Natalia Zhukavets

On small distances of small 2-groups

Commentationes Mathematicae Universitatis Carolinae, Vol. 42 (2001), No. 2, 247--257

Persistent URL: http://dml.cz/dmlcz/119240

Comment.Math.Univ.Carolin. 42,2 (2001)247–257

On small distances of small 2-groups

Natalia Zhukavets

Abstract. The paper reports the results of a search for pairs of groups of order n that can be placed in the distance $n^2/4$ for the case when $n \in \{16, 32\}$. The constructions that are used are of the general character and some of their properties are discussed as well.

Keywords: 2-groups, distances of groups

Classification: Primary 20D60; Secondary 05B15

1. Introduction

Let $G(\circ)$ and $G(*)$ be finite groups of order n. Since they are defined on the same set, one can measure their *distance* $\operatorname{dist}(\circ, *)$ as the number of pairs $(a, b) \in G \times G$ with $a \circ b \neq a * b$.

It is known ([2]) that $\operatorname{dist}(\circ, *) \leq n^2/9$ implies $G(\circ) \cong G(*)$. For 2-groups we have a sharper result ([3]), since for n a power of two one always has $G(\circ) \cong G(*)$ when $\operatorname{dist}(\circ, *) < n^2/4$. The latter estimate is the best possible, because there are many cases of non-isomorphic 2-groups that are in the distance $n^2/4$.

Say that groups G_1 and G_2 of the same order can be *positioned* in the distance d, if there exist groups $G(\circ) \cong G_1$ and $G(*) \cong G_2$ with $\operatorname{dist}(\circ, *) = d$.

In [3] there was described a general situation, in which groups G_1 and G_2 can be positioned in the distance $n^2/4$, where n is the common order of G_1 and G_2:

Theorem 1.1. *Suppose that groups G_1 and G_2 of the same order n have a common subgroup S that is of index two. Furthermore, suppose that for $i \in \{1, 2\}$ there exist such $a_i \in G_i \setminus S$ that $a_1 s a_1^{-1} = a_2 s a_2^{-1}$ for all $s \in S$. Then G_1 and G_2 can be positioned in the distance $n^2/4$.* □

This statement can be used to verify that C_{4k} and $C_{2k} \times C_2$ can be placed in the distance $4k^2$, $k \geq 1$ (where C_n means the cyclic group of order n), or that Q_{2^k} and D_{2^k}, $k \geq 3$, can be positioned in the distance 2^{2k-2} (we denote by D_{2^n} the dihedral group of order 2^n, and by Q_{2^n} the generalized quaternion group of order 2^n).

We shall use two different constructive methods in order to obtain from a group $G(\circ)$ such a group $G(*)$ that $\operatorname{dist}(\circ, *) = n^2/4$, $n = |G|$. The first of them reflects

Partially supported by MSM 113200007.

the above statement, and the second one is concerned with a bit more complicated situation, in which one deals with a normal subgroup of index 4, factor over which is isomorphic to E_4 in both groups (E_n denotes the elementary abelian group of order n).

Petr Vojtěchovský, in his diploma thesis [4], investigated (among others) groups of order 8 and obtained the following table:

	$[C_8]$	$[C_4 \times C_2]$	$[E_8]$	$[D_8]$	$[Q_8]$
$[C_8]$	16	16	18	24	24
$[C_4 \times C_2]$		16	16	16	16
$[E_8]$			24	16	24
$[D_8]$				16	16
$[Q_8]$					24

Here square brackets are used to denote the isomorphism class of a respective group, and each entry gives the minimal distance in which the groups from the corresponding class can be positioned (the diagonal refers to the situation when groups are isomorphic, but not identical).

This table shows that groups of order 8 yield a connected graph, when vertices of the graph are the (isomorphism classes of) groups of order 8, and edges are between those groups that can be positioned in the distance 16 (we shall be concerned here only with distances of non-isomorphic groups).

Now, it is quite natural to ask if a similar graph will be connected for groups of every order n, n a power of two.

The answer is known to be positive for $n \in \{2, 4, 8, 16, 32\}$, and the respective results are described in Section 3.

2. The methods

Proposition 2.1. *Let $G = G(\cdot)$ be a group, $S < G$ its subgroup of index 2, and $h \in Z(G) \cap S$. Define a new operation $\star$ on G by*

$$u \star v = \begin{cases} uv, & \text{if } u \in S \text{ or } v \in S, \\ uvh, & \text{if } u \in G \setminus S \text{ and } v \in G \setminus S. \end{cases}$$

Then $G(\star)$ is a group. $\square$

Proposition 2.2. *Let $G = G(\cdot)$ be a group, $U < G$ and $V < G$ its subgroups of index 2, $S = U \cap V$ a subgroup of index 4, and $h \in Z(S)$ such an element that $huh = u$ for all $u \in U \setminus S$ and $hvh = v$ for all $v \in V \setminus S$. Define a new operation $\star$ on G by*

$$u \star v = \begin{cases} uv, & \text{if } u \in U \text{ or } v \in V, \\ uvh, & \text{if } u \notin U \text{ and } v \in U \setminus S, \\ uvh^{-1}, & \text{if } u \notin U \text{ and } v \in G \setminus (U \cup V). \end{cases}$$

Then $G(\star)$ is a group. □

The proofs in both cases consist of showing that the operation $\star$ is associative. That can be done by a direct verification, and hence the proof is omitted here (a somewhat shorter proof that does not resort to a blind verification of all cases can be found in [5]).

The group $G(\star)$ obtained by the method of Proposition 2.1 will be denoted by $G[S,h]$, and the group obtained by the method of Proposition 2.2 will be denoted by $G[U,V,h]$. It is obvious that $\operatorname{dist}(\cdot,\star) = n^2/4$ holds in both cases, if G is finite and of order n.

The following statement can be, again, verified in a direct way, and so the proof is not included.

Proposition 2.3. *Let $G = G(\cdot)$ be a group.*

(i) *If $S < G$, $|G : S| = 2$, $h \in Z(G) \cap S$ and $G(\star) = G[S,h]$, then $G(\cdot) = G(\star)[S,h^{-1}]$.*

(ii) *If $U < G$, $V < G$, $|G : U| = |G : V| = 2$, $S = U \cap V$, $|G : S| = 4$, $h \in Z(S)$ and $hxh = x$ for all $x \in (U \cup V) \setminus S$, and if $G(\star) = G[U,V,h]$, then $G(\cdot) = G(\star)[U,V,h^{-1}]$.* □

Say that groups G_1 and G_2 are 2-*related* if $G_2 \cong G_1[S,h]$ for some $h \in Z(G_1) \cap S$, where $S < G_1$ and $|G_1 : S| = 2$. Say that groups G_1 and G_2 are 4-*related* if $G_2 \cong G_1[U,V,h]$ for some $h \in Z(S)$, where $U < G_1$, $V < G_1$, $|G_1 : U| = |G_1 : V| = 2$, $S = U \cap V$, $|G_1 : S| = 4$ and $hxh = x$ for all $x \in (U \cup V) \setminus S$. Put $Q(U,V) = \{h \in Z(S);\ hxh = x \text{ for all } x \in (U \cup V) \setminus S\}$.

We have observed in Proposition 2.3 that the relation of being 2-related (4-related) is symmetric. Moreover, under the notations of Proposition 2.2, one can define another operation $\circledast$ on G by

$$v \circledast u = \begin{cases} vu, & \text{if } v \in V \text{ or } u \in U, \\ vuh^{-1}, & \text{if } v \notin V \text{ and } u \in V \setminus S, \\ vuh, & \text{if } v \notin V \text{ and } u \in G \setminus (U \cup V). \end{cases}$$

Then the mapping $\alpha : G \to G$, $\alpha(a) = a$ for $a \in U \cup V$ and $\alpha(a) = ah^{-1}$ for $a \in G \setminus (U \cup V)$, is an isomorphism of groups $G(\star) \cong G(\circledast)$.

It is easy to verify that if the operation $\star$ is defined as in Proposition 2.1 and if $x^\star$ denotes the inverse of $x \in G$ with respect to $\star$, then the equality $xyx^{-1} = x \star y \star x^\star$ holds for all $x, y \in G$. Hence the groups G_1 and G_2 are 2-related if and only if they satisfy conditions of Theorem 1.1.

We are not going to develop here the theory of 2-related and 4-related groups in full. That has been done partly in [5], and a paper that will cover various aspects of those constructions is under preparation. The aim of this paper is to illustrate in this section the concept of 2-relatedness and 4-relatedness upon groups D_{2^k},

Q_{2^k} and SD_{2^k} (where SD_{2^n} denotes the semidihedral group of order 2^n), and to discuss, in Section 3 the powers and limitations of this methods in the case of small orders.

We have already mentioned in Introduction that groups Q_{2^k} and D_{2^k}, $k \geq 3$, can be positioned in the distance 2^{2k-2}. Moreover, in [1] there was shown that groups D_{2^k} and SD_{2^k}, $k \geq 4$, can be positioned in the distance 2^{2k-2} as well.

First we give some general observations.

Lemma 2.4. *If $\alpha \in \mathrm{Aut}(G)$, $S < G$ is a subgroup of index 2 and $h \in Z(G) \cap S$, then α is also an isomorphism $G[S,h] \cong G[\alpha(S), \alpha(h)]$.*

Proof: Denote the operation of $G[S,h]$ by $\star$ and the operation of $G[\alpha(S), \alpha(h)]$ by $\circledast$. Then for $u, v \in G$ with $\{u,v\} \cap S \neq \emptyset$ one has $\alpha(u \star v) = \alpha(uv) = \alpha(u)\alpha(v) = \alpha(u) \circledast \alpha(v)$. Suppose now that $u \in G \setminus S$ and $v \in G \setminus S$. Then $\alpha(u \star v) = \alpha(uvh) = \alpha(u)\alpha(v)\alpha(h) = \alpha(u) \circledast \alpha(v)$. $\square$

Lemma 2.5. *If $\alpha \in \mathrm{Aut}(G)$, $U < G$ and $V < G$ are different subgroups of index 2 and $h \in Q(U,V)$, then α is also an isomorphism*

$$G[U,V,h] \cong G[\alpha(U), \alpha(V), \alpha(h)].$$

Proof: Denote by $\star$ the operation of $G[U,V,h]$ and by $\circledast$ the operation of $G[\alpha(U), \alpha(V), \alpha(h)]$. Then for $u, v \in G$ with $u \in U$ or $v \in V$ one gets $\alpha(u \star v) = \alpha(uv) = \alpha(u)\alpha(v) = \alpha(u) \circledast \alpha(v)$. If $u \notin U$ and $v \in U \setminus V$, then $\alpha(u \star v) = \alpha(uvh) = \alpha(u)\alpha(v)\alpha(h) = \alpha(u) \circledast \alpha(v)$, and in the case $u \notin U$ and $v \in G \setminus (U \cup V)$ one gets $\alpha(u \star v) = \alpha(uvh^{-1}) = \alpha(u)\alpha(v)\alpha(h)^{-1} = \alpha(u) \circledast \alpha(v)$. $\square$

Lemma 2.6. *If $U < G$ and $V < G$ are two different subgroups of index 2, and $h \in Q(U,V)$ equals k^2 for some $k \in Q(U,V)$, then $G[U,V,h] \cong G$.*

Proof: Choose $u \in U \setminus S$, $v \in V \setminus S$, $S = U \cap V$ and put $u' = u$ and $v' = vk$. Furthermore, put $G(\star) = G[U,V,h]$. The automorphisms of S which are induced by elements of U or V are the same both in G and $G(\star)$. As k belongs to $Q(U,V) \leqslant Z(S)$, we see that v and v' induce the same automorphism of S. Furthermore, $u' \star u' = u^2$ holds trivially, and $v' \star v' = vkvk = v^2$ follows from $k \in Q(U,V)$. Now, $u' \star v' = uvk \in G \setminus (U \cup V)$, and so $(u' \star v') \star (u' \star v') = uvkuvkh^{-1} = uvkuvk^{-1}$, which equals $(uv)(uv)$. Therefore, rules $s \mapsto s$ $(s \in S)$, $u \mapsto u'$, $v \mapsto v'$ induce an isomorphism $G \cong G[U,V,h]$. $\square$

Lemma 2.7. *Suppose that $U < G$ and $V < G$ are two different subgroups of index 2 and h_1, h_2 are elements of $Q(U,V)$. If $h_1^{-1}h_2 = k^2$ for some $k \in Q(U,V)$, then $G[U,V,h_1] \cong G[U,V,h_2]$.*

Proof: Put $G_i = G[U,V,h_i]$, $i \in \{1,2\}$. Denote by $\star$ the operation of G_1 and by $\circledast$ the operation of G_2 and consider $u,v \in G$. If $u \in U$ or $v \in V$, then $u \circledast v = uv = u \star v$. Assume $u \in G \setminus U$. If $v \in U \setminus V$, then $u \circledast v = uvh_1k^2 = u \star v \star k^2$. If $v \in G \setminus (U \cup V)$, then $u \circledast v = uvh_1^{-1}k^{-2} = u \star v \star k^{-2}$. But then $G_1 \cong G_2$ by Lemma 2.6. □

Note the well known fact that if G is non-abelian of order 2^{n+1} with a cyclic subgroup C of index 2, then either $G \cong D_{2^{n+1}},\ n \geq 2$, or $G \cong Q_{2^{n+1}},\ n \geq 2$, or $G \cong SD_{2^{n+1}},\ n \geq 3$, or $G \cong \mathrm{Mod}_{2^{n+1}},\ n \geq 3$. Recall the defining relations of these groups:

$$\begin{aligned} D_{2^{n+1}}: &\qquad x^{2^n} = 1,\ y^2 = 1,\ yxy^{-1} = x^{-1};\\ Q_{2^{n+1}}: &\qquad x^{2^n} = 1,\ y^2 = x^{2^{n-1}},\ yxy^{-1} = x^{-1};\\ SD_{2^{n+1}}: &\qquad x^{2^n} = 1,\ y^2 = 1,\ yxy^{-1} = x^{-1+2^{n-1}} \text{ and}\\ \mathrm{Mod}_{2^{n+1}}: &\qquad x^{2^n} = 1,\ y^2 = 1,\ yxy^{-1} = x^{1+2^{n-1}}. \end{aligned}$$

Now we are ready to study the 2-relatedness of the groups $D_{2^{n+1}}$, $Q_{2^{n+1}}$ and $SD_{2^{n+1}}$.

If $U < G$ is a subgroup of index 2, then either $U = C$ or $|U : U \cap C| = 2$. Assume $C = \langle x \rangle$ and choose $y \in G \setminus C$ so that the order of y is the least possible. If $U \neq C$, then the group $\langle x^2 \rangle = U \cap C$ is of index 4 in G and $G/\langle x^2 \rangle$ is a four element group of exponent 2.

Group G is assumed not to be cyclic, and hence it has at least one subgroup U of index 2 that is different from C. Therefore, the only subgroups of index 2 in G are $\langle x \rangle$, $\langle x^2, y \rangle$ and $\langle x^2, xy \rangle$, and $\langle x^2 \rangle$ is the only subgroup of G which yields a factor isomorphic to E_4.

Conditions of Theorem 1.1 are satisfied, and so the groups $D_{2^{n+1}}$ and $Q_{2^{n+1}}$ are 2-related by means of C and, as any non-abelian group cannot be 2-related to an abelian group, we see that none of these four groups can be 2-related to any other group by means of C.

Other subgroups of index 2 will be investigated later. However, just now note that the centre of $D_{2^{n+1}}$, $Q_{2^{n+1}}$ and $SD_{2^{n+1}}$ is a two element group and so $h = x^{2^{n-1}}$ is the only possible choice for the definition of a new operation $\star$ when proceeding like in Proposition 2.1.

Consider now $G = SD_{2^{n+1}}$. If $S = \langle x^2, y \rangle$, then $S \cong D_{2^n}$ and for $G(\star) = G[S, x^{2^{n-1}}]$ we obtain $x \star x = x^{2+2^{n-1}}$ and $y \star x \star y^\star = yxy^{-1} = x^{-1+2^{n-1}} = x^\star$. The group $G(\star)$ is thus isomorphic to $D_{2^{n+1}}$. If $S = \langle x^2, xy \rangle$, then $S \cong Q_{2^n}$ and in $G(\star) = G[S, x^{2^{n-1}}]$ one gets $x \star x = x^{2+2^{n-1}}$, $y \star y = x^{2^{n-1}}$, $y \star x \star y^\star = yxy^{-1} = x^{-1+2^{n-1}} = x^\star$ and hence $G(\star) \cong Q_{2^{n+1}}$.

If G is $D_{2^{n+1}}$ or $Q_{2^{n+1}}$, then there exists an automorphism that fixes x and sends y to xy. Hence by Lemma 2.4 only the case $S = \langle x^2, y \rangle$ needs to be considered. For $G = Q_8$ one can use the automorphism argument again, since in this case $S = \langle y \rangle$ and there exists an automorphism with $x \mapsto y$ and $y \mapsto x$. If $G = D_8$, then S is elementary abelian and $h = x^2$ equals $y^x y$. Elements x and $x' = xy^{-1}$ induce the same automorphism of S. Furthermore, $x' \star x' = xy^{-1}xy^{-1}h = (xy^{-1}x)y^x = xy^{-1}yx = x^2$, and there exists an isomorphism $G \cong G[S,h]$ with $s \mapsto s$ and $xs \mapsto x's$ for all $s \in S$. Assume now $n \geq 3$. Up to an isomorphism just one 2-related group can be obtained from G, and as $SD_{2^{n+1}}$ is 2-related to G, we see that $SD_{2^{n+1}}$ is the only possibility.

So, we have proved the following statement:

Proposition 2.8. (i) *The groups Q_8 and D_8 are 2-related and there exists, up to an isomorphism, no other group 2-related to any of them.*

(ii) *Assume $n \geq 4$. The groups D_{2^n}, Q_{2^n} and SD_{2^n} are pairwise 2-related and there exists, up to an isomorphism, no other group 2-related to any of them.* □

Let us now study which groups will be 4-related. Suppose again that G is one of the groups $D_{2^{n+1}}$, $Q_{2^{n+1}}$ or $SD_{2^{n+1}}$, $U < G$ and $V < G$ are subgroups of index 2 and $S = U \cap V$ is a subgroup of index 4. As was shown above, S is necessary isomorphic to $\langle x^2 \rangle$. To define a new operation described in Proposition 2.2 we can use an element $h \in Z(S) = S$ which satisfies $huh = u$ for all $u \in U \setminus S$ and $hvh = v$ for all $v \in V \setminus S$.

Assume $n \geq 3$. If one of the subgroups, say U, is cyclic, then only the choice $h = x^{2^{n-1}}$ is possible.

In $SD_{2^{n+1}}$ one then gets $y \star x \star y^\star = yxy^{-1}x^{2^{n-1}} = x^{-1} = x^\star$. If $V = \langle x^2, y \rangle$, then $y \star y = y^2 = 1$, and $G(\star)$ is isomorphic to $D_{2^{n+1}}$. If $V = \langle x^2, xy \rangle$, then $y \star y = y^2 x^{2^{n-1}} = x^{2^{n-1}}$ and $G(\star) \cong Q_{2^{n+1}}$.

For $V = \langle x^2, y \rangle$ we obtain in $D_{2^{n+1}}$ relations $y \star y = 1$, $y \star x \star y^\star = yxy^{-1}x^{2^{n-1}} = x^{-1+2^{n-1}}$ and in $Q_{2^{n+1}}$ relations $(xy) \star (xy) = xyxyx^{2^{n-1}} = 1$, $(xy) \star x \star (xy)^\star = (xyxx^{2^{n-1}}) \star (xy) = xyxx^{2^{n-1}}xyx^{2^{n-1}} = xyx^2y^{-1}y^2 = x^{-1+2^{n-1}}$. In both cases $G(\star) \cong SD_{2^{n+1}}$. Moreover, by Lemma 2.5, the choice $V = \langle x^2, xy \rangle$ will bring us the new group isomorphic to $SD_{2^{n+1}}$ as well as there exists an automorphism with $x \mapsto x$ and $y \mapsto xy$.

It remains to consider the case $U = \langle x^2, y \rangle$ and $V = \langle x^2, xy \rangle$. Now the equalities $hyh = y$ and $hxyh = xy$ hold for any $h \in S$ but, by Lemmas 2.6 and 2.7, the choice of h can be limited just to x^2. In all groups the relations $x \star x = 1$, $x \star x^2 \star x^\star = x^3 \star x = x^2$, $y \star x^2 \star y^\star = yx^2 \star y^{-1} = x^{-2}$ and $x \star y \star x = xyx$ are true. If G is $D_{2^{n+1}}$ or $Q_{2^{n+1}}$, then xyx equals y, and hence $G(\star) \cong D_{2^n} \times C_2$ if $G = D_{2^{n+1}}$, and $G(\star) \cong Q_{2^n} \times C_2$ if $G = Q_{2^{n+1}}$. If $G = SD_{2^{n+1}}$, then $xyx = yx^{2^{n-1}}$ and we can see that $G(\star)$ is isomorphic to a group with the defining relations $\langle x, y, z;\ x^{2^{n-1}} = 1,\ y^2 = 1,\ z^2 = 1,\ yxy = x^{-1},\ zxz = x,\ zyz = yx^{2^{n-2}} \rangle$.

If $G = Q_8$, then, by Lemma 2.5 only one 4-related group exists, as all subgroups of index 2 can be permuted by automorphisms. This group is isomorphic to $C_4 \times C_2$. We can illustrate this fact by the following multiplication tables:

Q_8	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	1	0	7	6	4	5
3	3	2	0	1	6	7	5	4
4	4	5	6	7	1	0	3	2
5	5	4	7	6	0	1	2	3
6	6	7	5	4	2	3	1	0
7	7	6	4	5	3	2	0	1

$C_4 \times C_2$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	1	0	3	2
5	5	4	7	6	0	1	2	3
6	6	7	5	4	3	2	1	0
7	7	6	4	5	2	3	0	1

If $G = D_8$, then two of subgroups of index 2 can be exchanged by an automorphism. The only choice for h is x^2. There can thus exist at most two groups 4-related to D_8. One of these groups is isomorphic to $C_4 \times C_2$ and the other group is isomorphic to E_8. These facts can be verified also by the multiplication tables:

D_8	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	7	6	5	4
3	3	2	1	0	6	7	4	5
4	4	5	6	7	1	0	3	2
5	5	4	7	6	0	1	2	3
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

$C_4 \times C_2$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	1	0	3	2
5	5	4	7	6	0	1	2	3
6	6	7	4	5	3	2	1	0
7	7	6	5	4	2	3	0	1

D_8	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	7	6	5	4
3	3	2	1	0	6	7	4	5
4	4	5	6	7	1	0	3	2
5	5	4	7	6	0	1	2	3
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

E_8	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

Now we are ready to formulate a statement that fully describes 4-relatedness with respect to $Q_{2^{n+1}}$ and $D_{2^{n+1}}$, $n \geq 2$, and to $SD_{2^{n+1}}$, $n \geq 3$.

Proposition 2.9. (i) *Group Q_8 is 4-related, up to an isomorphism, only to $C_4 \times C_2$.*

(ii) *Group D_8 is 4-related, up to an isomorphism, only to groups E_8 and $C_4 \times C_2$.*

(iii) *If $n \geq 3$, then $D_{2^{n+1}}$ is 4-related, up to an isomorphism, just to groups $SD_{2^{n+1}}$ and $D_{2^n} \times C_2$.*

(iv) *If $n \geq 3$, then $Q_{2^{n+1}}$ is 4-related, up to an isomorphism, just to groups $SD_{2^{n+1}}$ and $Q_{2^n} \times C_2$.*

(v) *The groups to which $SD_{2^{n+1}}$, $n \geq 4$, is 4-related, are — up to an isomorphism — the following ones: $D_{2^{n+1}}$, $Q_{2^{n+1}}$ and the group with the defining relations $\langle x, y, z;\ x^{2^{n-1}} = 1,\ y^2 = 1,\ z^2 = 1,\ yxy = x^{-1},\ zxz = x,\ zyz = yx^{2^{n-2}} \rangle$. The latter group is a semidirect product of $C_{2^{n-1}} \times C_2$ and C_2.* □

Some further results about 2-relatedness and 4-relatedness can be found in [5], and will appear later in a paper which is under preparation. Let us mention here that the situation is quite simple when at least one of the groups is abelian, and that Mod_{2^n} can be subjected to the same analysis as D_{2^n}, Q_{2^n} and SD_{2^n}.

3. The computations

Say that groups H and K are *transitively* 2, 4*-related*, if $H \cong K$ or if there exists a chain of groups $G_1, \ldots, G_n$ such that $H \cong G_1$, $K \cong G_n$, $n > 1$, and for each i, $1 \leq i \leq n-1$, the groups G_i and G_{i+1} are 2-related or 4-related.

Theorem 3.1. (i) *Any two groups of order n, where $n \in \{2, 4, 8, 16\}$, are transitively 2, 4-related.*

(ii) *Any two groups of order 32 are transitively 2, 4-related, but for one exception: the group with the defining relations*

$$\langle x, y, z;\ x^4 = 1, y^2 = 1, z^4 = 1, xyx^{-1} = z^2 y, xzx^{-1} = zy, yzy^{-1} = z \rangle$$

is not 2, 4-related to any non-isomorphic group. □

The proof of (i) for $n = 2$ is void, and for $n = 4$ one can use the well known table pair of E_4 and C_4:

E_4	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

C_4	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The case $n = 8$ follows from Vojtěchovský's table (see Introduction), and the cases $n \in \{16, 32\}$ are considered in detail in my thesis [5].

I have considered the defining relations of all groups of order $n \in \{16, 32\}$, and I have systematically enumerated all possible parameters S and h (or U, V and h) for each of these groups. Some situations could have been easily refuted because of an obvious isomorphism to the original group or by general statements like Propositions 2.8 and 2.9. In the remaining situations I worked out the defining relations of the new group and, often using GAP, I found the group to which the 'new' group is isomorphic.

One gets from Theorem 3.1(ii) that the constructions of 2-related and 4-related groups are not sufficient to proof the conjecture that for each n, n a power of two, and for all groups H and K, $|H| = |K| = n$, one can find a chain $G_1, \ldots, G_k$ of such groups of order n that $G_1 \cong H$, $G_k \cong K$, and G_i and G_{i+1} can be positioned in the distance $n^2/4$ for every i, $1 \le i < k$.

However, for $n = 32$ this conjecture holds. In fact, the failure of 2,4-relatedness to provide the transitive connection led Aleš Drápal to look for further methods how close 2-groups can be constructed and one of the new methods really worked for the case of the group described in Theorem 3.1(ii). This group can be positioned in the distance 256 to several groups, one of them being the group with the defining relations

$$\langle x, y, z;\ x^8 = 1, y^2 = x^4, z^2 = 1, xyx^{-1} = y^{-1}z, zxz^{-1} = x^5, yzy^{-1} = z \rangle.$$

The details will be given in a later paper.

This paper is concluded by the proof of the negative part of Theorem 3.1(ii). We shall thus prove:

Lemma 3.2. *The group G with the defining relations*

$$\langle x, y, z;\ x^4 = 1, y^2 = 1, z^4 = 1, xyx^{-1} = z^2y, xzx^{-1} = zy, yzy^{-1} = z \rangle$$

is not $2,4$*-related to any non-isomorphic group.*

Proof: This group is a semidirect product of a normal subgroup $N = \langle z, y \rangle \cong C_4 \times C_2$ and a cyclic subgroup $\langle x \rangle \cong C_4$. Really, for any integer numbers $a, b \in \mathbb{Z}$ one has $xz^ay^bx^{-1} = z^{a+2b}y^{a+b}$.

Suppose that M is a maximal subgroup of G which does not contain N. Then $G = NM$ and $C_4 \cong G/N \cong NM/N \cong M/(N \cap M)$. Now, $N \cap M$ has index 4 in M, and hence $|N : N \cap M| = 2$. Moreover, $N \cap M$ is normal in G, since $N \trianglelefteq G$ and $M \trianglelefteq G$. So the intersection $N \cap M$ must be $\langle z^2, y \rangle$, because $xzx^{-1} = zy$, $xzyx^{-1} = z^{-1}$ imply that neither z nor zy lies in $N \cap M$. Then $\langle z^2, y \rangle$ is the unique subgroup of N which is of index 2 and normal in G.

Put $K = \langle z^2, y \rangle$, and note that G/K is isomorphic to $C_4 \times C_2$ and has generators xK and zK. Our remarks above show that K is a subgroup of $\Phi(G)$, the intersection of all maximal subgroups of G. Therefore, $\Phi(G) = \langle K, x^2\rangle$ and $G/\Phi(G) \cong C_2 \times C_2$. From $xz^2x^{-1} = zyzy = z^2$ it follows that z^2 lies in the center of a group G and, from the general properties of the center of a semidirect product, $Z(G) = \langle z^2\rangle$.

Therefore, the only subgroups of index 2 in G are $M_1 = \langle K, x\rangle = \langle x, z^2, y\rangle$, $M_2 = \langle K, x^2, z\rangle = \langle x^2, z, y\rangle$ and $M_3 = \langle K, x^2, xz\rangle = \langle xz, z^2, y\rangle$, because $(xz)^2 = xzxz = xzzyx = z^2xyx^{-1}x^2 = yx^2$. If $A \trianglelefteq G$ satisfies $G/A \cong C_2 \times C_2$, then A contains $\Phi(G)$. Since $\Phi(G)$ is of index 4, we see that A has to equal $\Phi(G)$.

Note that $x^2yx^2 = y$. Therefore, $\Phi(G) = \langle x^2\rangle \times \langle z^2\rangle \times \langle y\rangle$ is elementary abelian and h (as in Propositions 2.1 or 2.2) must be from the center of G, so $h = z^2$. It is easy to verify that there exists an automorphism $\varphi \in \mathrm{Aut}(G)$ with $x \mapsto xz^2,\ z \mapsto z,\ y \mapsto y$, and that $\varphi(M_1) = M_3$, $\varphi(M_2) = M_2$ and $\varphi(M_3) = M_1$.

Let us describe the isomorphism types of maximal subgroups of G. From the defining relations one obtains $x^2zx^2 = x(xzx^{-1})x^{-1} = xzyx^{-1} = zyz^2y = z^{-1}$, and so $M_2 = \langle x^2, z\rangle \times \langle y\rangle \cong D_8 \times C_2$. It is clear that in M_1 equalities $x^4 = 1,\ y^2 = 1,\ (z^2)^2 = 1,\ xz^2x^{-1} = z^2,\ yxy^{-1} = z^2x$ and $yz^2y^{-1} = z^2$ hold. And so M_1 is a semidirect product of its normal subgroup $\langle x, z^2\rangle \cong C_4 \times C_2$ and a two-element group $\langle y\rangle$.

We shall now look for groups that are 4-related with the group G. By Lemma 2.5, only two cases need to be considered, since $G[M_1, M_2, z^2]$ is isomorphic to $G[M_3, M_2, z^2]$.

Consider first the case $U = M_1$, $V = M_2$, and denote $G[U, V, z^2]$ by $G(\star)$. Because M_1 and M_2 are subgroups of $G(\star)$, elements x, y, z have in $G(\star)$ the same order as in $G = G(\cdot)$ and, because $\{x, y\} \in U$ and $\{y, z\} \in V$, equalities $x \star y \star x^\star = z^2 \star y$, $y \star z \star y^\star = z$ hold (here, as usual, we denote by $x^\star$ the inverse of $x \in G$ with respect to $\star$). Put $y_1 = z^2y = z^2 \star y$. Then $y_1 \star y_1 = (z^2y) \star (z^2y) = y^2 = 1$, $x \star y_1 \star x^\star = y = z^2 \star y_1$, $y_1 \star z \star y_1^\star = z$ and $x \star z \star x^\star = (xz) \star x^{-1} = xzx^{-1}z^2 = zyz^2 = z \star y_1$. Hence sending $x \mapsto x,\ z \mapsto z,\ y \mapsto y_1$ defines an isomorphism $G(\cdot) \cong G(\star)$.

In the case $U = M_1$ and $V = M_3$ put $z_1 = zx^2$, $y_1 = z^2y$. The elements y_1 and x have in the group $G(\star) = G[U, V, z^2]$ orders 2 and 4, respectively, since both are in M_1. Furthermore, $z_1 \star z_1 = (zx^2) \star (zx^2) = zx^2zx^2z^2 = zxzyx^{-1}z^2 = zzyz^2yz^2 = z^2$, and hence z_1 has in $G(\star)$ the order 4. The element z^2 belongs to the center of $G(\star)$, and $y_1 \star z_1 = y_1z_1 = z^2yzx^2 = z^3x^2y$ equals $z_1 \star y_1 = z_1y_1 = zx^2z^2y = z^3x^2y$. It is now straightforward to check the remaining relations: $x \star z_1 \star x^\star = xz_1x^{-1}z^2 = xzx^{-1}x^2z^2 = zyx^2z^2 = zx^2z^2y = z_1y_1 = z_1 \star y_1$ and $x \star y_1 \star x^\star = xy_1x^{-1} = xz^2yx^{-1} = z^2z^2y = z^2 \star y_1$. Therefore, $x \mapsto x$, $z \mapsto z_1$, $y \mapsto y_1$ defines an isomorphism $G(\cdot) \cong G(\star)$.

Let us now consider the case of 2-related groups. Lemma 2.4 gives an isomorphism $G[M_1, z^2] \cong G[M_3, z^2]$. If $S = M_1$, then it is enough to note that $(zx^2) \star (zx^2) = zx^2zx^2z^2 = z^2$. Indeed, inner automorphisms generated by z and $z_1 = zx^2$ coincide on M_1, $z_1 \star z_1 = z \cdot z$, and so substituting z by z_1 gives an isomorphism $G \cong G[M_1, z^2]$. If $S = M_2$, put $a = xy$ and $b = x$. Then $a \cdot a = xyxy = xyz^2yx = x^2z^2 = x \star x = b \star b$, and for any $s \in S$ one has $asa^{-1} = xysy^{-1}x^{-1} = xsx^{-1} = b \star s \star b^\star$. So, groups G and $G[S, z^2]$ are isomorphic.

$\square$

References

[1] Donovan D., Oates-Williams S., Praeger Ch.E., *On the distance between distinct group Latin squares*, J. Combin. Des. **5** (1997), 235–248.

[2] Drápal A., *How far apart can the group multiplication table be?*, European J. Combin. **13** (1992), 335–343.

[3] Drápal A., *Non-isomorphic* 2*-groups coincide at most in three quarters of their multiplication tables*, European J. Combin. **20** (2000), 301–321.

[4] Vojtěchovský P., *O Hammingově vzdálenosti grup*, M.D. Thesis (in Czech), Charles University, Prague, 1998.

[5] Zhukavets N., *Close* 2*-groups*, Ph.D. Thesis, Charles University, Prague, in preparation.

Department of Algebra, Faculty of Mathematics and Physics, Charles University, Sokolovská 83, 186 75 Prague 8, Czech Republic

(*Received* June 20, 2000)