Journal of Generalized Lie Theory and Applications Vol. 2 (2008), No. 3, 157–161

A characterization of a class of 2-groups by their defining relations [1]

Tatjana GRAMUSHNJAK

Institute of Mathematics and Natural Sciences, Tallinn University, Narva mnt. 25, 10120 Tallinn, Estonia

E-mail: tatjana@tlu.ee

Abstract

Let n, m be integers such that $n \geq 3$, $m > 0$ and C_k a cyclic group of order k. All groups which can be presented as a semidirect product $(C_{2^{n+m}} \times C_{2^n}) \rightthreetimes C_2$ are described.

2000 MSC: 20E22, 20D40

1 Introduction

All non-Abelian groups of order < 32 are described in [1] (Table 1 at the end of the book). M. Jr. Hall and J. K. Senior [3] have given a fully 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 $(C_{2^2} \times C_{2^2}) \rightthreetimes C_2$ and some of them as a semidirect product $(C_{2^3} \times C_2) \rightthreetimes C_2$. As a generalization of the first case, in [2] all groups of the form $(C_{2^n} \times C_{2^n}) \rightthreetimes C_2$, $n \geqslant 3$, are described. It turned out that there exist only 17 non-isomorphic groups of this form (for a fixed n). In this paper we generalize the second case. Namely, we shall describe all finite 2-groups which can be presented in the form $(C_{2^{n+m}} \times C_{2^n}) \rightthreetimes C_2$, where $n \geq 3$ and $m \geqslant 1$. Clearly, each such group G is given by three generators a, b, c and by the defining relations

$$a^{2^{n+m}} = b^{2^n} = c^2 = 1, \quad ab = ba, \quad c^{-1}ac = a^p b^q, \quad c^{-1}bc = a^r b^s \tag{1.1}$$

for some $p, r \in \mathbb{Z}_{2^{n+m}}$ and $q,\ s \in \mathbb{Z}_{2^n}$ ($\mathbb{Z}_{2^k}$ – the ring of residue classes modulo 2^k).

The aim of this paper is to prove

Theorem 1.1. *For fixed $m > 0$ and $n \geqslant 3$ the number of groups which can be given by relations* (1.1) *is*

$$3 \cdot 4^n + 32 \quad (\textit{if } m = 1), \quad 4 \cdot 4^n + 32 \quad (\textit{if } m = 2), \quad 5 \cdot 4^n + 32 \quad (\textit{if } m \geqslant 3)$$

All possible values of (p, q, r, s) are given in Propositions 3.1, 3.2, 3.3 *if $m < n$, in* 3.1, 3.2 *if $m = n$ and in* 3.4, 3.5 *if $m > n$.*

2 Main concepts for the proof of Theorem 1.1

Let $G = (\langle a \rangle \times \langle b \rangle) \rightthreetimes \langle c \rangle$ be a group given by (1.1). An element c induces an inner automorphism $\widehat{c}$ of order two (the case $\widehat{c} = 1$ is also included) of group $\langle a \rangle \times \langle b \rangle$:

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

[1] Presented at the 3rd Baltic-Nordic Workshop "Algebra, Geometry, and Mathematical Physics", Göteborg, Sweden, October 11–13, 2007.

Therefore, we have to find all automorphisms of $\langle a\rangle \times \langle b\rangle$ of order two. The map $a\varphi = a^p b^q$, $b\varphi = a^r b^s$ induces an endomorphism of group $\langle a\rangle \times \langle b\rangle$ if and only if $r \equiv 0 \pmod{2^m}$. This endomorphism is an automorphism, if and only if $p \equiv s \equiv 1 \pmod 2$. This map is an automorphism of order two if and only if (p, q, r, s) satisfy the system

$$\begin{cases} p^2 + rq \equiv 1 \\ pr + rs \equiv 0 \end{cases} \pmod{2^{n+m}}, \quad \begin{cases} pq + sq \equiv 0 \\ qr + s^2 \equiv 1 \end{cases} \pmod{2^n} \tag{2.1}$$
$$p \equiv s \equiv 1 \pmod 2, \quad r \equiv 0 \pmod{2^m}$$

Our purpose is to solve system (2.1). Note that the two first subsystems of (2.1) imply the following system modulo 2^n:

$$p^2 + rq \equiv 1, \quad pr + rs \equiv 0, \quad pq + sq \equiv 0, \quad qr + s^2 \equiv 1 \tag{2.2}$$

The solutions (p, q, r, s) of system (2.2) form a set $\mathcal{M}$ which was described in [2]. In [2] the set $\mathcal{M}$ was given as the union of disjoined subsets $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_{10}$.

Let $(p, q, r, s) = (f, q, g, s) \in \mathcal{M}$ be a solution of system (2.2), where $q, g \in \mathbb{Z}_{2^n}$ and $f, s \in \mathbb{Z}^*_{2^n}$ ($\mathbb{Z}^*_{2^n}$ denotes the set of all invertible elements of $\mathbb{Z}_{2^n}$). Then p and r can be replaced in (2.1) by

$$p = f + 2^n x, \quad r = g + 2^n y, \quad \text{where} \quad x, y \in \mathbb{Z}_{2^m}$$

Now it is easy to see that system (2.1) is equivalent to the system

$$(f + 2^n x)^2 + (g + 2^n y)\, q \equiv 1 \pmod{2^{n+m}}, \quad (g + 2^n y)\,(f + 2^n x + g) \equiv 0 \pmod{2^{n+m}} \tag{2.3}$$

where $(f, q, g, s) \in \mathcal{M}$, $q, g \in \mathbb{Z}_{2^n}$, $f, s \in \mathbb{Z}^*_{2^n}$ and

$$g \equiv 0 \pmod{2^m} \ \text{ if } m \leqslant n, \quad y \equiv 0 \pmod{2^{m-n}} \quad \text{and } g = 0 \ \text{ if } m > n \tag{2.4}$$

Remark, that $h \in \mathbb{Z}_k$ means the representative of residue class; moreover, we always can choose $h \in \{0, 1, \ldots, k-1\}$.

Because the length of the paper is limited, for most of statements we give only idea of proof.

3 Solving system (2.1)

3.1 The case $m \leqslant n$

Assume that $m \leqslant n$. Then $g \equiv 0 \pmod{2^m}$ and system (2.3) takes the form

$$f^2 + 2^{n+1} f x + (g + 2^n y)\, q \equiv 1 \pmod{2^{n+m}}, \quad (g + 2^n y)\,(f + s) \equiv 0 \pmod{2^{n+m}} \tag{3.1}$$

Proposition 3.1. *Assume that $m \leqslant n$ and q is odd. Then the solutions (p, q, r, s) of (2.1) are of the form $(i + 2^n x, j, g + 2^n y, -i)$, where*

$$y \equiv \left(\left(1 - i^2 - gj\right)/2^n - 2ix\right) j^{-1} \pmod{2^m}, \quad x \in \mathbb{Z}_{2^m}$$

and $g = (1 - i^2)j^{-1}$, $i = i_0 + 2^m k$, $k \in \mathbb{Z}_{2^{n-m}}$, where $i_0 \in \left\{1, -1 + 2^m, \pm 1 + 2^{m-1}\right\}$ if $m \geqslant 3$, $i_0 \in \{1, -1 + 2^m\}$ if $m = 2$, $i_0 = 1$ if $m = 1$. There are exactly 2^{2n+1} solutions of this form if $m \geqslant 3$, exactly 2^{2n} solutions if $m = 2$ and exactly 2^{2n-1} solutions if $m = 1$.

Proof. The condition of the proposition, conditions (2.4) and $f, s \in \mathbb{Z}^*_{2^n}$ by [2] are satisfied for solution of (2.2) from the set $\mathcal{M}_2 = \left\{\left(i, j, (1 - i^2)j^{-1}, -i\right) \mid i \in \mathbb{Z}^*_{2^n},\ j \in \mathbb{Z}^*_{2^n}\right\}$. While $g = (1 - i^2)j^{-1} \equiv 0 \pmod{2^m}$, we have $i^2 \equiv 1 \pmod{2^m}$, i.e $i = i_0 + 2^m k$, where $k \in \mathbb{Z}_{2^{n-m}}$ and $i_0 \in \left\{1, -1 + 2^m, \pm 1 + 2^{m-1}\right\}$ if $m \geqslant 3$, $i_0 \in \{1, -1 + 2^m\}$ if $m = 2$, $i_0 = 1$ if $m = 1$. Since

$f+s=2^n$ and $g \equiv 0 \pmod{2^m}$, the second congruence of (3.1) holds for every $x, y \in \mathbb{Z}_{2^m}$. From the first congruence of (3.1) we get the value for y. Now let us find the number of solutions of the system (2.1). We have 2^{n-m} choices for number k, 2^{n-1} choices for odd number j, 2^m choices for number x. For i_0 we have $z=4$ choices if $m \geqslant 3$, $z=2$ choices if $m=2$ and $z=1$ choice if $m=1$. This implies that for the number i we have $z \cdot 2^{n-m}$ choices and the number of solutions of the system is equal to the number of triples (i,j,x) and $|\{(i,j,x)\}| = z \cdot 2^{n-m} \cdot 2^{n-1} \cdot 2^m = z \cdot 2^{2n-1}$. □

Proposition 3.2. *Assume that $m \leqslant n$, q is even and $i \in \left\{\varepsilon, \varepsilon+2^{n-1}\right\}$ $(\varepsilon = \pm 1)$. Then the solutions of (2.1) are:*

1) $\left(i+2^n x, 2^s u, 2^t v+2^n y, -i+2^{n-1}z\right)$, where $y \in \mathbb{Z}_{2^m}$ (if $m<n$ or if $m=n$ and $z=0$), $y \in 2\mathbb{Z}_{2^{m-1}}$ (if $m=n$ and $z=1$), $1 \le s \le n, u \in \mathbb{Z}^*_{2^{n-s}}, m+z \leqslant t \leqslant n, v \in \mathbb{Z}^*_{2^{n-t}}$ and in the case $m<n$ if $i=\varepsilon$ then $x=x_1$, $s+t>n$, if $i=\varepsilon+2^{n-1}$ then $x=x_2$, $s+t=n$; in the case $m=n$ then $i=\varepsilon$, $x=x_1$, $2^t v=0$, where

$$x_1 \equiv (-1+\varepsilon)\, 2 - \varepsilon x_0 \left(\operatorname{mod} 2^{m-1}\right), \quad x_2 \equiv -\varepsilon\left(2^{n-3}+(\varepsilon+uv)/2+2^{s-1}yu\right)\left(\operatorname{mod} 2^{m-1}\right)$$

and $x_0 = 2^{t+s-n-1}u\left(v+2^{n-t}y\right)$ (if $m<n$), $x_0 = 2^{s-1}uy$ (if $m=n$). There are exactly $(2n-2m+1)\, 2^{n+m+1}$ solutions of this form if $m<n$ and $3 \cdot 2^{2n}$ solutions if $m=n$.

2) $\left(i+2^n x, 2^{n-1}u, 2^n y, i+2^{n-1}z\right)$, $i \in \{1, -1+2^n\}$, $u, z \in \mathbb{Z}_2$, $y \equiv 0 \pmod{2^{m-1}}$ and

$$x \equiv 0 \pmod{2^{m-1}} \quad \text{if } i=1,\ x \equiv -1 \pmod{2^{m-1}} \quad \text{if } i=-1+2^n$$

There are exactly 32 solutions of this form.

Proof. To prove the proposition, by [2] we must consider the following sets of solutions of (2.2):

$$\mathcal{M}_4 \cup \mathcal{M}_7 = \left\{\left(i, 2^s u, 2^t v, -i+2^{n-1}z\right) \mid 1 \le s,\, t \le n; s+t \ge n;\ u \in \mathbb{Z}^*_{2^{n-s}},\ v \in \mathbb{Z}^*_{2^{n-t}}\right\}$$
$$\mathcal{M}_5 \cup \mathcal{M}_6 = \left\{\left(i+2^{n-1}z, 2^{n-1}u, 2^{n-1}v, i+2^{n-1}z\right) \mid u,\, v \in \mathbb{Z}_2,\ i=\pm 1\right\}$$
$$\mathcal{M}_8 \cup \mathcal{M}_9 = \left\{\left(i, 2^{n-1}u, 2^{n-1}v, i+2^{n-1}\right) \mid u,\, v \in \mathbb{Z}_2\right\}$$

where $z \in \mathbb{Z}_2$. Solving system (3.1) for each solution of (2.2) from given sets we get from the second congruence in (3.1) the condition for y and from the first congruence in (3.1) the values for x. The solutions of system (2.2) belonging to set $\mathcal{M}_4 \cup \mathcal{M}_7$ give us solution 1) of system (2.1). The solutions of system (2.2) belonging to sets $\mathcal{M}_5 \cup \mathcal{M}_6$, $\mathcal{M}_8 \cup \mathcal{M}_9$ give solution 2) of system (2.1). □

Proposition 3.3. *Assume that $m \leqslant n$, $q=2^t u$ and $g=2^r v$ are both nonzero even numbers, $s \notin \left\{\pm 1, \pm 1+2^{n-1}\right\}$ is odd ($s=\varepsilon+2^{t+r-1}p$, $p \in \mathbb{Z}^*_{2^{n-t-r+1}}, \varepsilon=\pm 1, 1 \le t < n$, $m+k \le r \le n-1, 3 \leqslant t+r < n$, $v=-\left(\varepsilon+2^{t+r-2}p\right) p u^{2^{n-t-r}-1}+2^{n-t-r+1}l$ $(l \in \mathbb{Z}_{2^{t-1}})$) and $k \in \{0,1\}$. Then system (2.1) have solutions only if $m<n$, and these solutions are $\left(s+2^n x, 2^t u, 2^r v+2^n y, -s+2^{n-1}k\right)$, where $x, y \in \mathbb{Z}_2$ (if $m=1$) and if $m>1$ then $y \in \mathbb{Z}_{2^m}$, $x \equiv s^{-1}\left(-\left(\varepsilon p+uv+2^{t+r-2}p^2\right)/2^{n+1-t-r}-2^{t-1}yu\right) \pmod{2^{m-1}}$. If $m=1$ there are $2^{n+2}\left(5 \cdot 2^{n-3}-2n+1\right)$ solutions of this form. If $m>1$ there are $3 \cdot 2^{2n}-2^{n+m+1}(2n-2m+1)$ solutions.*

Proof. Let us now consider the set $\mathcal{M}_{10}$. The solutions of system (2.2) from this set have the form $\left(i, 2^t u, 2^r v, -i+2^{n-1}k\right)$, where $1 \le r, t \le n-1$, $3 \le r+t \le n-1$, $p \in \mathbb{Z}^*_{2^{n-t-r+1}}$, $k \in \mathbb{Z}_2, u \in \mathbb{Z}^*_{2^{n-t}}$, $v \in \mathbb{Z}^*_{2^{n-r}}$, and

$$uv+(\pm 1+2^{t+r-2}p)p \equiv 0 \pmod{2^{n-r-t}} \tag{3.2}$$

The condition $g=2^r v \equiv 0 \pmod{2^m}$ holds only if $r \geqslant m$. The second congruence of (3.1), i.e

$$\left(2^n+2^{n-1}k\right)\left(2^r v+2^n y\right)+2^n x 2^r v \equiv 0 \pmod{2^{n+m}}$$

holds in the case if $k=0$ for every $r \geqslant m$ and in the case if $k=1$ it holds for every $r \geqslant m+1$. Since $s^2-1=\pm 2^{t+r}p+2^{2(t+r-1)}p^2$, the first congruence of (3.1), i.e

$$s^2+2^{n+1}sx+\left(2^r v+2^n y\right)2^t u \equiv 1 \pmod{2^{n+m}}$$

implies

$$2^{n+1-t-r}sx+2^{n-t}yu+\left(\pm p+uv+2^{t+r-2}p^2\right) \equiv 0 \pmod{2^{n+m-t-r}} \tag{3.3}$$

Since $n-t \geqslant n+1-t-r$, this congruence holds if and only if

$$\pm p+vu+2^{t+r-2}p^2 \equiv 0 \pmod{2^{n+1-t-r}}$$

The last condition is stronger than (3.2) and implies $v \equiv -\left(\pm 1+2^{t+r-2}p\right)pu^{-1} \pmod{2^{n+1-t-r}}$, where u^{-1} is the inverse of the odd number u by modulo $2^{n+1-t-r}$, i.e $u^{-1}=u^{2^{n-t-r}-1}$. Since $v \in \mathbb{Z}^*_{2^{n-r}}$, for v we have $2^{n-r}/2^{n+1-t-r}=2^{t-1}$ values by modulo 2^{n-r} in the form

$$v=-\left(\pm 1+2^{t+r-2}p\right)pu^{2^{n-t-r}-1}+2^{n-t-r+1}l, \quad \text{where } l \in \mathbb{Z}_{2^{t-1}}$$

It follows from (3.3), that in the case $m=1$ we have $x, y \in \mathbb{Z}_2$ and in the case $m>1$ we have

$$x \equiv s^{-1}\left(-\left(\pm p+uv+2^{t+r-2}p^2\right)2^{n+1-t-r}-2^{t-1}yu\right) \pmod{2^{m-1}}$$

Calculating the number of all obtained solutions, we get the second statement of proposition. □

3.2 The case $m>n$

The condition $g+2^n y \equiv 0 \pmod{2^m}$ implies $g=0$ 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 $z=2^k w$ ($k \in \mathbb{Z}_n$ and $w \in \mathbb{Z}^*_{2^{n-k}}$). System (2.3) has now the form

$$(f+2^n x)^2+2^m zq \equiv 1 \pmod{2^{n+m}}, \quad 2^m z(f+s) \equiv 0 \pmod{2^{n+m}} \tag{3.4}$$

Lemma 3.1. *The solution of the congruence*

$$(f+2^n x)^2 \equiv 1 \pmod{2^{n+m}}, \quad \text{where} \quad f \in \left\{\pm 1, \pm 1+2^{n-1}\right\}$$

is: 1) $x \in \left\{0, 2^{m-1}\right\}$ if $f=1$, 2) $x \in \left\{-1+2^{m-1}, -1+2^m\right\}$ if $f=-1$, and 3) $x \in \varnothing$ if $f=\pm 1+2^{n-1}$.

Proof. The solutions of $b^2 \equiv 1 \pmod{2^{n+m}}$ are $b \in \left\{1, -1+2^{n+m}, 1+2^{n+m-1}, -1+2^{n+m-1}\right\}$, i.e $2^n x \in \left\{1-f, -1-f+2^{n+m}, 1-f+2^{n+m-1}, -1-f+2^{n+m-1}\right\}$. 1) If $f=1$, then $2^n x \in \left\{0, -2+2^{n+m}, 2^{n+m-1}, -2+2^{n+m-1}\right\}$, $2^n x \in \left\{0, 2^{n+m-1}\right\}$ and $x \in \left\{0, 2^{m-1}\right\}$. 2) If $f=-1=-1+2^n$, then $2^n x \in \{2-2^n+2^{n+m}, -2^n+2^{n+m}, 2-2^n+2^{n+m-1}, -2^n+2^{n+m-1}\}$, $2^n x \in \left\{-2^n+2^{n+m}, -2^n+2^{n+m-1}\right\}$ and $x \in \left\{-1+2^m, -1+2^{m-1}\right\}$. 3) If $f=\pm 1+2^{n-1}$, then $2^n x \in \left\{-2^{n-1}+2^{n+m}, -2^{n-1}+2^{n+m-1}, \mp 2-2^{n-1}+2^{n+m}, \mp 2-2^{n-1}+2^{n+m-1}\right\}$ and $x \in \varnothing$. □

Lemma 3.2. *The solution of the congruence*

$$(f+2^n x)^2 \equiv 1-2^m zq \pmod{2^{n+m}}$$

where $f \in \left\{\pm 1, \pm 1+2^{n-1}\right\}$, $q=2^s u$, $z=2^k w$, ($k=1,2,...,n-1$ and $w \in \mathbb{Z}^*_{2^{n-k}}$) and $zq \neq 0 \pmod{2^n}$ is: 1) $x=2^{m-n+k+s-1}p$ (if $f=1$, $\varepsilon=+1$), 2) $x=2^{m-n+k+s-1}p-1$ (if $f=-1$, $\varepsilon=-1$), and 3) $x \in \varnothing$ (if $f=\pm 1+2^{n-1}$), where $p \in \mathbb{Z}^*_{2^{n-k-s+1}}$, $i \in \mathbb{Z}_{2^s}$ and

$$z=2^k\left(-\left(\varepsilon+2^{m+k+s-2}p\right)pu^{2^{n-k-s-1}-1}+2^{n-k-s}i\right)$$

Proof. Denote $f+2^n x = a$, $s+k = l$. Then $a^2-1 \equiv -2^{m+l}uw \pmod{2^{n+m}}$. Using (2.1)–(2.10) in [2], we get that the solution of the last congruence is

$$a = \varepsilon + 2^{m+l-1}p, \quad q = 2^s u, \quad z = 2^k\left(-\left(\varepsilon + 2^{m+l-2}p\right)pu^{2^{n-l-1}-1} + 2^{n-l}i\right)$$

where $s,k = 1,2,...,n-1$, $s+k<n$, $\varepsilon = \pm 1$, $u \in \mathbb{Z}^*_{2^{n-s}}$, $p \in \mathbb{Z}^*_{2^{n-l+1}}$, $i \in \mathbb{Z}_{2^s}$.

Now let us find x. Since $f + 2^n x \in \left\{1+2^{m+l-1}p, -1+2^{m+l-1}p\right\}$, it follows that $2^n x \in \left\{1-f+2^{m+l-1}p, -1-f+2^{m+l-1}p\right\}$. 1) If $f=1$, then $2^n x \in \left\{2^{m+l-1}p, -2+2^{m+l-1}p\right\}$, $2^n x \in \left\{2^{m+l-1}p\right\}$ and $x = 2^{m-n+l-1}p$. 2) Analogously, if $f = -1 = -1+2^n$, then $2^n x \in \left\{2-2^n+2^{m+l-1}p, -2^n+2^{m+l-1}p\right\}$, $2^n x \in \left\{-2^n+2^{m+l-1}p\right\}$ and $x = 2^{m-n+l-1}p-1$. 3) If $f = \pm 1 + 2^{n-1}$, then $2^n x \in \left\{\mp 2 - 2^{n-1} + 2^{m+l-1}p, -2^{n-1}+2^{m+l-1}p\right\}$ and $x \in \varnothing$. □

Denote by x_1 solutions from Lemma 3.1 and by x_2, z_2 solutions from Lemma 3.2.

Proposition 3.4. *Assume that $m > n$ and the number q is odd ($q = j \in \mathbb{Z}^*_{2^n}$). Then the solutions of* (2.1) *are: 1) $\left(i+2^n x, j, 2^{m+k}w, -i\right)$, where $x = 2^{m-n+k-1}p + \frac{-1+i}{2}$, $i = \pm 1$, $k \in \mathbb{Z}_n$, $p \in \mathbb{Z}^*_{2^{n-k+1}}$, $w = -\left(i+2^{m+k-2}p\right)pj^{2^{n-k-1}-1}$; 2) $(i+2^n x, j, 0, -i)$, where $x \in \left\{0, 2^{m-1}\right\}$ if $i=1$ and $x \in \left\{-1+2^{m-1}, -1+2^m\right\}$ if $i=-1$. There are 2^{2n+1} solutions of these forms.*

Proof. Consider the solutions of system (2.2) belonging to the set $\mathcal{M}_3$. The second congruence of (3.4) holds for every $z \in \mathbb{Z}_{2^n}$. To solve the first congruence of (3.4), consider two cases for z: 1) $z = 2^k w$, $w \in \mathbb{Z}^*_{2^{n-k}}$, $k \in \mathbb{Z}_n$ and 2) $z = 0$ (i.e $y = 0$). In the first case using Lemma 3.2, we get solution 1) and in the second case, using Lemma 3.1, we get solution 2). □

Proposition 3.5. *Assume that $m > n$, $f \in \left\{\pm 1, \pm 1 + 2^{n-1}\right\}$ and both numbers q and g are even. Then* (2.1) *have solutions only in case $f = i = \pm 1$ and these solutions are:*

1) $\left(i+2^n x_1, 2^s u, 0, -i+2^{n-1}r\right)$ $\quad (s = 1,2,...,n)$
2) $\left(i+2^n x_1, 0, 2^m z, -i+2^{n-1}r\right)$ $\quad (z \in (1+r)\mathbb{Z}_{2^{n-r}} \setminus \{0\})$
3) $\left(i+2^n x_1, 2^s u, 2^{m+k}w, -i+2^{n-1}r\right)$ $\quad (r \leqslant k \leqslant n-1,\ w \in \mathbb{Z}^*_{2^{n-k}},\quad n-k \leqslant s \leqslant n-1)$
4) $\left(i+2^n x_2, 2^s u, 2^m z_2, -i+2^{n-1}r\right)$ $\quad (k = r, r+1, ..., n-1,\ s = 1, ..., n-k-1)$
5) $\left(i+2^n x_1, 2^{n-1}h, 2^m z, i+2^{n-1}r\right)$ $\quad (h \in \mathbb{Z}_2,\ z \in \left\{0, 2^{n-1}\right\})$

where $u \in \mathbb{Z}^*_{2^{n-s}}$, $r \in \mathbb{Z}_2$. There are $3 \cdot 4^n + 32$ solutions of these forms.

Proof. Consider solutions of system (2.2) belonging to the sets $\mathcal{M}_4 \cup \mathcal{M}_7$, $\mathcal{M}_5 \cup \mathcal{M}_6$, $\mathcal{M}_8 \cup \mathcal{M}_9$. Solving system (3.4) and using lemmas 3.1 and 3.2, we get from the set $\mathcal{M}_4 \cup \mathcal{M}_7$ solutions 1), 2), 3), 4) and from sets $\mathcal{M}_5 \cup \mathcal{M}_6$, $\mathcal{M}_8 \cup \mathcal{M}_9$ solution 5). Calculating the number of all obtained solutions, we get the second statement of the proposition. □

Acknowledgement

Research was supported by the Estonian Science Foundation Research Grant 5900, 2004-2007.

References

[1] H. Coxeter and W. Moser. *Generators and relations for discrete groups.* Springer-Verlag, 1972.
[2] T. Gramushnjak and P. Puusemp. Description of a Class of 2-Groups. J. Nonlinear Math. Phys. **13** (2006), Supplement, 55-65.
[3] M. Hall and J. Senior. *The groups of order* $2^n, n \leq 6$. Macmillan, New York; Collier–Macmillan, London, 1964.

Received January 20, 2008
Revised April 13, 2008