Proceedings of the Estonian Academy of Sciences,
2010, **59**, 4, 370–374
doi: 10.3176/proc.2010.4.17
Available online at www.eap.ee/proceedings

MATHEMATICS

Finding a class of 2-groups

Tatjana Tamberg[a,b]

[a] Department of Mathematics, Tallinn University, Narva mnt. 25, 10120 Tallinn, Estonia
[b] Institute of Cybernetics at Tallinn University of Technology, Akadeemia tee 21, 12618 Tallinn, Estonia; tatjana@tlu.ee

Received 17 April 2009, accepted 25 June 2009

Abstract. Let $n \geq 3$ be an integer and C_m denote a cyclic group of order m. All groups which can be presented as a semidirect products $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$ are described. These groups are given by generators and defining relations.

Key words: group, semidirect product, automorphism.

1. INTRODUCTION

All non-Abelian groups of order < 32 are described in [1] (see table 1 at the end of the book). These groups are characterized by their endomorphism semigroups in [7–9]. Our aim is to describe the groups of order 32 by their endomorphism semigroups and to generalize the obtained results for some other classes of finite 2-groups. Hall and Senior [6] gave a full description of all groups of order 2^n, $n \leq 6$. There exist exactly 51 non-isomorphic groups of order 32. Some of them can be presented as a semidirect product $(C_{2^2} \times C_{2^2}) \leftthreetimes C_2$ and some of them in the form $(C_{2^3} \times C_2) \leftthreetimes C_2$. In [3] and [5] it is proved that all groups in these forms are determined by their endomorphism semigroups in the class of all groups. As a generalization of the case of groups which can be presented as a semidirect product $(C_{2^2} \times C_{2^2}) \leftthreetimes C_2$, in [4] all groups of the form $(C_{2^n} \times C_{2^n}) \leftthreetimes C_2$, $n \geqslant 3$, are described. It turned out that for a fixed $n \geq 3$ there exist only 17 non-isomorphic groups of this form. As a generalization of the second case, i.e., of groups which can be presented as a semidirect product $(C_{2^3} \times C_2) \leftthreetimes C_2$, in [2] all groups of the form $(C_{2^{n+m}} \times C_{2^n}) \leftthreetimes C_2$, $n \geqslant 3, m \geqslant 1$, are described by their defining relations.

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

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

for some $p, q, r, s \in \mathbb{Z}_{2^n}$ ($\mathbb{Z}_{2^n}$ is the ring of residue classes modulo 2^n). An element c generates an inner automorphism $\widehat{c}$ for which $\widehat{c}^{\,4} = 1$:

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

In order to find all groups in the given form, we have to find all automorphisms φ of the group $C_{2^n} \times C_{2^n}$ for which $\varphi^4 = 1$.

2. PRELIMINARIES

The group $C_{2^n} \times C_{2^n}$ is given by defining relations as follows:

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

It is clear that the map

$$\varphi : C_{2^n} \times C_{2^n} \longrightarrow C_{2^n} \times C_{2^n}, \quad a\varphi = a^p b^q, \quad b\varphi = a^r b^s, \tag{1}$$

where $p, q, r, s \in \mathbb{Z}_{2^n}$, preserves the defining relations of the group $C_{2^n} \times C_{2^n}$ and is an endomorphism of this group. Endomorphism (1) is an automorphism of $C_{2^n} \times C_{2^n}$ satisfying the equation $\varphi^4 = 1$ if and only if (p, q, r, s) is a solution of the next system modulo 2^n:

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

Endomorphism (1) is an automorphism of order 1 or 2 if and only if (p, q, r, s) satisfies the next system modulo 2^n:

$$\begin{cases} p^2 + rq \equiv 1, \ p^2 - s^2 \equiv 0, \\ q(p+s) \equiv r(p+s) \equiv 0. \end{cases} \tag{3}$$

If (p, q, r, s) satisfies system (2), then $p \equiv s \,(\mathrm{mod}\, 2)$. Assuming that $p \equiv s \,(\mathrm{mod}\, 2)$, it is easy to check that system (2) is equivalent to the system

$$\begin{cases} \left(p^2 + rq\right)^2 \equiv 1 \pmod{2^n}, \\ q\,(p+s) \equiv 0, \ \ r\,(p+s) \equiv 0, \ \ (p-s)\,(p+s) \equiv 0 \ \left(\mathrm{mod}\, 2^{n-1}\right). \end{cases} \tag{4}$$

3. SOLUTIONS OF SYSTEM (4)

In this section all $\varphi \in \mathrm{Aut}(C_{2^n} \times C_{2^n})$ satisfying $\varphi^4 = 1$ will be found ($n \geq 3$). For this purpose we have to solve system (4) under the assumption $p \equiv s \,(\mathrm{mod}\, 2)$. This assumption and the first equivalence of (4) imply that we have to study the following three cases: 1) p and s are even ($p, s \in 2\mathbb{Z}_{2^{n-1}}$), which implies that $q, r \in \mathbb{Z}^*_{2^n}$; 2) p and s are odd ($p, s \in \mathbb{Z}^*_{2^n}$, where $\mathbb{Z}^*_{2^n}$ denotes the group of invertible elements of the ring $\mathbb{Z}_{2^n}$), one of the numbers q and r is odd; 3) p and s are odd, q and r are even ($p, s \in \mathbb{Z}^*_{2^n}$; $q, r \in 2\mathbb{Z}_{2^{n-1}}$).

Proposition 1. *Let $p, s \in 2\mathbb{Z}_{2^{n-1}}$ and $q, r \in \mathbb{Z}^*_{2^n}$. Then map* (1) *is an automorphism of order* 1, 2 *or* 4 *of the group $C_{2^n} \times C_{2^n}$ if and only if*

$$s = -p + 2^{n-1}x,\ x \in \mathbb{Z}_2;\ q \in \mathbb{Z}^*_{2^n};\ r = (t - p^2)q^{-1},\ t \in \left\{\pm 1,\ \pm 1 + 2^{n-1}\right\}.$$

The number of those automorphisms is 2^{2n+1}.

The obtained automorphism is 1 *or has order* 2 *if and only if $t = 1$ and $x = 0$. The number of those automorphisms is* 2^{2n-2}.

Proof. Assume that $p, s \in 2\mathbb{Z}_{2^{n-1}}$ and $q, r \in \mathbb{Z}^*_{2^n}$. Denote $t = p^2 + rq$. Then system (4) is satisfied if and only if

$$q \in \mathbb{Z}^*_{2^n},\ s = -p + 2^{n-1}x,\ x \in \mathbb{Z}_2,\ r = (t - p^2)q^{-1},\ t \in \left\{\pm 1,\ \pm 1 + 2^{n-1}\right\}.$$

The obtained automorphism is 1 or has order 2, i.e., satisfies system (3), if and only if $t = 1$ and $x = 0$. Hence we get immediately the statements of Proposition 1. □

Proposition 2. *Let $p, s \in \mathbb{Z}^*_{2^n}$; $q, r \in \mathbb{Z}_{2^n}$ and $q \in \mathbb{Z}^*_{2^n}$ or $r \in \mathbb{Z}^*_{2^n}$. Then map* (1) *is an automorphism of order* 1, 2 *or* 4 *of the group $C_{2^n} \times C_{2^n}$ if and only if $s = -p + 2^{n-1}x$, $x \in \mathbb{Z}_2$ and* 1) *$q \in \mathbb{Z}^*_{2^n}$, $r = (t - p^2)q^{-1}$,* 2) *$r \in \mathbb{Z}^*_{2^n}$, $q = (t - p^2)r^{-1}$, where $t \in \{\pm 1, \pm 1 + 2^{n-1}\}$. The number of those automorphisms is 2^{2n+2}.*

The obtained automorphism is 1 *or has order* 2 *if and only if $t = 1$ and $x = 0$. The number of those automorphisms is 2^{2n-1}.*

Proof. Assume that p, s and one of the numbers q, r are odd. Denote $t = p^2 + rq$. Then system (4) is satisfied if and only if

$$s = -p + 2^{n-1}x,\ x \in \mathbb{Z}_2,\ t \in \{\pm 1,\ \pm 1 + 2^{n-1}\},$$

i.e., if $rq \in \{\pm 1 - p^2,\ \pm 1 + 2^{n-1} - p^2\}$. The obtained automorphism is 1 or has order 2, i.e., satisfies system (3), if and only if $t = 1$ and $x = 0$. Hence we get immediately the statements of Proposition 2. □

We have now to consider the last case: $p, s \in \mathbb{Z}^*_{2^n}$; $q, r \in 2\mathbb{Z}_{2^{n-1}}$. For the discussion of this case we will separate the cases $n = 3$ and $n \geq 4$. In the case $n = 3$ we get by easy calculations the following result.

Proposition 3. *Let $n = 3$ and $p, s \in \mathbb{Z}^*_8$, $q, r \in 2\mathbb{Z}_4$. Then map* (1) *is always an automorphism of order* 1, 2 *or* 4 *of the group $C_8 \times C_8$. The number of such automorphisms is $2^8 = 256$.*

The obtained automorphism is 1 *or has order* 2 *in the following three cases:* 1) *$r, q \in 4\mathbb{Z}_2$;* 2) *$s = -p + 4z$, $z \in \mathbb{Z}_2$, $r \in 4\mathbb{Z}_2$, $q \in 2\mathbb{Z}^*_4$;* 3) *$s = -p + 4z$, $z \in \mathbb{Z}_2$, $r \in 2\mathbb{Z}^*_4$, $q \in 4\mathbb{Z}_2$. The number of those automorphisms is $2^7 = 128$.*

Assume always in the following part of this section that $n \geq 4$ and $p, s \in \mathbb{Z}^*_{2^n}$; $q, r \in 2\mathbb{Z}_{2^{n-1}}$, i.e.,

$$r = 2^f u,\ q = 2^g v,\ u \in \mathbb{Z}^*_{2^{n-f}},\ v \in \mathbb{Z}^*_{2^{n-g}},\ 1 \leq f, g \leq n. \tag{5}$$

Lemma 1. *Let $n \geq 4$. The triple p, q, r (where $p \in \mathbb{Z}^*_{2^n}$ and $q, r \in 2\mathbb{Z}_{2^{n-1}}$ are given by* (5)) *satisfies the congruence $(p^2 + rq)^2 \equiv 1 \pmod{2^n}$ only in the following cases*:

a) *$p = \pm 1 + 2^{n-2}x$, $x \in \mathbb{Z}_4$, if $f + g \geq n - 1$ (the number of triples p, q, r of this form is $(n-1)\,2^{n+3}$);*

b) *$p = \varepsilon + 2^{f+g-1}x$, $v = (2^{n-f-g-1}t - x(\varepsilon + 2^{f+g-2}x))u^{-1+2^{n-f-g-1}} + 2^{n-f-g}k$, where $\varepsilon = \pm 1$, $x \in \mathbb{Z}^*_{2^{n-f-g+1}}$, $k \in \mathbb{Z}_{2^f}$, $t \in \mathbb{Z}_2$, if $3 \leq f + g < n - 1$ (the number of triples p, q, r of this form is $2^{n+3}\left(3 \cdot 2^{n-4} - n + 1\right)$).*

Proof. Assume that $f + g \geq n - 1$. Then

$$(p^2 + rq)^2 = (p^2 + 2^{f+g}uv)^2 = p^4 + 2^{f+g+1}p^2uv + 2^{2(f+g)}u^2v^2 \equiv p^4 \pmod{2^n}$$

and the congruence $(p^2 + rq)^2 \equiv 1 \pmod{2^n}$ is equivalent to the congruence $p^4 \equiv 1 \pmod{2^n}$. The solutions of the last congruence are $p = \pm 1 + 2^{n-2}x$, $x \in \mathbb{Z}_4$, i.e., statement a) is true.

Assume now that $f + g < n - 1$ and let us find the solutions of the congruence $(p^2 + rq)^2 \equiv 1 \pmod{2^n}$. Clearly, $p^2 + rq = \pm 1 + 2^{n-1}t$, $p^2 = \pm 1 + 2^{n-1}t - 2^{f+g}uv$, where $t \in \mathbb{Z}_2$. Since $p^2 \equiv 1 \pmod 8$, we have $f + g \geq 3$ and

$$p^2 = 1 + 2^{n-1}t - 2^{f+g}uv,\ t \in \mathbb{Z}_2. \tag{6}$$

The congruence $p^2 + rq \equiv 1 \pmod{2^n}$ was solved in [4]. Using the same technique, we obtain all solutions of equation (6). The result is given as statement b) of Lemma 1. □

Proposition 4. *Let $p, s \in \mathbb{Z}^*_{2^n}$, $n \geq 4$, and the pair q, r be given by* (5). *Then map* (1) *is an automorphism of order* 1, 2 *or* 4 *of the group $C_{2^n} \times C_{2^n}$ if and only if one of the following three conditions holds*:

I) *$f, g \geq n - 2$, $s = p - 2^{n-2}z$, $z \in \mathbb{Z}_4$ and the triple p, q, r is given by item* a) *of Lemma* 1;

II) *$s = -p + 2^{n-2}z$, $z \in \mathbb{Z}^*_4$ and the triple p, q, r is given by item* a) *or* b) *of Lemma* 1;

III) *$s = -p + 2^{n-1}z$, $z \in \mathbb{Z}_2$ and the triple p, q, r is given by item* a) *or* b) *of Lemma* 1.

The number of these automorphisms is $3 \cdot 2^{2n+1} + 2^9$.

The automorphisms obtained in case II) *have always order* 4. *In cases* I) *and* III) *an obtained automorphism has order* 1 *or* 2 *if and only if, respectively,*

I) $x \in 2\mathbb{Z}_2,\ z \in 2\mathbb{Z}_2,\ f, g \geq n-1$;
IIIa) $x \in 2\mathbb{Z}_2,\ f+g \geq n$ *or* $x \in \mathbb{Z}_4^*,\ f+g = n-1$;
IIIb) $t = 0$.
The number of obtained automorphisms of orders 1 *and* 2 *is* $3 \cdot 2^{2n-1} + 32$.

Proof. It is necessary to solve system (4) under the assumptions made in Proposition 4. Solutions p, q, r of the first congruence of (4) were found in Lemma 1. Let us find among them those that satisfy also the last three congruences of (4). We separate the cases $p+s \not\equiv 0 \,(\mathrm{mod}\, 2^{n-1})$ and $p+s \equiv 0 \,(\mathrm{mod}\, 2^{n-1})$.

Assume that $p+s \not\equiv 0 \,(\mathrm{mod}\, 2^{n-1})$, i.e.,

$$p+s = 2^m k,\ 1 \leq m < n-1,\ k \in \mathbb{Z}_{2^{n-m}}^*.$$

The last three congruences of (4) imply that

$$m \geq n-f-1,\ m \geq n-g-1,\ p-s \equiv 0 \,(\mathrm{mod}\, 2^{n-m-1}).$$

Therefore, for $p-s$ we have two cases: i) $p-s = 2^{n-m-1}w$ for some $w \in \mathbb{Z}_{2^{m+1}}^*$ and ii) $p-s = 2^{n-1}w$ for some $w \in \mathbb{Z}_2$. In case i) we have that $2p = (p+s)+(p-s) = 2^m k + 2^{n-m-1}w$ and

$$p = 2^{m-1}k + 2^{n-m-2}w. \tag{7}$$

Since p is odd, equality (7) is possible if $m = n-2$ or $m = 1$. If $n = m-2$, then

$$p = 2^{n-3}k + w,\ p-s = 2w,\ s = p-2w = p-2(p-2^{n-3}k) = -p+2^{n-2}k,$$

which corresponds to case II) of Proposition 4. If $m = 1$, then we obtain $f, g \geq n-2$, $p = k+2^{n-3}w$, and

$$s = -p+2k = -p+2(p-2^{n-3}w) = p-2^{n-2}w, \text{ where } w \in \mathbb{Z}_4^*.$$

Analogously, in case ii) we obtain also $m = 1$, $f, g \geq n-2$ and $s = p-2^{n-1}w$. So we get $s = p-2^{n-2}w$ for some $w \in \mathbb{Z}_4$, which corresponds to case I) of Proposition 4.

In the case $p+s \equiv 0 \,(\mathrm{mod}\, 2^{n-1})$ the last three congruences of (4) hold and we get case III) of Proposition 4.

After finding from the set of solutions of (4) those that satisfy system (3), we get all automorphisms of order 1 or 2 of the group $C_{2^n} \times C_{2^n}$. The result is formulated in the proposition. The statements on the numbers of automorphisms follow after easy calculations by using the values of the corresponding parameters. □

4. MAIN RESULT

We summarize the results obtained in previous sections in the following theorem.

Theorem 1. *Assume that* $n \geq 3$. *For each automorphism* φ *of the group* $C_{2^n} \times C_{2^n}$ *for which* $\varphi^4 = 1$ *the group*

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

is isomorphic to a semidirect product $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$. *Conversely, each semidirect product* $(C_{2^n} \times C_{2^n}) \leftthreetimes C_4$ *is isomorphic to a group* G_φ *for some* $\varphi \in \mathrm{Aut}(C_{2^n} \times C_{2^n})$, $\varphi^4 = 1$. *All these automorphisms are described in Propositions* 1–4.

Remark. If $\varphi \neq \psi$, then it is possible that the groups G_φ and G_ψ are isomorphic. We will find all non-isomorphic groups among these groups in some of our next papers.

ACKNOWLEDGEMENT

This work was partially supported by the Estonian Ministry of Education and Research (project SF0140083s08).

REFERENCES

1. Coxeter, H. S. M. and Moser, W. O. J. *Generators and Relations for Discrete Groups*. Springer-Verlag, 1972.
2. Gramushnjak, T. A characterization of a class of 2-groups by their defining relations. *J. Gen. Lie Theory Appl.*, 2008, **2**, 157–161.
3. Gramushnjak, T. and Puusemp, P. A characterization of a class of groups of order 32 by their endomorphism semigroups. *Algebras Groups Geom.*, 2005, **22**, 387–412.
4. Gramushnjak, T. and Puusemp, P. Description of a class of 2-Groups. *J. Nonlinear Math. Phys.*, 2006, **13**, 55–65.
5. Gramushnjak, T. and Puusemp, P. A characterization of a class of 2-groups by their endomorphism semigroups. Ch. 14 In *Generalized Lie Theory in Mathematics, Physics and Beyond* (Silvestrov, S. et al., eds). Springer-Verlag, Berlin, 2009, 151–159.
6. Hall, M., Jr. and Senior, J. K. *The Groups of Order* 2^n, $n \leq 6$. Macmillan, New York; Collier-Macmillan, London, 1964.
7. Puusemp, P. Non-abelian groups of order 16 and their endomorphism semigroups. *J. Math. Sci.*, 2005, **131**, 6098–6111.
8. Puusemp, P. Groups of order less than 32 and their endomorphism semigroups. *J. Nonlinear Math. Phys.*, 2006, **13**, Supplement, 93–101.
9. Puusemp, P. Groups of order 24 and their endomorphism semigroups. *J. Math. Sci.*, 2007, **144**, 3980–3992.

Ühe 2-rühmade klassi leidmine

Tatjana Tamberg

On jätkatud mõningate 2-rühmade klasside kirjeldamist moodustajate ja määravate seoste abil. On leitud kõik 2-rühmad, mis on esitatavad kujul $G = (C_{2^n} \times C_{2^n}) \leftthreetimes C_4$. Selleks on leitud selle rühma normaaljagaja $C_{2^n} \times C_{2^n}$ kõik ülimalt neljandat järku automorfismid. Osutub, et on olemas 640 (kui $n = 3$), $12 \cdot 4^n + 512$ (kui $n \geqslant 4$) rühma, mis on esitatavad antud kujul. Leitud 2-rühmade omavahelise isomorfsuse küsimust siin uuritud ei ole.