \left\{\left(1, 1+2^{n-1}\right), \left(3, 1+2^{n-2}\right)\right\}$	
$\mathcal{K}_{42}$	2	$f+g=2n-4,\ uv\equiv 3 \pmod 4,$ $(l,p) \in \left\{(1,1), \left(3, 1+3\cdot 2^{n-2}\right)\right\}$	8
		$f+g=2n-4,\ uv\equiv 1 \pmod 4,$ $(l,p) \in \left\{\left(1, 1+2^{n-1}\right), \left(3, 1+2^{n-2}\right)\right\}$	
$\mathcal{K}_{43}$	1	$(l,p) \in \left\{\left(1, 1+2^{n-1}\right), \left(3, 1+2^{n-2}\right)\right\}$	14
	2	$l=1,\ p=1,\ f+g=2n-3$	10
		$l=1,\ p=1+2^{n-1},\ f+g=2n-2$	
		$l=3,\ p=1+2^{n-2},\ f+g=2n-2$	
		$l=3,\ p=1+3\cdot 2^{n-2},\ f+g=2n-3$	
$\mathcal{K}_{44}$	1	$(l,p) \in \left\{\left(1, -1+2^{n-1}\right), \left(3, -1+2^{n-2}\right)\right\}$	14
	2	$l=1,\ p=-1+2^{n-1},\ f+g=2n-2$	10
		$l=1,\ p=-1+2^{n},\ f+g=2n-3$	
		$l=3,\ p=-1+2^{n-2},\ f+g=2n-2$	
		$l=3,\ p=-1+3\cdot 2^{n-2},\ f+g=2n-3$	
$\mathcal{K}_{45}$	2	$f+g=2n-4,\ uv\equiv 1 \pmod 4,$ $(l,p) \in \left\{\left(1, -1+2^{n-1}\right), \left(3, -1+2^{n-2}\right)\right\}$	8
		$f+g=2n-4,\ uv\equiv 3 \pmod 4,$ $(l,p) \in \left\{\left(1, -1+2^{n}\right), \left(3, -1+3\cdot 2^{n-2}\right)\right\}$	
$\mathcal{K}_{46}$	2	$f+g=2n-4,\ uv\equiv 3 \pmod 4,$ $(l,p) \in \left\{\left(1, -1+2^{n-1}\right), \left(3, -1+2^{n-2}\right)\right\}$	8
		$f+g=2n-4,\ uv\equiv 1 \pmod 4,$ $(l,p) \in \left\{\left(1, -1+2^{n}\right), \left(3, -1+3\cdot 2^{n-2}\right)\right\}$	
$\mathcal{K}_{47}$	1	$(l,p) \in \left\{\left(1, -1+2^{n}\right), \left(3, -1+3\cdot 2^{n-2}\right)\right\}$	14
	2	$l=1,\ p=-1+2^{n-1},\ f+g=2n-3$	10
		$l=1,\ p=-1+2^{n},\ f+g=2n-2$	
		$l=3,\ p=-1+2^{n-2},\ f+g=2n-3$	
		$l=3,\ p=-1+3\cdot 2^{n-2},\ f+g=2n-2$	

Table 10. Matrices from Proposition 3.6, form 2), $n \geqslant 4$

Cl	R	condition	NoE
$\mathcal{K}_{48}$	1	$(l,p) \in \left\{(3,-1+2^n), \left(1,-1+2^{n-2}\right)\right\}$	14
	2	$l=3$, $p=-1+2^{n-1}$, $f+g=2n-3$	10
		$l=3$, $p=-1+2^n$, $f+g=2n-2$	
		$l=1$, $p=-1+2^{n-2}$, $f+g=2n-2$	
		$l=1$, $p=-1+3\cdot 2^{n-2}$, $f+g=2n-3$	
$\mathcal{K}_{49}$	2	$f+g=2n-4$, $uv \equiv 3 \pmod 4$, $(l,p) \in \left\{\left(3,-1+2^{n-1}\right), \left(1,-1+3\cdot 2^{n-2}\right)\right\}$	8
		$f+g=2n-4$, $uv \equiv 1 \pmod 4$, $(l,p) \in \left\{\left(3,-1+2^n\right), \left(1,-1+2^{n-2}\right)\right\}$	
$\mathcal{K}_{50}$	2	$f+g=2n-4$, $uv \equiv 1 \pmod 4$, $(l,p) \in \left\{\left(3,-1+2^{n-1}\right), \left(1,-1+3\cdot 2^{n-2}\right)\right\}$	8
		$f+g=2n-4$, $uv \equiv 3 \pmod 4$, $(l,p) \in \left\{\left(3,-1+2^n\right), \left(1,-1+2^{n-2}\right)\right\}$	
$\mathcal{K}_{51}$	1	$(l,p) \in \left\{\left(3,-1+2^{n-1}\right), \left(1,-1+3\cdot 2^{n-2}\right)\right\}$	14
	2	$l=3$, $p=-1+2^{n-1}$, $f+g=2n-2$	10
		$l=3$, $p=-1+2^n$, $f+g=2n-3$	
		$l=1$, $p=-1+2^{n-2}$, $f+g=2n-3$	
		$l=1$, $p=-1+3\cdot 2^{n-2}$, $f+g=2n-2$	
$\mathcal{K}_{52}$	1	$(l,p) \in \left\{(3,1), \left(1,1+2^{n-2}\right)\right\}$	14
	2	$l=3$, $p=1$, $f+g=2n-2$	10
		$l=3$, $p=1+2^{n-1}$, $f+g=2n-3$	
		$l=1$, $p=1+2^{n-2}$, $f+g=2n-2$	
		$l=1$, $p=1+3\cdot 2^{n-2}$, $f+g=2n-3$	
$\mathcal{K}_{53}$	2	$f+g=2n-4$, $uv \equiv 1 \pmod 4$, $(l,p) \in \left\{(3,1), \left(1,1+2^{n-2}\right)\right\}$	8
		$f+g=2n-4$, $uv \equiv 3 \pmod 4$, $(l,p) \in \left\{\left(3,1+2^{n-1}\right), \left(1,1+3\cdot 2^{n-2}\right)\right\}$	
$\mathcal{K}_{54}$	2	$f+g=2n-4$, $uv \equiv 3 \pmod 4$, $(l,p) \in \left\{(3,1), \left(1,1+2^{n-2}\right)\right\}$	8
		$f+g=2n-4$, $uv \equiv 1 \pmod 4$, $(l,p) \in \left\{\left(3,1+2^{n-1}\right), \left(1,1+3\cdot 2^{n-2}\right)\right\}$	
$\mathcal{K}_{55}$	1	$(l,p) \in \left\{\left(3,1+2^{n-1}\right), \left(1,1+3\cdot 2^{n-2}\right)\right\}$	14
	2	$l=3$, $p=1$, $f+g=2n-3$	10
		$l=3$, $p=1+2^{n-1}$, $f+g=2n-2$	
		$l=1$, $p=1+2^{n-2}$, $f+g=2n-3$	
		$l=1$, $p=1+3\cdot 2^{n-2}$, $f+g=2n-2$	

Table 10 (continued). Matrices from Proposition 3.6, form 2), $n \geqslant 4$

For the next table we denote expression $uv - 2^{n-(f+g)-1}y + \left(\varepsilon + 2^{f+g-2}p\right)p$ by ls.

Cl	F	R	condition	NoE
$\mathcal{K}_{56}$	3)	1	$p \in \left\{-1+2^{n-1}, 1+2^{n-2}\right\}$	$n1$
		2	$p \in \left\{-1+2^{n-1}, 1+2^{n-2}\right\},\ f+g>n$	$n2$
			$p \in \left\{-1+2^{n}, 1+3\cdot 2^{n-2}\right\},\ f+g=n$	
	4)		$\varepsilon=1,\ y=1,\ ls \equiv 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon=-1,\ y=0,\ ls \equiv M+2^{n-3}p \pmod{2M}$	
	5)		$p=1,\ uv \equiv 1 \pmod 4$	$n6$
			$p=1+2^{n-1},\ uv \equiv 3 \pmod 4$	
$\mathcal{K}_{57}$	3)	1	$p \in \left\{-1+2^{n}, 1+3\cdot 2^{n-2}\right\}$	$n1$
		2	$p \in \left\{-1+2^{n-1}, 1+2^{n-2}\right\},\ f+g=n$	$n2$
			$p \in \left\{-1+2^{n}, 1+3\cdot 2^{n-2}\right\},\ f+g>n$	
	4)		$\varepsilon=1,\ y=1,\ ls \equiv M+3\cdot 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon=-1,\ y=0,\ ls \equiv 3\cdot 2^{n-3}p \pmod{2M}$	
	5)		$p=1,\ uv \equiv 3 \pmod 4$	$n6$
			$p=1+2^{n-1},\ uv \equiv 1 \pmod 4$	
$\mathcal{K}_{60}$	3)	1	$p \in \left\{1, -1+3\cdot 2^{n-2}\right\}$	$n1$
		2	$p \in \left\{1, -1+3\cdot 2^{n-2}\right\},\ f+g>n$	$n2$
			$p \in \left\{1+2^{n-1}, -1+2^{n-2}\right\},\ f+g=n$	
	4)		$\varepsilon=1,\ y=0,\ ls \equiv 3\cdot 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon=-1,\ y=1,\ ls \equiv -2^{n-3}p \pmod{2M}$	
	5)		$p=-1+2^{n-1},\ uv \equiv 3 \pmod 4$	$n6$
			$p=-1+2^{n},\ uv \equiv 1 \pmod 4$	
$\mathcal{K}_{61}$	3)	1	$p \in \left\{1+2^{n-1}, -1+2^{n-2}\right\}$	$n1$
		2	$p \in \left\{1, -1+3\cdot 2^{n-2}\right\},\ f+g=n$	$n2$
			$p \in \left\{1+2^{n-1}, -1+2^{n-2}\right\},\ f+g>n$	
	4)		$\varepsilon=1,\ y=0,\ ls \equiv M+2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon=-1,\ y=1,\ ls \equiv M+2^{n-3}p \pmod{2M}$	
	5)		$p=-1+2^{n-1},\ uv \equiv 1 \pmod 4$	$n6$
			$p=-1+2^{n},\ uv \equiv 3 \pmod 4$	

Table 11. Matrices described in Proposition 3.6, forms 3), 4) and 5), $n \geqslant 4$, $l = 3$

Cl	F	R	condition	NoE
$\mathcal{K}_{58}$	3)	1	$p \in \{1, -1+2^{n-2}\}$	$n1$
		2	$p \in \{1, -1+2^{n-2}\},\ f+g > n$	$n2$
			$p \in \{1+2^{n-1}, -1+3\cdot 2^{n-2}\},\ f+g = n$	
	4)		$\varepsilon = 1,\ y = 0,\ ls \equiv 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon = -1,\ y = 1,\ ls \equiv M + 2^{n-3}p \pmod{2M}$	
	5)		$p = -1+2^{n-1},\ uv \equiv 1 \pmod 4$	$n6$
			$p = -1+2^{n},\ uv \equiv 3 \pmod 4$	
$\mathcal{K}_{59}$	3)	1	$p \in \{1+2^{n}, -1+3\cdot 2^{n-2}\}$	$n1$
		2	$p \in \{1, -1+2^{n-2}\},\ f+g = n$	$n2$
			$p \in \{1+2^{n-1}, -1+3\cdot 2^{n-2}\},\ f+g > n$	
	4)		$\varepsilon = 1,\ y = 0,\ ls \equiv M - 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon = -1,\ y = 1,\ ls \equiv -2^{n-3}p \pmod{2M}$	
	5)		$p = -1+2^{n-1},\ uv \equiv 3 \pmod 4$	$n6$
			$p = -1+2^{n},\ uv \equiv 1 \pmod 4$	
$\mathcal{K}_{62}$	3)	1	$p \in \{-1+2^{n}, 1+2^{n-2}\}$	$n1$
		2	$p \in \{-1+2^{n}, 1+2^{n-2}\},\ f+g > n$	$n2$
			$p \in \{-1+2^{n-1}, 1+3\cdot 2^{n-2}\},\ f+g = n$	
	4)		$\varepsilon = 1,\ y = 1,\ ls \equiv 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon = -1,\ y = 0,\ ls \equiv 2^{n-3}p \pmod{2M}$	
	5)		$p = 1,\ uv \equiv 1 \pmod 4$	$n6$
			$p = 1+2^{n-1},\ uv \equiv 3 \pmod 4$	
$\mathcal{K}_{63}$	3)	1	$p \in \{-1+2^{n-1}, 1+3\cdot 2^{n-2}\}$	$n1$
		2	$p \in \{-1+2^{n}, 1+2^{n-2}\},\ f+g = n$	$n2$
			$p \in \{-1+2^{n-1}, 1+3\cdot 2^{n-2}\},\ f+g > n$	
	4)		$\varepsilon = 1,\ y = 1,\ ls \equiv M - 2^{n-3}p \pmod{2M}$	$n5$
			$\varepsilon = -1,\ y = 0,\ ls \equiv M - 2^{n-3}p \pmod{2M}$	
	5)		$p = 1,\ uv \equiv 3 \pmod 4$	$n6$
			$p = 1+2^{n-1},\ uv \equiv 1 \pmod 4$	

Table 12. Matrices described in Proposition 3.6, forms 3), 4) and 5), $n \geqslant 4$, $l = 1$

Remark. If $f+g = 3$, then $2^{n-3} \equiv 2^{n-(f+g)} \pmod{2^{n-(f+g)+1}}$, and if $f+g \geqslant 4$, then $2^{n-3} \equiv 0 \pmod{2^{n-(f+g)+1}}$.

E Representatives of conjugacy classes of matrices over $\mathbb{Z}_{2^n}$ of order 4

Representatives of conjugacy classes in the case if $n = 3$ are $\mathcal{A}_1 - \mathcal{A}_7$ and $\mathcal{A}_8^3 - \mathcal{A}_{19}^3$ and in the case if $n \geqslant 4$ are $\mathcal{A}_1 - \mathcal{A}_7$ and $\mathcal{A}_8 - \mathcal{A}_{63}$.
If $n \geqslant 3$

$$\begin{array}{ll}
\mathcal{A}_1 = \left\{\{0,1\},\left\{-1+2^{n-1},0\right\}\right\} & \mathcal{A}_2 = \left\{\{0,1\},\left\{1+2^{n-1},0\right\}\right\} \\
\mathcal{A}_3 = \{\{0,1\},\{-1+2^n,0\}\} & \mathcal{A}_4 = \left\{\{0,1\},\left\{1,2^{n-1}\right\}\right\} \\
\mathcal{A}_5 = \left\{\{0,1\},\left\{-1+2^{n-1},2^{n-1}\right\}\right\} & \mathcal{A}_6 = \left\{\{0,1\},\left\{1+2^{n-1},2^{n-1}\right\}\right\} \\
\mathcal{A}_7 = \left\{\{0,1\},\left\{-1+2^n,2^{n-1}\right\}\right\} &
\end{array}$$

If $n = 3$:

$$\begin{array}{lll}
\mathcal{A}_8^3 = \{\{1,2\},\{2,7\}\} & \mathcal{A}_9^3 = \{\{3,2\},\{2,5\}\} & \mathcal{A}_{10}^3 = \{\{1,2\},\{2,3\}\} \\
\mathcal{A}_{11}^3 = \{\{5,2\},\{2,7\}\} & \mathcal{A}_{12}^3 = \{\{1,0\},\{2,1\}\} & \mathcal{A}_{13}^3 = \{\{1,2\},\{2,1\}\} \\
\mathcal{A}_{14}^3 = \{\{1,2\},\{4,1\}\} & \mathcal{A}_{15}^3 = \{\{1,6\},\{2,1\}\} & \mathcal{A}_{16}^3 = \{\{3,0\},\{2,3\}\} \\
\mathcal{A}_{17}^3 = \{\{3,2\},\{2,3\}\} & \mathcal{A}_{18}^3 = \{\{3,2\},\{4,3\}\} & \mathcal{A}_{19}^3 = \{\{3,2\},\{6,3\}\}
\end{array}$$

If $n \geqslant 4$:

$$\begin{array}{l}
\mathcal{A}_8 = \left\{\left\{-1+2^{n-2},0\right\},\left\{0,1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_9 = \left\{\left\{1+2^{n-2},0\right\},\left\{0,-1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{10} = \left\{\left\{-1+2^{n-2},0\right\},\left\{0,1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{11} = \left\{\left\{-1+3\cdot 2^{n-2},0\right\},\left\{0,1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{12} = \left\{\left\{-1+2^{n-2},0\right\},\left\{0,-1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{13} = \left\{\left\{-1+2^{n-2},0\right\},\left\{0,-1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{14} = \left\{\left\{1+2^{n-2},0\right\},\left\{0,1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{15} = \left\{\left\{1+2^{n-2},0\right\},\left\{0,1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{16} = \left\{\left\{-1+3\cdot 2^{n-2},0\right\},\left\{0,-1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{17} = \left\{\left\{1+3\cdot 2^{n-2},0\right\},\left\{0,1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{18} = \left\{\left\{-1+2^{n-2},0\right\},\left\{2^{n-2},-1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{19} = \left\{\left\{-1+2^{n-2},0\right\},\left\{2^{n-2},-1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{20} = \left\{\left\{1+2^{n-2},0\right\},\left\{2^{n-2},1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{21} = \left\{\left\{1+2^{n-2},0\right\},\left\{2^{n-2},1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{22} = \left\{\left\{-1+2^{n-2},0\right\},\left\{2^{n-1},-1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{23} = \left\{\left\{1+2^{n-2},0\right\},\left\{2^{n-1},1+2^{n-2}\right\}\right\} \\
\mathcal{A}_{24} = \left\{\left\{-1+3\cdot 2^{n-2},0\right\},\left\{2^{n-1},-1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{25} = \left\{\left\{1+3\cdot 2^{n-2},0\right\},\left\{2^{n-1},1+3\cdot 2^{n-2}\right\}\right\} \\
\mathcal{A}_{26} = \left\{\left\{-1+2^n,0\right\},\left\{2^{n-2},-1+2^{n-1}\right\}\right\} \\
\mathcal{A}_{27} = \left\{\left\{-1+2^n,2^{n-2}\right\},\left\{2^{n-1},-1+2^n\right\}\right\} \\
\mathcal{A}_{28} = \left\{\{1,0\},\left\{2^{n-2},1+2^{n-1}\right\}\right\}
\end{array}$$

$$\mathcal{A}_{29} = \left\{\left\{1, 2^{n-2}\right\}, \left\{2^{n-1}, 1\right\}\right\}$$
$$\mathcal{A}_{30} = \left\{\left\{-1+2^{n}, 2^{n-2}\right\}, \left\{2^{n-2}, -1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{31} = \left\{\left\{-1+2^{n}, 2^{n-2}\right\}, \left\{3\cdot 2^{n-2}, -1+2^{n}\right\}\right\}$$
$$\mathcal{A}_{32} = \left\{\left\{1, 2^{n-2}\right\}, \left\{2^{n-2}, 1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{33} = \left\{\left\{1, 2^{n-2}\right\}, \left\{3\cdot 2^{n-2}, 1\right\}\right\}$$
$$\mathcal{A}_{34} = \left\{\left\{-1+2^{n}, 2^{n-2}\right\}, \left\{2^{n-1}, -1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{35} = \left\{\left\{-1+2^{n}, 0\right\}, \left\{2^{n-2}, -1+2^{n}\right\}\right\}$$
$$\mathcal{A}_{36} = \left\{\left\{1, 2^{n-2}\right\}, \left\{2^{n-1}, 1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{37} = \left\{\left\{1, 0\right\}, \left\{2^{n-2}, 1\right\}\right\}$$
$$\mathcal{A}_{38} = \left\{\left\{-1+2^{n-2}, 2^{n-1}\right\}, \left\{2^{n-1}, -1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{39} = \left\{\left\{1+2^{n-2}, 2^{n-1}\right\}, \left\{2^{n-1}, 1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{40} = \left\{\left\{1, 0\right\}, \left\{0, 1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{41} = \left\{\left\{1, 2^{n-2}\right\}, \left\{2^{n-2}, 1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{42} = \left\{\left\{1, 2^{n-2}\right\}, \left\{3\cdot 2^{n-2}, 1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{43} = \left\{\left\{1+2^{n-1}, 0\right\}, \left\{0, 1+2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{44} = \left\{\left\{-1+2^{n-1}, 0\right\}, \left\{0, -1+2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{45} = \left\{\left\{-1+2^{n-1}, 2^{n-2}\right\}, \left\{2^{n-2}, -1+2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{46} = \left\{\left\{-1+2^{n-1}, 2^{n-2}\right\}, \left\{3\cdot 2^{n-2}, -1+2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{47} = \left\{\left\{-1+2^{n}, 0\right\}, \left\{0, -1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{48} = \left\{\left\{-1+2^{n-2}, 0\right\}, \left\{0, -1+2^{n}\right\}\right\}$$
$$\mathcal{A}_{49} = \left\{\left\{-1+2^{n-2}, 2^{n-2}\right\}, \left\{2^{n-2}, -1+2^{n}\right\}\right\}$$
$$\mathcal{A}_{50} = \left\{\left\{-1+2^{n-2}, 2^{n-2}\right\}, \left\{3\cdot 2^{n-2}, -1+2^{n}\right\}\right\}$$
$$\mathcal{A}_{51} = \left\{\left\{-1+3\cdot 2^{n-2}, 0\right\}, \left\{0, -1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{52} = \left\{\left\{1+2^{n-2}, 0\right\}, \left\{0, 1\right\}\right\}$$
$$\mathcal{A}_{53} = \left\{\left\{1+2^{n-2}, 2^{n-2}\right\}, \left\{2^{n-2}, 1\right\}\right\}$$
$$\mathcal{A}_{54} = \left\{\left\{1+2^{n-2}, 2^{n-2}\right\}, \left\{3\cdot 2^{n-2}, 1\right\}\right\}$$
$$\mathcal{A}_{55} = \left\{\left\{1+3\cdot 2^{n-2}, 0\right\}, \left\{0, 1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{56} = \left\{\left\{-1+2^{n-1}, 0\right\}, \left\{0, 1+2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{57} = \left\{\left\{-1+2^{n}, 0\right\}, \left\{0, 1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{58} = \left\{\left\{-1+2^{n-2}, 0\right\}, \left\{0, 1\right\}\right\}$$
$$\mathcal{A}_{59} = \left\{\left\{-1+3\cdot 2^{n-2}, 0\right\}, \left\{0, 1+2^{n-1}\right\}\right\}$$
$$\mathcal{A}_{60} = \left\{\left\{1, 0\right\}, \left\{0, -1+3\cdot 2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{61} = \left\{\left\{1+2^{n-1}, 0\right\}, \left\{0, -1+2^{n-2}\right\}\right\}$$
$$\mathcal{A}_{62} = \left\{\left\{1+2^{n-2}, 0\right\}, \left\{0, -1+2^{n}\right\}\right\}$$
$$\mathcal{A}_{63} = \left\{\left\{1+3\cdot 2^{n-2}, 0\right\}, \left\{0, -1+2^{n-1}\right\}\right\}$$

F ELULOOKIRJELDUS

1. **Isikuandmed:**

   Ees-ja perekonnanimi: Tatjana Tamberg
   enne okt. 2008: Gramušnjak
   Sünniaeg ja -koht: 15. november 1973, Tallinn
   Kodakondsus: Eesti

2. **Kontaktandmed:**

   Aadress: Sütiste tee 3-62, Tallinn, 13419
   Telefon: 6 527 921
   E-posti aadress: tatjana@tlu.ee

3. **Hariduskäik:**

Õppeasutus (nimetus lõpetamise ajal)	**Lõpetamise aeg**	**Haridus (eriala/kraad)**
Tallinna Pedagoogikaülikool	1999	MSc matemaatika alal
Tallinna Pedagoogikaülikool	1996	BSc matemaatika alal
Tallinna 53. Keskkool	1991	keskharidus

4. **Keelteoskus:**

Keel	**Tase**
vene	emakeel
eesti	kõrgtase
inglise	kesktase
saksa	algtase

5. **Teenistuskäik:**

Töötamise aeg	**Tööandja nimetus**	**Ametikoht**
2010 - 2015	Tallinna Ülikool, Matemaatika ja Loodusteaduste Instituut, Matemaatika osakond	lektor
2009 - 2012	Tallinna Tehnikaülikool, Küberneetika Instituut	teadur
2006 - 2010	Tallinna Ülikool, Matemaatika ja Loodusteaduste Instituut, Matemaatika osakond	assistent
1996 - 2006	Tallinna Pedagoogikaülikool, Matemaatika- ja Loodusteaduskond, Matemaatika osakond	assistent

6. **Teadustegevus:** ETF5900 ja ETF8627 põhitäitja; osalesin (ettekannetega) kuuel rahvusvahelisel konverentsil; ilmus 5 teaduslikku artiklit eelretsenseeritavates rahvusvahelistes ajakirjades või kogumikes.

7. **Kaitstud lõputööd:** magistritöö "Positiivselt määratud ruutvormide C-tüüpide leidmise probleemidest", 1999, (juh.) prof. Paul Tammela

8. **Teadustöö põhisuunad:** lõplikud 2-rühmad, mõnede lõplikute 2-rühmade kirjeldus nende endomorfismipoolrühmadega.

9. **Teised uurimisprojektid:** SF0140083s08 (Mittelineaarsed, puuduliku informatsiooni ja keeruka struktuuriga matemaatilised mudelid)

G CURRICULUM VITAE

1. **Personal data:**

Name:	Tatjana Tamberg before oct. 2008: Gramušnjak
Date and place of birth:	November 15, 1973, Tallinn

2. **Contact information:**

Address:	Sütiste tee 3-62, Tallinn, 13419
Phone:	6 527 921
E-mail:	tatjana@tlu.ee

3. **Education:**

Educational institution	**Graduational year**	**Education (field of study/degree)**
Pedagogical University of Tallinn	1999	MSc in Mathematics
Pedagogical University of Tallinn	1996	BSc in Mathematics
Tallinn High School No. 53	1991	High school

4. **Language competence:**

Language	**Level**
russian	native
estonian	fluent
english	average
german	basic

5. **Professional Employment:**

Period	**Organisation**	**Position**
2010 - 2015	Tallinn University, Institute of Mathematics and Natural Sciences, dept. of Mathematics	lecturer
2009 - 2012	Tallinn University of Technology, Institute of Cybernetics	researcher
2006 - 2010	Tallinn University, Institute of Mathematics and Natural Sciences, dept. of Mathematics	assist. prof.
1996 - 2006	Pedagogical University of Tallinn, Faculty of Mathematics and Natural Sciences, dept. of Mathematics	assist. prof.

6. **Scientific work:** research staff of ETF5900 and ETF8627, it is published 5 papers in pre-reviewed journals or proceedings, it is attended 6 international conferences (with conference presentations)

7. **Defended theses:** Master's Thesis "On problems of finding of C-types of positive definite quadratic forms" 1999, (sup.) prof. Paul Tammela

8. **Main areas of scientific work / Current research topic:** finite 2-groups, characterization of some finite 2-groups by their endomorphism semigroups.

9. **Other research projects:** SF0140083s08 (Mathematical models with nonlinearities, incomplete information and structural complexity)

DISSERTATIONS DEFENDED AT TALLINN UNIVERSITY OF TECHNOLOGY ON *NATURAL AND EXACT SCIENCES*

1. **Olav Kongas**. Nonlinear Dynamics in Modeling Cardiac Arrhytmias. 1998.

2. **Kalju Vanatalu**. Optimization of Processes of Microbial Biosynthesis of Isotopically Labeled Biomolecules and Their Complexes. 1999.

3. **Ahto Buldas**. An Algebraic Approach to the Structure of Graphs. 1999.

4. **Monika Drews**. A Metabolic Study of Insect Cells in Batch and Continuous Culture: Application of Chemostat and Turbidostat to the Production of Recombinant Proteins. 1999.

5. **Eola Valdre**. Endothelial-Specific Regulation of Vessel Formation: Role of Receptor Tyrosine Kinases. 2000.

6. **Kalju Lott**. Doping and Defect Thermodynamic Equilibrium in ZnS. 2000.

7. **Reet Koljak**. Novel Fatty Acid Dioxygenases from the Corals *Plexaura homomalla* and *Gersemia fruticosa.* 2001.

8. **Anne Paju**. Asymmetric oxidation of Prochiral and Racemic Ketones by Using Sharpless Catalyst. 2001.

9. **Marko Vendelin**. Cardiac Mechanoenergetics *in silico*. 2001.

10. **Pearu Peterson**. Multi-Soliton Interactions and the Inverse Problem of Wave Crest. 2001.

11. **Anne Menert**. Microcalorimetry of Anaerobic Digestion. 2001.

12. **Toomas Tiivel**. The Role of the Mitochondrial Outer Membrane in *in vivo* Regulation of Respiration in Normal Heart and Skeletal Muscle Cell. 2002.

13. **Olle Hints**. Ordovician Scolecodonts of Estonia and Neighbouring Areas: Taxonomy, Distribution, Palaeoecology, and Application. 2002.

14. **Jaak Nõlvak**. Chitinozoan Biostratigrapy in the Ordovician of Baltoscandia. 2002.

15. **Liivi Kluge**. On Algebraic Structure of Pre-Operad. 2002.

16. **Jaanus Lass**. Biosignal Interpretation: Study of Cardiac Arrhytmias and Electromagnetic Field Effects on Human Nervous System. 2002.

17. **Janek Peterson**. Synthesis, Structural Characterization and Modification of PAMAM Dendrimers. 2002.

18. **Merike Vaher**. Room Temperature Ionic Liquids as Background Electrolyte Additives in Capillary Electrophoresis. 2002.

19. **Valdek Mikli**. Electron Microscopy and Image Analysis Study of Powdered Hardmetal Materials and Optoelectronic Thin Films. 2003.

20. **Mart Viljus**. The Microstructure and Properties of Fine-Grained Cermets. 2003.

21. **Signe Kask**. Identification and Characterization of Dairy-Related *Lactobacillus.* 2003

22. **Tiiu-Mai Laht**. Influence of Microstructure of the Curd on Enzymatic and Microbiological Processes in Swiss-Type Cheese. 2003.

23. **Anne Kuusksalu**. 2–5A Synthetase in the Marine Sponge *Geodia cydonium*. 2003.

24. **Sergei Bereznev**. Solar Cells Based on Polycristalline Copper-Indium Chalcogenides and Conductive Polymers. 2003.

25. **Kadri Kriis**. Asymmetric Synthesis of C_2-Symmetric Bimorpholines and Their Application as Chiral Ligands in the Transfer Hydrogenation of Aromatic Ketones. 2004.

26. **Jekaterina Reut**. Polypyrrole Coatings on Conducting and Insulating Substracts. 2004.

27. **Sven Nõmm**. Realization and Identification of Discrete-Time Nonlinear Systems. 2004.

28. **Olga Kijatkina**. Deposition of Copper Indium Disulphide Films by Chemical Spray Pyrolysis. 2004.

29. **Gert Tamberg**. On Sampling Operators Defined by Rogosinski, Hann and Blackman Windows. 2004.

30. **Monika Übner**. Interaction of Humic Substances with Metal Cations. 2004.

31. **Kaarel Adamberg**. Growth Characteristics of Non-Starter Lactic Acid Bacteria from Cheese. 2004.

32. **Imre Vallikivi**. Lipase-Catalysed Reactions of Prostaglandins. 2004.

33. **Merike Peld**. Substituted Apatites as Sorbents for Heavy Metals. 2005.

34. **Vitali Syritski**. Study of Synthesis and Redox Switching of Polypyrrole and Poly(3,4-ethylenedioxythiophene) by Using *in-situ* Techniques. 2004.

35. **Lee Põllumaa**. Evaluation of Ecotoxicological Effects Related to Oil Shale Industry. 2004.

36. **Riina Aav**. Synthesis of 9,11-Secosterols Intermediates. 2005.

37. **Andres Braunbrück**. Wave Interaction in Weakly Inhomogeneous Materials. 2005.

38. **Robert Kitt**. Generalised Scale-Invariance in Financial Time Series. 2005.

39. **Juss Pavelson**. Mesoscale Physical Processes and the Related Impact on the Summer Nutrient Fields and Phytoplankton Blooms in the Western Gulf of Finland. 2005.

40. **Olari Ilison**. Solitons and Solitary Waves in Media with Higher Order Dispersive and Nonlinear Effects. 2005.

41. **Maksim Säkki**. Intermittency and Long-Range Structurization of Heart Rate. 2005.

42. **Enli Kiipli**. Modelling Seawater Chemistry of the East Baltic Basin in the Late Ordovician–Early Silurian. 2005.

43. **Igor Golovtsov**. Modification of Conductive Properties and Processability of Polyparaphenylene, Polypyrrole and polyaniline. 2005.

44. **Katrin Laos**. Interaction Between Furcellaran and the Globular Proteins (Bovine Serum Albumin .β-Lactoglobulin). 2005.

45. **Arvo Mere**. Structural and Electrical Properties of Spray Deposited Copper Indium Disulphide Films for Solar Cells. 2006.

46. **Sille Ehala**. Development and Application of Various On- and Off-Line Analytical Methods for the Analysis of Bioactive Compounds. 2006.

47. **Maria Kulp**. Capillary Electrophoretic Monitoring of Biochemical Reaction Kinetics. 2006.

48. **Anu Aaspõllu.** Proteinases from *Vipera lebetina* Snake Venom Affecting Hemostasis. 2006.

49. **Lyudmila Chekulayeva**. Photosensitized Inactivation of Tumor Cells by Porphyrins and Chlorins. 2006.

50. **Merle Uudsemaa**. Quantum-Chemical Modeling of Solvated First Row Transition Metal Ions. 2006.

51. **Tagli Pitsi**. Nutrition Situation of Pre-School Children in Estonia from 1995 to 2004. 2006.

52. **Angela Ivask**. Luminescent Recombinant Sensor Bacteria for the Analysis of Bioavailable Heavy Metals. 2006.

53. **Tiina Lõugas**. Study on Physico-Chemical Properties and Some Bioactive Compounds of Sea Buckthorn (*Hippophae rhamnoides* L.). 2006.

54. **Kaja Kasemets**. Effect of Changing Environmental Conditions on the Fermentative Growth of *Saccharomyces cerevisae* S288C: Auxo-accelerostat Study. 2006.

55. **Ildar Nisamedtinov**. Application of ^{13}C and Fluorescence Labeling in Metabolic Studies of *Saccharomyces* spp. 2006.

56. **Alar Leibak**. On Additive Generalisation of Voronoï's Theory of Perfect Forms over Algebraic Number Fields. 2006.

57. **Andri Jagomägi**. Photoluminescence of Chalcopyrite Tellurides. 2006.

58. **Tõnu Martma**. Application of Carbon Isotopes to the Study of the Ordovician and Silurian of the Baltic. 2006.

59. **Marit Kauk**. Chemical Composition of $CuInSe_2$ Monograin Powders for Solar Cell Application. 2006.

60. **Julia Kois**. Electrochemical Deposition of $CuInSe_2$ Thin Films for Photovoltaic Applications. 2006.

61. **Ilona Oja Açik**. Sol-Gel Deposition of Titanium Dioxide Films. 2007.

62. **Tiia Anmann**. Integrated and Organized Cellular Bioenergetic Systems in Heart and Brain. 2007.

63. **Katrin Trummal**. Purification, Characterization and Specificity Studies of Metalloproteinases from *Vipera lebetina* Snake Venom. 2007.

64. **Gennadi Lessin**. Biochemical Definition of Coastal Zone Using Numerical Modeling and Measurement Data. 2007.

65. **Enno Pais**. Inverse problems to determine non-homogeneous degenerate memory kernels in heat flow. 2007.

66. **Maria Borissova**. Capillary Electrophoresis on Alkylimidazolium Salts. 2007.

67. **Karin Valmsen**. Prostaglandin Synthesis in the Coral *Plexaura homomalla*: Control of Prostaglandin Stereochemistry at Carbon 15 by Cyclooxygenases. 2007.

68. **Kristjan Piirimäe**. Long-Term Changes of Nutrient Fluxes in the Drainage Basin of the Gulf of Finland – Application of the PolFlow Model. 2007.

69. **Tatjana Dedova**. Chemical Spray Pyrolysis Deposition of Zinc Sulfide Thin Films and Zinc Oxide Nanostructured Layers. 2007.

70. **Katrin Tomson**. Production of Labelled Recombinant Proteins in Fed-Batch Systems in *Escherichia coli*. 2007.

71. **Cecilia Sarmiento**. Suppressors of RNA Silencing in Plants. 2008.

72. **Vilja Mardla**. Inhibition of Platelet Aggregation with Combination of Antiplatelet Agents. 2008.

73. **Maie Bachmann**. Effect of Modulated Microwave Radiation on Human Resting Electroencephalographic Signal. 2008.

74. **Dan Hüvonen**. Terahertz Spectroscopy of Low-Dimensional Spin Systems. 2008.

75. **Ly Villo**. Stereoselective Chemoenzymatic Synthesis of Deoxy Sugar Esters Involving *Candida antarctica* Lipase B. 2008.

76. **Johan Anton**. Technology of Integrated Photoelasticity for Residual Stress Measurement in Glass Articles of Axisymmetric Shape. 2008.

77. **Olga Volobujeva**. SEM Study of Selenization of Different Thin Metallic Films. 2008.

78. **Artur Jõgi**. Synthesis of 4'-Substituted 2,3'-dideoxynucleoside Analogues. 2008.

79. **Mario Kadastik**. Doubly Charged Higgs Boson Decays and Implications on Neutrino Physics. 2008.

80. **Fernando Pérez-Caballero**. Carbon Aerogels from 5-Methylresorcinol-Formaldehyde Gels. 2008.

81. **Sirje Vaask**. The Comparability, Reproducibility and Validity of Estonian Food Consumption Surveys. 2008.

82. **Anna Menaker**. Electrosynthesized Conducting Polymers, Polypyrrole and Poly(3,4-ethylenedioxythiophene), for Molecular Imprinting. 2009.

83. **Lauri Ilison**. Solitons and Solitary Waves in Hierarchical Korteweg-de Vries Type Systems. 2009.

84. **Kaia Ernits**. Study of In_2S_3 and ZnS Thin Films Deposited by Ultrasonic Spray Pyrolysis and Chemical Deposition. 2009.

85. **Veljo Sinivee**. Portable Spectrometer for Ionizing Radiation "Gammamapper". 2009.

86. **Jüri Virkepu**. On Lagrange Formalism for Lie Theory and Operadic Harmonic Oscillator in Low Dimensions. 2009.

87. **Marko Piirsoo**. Deciphering Molecular Basis of Schwann Cell Development. 2009.

88. **Kati Helmja**. Determination of Phenolic Compounds and Their Antioxidative Capability in Plant Extracts. 2010.

89. **Merike Sõmera**. Sobemoviruses: Genomic Organization, Potential for Recombination and Necessity of P1 in Systemic Infection. 2010.

90. **Kristjan Laes**. Preparation and Impedance Spectroscopy of Hybrid Structures Based on $CuIn_3Se_5$ Photoabsorber. 2010.

91. **Kristin Lippur**. Asymmetric Synthesis of 2,2'-Bimorpholine and its 5,5'-Substituted Derivatives. 2010.

92. **Merike Luman**. Dialysis Dose and Nutrition Assessment by an Optical Method. 2010.

93. **Mihhail Berezovski**. Numerical Simulation of Wave Propagation in Heterogeneous and Microstructured Materials. 2010.

94. **Tamara Aid-Pavlidis**. Structure and Regulation of BDNF Gene. 2010.

95. **Olga Bragina**. The Role of Sonic Hedgehog Pathway in Neuro- and Tumorigenesis. 2010.

96. **Merle Randrüüt**. Wave Propagation in Microstructured Solids: Solitary and Periodic Waves. 2010.

97. **Marju Laars**. Asymmetric Organocatalytic Michael and Aldol Reactions Mediated by Cyclic Amines. 2010.

98. **Maarja Grossberg**. Optical Properties of Multinary Semiconductor Compounds for Photovoltaic Applications. 2010.

99. **Alla Maloverjan**. Vertebrate Homologues of Drosophila Fused Kinase and Their Role in Sonic Hedgehog Signalling Pathway. 2010.

100. **Priit Pruunsild**. Neuronal Activity-Dependent Transcription Factors and Regulation of Human *BDNF* Gene. 2010.

101. **Tatjana Knjazeva**. New Approaches in Capillary Electrophoresis for Separation and Study of Proteins. 2011.

102. **Atanas Katerski**. Chemical Composition of Sprayed Copper Indium Disulfide Films for Nanostructured Solar Cells. 2011.

103. **Kristi Timmo.** Formation of Properties of $CuInSe_2$and $Cu_2ZnSn(S,Se)_4$ Monograin Powders Synthesized in Molten KI. 2011.

104. **Kert Tamm**. Wave Propagation and Interaction in Mindlin-Type Microstructured Solids: Numerical Simulation. 2011.

105. **Adrian Popp**. Ordovician Proetid Trilobites in Baltoscandia and Germany. 2011.

106. **Ove Pärn**. Sea Ice Deformation Events in the Gulf of Finland and This Impact on Shipping. 2011.

107. **Germo Väli**. Numerical Experiments on Matter Transport in the Baltic Sea. 2011.
108. **Andrus Seiman**. Point-of-Care Analyser Based on Capillary Electrophoresis. 2011.
109. **Olga Katargina**. Tick-Borne Pathogens Circulating in Estonia (Tick-Borne Encephalitis Virus, *Anaplasma phagocytophilum*, *Babesia* Species): Their Prevalence and Genetic Characterization. 2011.
110. **Ingrid Sumeri**. The Study of Probiotic Bacteria in Human Gastrointestinal Tract Simulator. 2011.
111. **Kairit Zovo**. Functional Characterization of Cellular Copper Proteome. 2011.
112. **Natalja Makarytsheva**. Analysis of Organic Species in Sediments and Soil by High Performance Separation Methods. 2011.
113. **Monika Mortimer**. Evaluation of the Biological Effects of Engineered Nanoparticles on Unicellular Pro- and Eukaryotic Organisms. 2011.
114. **Kersti Tepp**. Molecular System Bioenergetics of Cardiac Cells: Quantitative Analysis of Structure-Function Relationship. 2011.
115. **Anna-Liisa Peikolainen**. Organic Aerogels Based on 5-Methylresorcinol. 2011.
116. **Leeli Amon**. Palaeoecological Reconstruction of Late-Glacial Vegetation Dynamics in Eastern Baltic Area: A View Based on Plant Macrofossil Analysis. 2011.
117. **Tanel Peets**. Dispersion Analysis of Wave Motion in Microstructured Solids. 2011.
118. **Liina Kaupmees**. Selenization of Molybdenum as Contact Material in Solar Cells. 2011.
119. **Allan Olspert**. Properties of VPg and Coat Protein of Sobemoviruses. 2011.
120. **Kadri Koppel**. Food Category Appraisal Using Sensory Methods. 2011.
121. **Jelena Gorbatšova**. Development of Methods for CE Analysis of Plant Phenolics and Vitamins. 2011.
122. **Karin Viipsi**. Impact of EDTA and Humic Substances on the Removal of Cd and Zn from Aqueous Solutions by Apatite. 2012.
123. **David Schryer**. Metabolic Flux Analysis of Compartmentalized Systems Using Dynamic Isotopologue Modeling. 2012.
124. **Ardo Illaste**. Analysis of Molecular Movements in Cardiac Myocytes. 2012.
125. **Indrek Reile**. 3-Alkylcyclopentane-1,2-Diones in Asymmetric Oxidation and Alkylation Reactions. 2012.