



www.theoryofgroups.ir

International Journal of Group Theory
ISSN (print): 2251-7650, ISSN (on-line): 2251-7669
Vol. 9 No. 2 (2020), pp. 95-111.
© 2020 University of Isfahan



www.ui.ac.ir

GROUPS WITH NUMERICAL RESTRICTIONS ON MINIMAL GENERATING SETS

LEONID A. KURDACHENKO, PATRIZIA LONGOBARDI AND MERCEDE MAJ*

Communicated by Gunnar Traustason

ABSTRACT. We study an inverse problem of small doubling type. We investigate the structure of a finitely generated group G such that for any set S of generators of G of minimal order we have $|S^2| \leq 3|S| - \beta$, where $\beta \in \{1, 2, 3\}$.

1. Introduction

Let G denote an arbitrary group. If S is a subset of G , then we write

$$S^2 = \{xy \mid x, y \in S\}.$$

If G is an additive group, then we put

$$2S = \{x + y \mid x, y \in S\}.$$

A well-known problem in additive number theory is to find the precise structure of S in the case when S is a finite subset of G and

$$|S^2| \leq \alpha|S| + \beta$$

with α (the doubling coefficient) and $|\beta|$ small. Problems of this kind are called *inverse problems of small doubling type*. In the additive group of integers, these problems were detailed investigated by

MSC(2010): Primary: 20E34, 20F05; Secondary: 11P70.

Keywords: Small doubling, minimal generating subsets, inverse problems.

Received: 15 January 2019, Accepted: 01 February 2019.

*Corresponding author.

<http://dx.doi.org/10.22108/ijgt.2019.115131.1526>

G. A. Freiman in [6], [7], [8] and [9]. It is very easy to prove that if S is a finite subset of integers, $|S| = k$, then $|2S| \geq 2|S| - 1$, and $|2S| = 2|S| - 1$ if and only if there exist integers a, q such that $S = \{a, a + q, a + 2q, \dots, a + (k - 1)q\}$, i.e. S is an arithmetic progression of length k . In his famous theorem, Freiman proved that if S is a finite set of integers with $k \geq 3$ elements and $|2S| \leq 3k - 4$, then there exist integers a, q such that $q > 0$ and $S \subseteq \{a, a + q, a + 2q, \dots, a + (2k - 4)q\}$. He obtained similar results if $|2S| \leq 3|S| - 3$, or $|2S| \leq 3|S| - 2$. For other authors results of this type please see [27], [5], [22], [32], [33] and [34].

In arbitrary abelian groups, inverse problems have been studied by many other authors (see, for example, [1], [20], [18], [27], [30] and [19]). This study was initiated by M. Kneser [26].

More recently, small doubling problems in non-abelian groups have also been studied, see for example [2], [36], [4]. We also refer to recent surveys [19], [31], [3] and books [28] and [35].

In a series of papers with G. A. Freiman, M. Herzog, Y. V. Stanchescu, A. Plagne and D. J. S. Robinson (see [10, 11, 12, 13, 14, 15, 16] and [24]) the last two authors of the current paper studied small doubling problems in an orderable group.

J. H. B Kemperman showed that if S is a finite subset of any torsion-free group, then $|S^2| \geq 2|S| - 1$ (see [25]), while G. A. Freiman and B. M. Schein proved that if $|S| = k$, then $|S^2| = 2|S| - 1$ if and only if $S = \{a, aq, \dots, aq^{k-1}\}$, i.e. S is a geometric progression and either $aq = qa$ or $aq a^{-1} = q^{-1}$ (see [17]). Therefore it is quite natural to ask what is the structure of S in the case when S is a finite subset of a group G , $|S| = k \geq 3$ and $|S^2| \leq 3|S| - \beta$, where $\beta = 1, 2, 3, 4$. It could be also interesting to know the structure of $\langle S \rangle$ if S is a finite subset of a group and $|S^2| \leq 3|S| - \beta$ where $\beta = 1, 2, 3, 4$. There is an old conjecture by G. Freiman stating that if S is a finite subset of a torsion-free group, $1 \in S$ and $|S^2| \leq 3k - 4$, then $\langle S \rangle$ is abelian (see [21, p. 250]).

If G is a finitely generated group, we denote by $d(G)$ the minimal order of a finite set of generators of G . In the current paper, we investigate the structure of a finitely generated group G in which $|S^2| \leq 3|S| - \beta$, $\beta = 1, 2, 3$ for **any** generating subset S of G of minimal order.

The present paper is organized as follows.

In section 2, we studied the case $|S^2| \leq 3k - 3$ and we proved the following Theorem.

Theorem 2.4. *Let G be a finitely generated group with $d(G) = n$. Suppose that $|S^2| \leq 3|S| - 3$, for any generating subset S of G such that $|S| = n$. Then G is a group of one of the following types:*

- (i) G is the quaternion group of order 8,
- (ii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle$, where $x_2^2 = x_3^2 = x_4^2 = x_5^2 = 1$,
- (iii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle$, where $x_3^2 = x_4^2 = 1$,
- (iv) G is abelian and $n \leq 3$.

Conversely, if G satisfies one of (i) – (iii), or (iv) with $n > 1$, then $|S^2| \leq 3|S| - 3$, for any generating subset S of G with $|S| = d(G)$.

In section 3, we studied the case $|S^2| \leq 3|S| - 2$. Obviously, if $|S| = 2$, then $|S^2| \leq 3|S| - 2$, therefore we assume $d(G) \geq 3$. We proved the following Theorem.

Theorem 3.5. *Let G be a finitely generated group with $d(G) = n \geq 3$. Suppose that $|S^2| \leq 3|S| - 2$, for any generating subset S of G such that $|S| = n$. Then G is a group of one of the following types:*

- (i) $G = \langle x_1, x_2, x_3 \mid x_1^2 = x_2^2 = x_3^2 = c \in Z(G), c^2 = 1, x_j x_i x_j^{-1} = x_i^3, i \neq j, 1 \leq i, j \leq 3 \rangle \simeq Q_8 \times \langle d \rangle, |d| = 2,$
- (ii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle \times \langle x_6 \rangle,$ where $x_1^2 = x_2^2 = x_3^2 = x_4^2 = x_5^2 = x_6^2 = 1,$
- (iii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle,$ where $x_3^2 = x_4^2 = x_5^2 = 1,$
- (iv) G is abelian and $n \leq 4.$

Conversely, if G satisfies one of (i) – (iv), then $|S^2| \leq 3|S| - 2$, for any generating subset S of G with $|S| = d(G).$

Finally, in section 4, we studied the case $|S^2| \leq 3|S| - 1$. We proved the following result.

Theorem 4.6. *Let G be a finitely generated group with $d(G) = n \geq 3$. Suppose that $|S^2| \leq 3|S| - 1$, for any generating subset S of G such that $|S| = n$. Then G is a group of one of the following types:*

- (i) $G = \langle x_1, x_2 \rangle \langle x_3 \rangle, x_3^4 = 1, x_1 x_2 = x_2 x_1, x_3^{-1} x_1 x_3 = x_1^{-1}, x_3^{-1} x_2 x_3 = x_2^{-1},$
- (ii) $G = \langle x_1, x_2 \rangle \langle x_3 \rangle, x_1^4 = x_2^4 = x_3^4 = 1, x_1 x_3 = x_3 x_1, x_2 x_3 = x_3 x_2, x_2^{-1} x_1 x_2 = x_1^{-1}, x_1^2 x_2^2 x_3^2 = 1,$
- (iii) $G = \langle x_1, x_2 \rangle \rtimes \langle x_3 \rangle, x_1^4 = x_2^4 = x_3^2 = 1, x_1^2 = x_2^2, x_2^{-1} x_1 x_2 = x_1^{-1}, x_3^{-1} x_1 x_3 = x_1^{-1}, x_3^{-1} x_2 x_3 = x_2^{-1},$
- (iv) $G \simeq D_4 \times C_2,$
- (v) $G \simeq Q_8 \times C_2,$
- (vi) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle \times \langle x_6 \rangle,$ where $x_2^2 = x_3^2 = x_4^2 = x_5^2 = x_6^2 = 1,$
- (vii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle,$ where $x_4^2 = x_5^2 = 1,$
- (viii) G is abelian and $n \leq 4.$

Conversely, if G satisfies one of (i) – (viii), then $|S^2| \leq 3|S| - 1$, for any generating subset S of G with $|S| = d(G).$

We refer to [29] for notation, in particular we will denote C_n the cyclic group of order n , Q_8 the quaternion group of order 8, and D_n the dihedral group of order $2n$.

2. Minimal generating subsets S with $|S^2| \leq 3|S| - 3$

We start this section with the following useful Proposition.

Proposition 2.1. *Let G be a finitely generated group with $d(G) = n \geq 3$.*

If G is not abelian, then G includes a subset Y such that $G = \langle Y \rangle, |Y| = n$, and Y^2 contains at least $\frac{1}{2}(n^2 + n)$ elements.

Proof. Let S be a finite subset of G such that $G = \langle S \rangle$ and $|S| = n$. Write $S = \{x_1, x_2, \dots, x_n\}$. Since G is not abelian, there exist $i, j \in \{1, \dots, n\}, i \neq j$ such that $x_i x_j \neq x_j x_i$. Without loss of generality

we can suppose $x_1x_2 \neq x_2x_1$. Suppose now that $x_1x_j = x_jx_1$ for some $j > 2$, and let j be minimum with this property. Then $x_1(x_2x_j) = (x_1x_2)x_j \neq (x_2x_1)x_j = x_2(x_1x_j) = x_2(x_jx_1) = (x_2x_j)x_1$. Put $S_1 = \{x_1, \dots, x_{j-1}, x_2x_j, x_{j+1}, \dots, x_n\}$, then $G = \langle S_1 \rangle$ and $|S_1| = n$. Using the above arguments, after finitely many steps we obtain a subset $Y = \{y_1, y_2, \dots, y_n\}$ of order n such that $y_1y_j \neq y_jy_1$ for all $j > 1$, and such that $G = \langle Y \rangle$. Suppose that $y_jy_k = y_my_t$ where $j \neq k, m \neq t, j \neq m$. Then $k \neq t$. If $j \neq t$ then $y_j \in \langle Y \setminus \{y_j\} \rangle$. If $j = t$ then $y_k = y_j^{-1}y_my_j$, so that $y_k \in \langle Y \setminus \{y_k\} \rangle$. In both cases we obtain $d(G) \leq n - 1$. This contradiction shows that $y_jy_k \neq y_my_t$ whenever $|\{j, k, m, t\}| \geq 3$. Consider now the elements:

$$y_1y_2, \dots, y_1y_n, y_2y_3, \dots, y_2y_n, \dots, y_{n-1}y_n.$$

By the previous arguments these elements are pairwise different. Also the elements

$$y_2y_1, \dots, y_ny_1$$

are pairwise different. By the previous arguments $y_jy_1 \neq y_sy_k$ for $j \geq 2, 1 \leq s < k \leq n$. Finally the element y_1^2 is different from the previous ones. It follows that the subset Y^2 has at least

$$(n - 1) + (n - 2) + \dots + 2 + 1 + (n - 1) + 1 = \frac{1}{2}(n^2 - n) + n = \frac{1}{2}(n^2 + n)$$

elements. □

Corollary 2.2. *Let G be a finitely generated group with $d(G) = n \geq 3$.*

Suppose that $|S^2| \leq 3|S| - 3$ for each generating subset S of G such that $|S| = n$.

Then G is abelian.

Proof. Suppose G non-abelian. By Proposition 2.1, G has a finite subset Y such that $G = \langle Y \rangle, |Y| = n$ and $|Y^2| \geq \frac{1}{2}(n^2 + n)$. Since $|Y^2| \leq 3|Y| - 3$, we obtain $\frac{1}{2}(n^2 + n) \leq 3n - 3$. It follows that $n \leq 3$. Thus $Y = \{y_1, y_2, y_3\}$. From the proof of Proposition 2.1 we can see that Y^2 contains the elements: $y_1^2, y_1y_2, y_1y_3, y_2y_1, y_3y_1, y_2y_3$, that are pairwise different. Since $|Y^2| = 6, Y^2 = \{y_1^2, y_1y_2, y_1y_3, y_2y_1, y_3y_1, y_2y_3\}$. On the other hand $y_3y_2 \in Y^2$ and by the previous remarks we have only the possibility $y_2y_3 = y_3y_2$. Put $M = \{y_1, y_1y_2, y_3\}$. Now it is easy to check that the set $\{y_1^2, y_1y_3, y_3y_1, y_1y_1y_2, y_1y_2y_1, y_1y_2y_3, y_3y_1y_2\}$ has order 7: in particular $(y_1y_2)y_3 \neq y_3(y_1y_2)$ since $y_2y_3 = y_3y_2$. It follows that M^2 contains at least 7 elements and we obtain the final contradiction. □

Corollary 2.3. *Let G be a finitely generated group with $d(G) = 2$.*

Suppose that $|S^2| \leq 3|S| - 3$ for each generating subset S of G such that $|S| = 2$.

Then G is abelian or G is the quaternion group of order 8.

Conversely if either G is abelian or $G \simeq Q_8$, then $|S^2| \leq 3|S| - 3$ for each generating set S of G such that $|S| = 2$.

Proof. Suppose that G is non-abelian. Then $G = \langle x, y \rangle$ where $xy \neq yx$. By our condition $|S^2| \leq 3|S| - 3 = 3$. We have $S^2 = \{x^2, y^2, xy, yx\}$. Then $x^2 = y^2$. Suppose that $x^2 = y^2 = c \neq 1$. Then

$c \in \zeta(G)$. We have also $G = \langle x, xy \rangle$. Then $x(xy) \neq (xy)x$, hence $x^2 = (xy)^2$ and also $y^2 = (xy)^2$. Furthermore, from $G = \langle x, cy \rangle$ and $c \in \zeta(G)$ we get $y^2 = x^2 = (cy)^2 = c^2y^2$ from which $c^2 = 1$. Using $x^2 = (xy)^2$, we obtain that $x = yxy$. It follows that $xy^{-1} = yx$ and hence $y^{-1} = x^{-1}yx$. Thus the subgroup $\langle y \rangle$ is normal in G . By the same reason also $\langle x \rangle$ is normal in G . Finally $x^4 = (x^2)^2 = c^2 = 1$ and similarly $y^4 = 1$. It follows that G is the quaternion group of order 8. Suppose now $x^2 = y^2 = 1$. Since $G = \langle x, xy \rangle$, we obtain $(xy)^2 = x^2 = 1$. It follows that $y^{-1}xy = yxy = x^{-1} = x$, so $xy = yx$ and we obtain a contradiction.

Conversely, if G is abelian and $S = \{x, y\}$, then $S^2 = \{x^2, xy, y^2\}$, and $|S^2| \leq 3 = 3|S| - 3$. If $G \simeq Q_8$, and $S = \{x, y\}$, $G = \langle S \rangle$, then $x^2 = y^2$ and $S^2 = \{xy, yx, x^2\}$, as required. \square

Now we can prove Theorem 2.4.

Theorem 2.4. *Let G be a finitely generated group with $d(G) = n$. Suppose that $|S^2| \leq 3|S| - 3$ for any generating subset S of G such that $|S| = n$. Then G is a group of one of the following types:*

- (i) G is the quaternion group of order 8,
- (ii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle$, where $x_2^2 = x_3^2 = x_4^2 = x_5^2 = 1$,
- (iii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle$, where $x_3^2 = x_4^2 = 1$,
- (iv) G is abelian and $n \leq 3$.

Conversely, if G satisfies one of (i) – (iii), or (iv) with $n > 1$, then $|S^2| \leq 3|S| - 3$, for any generating subset S of G with $|S| = d(G)$.

Proof. If $n = 2$, then Corollary 2.3 shows that either G is the quaternion group of order 8 or G is abelian. If $n = 3$, then Corollary 2.2 shows that G is abelian. Hence either (i) or (iv) holds.

Now suppose $n \geq 4$. Then G is abelian by Corollary 2.2 and G is a finitely generated abelian group with $d(G) = n$. Choose an arbitrary generating subset S of G such that $|S| = n$. Let $S = \{g_1, \dots, g_n\}$. Clearly $S^2 = A \cup B$ where $A = \{g_j g_m \mid 1 \leq j < m \leq n\}$, $B = \{g_j^2 \mid 1 \leq j \leq n\}$. Suppose that $g_j g_m = g_s g_k$ where $(j, m) \neq (s, k)$, $j < m$, $s < k$. If $\{j, m\} \cap \{s, k\} = \emptyset$, then $g_m = g_j^{-1} g_s g_k$, and we obtain a contradiction with the minimality of S . Suppose that $s \in \{j, m\}$. If $s = j$, then $g_m = g_k$, which is impossible. If $s = m$, then $g_j = g_s g_k g_s^{-1}$, and we obtain a contradiction with the minimality of S . Using similar arguments we obtain a contradiction if $k \in \{j, m\}$. It follows that the elements of the subset A are pairwise different, and arguing analogously, that A and B are disjoint. Then $|S^2| = \frac{1}{2}n(n - 1) + d$ where $d = |B|$. We note that $d \leq n$. Thus $\frac{1}{2}n(n - 1) + 1 \leq 3n - 3$, so that $n \leq 5$. If $n = 4$, then $\frac{1}{2}n(n - 1) + d = 6 + d \leq 3n - 3 = 9$. It follows that $d \leq 3$, so that we can suppose $g_3^2 = g_4^2$. Since G is a finitely generated abelian group with $d(G) = 4$, we have $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle$, for some elements x_1, x_2, x_3, x_4 . Clearly $\{x_1, x_2, x_3, x_4\}$ is a minimal generating subset for G . Then, arguing as before, we can suppose $x_3^2 = x_4^2$. That is possible only in the case when $x_3^2 = x_4^2 = 1$. If $n = 5$, then $\frac{1}{2}n(n - 1) + d = 10 + d \leq 3n - 3 = 12$. It follows that $d \leq 2$, so that we can suppose $g_2^2 = g_3^2 = g_4^2 = g_5^2$. Since G is a finitely generated abelian group with

$d(G) = 5$, we have $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle$, for some elements x_1, x_2, x_3, x_4, x_5 . We can suppose $x_2^2 = x_3^2 = x_4^2 = x_5^2$ and, as in the previous case, we obtain that $x_2^2 = x_3^2 = x_4^2 = x_5^2 = 1$.

Conversely, suppose that G satisfies (i), or (ii), or (iii), or (iv) with $n > 1$. It is easy to prove that $|S^2| \leq 3|S| - 3$ if $|S| = n = d(G)$ and $G = \langle S \rangle$. In fact, if G is abelian and $n = 3$, then $|S^2| \leq \frac{1}{2}n(n-1) + 3 = 6 = 3|S| - 3$. If (iii) holds with $n = 4$, then $|B| \leq 3$, where $B = \{g^2 \mid g \in S\}$, and $|S^2| \leq \frac{1}{2}n(n-1) + 3 = 8 = 3|S| - 3$. If (ii) holds with $n = 5$, then $|B| \leq 2$, and $|S^2| \leq \frac{1}{2}n(n-1) + 2 = 12 = 3|S| - 3$, and finally if (i) holds, then the result follows from Corollary 2.3. \square

From Theorem 2.4 it follows the following easy Corollary.

Corollary 2.5. *Let G be a finitely generated group with $d(G) = n$.*

Suppose that $|S^2| \leq 3|S| - 3$ for each generating subset S of G such that $|S| = n$.

If G is torsion-free, then G is abelian and $n \leq 3$.

3. Minimal generating subsets S with $|S^2| \leq 3|S| - 2$

In this section we will consider finitely generated groups G such that $|S^2| \leq 3|S| - 2$ for each generating subset S of G with the property $|S| = d(G)$.

Suppose that G is non-abelian and $d(G) = 2$. If $S = \{g_1, g_2\}$ is a generating subset of G , then clearly $g_1g_2 \neq g_2g_1$, so that $3 \leq |S^2| \leq 4 = 3|S| - 2$.

Therefore in the sequel we will assume that $d(G) \geq 3$.

We start with an easy more general Lemma.

Lemma 3.1. *Let G be a finitely generated group with $d(G) = n \geq 3$. Suppose that $|S^2| \leq 3|S| - 1$ for each generating subset S of G such that $|S| = n$. If G is non-abelian, then $n \in \{3, 4\}$.*

Proof. Since G is non-abelian, Proposition 2.1 shows that G has a finite subset Y such that $G = \langle Y \rangle$, $|Y| = n$ and $|Y^2| \geq \frac{1}{2}(n^2 + n)$. Thus we have $\frac{1}{2}(n^2 + n) \leq 3n - 1$. It follows that $n^2 - 5n + 2 \leq 0$. This is possible only if $n \in \{3, 4\}$. \square

Now we show that in the case $n = d(G) = 4$ and $|S^2| \leq 3|S| - 1$ for each generating subset S of G such that $|S| = n$, again we obtain that G is abelian.

Lemma 3.2. *Let G be a finitely generated group with $d(G) = 4$.*

Suppose that $|S^2| \leq 11$ for each generating subset S of G such that $|S| = 4$.

Then G is abelian.

Proof. Suppose the contrary, so let G be non-abelian. Then, arguing as in the proof of Proposition 2.1, we obtain that G contains a subset $S = \{x_1, x_2, x_3, x_4\}$ such that $G = \langle S \rangle$ and the set

$$L = \{x_1^2, x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4, x_4x_1, x_3x_1, x_2x_1\}$$

has order 10. Now consider the set $T = \{y_1, y_2, y_3, y_4\}$, where $y_2 = x_1x_2$, $y_j = x_j$ whenever $j \neq 2$. It is easy to see that the set

$$V = \{y_1^2, y_1y_2, y_1y_3, y_1y_4, y_2y_3, y_2y_4, y_3y_4, y_4y_1, y_3y_1, y_2y_1\}$$

has order 10. If $x_2x_3 = x_3x_2$, then $y_2y_3 \neq y_3y_2$ and $T^2 = V \cup \{y_3y_2\}$. Therefore $x_2x_4 \neq x_4x_2$ otherwise $y_2y_4 \neq y_4y_2$ and $|T^2| > 11$. Arguing analogously with x_3 we get that it is not possible to have simultaneously $x_3x_2 = x_2x_3$ and $x_3x_4 = x_4x_3$ and, arguing with x_4 , to have simultaneously $x_4x_2 = x_2x_4$ and $x_4x_3 = x_3x_4$. From this it follows that $x_\alpha x_\beta \neq x_\beta x_\alpha, x_\alpha x_\gamma \neq x_\gamma x_\alpha$ for suitable α, β, γ such that $\{2, 3, 4\} = \{\alpha, \beta, \gamma\}$. But this implies $|S^2| > 11$, the final contradiction. \square

Now we study the case $n = d(G) = 3$ and $|S^2| \leq 3|S| - 2$ for each generating subset S of G such that $|S| = n$. Our first remark is the following Lemma.

Lemma 3.3. *Let G be a finitely generated group with $d(G) = 3$.*

Suppose that $|X^2| \leq 7$ for each generating subset X of G such that $|X| = 3$. If G is non-abelian and $S = \{x_1, x_2, x_3\}$ is a subset of G such that $G = \langle S \rangle$ and $|\{x_1^2, x_1x_2, x_1x_3, x_2x_3, x_2x_1, x_3x_1\}| = 6$, then

$$x_1^2 = x_2^2 = x_3^2.$$

Proof. Write $L = \{x_1^2, x_1x_2, x_1x_3, x_2x_3, x_2x_1, x_3x_1\}$ and assume by contradiction that $x_2^2 \neq x_1^2$. Then $S^2 = L \cup \{x_2^2\}$ has order 7. This implies, arguing as usual, that $x_2x_3 = x_3x_2$.

Consider the set $T = \{y_1, y_2, y_3\}$ where $y_1 = x_1, y_2 = x_2, y_3 = x_1x_3$. Obviously $G = \langle T \rangle$ and it is easy to see that $V = \{y_1^2, y_2^2, y_1y_2, y_1y_3, y_2y_3, y_3y_1, y_2y_2\}$ has order 7. But $x_2x_3 = x_3x_2$ implies $y_2y_3 \neq y_3y_2$, then the subset $V \cup \{y_3y_2\}$ of T^2 has order 8, a contradiction. A similar argument holds if $x_3^2 \neq x_1^2$, so $x_1^2 = x_2^2 = x_3^2$, as required. \square

Now we can prove the following Proposition that gives a description of G if $d(G) = 3$ and $|S^2| \leq 7$.

Proposition 3.4. *Let G be a finitely generated group with $d(G) = 3$. Suppose that $|S^2| \leq 7$ for each generating subset S of G such that $|S| = 3$. If G is non-abelian, then*

$$G = \langle x_1, x_2, x_3 \mid x_1^2 = x_2^2 = x_3^2 = c \in \zeta(G), c^2 = 1, x_jx_kx_j^{-1} = x_k^3, 1 \leq j, k \leq 3, j \neq k \rangle \simeq Q_8 \times \langle d \rangle, |d| = 2.$$

Conversely, if $G = Q_8 \times \langle d \rangle$ with $|d| = 2$, then $d(G) = 3$ and $|S^2| \leq 7$ for every generating subset S of G with $|S| = 3$.

Proof. Arguing as in the proof of Proposition 2.1, we find a subset $S = \{x_1, x_2, x_3\}$ of G such that $G = \langle S \rangle$ and $|\{x_1^2, x_1x_2, x_1x_3, x_2x_3, x_2x_1, x_3x_1\}| = 6$. Then by Lemma 3.3 we have

$$x_1^2 = x_2^2 = x_3^2.$$

Put $y_1 = x_1, y_2 = x_1x_2, y_3 = x_3, S_1 = \{y_1, y_2, y_3\}$. Then $G = \langle S_1 \rangle$ and it is easy to prove that $|\{y_1^2, y_1y_2, y_1y_3, y_2y_3, y_2y_1, y_3y_1\}| = 6$. Therefore, again by Lemma 3.3, we have

$$y_1^2 = y_2^2 = y_3^2.$$

From $y_1^2 = y_2^2$ it follows $x_1^2 = x_1x_2x_1x_2$, so $x_1 = x_2x_1x_2$ and $x_1^{-1}x_2x_1 = x_2^{-1}$. It follows that $[x_2, x_1] = x_2^{-2}$. On the other hand $x_1^2 = x_2^2$, so we have $x_2x_2 = x_1x_2x_1x_2$, thus $x_2 = x_1x_2x_1$ and $x_2^{-1}x_1x_2 = x_1^{-1}$. It follows that $[x_1, x_2] = x_1^{-2}$. We have now $x_2^{-2} = [x_2, x_1] = [x_1, x_2]^{-1} = x_1^2 = x_2^2$, hence $x_2^4 = 1$. Then also $x_1^4 = (x_1^2)^2 = (x_2^2)^2 = 1$ and $x_3^4 = 1$. The equality $x_1^2 = x_2^2 = x_3^2 = c$ shows that $c \in Z(G)$ and $|c| = 2$. Arguing as before we obtain that $[x_1, x_3] = x_1^{-2} = x_3^2 = x_2^2$ and $[x_2, x_3] = x_2^{-2} = x_3^2 = x_2^2$. Obviously $\langle x_1, x_2 \rangle \simeq Q_8$. From $x_1x_2x_3x_1x_2x_3 = (x_1x_2)^2x_3^2 = 1$ we obtain the result.

Conversely, let $G = Q_8 \times \langle d \rangle, |d| = 2$. Then $x^2 = y^2$ for every $x, y \in G$ with $x^2 \neq 1$ and $y^2 \neq 1$. Moreover $s \in Z(G)$ for every s in G of order 2. Now let $S = \{x_1, x_2, x_3\}$. If there exists $i \in \{1, 2, 3\}$, say $i = 1$ such that $x_1^2 = 1$ then $x_1 \in Z(G)$,

$$S^2 = \{x_1^2, x_1x_2, x_1x_3, x_2x_3, x_2^2, x_3x_2, x_3^2\},$$

and $|S^2| \leq 7$. If $x_i^2 \neq 1$ for every $i \in \{1, 2, 3\}$, then $x_1^2 = x_2^2 = x_3^2$,

$$S^2 = \{x_1^2, x_1x_2, x_1x_3, x_2x_3, x_2x_1, x_3x_1, x_3x_2\}$$

and again $|S^2| \leq 7$. The result is proved. □

Now we can prove Theorem 3.5.

Theorem 3.5. *Let G be a finitely generated group with $d(G) = n \geq 3$. Suppose that $|S^2| \leq 3|S| - 2$ for any generating subset S of G such that $|S| = n$. Then G is a group of one of the following types:*

- (i) $G = \langle x_1, x_2, x_3 \mid x_1^2 = x_2^2 = x_3^2 = c \in Z(G), c^2 = 1, x_jx_ix_j^{-1} = x_i^3, i \neq j, 1 \leq i, j \leq 3 \rangle \simeq Q_8 \times \langle d \rangle, |d| = 2,$
- (ii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle \times \langle x_6 \rangle,$ where $x_1^2 = x_2^2 = x_3^2 = x_4^2 = x_5^2 = x_6^2 = 1,$
- (iii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle,$ where $x_3^2 = x_4^2 = x_5^2 = 1,$
- (iv) G is abelian and $n \leq 4.$

Conversely, if G satisfies one of (i) – (iv), then $|S^2| \leq 3|S| - 2$ for any generating subset S of G with $|S| = d(G).$

Proof. Suppose first that G is non-abelian. Then Lemma 3.1 shows that $n \in \{3, 4\}$. More precisely Lemma 3.2 shows that $d(G) = 3$. Then Proposition 3.4 implies that G is a group of type (i).

Assume now that G is abelian. Choose an arbitrary generating subset S of G such that $|S| = n$. Let $S = \{g_1, \dots, g_n\}$. Clearly $S^2 = A \cup B$ where $A = \{g_jg_m \mid 1 \leq j < m \leq n\}, B = \{g_j^2 \mid 1 \leq j \leq n\}$. As in a proof of Theorem 2.4 we can show that all elements of the subset A are pairwise different and

that A and B are disjoint. It follows that $|S^2| = \frac{1}{2}n(n - 1) + d$ where $d = |B|$. We note that $d \leq n$. Thus $\frac{1}{2}n(n - 1) + 1 \leq 3n - 2$, so that $n \leq 6$.

If $n = 5$, then $\frac{1}{2}n(n - 1) + d = 10 + d$. From $|S^2| \leq 3|S| - 2$ we obtain that $10 + d \leq 13$, thus $d \leq 3$. Therefore we can suppose $g_3^2 = g_4^2 = g_5^2$, and G is of type (iii).

If $n = 6$, then $\frac{1}{2}n(n - 1) + d = 15 + d$. From $|S^2| \leq 3|S| - 2$ we obtain that $15 + d \leq 16$, which implies that $d \leq 1$, so that $g_1^2 = g_2^2 = g_3^2 = g_4^2 = g_5^2 = g_6^2$ and G is a group of type (ii).

Conversely, suppose that G satisfies (i), then $d(G) = 3$ and by Proposition 3.4 $|S^2| \leq 7$ for every generating subset of G of order 3. Now suppose that (ii), or (iii), or (iv) holds, then G is abelian and for every subset S of G of order $n = d(G)$ we have $|S^2| = \frac{1}{2}n(n - 1) + d$ where $d = |B|$, $B = \{g^2 \mid g \in S\}$. Now if (ii) holds, then $n = 6$ and $d = 1$, and we have $|S^2| = 15 + 1 = 3|S| - 2$, as required; if (iii) holds, then $n = 5$ and $d = 3$, and we have $|S^2| \leq 10 + 3 = 3|S| - 2$, as required, and finally if (iv) holds, then $n \in \{3, 4\}$, $d \leq n$ and in any case $|S^2| \leq 3|S| - 2$ as required. \square

From Theorem 3.5 it follows the following easy Corollary.

Corollary 3.6. *Let G be a finitely generated group with $d(G) = n$.*

Suppose that $|S^2| \leq 3|S| - 2$ for each generating subset S of G such that $|S| = n$.

If G is torsion-free, then G is abelian and $n \leq 4$.

4. Minimal generating subsets S with $|S^2| \leq 3|S| - 1$

In this section we consider finitely generated groups G such that $|S^2| \leq 3|S| - 1$ for each generating subset S of G with the property $|S| = d(G)$.

First we assume G non-abelian. Hence by Lemmas 3.1 and 3.2 we have $d(G) = 3$.

Let $S = \{x_1, x_2, x_3\}$, with $G = \langle S \rangle$ non-abelian. From $|S^2| \leq 3|S| - 1 = 8$, it follows that either two of the elements x_1, x_2, x_3 have the same square or two of them commute. We study first the situation $|\{x_1^2, x_2^2, x_3^2\}| = 3$. In this case we can suppose, without loss of generality, $x_2x_3 = x_3x_2$. We start with the following Lemma.

Lemma 4.1. *Let $G = \langle x_1, x_2, x_3 \rangle$, with $d(G) = 3, x_2x_3 = x_3x_2, |\{x_1^2, x_2^2, x_3^2\}| = 3$. If $|T|^2 \leq 8$ for each generating subset T of G of order 3, then $x_2 \in Z(G)$ or $x_3 \in Z(G)$ or $x_2x_3 \in Z(G)$ or the following holds*

$$(i) \ G = \langle x_2, x_3 \rangle \langle x_1 \rangle, x_1^4 = 1, x_2x_3 = x_3x_2, x_1^{-1}x_2x_1 = x_2^{-1}, x_1^{-1}x_3x_1 = x_3^{-1}.$$

Proof. Suppose that $x_2 \notin Z(G), x_3 \notin Z(G), x_2x_3 \notin Z(G)$. Thus $x_1x_2 \neq x_2x_1$. Consider the subset $T = \{x_1, x_2, x_1x_2x_3\}$. Obviously $G = \langle T \rangle$, thus $|T^2| \leq 8$. By the hypothesis $x_1x_2 \neq x_2x_1$ and x_2 does not commute with $x_1x_2x_3$. If x_1 commutes with $x_1x_2x_3$, then $x_2x_3 \in Z(G)$, which is not the case. Hence from $|T^2| \leq 8$ we get that either $(x_1x_2x_3)^2 = x_1^2$ or $(x_1x_2x_3)^2 = x_2^2$. Arguing similarly on the subset $V = \{x_1, x_3, x_1x_2x_3\}$ we obtain that either $(x_1x_2x_3)^2 = x_1^2$ or $(x_1x_2x_3)^2 = x_3^2$. Then

$(x_1x_2x_3)^2 = x_1^2$, hence

$$(x_2x_3)^{x_1} = (x_2x_3)^{-1}.$$

Now consider the generating set $W = \{x_1, x_1x_2, x_3\}$ consisting of pairwise non-commuting elements. From $|W^2| \leq 8$ we get that either $(x_1x_2)^2 = x_1^2$ or $(x_1x_2)^2 = x_3^2$. Arguing similarly on $W_1 = \{x_1, x_1x_3, x_2\}$ we obtain that either $(x_1x_3)^2 = x_1^2$ or $(x_1x_3)^2 = x_2^2$.

First suppose that either $(x_1x_2)^2 = x_1^2$ or $(x_1x_3)^2 = x_1^2$, and without loss of generality, $(x_1x_2)^2 = x_1^2$. Then $x_2^{x_1} = x_2^{-1}$ and from $(x_2x_3)^{x_1} = (x_2x_3)^{-1}$ we obtain that also $x_3^{x_1} = x_3^{-1}$. Thus the equality $(x_1x_3)^2 = x_2^2$ is impossible, otherwise $x_2^2 = x_1x_3x_1x_3 = x_1^2x_3^{-1}x_3x_1x_3 = x_1^2$. Therefore $(x_1x_3)^2 = x_1^2$ and considering the generating subset of pairwise non-commuting elements $\{x_1^{-1}, x_2, x_1x_3\}$ we obtain that $(x_1x_3)^2 = x_1^{-2}$ and $x_1^4 = 1$, or $x_2^2 = x_1^{-2}$, and similarly, considering the subset $\{x_1^{-1}, x_1x_2, x_3\}$ that either $x_1^4 = 1$, or $x_3^2 = x_1^{-2}$, thus $x_1^4 = 1$ since $x_2^2 \neq x_3^2$. Therefore (i) holds.

Finally suppose $(x_1x_2)^2 = x_2^2$ and $(x_1x_3)^2 = x_2^2$. In this case the generating subset $\{x_1, x_1x_2, x_1x_3\}$ has elements with different squares. Hence two of them commute and the unique possibility is $x_1x_2x_1x_3 = x_1x_3x_1x_2$, then $(x_2^{-1}x_3)x_1 = x_1(x_2^{-1}x_3)$. But from $(x_1x_3)^2 = x_2^2$ we have also that x_2^2 commutes with x_1 . Hence x_2x_3 commutes with x_1 and then it is in $Z(G)$ a contradiction. \square

We will prove later that if G satisfies (i), then $|S^2| \leq 8$, for every generating subset S of G of order 3.

We continue our investigation assuming that there exists a generating subset S of G , with $S = \{x_1, x_2, x_3\}$, $|\{x_1^2, x_2^2, x_3^2\}| = 3$, $x_2^2 \neq x_3^2$, either x_2 or x_3 in $Z(G)$. Assume for example that $x_3 \in Z(G)$. Then $x_1x_2 \neq x_2x_1$, since G is not abelian. In this case the structure of G is described in the following Lemma.

Lemma 4.2. *Let $G = \langle x_1, x_2, x_3 \rangle$, with $d(G) = 3$, $|\{x_1^2, x_2^2, x_3^2\}| = 3$. Suppose that G is non-abelian and that $|T^2| \leq 8$ for each generating subset T of G of order 3. If $x_3 \in Z(G)$, then one of the following holds:*

- (j) $G = \langle a, b \rangle \times \langle c \rangle, c^2 = 1, a^4 = 1, a^b = a^{-1}$,
- (jj) $G = \langle a, b \rangle \langle c \rangle, a^4 = b^4 = c^4 = 1, ac = ca, bc = cb, a^b = a^{-1}, a^2b^2c^2 = 1$.

Proof. Consider the generating subset of pairwise non-commuting elements $V = \{x_1x_3, x_2x_3, x_1x_2x_3\}$. Then either $(x_1x_2x_3)^2 = (x_1x_3)^2$ or $(x_1x_2x_3)^2 = (x_2x_3)^2$, therefore either $(x_1x_2)^2x_3^2 = x_1^2x_3^2$ or $(x_1x_2)^2x_3^2 = x_2^2x_3^2$, hence either $(x_1x_2)^2 = x_1^2$ or $(x_1x_2)^2 = x_2^2$. Without loss of generality we can suppose $(x_1x_2)^2 = x_1^2$, hence

$$x_2^{x_1} = x_2^{-1}.$$

Now consider the generating subset of pairwise non-commuting elements $W = \{x_1^{-1}x_3, x_2x_3, x_1x_2x_3\}$. Then $(x_1^{-1}x_3)^2 = (x_2x_3)^2$ or $(x_1x_2x_3)^2 = (x_1^{-1}x_3)^2$ or $(x_1x_2x_3)^2 = (x_2x_3)^2$. The last equality implies the contradiction $x_1^2 = x_2^2$. From the first equality we get $x_1^{-2} = x_2^2$, and from $x_2^{x_1} = x_2^{-1}$ we get $x_2^4 = 1$

and then $x_1^4 = 1$. Finally from $(x_1x_2x_3)^2 = (x_1^{-1}x_3)^2$ we obtain $x_1^2 = x_1^{-2}$. In any case

$$x_1^4 = 1.$$

Now consider the generating subset of pairwise non-commuting elements $\{x_1, x_2, x_1x_2x_3\}$. Then either $(x_1x_2x_3)^2 = x_1^2$ or $(x_1x_2x_3)^2 = x_2^2$. Since $(x_1x_2)^2 = x_1^2$, the first equality implies $x_3^2 = 1$ and (j) holds. So assume $(x_1x_2x_3)^2 = x_2^2$, then

$$x_1^2x_3^2 = x_2^2.$$

Arguing analogously on the generating subset of pairwise non-commuting elements $\{x_1, x_2^{-1}, x_1x_2x_3\}$, we obtain that either $x_3^2 = 1$ and (j) holds, or $(x_1x_2x_3)^2 = x_2^{-2}$, or $x_1^2 = x_2^{-2}$. In the second case, from $x_1^2x_3^2 = x_2^2$ we get that $x_2^4 = 1$ and also that $x_3^4 = 1$ and $x_1^2x_2^2x_3^2 = 1$, therefore (jj) holds. Finally in the last case we have $x_1^{-2} = x_1^2 = x_2^{-2}$, which is a contradiction. \square

Notice that if (j) holds, then $G = \langle a, c \rangle \langle b \rangle$, with $a^b = a^{-1}, c^b = c = c^{-1}$, therefore (i) of Lemma 4.1 holds.

We will show later that if (jj) holds, then $|S^2| \leq 8$ for every generating subset S of G of order 3.

Now we assume that there exists a generating subset S of G , with $S = \{x_1, x_2, x_3\}, |\{x_1^2, x_2^2, x_3^2\}| = 3, x_2x_3$ in $Z(G)$. Notice that in this case if $(x_2x_3)^2 \neq x_1^2, x_2^2$, then the subset $\{x_1, x_2, x_2x_3\}$ satisfies the hypothesis of Lemma 4.2 and (j) or (jj) of Lemma 4.2 holds. Similarly if $(x_2x_3)^2 \neq x_1^2, x_3^2$, then the subset $\{x_1, x_3, x_2x_3\}$ satisfies the hypothesis of Lemma 4.2. Hence we can suppose $(x_2x_3)^2 = x_1^2$. In this case we can prove:

Lemma 4.3. *Let $G = \langle x_1, x_2, x_3 \rangle$, with $d(G) = 3, |\{x_1^2, x_2^2, x_3^2\}| = 3$. Suppose that G is non-abelian and that $|T^2| \leq 8$ for each generating subset T of G of order 3. If $x_2x_3 \in Z(G)$ and $(x_2x_3)^2 = x_1^2$, then (i) of Lemma 4.1 holds.*

Proof. Consider the generating subset of pairwise non-commuting elements $V = \{x_1, x_2, x_1x_3\}$. Then either $(x_1x_3)^2 = x_1^2$ or $(x_1x_3)^2 = x_2^2$. If $(x_1x_3)^2 = x_2^2$, consider the generating subset of pairwise non-commuting elements $W = \{x_1x_3, x_3, x_1^{-1}(x_2x_3)\}$. Then either $x_3^2 = (x_1^{-1}(x_2x_3))^2 = 1$, or $x_2^2 = (x_1x_3)^2 = (x_1^{-1}(x_2x_3))^2 = 1$. But if $x_3^2 = 1$ then from $x_2^2x_3^2 = (x_2x_3)^2 = x_1^2$ we get the contradiction $x_2^2 = x_1^2$, while if $x_2^2 = 1$ from $x_2^2x_3^2 = (x_2x_3)^2 = x_1^2$ we obtain the contradiction $x_3^2 = x_1^2$. Therefore

$$(x_1x_3)^2 = x_1^2, \text{ i.e. } (x_3)^{x_1} = x_3^{-1}.$$

Arguing analogously on the generating subset of pairwise non-commuting elements $V_1 = \{x_1, x_3, x_1x_2\}$ we obtain that either $(x_1x_2)^2 = x_1^2$ or $(x_1x_2)^2 = x_3^2$ and that the relation $(x_1x_2)^2 = x_3^2$ is not possible considering the subset $W_1 = \{x_1x_2, x_2, x_1^{-1}(x_2x_3)\}$. Therefore

$$(x_1x_2)^2 = x_1^2, \text{ i.e. } (x_2)^{x_1} = x_2^{-1}.$$

Finally

$$x_1^4 = 1.$$

In fact, considering the subset $V_2 = \{x_1^{-1}, x_2, x_1x_3\}$ we get $x_1^2 = (x_1x_3)^2 = x_1^{-2}$ and $x_1^4 = 1$, or $x_1^{-2} = x_2^2$ and from $x_2^{x_1} = x_2^{-1}$ it follows that $x_2^2 = (x_2^2)^{x_1} = x_2^{-2}$ thus $x_1^4 = x_2^4 = 1$. Therefore (i) of Lemma 4.1 holds. \square

Now we assume that $|\{x^2 \mid x \in S\}| \leq 2$ for each generating subset S of order 3. First suppose that $|\{x^2 \mid x \in S\}| = 1$ for each generating subset S of order 3. In this case G is abelian, as the following Lemma shows.

Lemma 4.4. *Let $G = \langle x_1, x_2, x_3 \rangle, d(G) = 3$, and suppose that $|\{x^2 \mid x \in S\}| = 1$ for each generating subset S of G of order 3. Then G is an elementary abelian 3-generated 2-group.*

Proof. We have $x_1^2 = x_2^2 = x_3^2 = (x_1x_2)^2 = (x_1x_3)^2$, hence $x_1^{x_2} = x_1^{-1}, x_2^{x_1} = x_2^{-1}, x_1^{x_3} = x_1^{-1}, x_3^{x_1} = x_3^{-1}$. Considering the subset $\{x_1x_2x_3, x_3, x_2x_3\}$ we have also that $(x_1x_2x_3)^2 = (x_2x_3)^2$, thus $x_1^{x_2x_3} = x_1^{-1}$. But we have also that $x_1^{x_2x_3} = x_1$, therefore $x_1^2 = 1$. Thus $x_2^2 = x_3^2 = x_1^2 = 1$, then G is abelian and an elementary abelian 2-group, as required. \square

Now suppose that there exists a generating subset S of G of order 3, with $|\{x^2 \mid x \in S\}| = 2$ and that $|\{x^2 \mid x \in T\}| \leq 2$ for each generating subset T of order 3 of G .

We can suppose $G = \langle x_1, x_2, x_3 \rangle$ with $x_1^2 = x_2^2 \neq x_3^2$. The structure of G follows from the following Proposition.

Proposition 4.5. *Let $G = \langle x_1, x_2, x_3 \rangle, d(G) = 3, x_1^2 = x_2^2 \neq x_3^2$ and suppose that $|\{x^2 \mid x \in T\}| \leq 2$ for each generating subset T of G of order 3. Then either G is abelian or one of the following holds:*

- (α) $G = \langle x_1, x_2 \rangle \rtimes \langle x_3 \rangle, \langle x_1, x_2 \rangle \simeq Q_8, x_3^2 = 1, x_1^{x_3} = x_1^{-1}, x_2^{x_3} = x_2^{-1};$
- (β) $G = \langle a, b \rangle \times \langle c \rangle, a^4 = b^2 = c^2 = 1, a^b = a^{-1}, G \simeq D_4 \times C_2;$
- (γ) $G = \langle a, b \rangle \times \langle c \rangle, a^4 = b^4 = c^2 = 1, a^2 = b^2, a^b = a^{-1}, G \simeq Q_8 \times C_2.$

Conversely, if (α) or (β) or (γ) holds, then $|\{x^2 \mid x \in T\}| \leq 2$ for each generating subset T of G of order 3.

Proof. Consider the generating subset $\{x_2, x_1x_3, x_3\}$, then either $(x_1x_3)^2 = x_3^2$ or $(x_1x_3)^2 = x_2^2 = x_1^2$. Arguing similarly on $\{x_1, x_2x_3, x_3\}$, then either $(x_2x_3)^2 = x_3^2$ or $(x_2x_3)^2 = x_1^2 = x_2^2$.

Furthermore, considering the generating subsets $\{x_1, x_3, x_1x_2x_3\}$ and $\{x_1, x_3, x_1x_2\}$ we obtain that either $(x_1x_2x_3)^2 = x_3^2$ or $(x_1x_2x_3)^2 = x_1^2$ and either $(x_1x_2)^2 = x_3^2$ or $(x_1x_2)^2 = x_1^2$.

First we show that

$$x_1^4 = x_2^4 = 1.$$

In fact, from $x_1^2 = x_2^2$ it follows that $x_1^2 \in C_G(x_2), x_2^2 \in C_G(x_1)$. Moreover, considering the generating subset $\{x_1^{x_3}, x_2, x_3\}$, we get either $(x_1^{x_3})^2 = x_3^2$ and the contradiction $x_1^2 = x_3^2$, or $(x_1^{x_3})^2 = x_1^2 = x_2^2$, thus $x_1^2 \in C_G(x_3)$ and $x_1^2 = x_2^2 \in Z(G)$. If $x_1^2 \neq x_3^{-2}$, then, considering the subset $\{x_1^{-1}, x_2, x_3\}$, we obtain $x_1^{-2} = x_2^2 = x_1^2$ and $x_1^4 = 1 = x_2^4$, as required. If $x_1^2 = x_3^{-2}$, then $x_3^2 \in Z(G)$. Thus the relation

$(x_1x_3)^2 = x_1^2$ implies $x_3^{x_1} = x_3^{-1}$ and $x_3^2 = (x_3^2)^{x_1} = x_3^{-2}$ implies $x_3^4 = 1$ and then $x_1^4 = 1$, while the relation $(x_1x_3)^2 = x_3^2$ implies $x_1^{x_3} = x_1^{-1}$ and $x_1^2 = (x_1^2)^{x_3} = x_1^{-2}$ and again $x_1^4 = 1$, as required.

Now our proof splits into four different cases.

Case I) $(x_1x_3)^2 = x_3^2$ and $(x_2x_3)^2 = x_3^2$. Then

$$x_1^{x_3} = x_1^{-1}, x_2^{x_3} = x_2^{-1}.$$

In this case $(x_1x_2x_3)^2 = x_1x_2x_3x_1x_2x_3 = x_1x_2x_1^{-1}x_2^{-1}x_3^2 = x_1x_2x_1^3x_2^3x_3^2 = x_1x_2x_1^2x_2^2x_1x_2x_3^2 = x_1x_2x_1^4x_1x_2x_3^2 = (x_1x_2)^2x_3^2$.

If $(x_1x_2x_3)^2 = x_3^2$, then $(x_1x_2)^2 = 1 = x_1^2x_2^2$ and $x_1x_2 = x_2x_1$. Furthermore, considering the generating subset $\{x_1, x_3, x_1x_2\}$, we obtain that either $x_1^2 = 1 = x_2^2$ and in this case G is abelian, or $x_3^2 = 1$ and in this case $G = \langle x_1x_2 \rangle \times \langle x_1, x_3 \rangle$ and (β) holds.

If $(x_1x_2x_3)^2 = x_1^2$ we have $x_1^2 = (x_1x_2)^2x_3^2$. Now, if $(x_1x_2)^2 = x_1^2$, then $\langle x_1, x_2 \rangle \simeq Q_8$. Furthermore the relation $(x_1x_2)^2x_3^2 = x_1^2$ implies $x_3^2 = 1$, thus G has the structure in (α) . If $(x_1x_2)^2 = x_3^2$, then $x_1^2 = x_3^4$, moreover, considering the generating subset $\{x_1, x_3^{-1}, x_1x_2\}$ we get $x_3^4 = 1$. Therefore $x_1^2 = 1 = x_2^2$, then $x_1^{x_3} = x_1$, $x_2^{x_3} = x_2$, and $G = \langle x_1x_2, x_1x_3 \rangle \rtimes \langle x_2 \rangle$, with $\langle x_1x_2, x_1x_3 \rangle \simeq Q_8$, $(x_1x_2)^{x_2} = (x_1x_2)^{-1}$, $(x_1x_3)^{x_2} = x_1x_3^3 = (x_1x_3)^{-1}$ and (α) holds.

Case II) Now suppose $(x_1x_3)^2 = x_1^2$ and $(x_2x_3)^2 = x_2^2$. Then

$$x_3^{x_1} = x_3^{-1}, x_3^{x_2} = x_3^{-1}.$$

First suppose $(x_1x_2x_3)^2 = x_3^2$. Then from $x_3^2 = (x_1x_2x_3)^2 = (x_1x_2)^2x_3^2$ we obtain

$$(x_1x_2)^2 = 1.$$

Then $(x_1x_2)^2 = x_1^2x_2^2$ implies $x_1x_2 = x_2x_1$.

Furthermore, considering the generating subset $\{x_1, x_3, x_1x_2\}$, we obtain that either $x_1^2 = 1$ or $x_3^2 = 1$.

If $x_1^2 = 1$, then $x_2^2 = x_1^2 = (x_1x_2)^2 = 1$, and, considering the generation subset $\{x_3^{-1}, x_1, x_1x_2x_3\}$, we get $x_3^{-2} = x_3^3$, thus $x_3^4 = 1$. Therefore

$$G = \langle x_3, x_1 \rangle \times \langle x_1x_2 \rangle$$

and (β) holds.

If $x_3^2 = 1$, then $x_3x_1 = x_1x_3$ and $x_3x_2 = x_2x_3$, therefore

$$G = \langle x_1, x_2 \rangle \times \langle x_3 \rangle$$

and G is abelian.

Now suppose $(x_1x_2x_3)^2 = x_1^2$. Then $x_1^2 = (x_1x_2)^2x_3^2$.

If $(x_1x_2)^2 = x_1^2$, then we obtain $x_3^2 = 1$. Hence

$$G = \langle x_1, x_2 \rangle \times \langle x_3 \rangle.$$

Furthermore $\langle x_1, x_2 \rangle \simeq Q_8$, then (γ) holds.

If $(x_1x_2)^2 = x_3^2$, then from $x_1^2 = (x_1x_2)^2x_3^2$ we obtain $x_1^2 = x_3^4$. Moreover, considering the subset $\{x_3^{-1}, x_1, x_1x_2\}$, we get either $x_3^{-2} = x_3^2$ and $x_3^4 = 1$ or $x_3^{-2} = x_1^2 \in C_G(x_1)$ and again $x_3^4 = 1$ since $x_3^{x_1} = x_3^{-1}$. Thus $x_3^4 = 1$ and $x_1^2 = x_2^2 = 1$, and from $(x_1x_2)^2 = x_3^2$ it follows that $x_2^{x_1} = x_2x_3^2$. Therefore $G = \langle x_3, x_1 \rangle \times \langle x_1x_2x_3 \rangle$, with $(x_1x_2x_3)^2 = 1$ and (β) holds.

Case III) Now suppose $(x_1x_3)^2 = x_1^2, (x_2x_3)^2 = x_3^2$.

Then

$$x_3^{x_1} = x_3^{-1}, x_2^{x_3} = x_2^{-1}.$$

In this case, arguing on the subset $\{x_3^{-1}, x_1, x_2x_3\}$ we get

$$x_3^4 = 1.$$

We have $(x_1x_2x_3)^2 = x_1x_2x_3x_1x_2x_3 = x_1x_2x_1x_2^{-1} = (x_1x_2)^2x_2^2$.

If $(x_1x_2x_3)^2 = x_3^2$, then $(x_1x_2)^2x_2^2 = x_3^2$. Arguing as before, if $(x_1x_2)^2 = x_3^2$, then $x_1^2 = x_2^2 = 1, \langle x_3, x_1x_2 \rangle \simeq Q_8, x_3^{x_1} = x_3^{-1}, (x_1x_2)^{x_1} = x_2x_1 = (x_1x_2)^{-1}$ and (α) holds. And the same happens if $(x_1x_2)^2 = x_1^2 = x_2^2$ since in this case $x_3^2 = 1$ and $G = \langle x_1, x_2 \rangle \rtimes \langle x_2x_3 \rangle$, where $\langle x_1, x_2 \rangle \simeq Q_8, (x_2x_3)^2 = 1, x_1^{x_2x_3} = x_1^{-1}, x_2^{x_2x_3} = x_2^{-1}$.

If $(x_1x_2x_3)^2 = x_1^2$, then $(x_1x_2)^2x_2^2 = x_2^2$ implies $(x_1x_2)^2 = 1$ and $x_1x_2 = x_2x_1$. Arguing as in previous cases, from $(x_1x_2)^2 = 1$ we obtain that either $x_3^2 = 1$ or $x_1^2 = 1$. In the first case $x_3^{x_1} = x_3$ implies that $G = \langle x_1x_3, x_2 \rangle \rtimes \langle x_3 \rangle$, with $(x_1x_3)^2 = x_1^2 = x_2^2, (x_1x_3)^{x_2} = x_1x_3x_2^2 = (x_1x_3)^{-1}, (x_1x_3)^{x_3} = x_1x_3, x_2^{x_3} = x_2^{-1}$, and (α) holds.

Finally, if $x_1^2 = x_2^2 = 1$, then $x_2 \in Z(G)$ and $G = \langle x_2 \rangle \times \langle x_3, x_1 \rangle \simeq C_2 \times D_4$.

Case IV) Finally suppose $(x_1x_3)^2 = x_3^2, (x_2x_3)^2 = x_2^2$. In this case we can argue as in case III) changing the role of x_1 and x_2 .

Conversely, assume that (α) holds, then, for every $g \in G, g = sx_3^\delta$ with $\delta \in \{0, 1\}, s \in \langle x_1, x_2 \rangle$. If $\delta = 0$, then $g^2 \in \{1, x_1^2 = x_2^2\}$. If $\delta = 1$, then $g^2 = sx_3sx_3 = ss^{-1}x_3^2 = 1$ if $sx_3 \neq x_3s$, while $g^2 = s^2x_3^2 = s^2 \in \{1, x_1^2\}$ if $sx_3 = x_3s$. Thus $|\{g^2 \mid g \in G\}| = 2$, and we have the result. If either (β) or (γ) holds, then, for every $g \in G$ we have $g = xc^\delta$ with $\delta \in \{0, 1\}$ and $x \in \langle a, b \rangle \simeq Q_8$ or $\simeq D_4$, then $g^2 = x^2 \in \{1, a^2\}$, and again $|\{g^2 \mid g \in G\}| = 2$. □

Now we can prove the main result of this section.

Theorem 4.6. *Let G be a finitely generated group with $d(G) = n \geq 3$. Suppose that $|S^2| \leq 3|S| - 1$ for any generating subset S of G such that $|S| = n$. Then G is a group of one of the following types:*

- (i) $G = \langle x_1, x_2 \rangle \langle x_3 \rangle, x_3^4 = 1, x_1x_2 = x_2x_1, x_3^{-1}x_1x_3 = x_1^{-1}, x_3^{-1}x_2x_3 = x_2^{-1}$,
- (ii) $G = \langle x_1, x_2 \rangle \langle x_3 \rangle, x_1^4 = x_2^4 = x_3^4 = 1, x_1x_3 = x_3x_1, x_2x_3 = x_3x_2, x_2^{-1}x_1x_2 = x_1^{-1}, x_1^2x_2^2x_3^2 = 1$,
- (iii) $G = \langle x_1, x_2 \rangle \rtimes \langle x_3 \rangle, x_1^4 = x_2^4 = x_3^2 = 1, x_1^2 = x_2^2, x_2^{-1}x_1x_2 = x_1^{-1}, x_3^{-1}x_1x_3 = x_1^{-1}, x_3^{-1}x_2x_3 = x_2^{-1}$,
- (iv) $G \simeq D_4 \times C_2$.
- (v) $G \simeq Q_8 \times C_2$.

- (vi) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle \times \langle x_6 \rangle$, where $x_2^2 = x_3^2 = x_4^2 = x_5^2 = x_6^2 = 1$,
- (vii) $G = \langle x_1 \rangle \times \langle x_2 \rangle \times \langle x_3 \rangle \times \langle x_4 \rangle \times \langle x_5 \rangle$, where $x_4^2 = x_5^2 = 1$,
- (viii) G is abelian and $n \leq 4$.

Conversely, if G satisfies one of (i)-(viii), then $|S^2| \leq 3|S| - 1$ for any generating subset S of G with $|S| = d(G)$.

Proof. First assume G non-abelian then Lemma 3.1 shows that $n \in \{3, 4\}$ and Lemma 3.2 shows that $d(G) = 3$. Then Lemmas 4.1, 4.2, 4.3, 4.4 and Proposition 4.5 imply that G is a group of one of the types (i) – (v).

Assume now that G is abelian. Choose an arbitrary generating subset S of G such that $|S| = n$. Let $S = \{g_1, \dots, g_n\}$. Clearly $S^2 = A \cup B$ where $A = \{g_j g_m \mid 1 \leq j < m \leq n\}$, $B = \{g_j^2 \mid 1 \leq j \leq n\}$. As in a proof of Theorem 2.4 we can show that all elements of the subset A are pairwise different and that A and B are disjoint. It follows that $|S^2| = \frac{1}{2}n(n - 1) + d$ where $d = |B|$. We note that $d \leq n$. Thus $\frac{1}{2}n(n - 1) + 1 \leq 3n - 1$, so that $n \leq 6$.

If $n = 5$, then $\frac{1}{2}n(n - 1) + d = 10 + d$. From $|S^2| \leq 3|S| - 1$ we obtain that $10 + d \leq 14$, thus $d \leq 4$. Therefore we can suppose $g_4^2 = g_5^2$, and G is of type (vii).

If $n = 6$, then $\frac{1}{2}n(n - 1) + d = 15 + d$. From $|S^2| \leq 3|S| - 1$ we obtain that $15 + d \leq 17$, which implies that $d \leq 2$, so that $g_2^2 = g_3^2 = g_4^2 = g_5^2 = g_6^2$, and G is a group of type (viii).

Conversely assume that (i) holds. Write $H = \langle x_1, x_2 \rangle \langle x_3^2 \rangle$. Then H is abelian, moreover $d^{x_3} = d^{-1}$ for every $d \in H$. Therefore for every $g \in G \setminus H$ we have $g = dx_3$, with $d \in H$ and $g^2 = dx_3 dx_3 = dd^{-1} x_3^2 = x_3^2$. Hence if $s, t, v \in G$, either two of them commute or two of them have the same square, thus $|\{s, t, v\}^2| \leq 8$, as required.

If (ii) holds, consider the central subgroup $W = \langle x_1^2, x_2^2, x_3^2 \rangle$. Then $d^2 = 1$ for any $d \in W$ and $G = W \langle x_1, x_2, x_3 \rangle$. We have only to consider three elements s, t, v in $G \setminus W$ which are pairwise non-commuting. But in this case it is not difficult to notice that the set $\{s^2, t^2, v^2\}$ has always order 2, since $x_1^2 x_2^2 x_3^2 = 1$.

A similar argument proves the result if (iii) holds, while Proposition 4.5 shows that the result is true if one of (iii) – (v) holds. Now suppose that one of (vi) – (viii) holds, then G is abelian, and for every subset S of G of order $n = d(G)$ we have $|S^2| = \frac{1}{2}n(n - 1) + d$ where $d = |B|$, $B = \{g^2 \mid g \in S\}$. Now if (vi) holds, then $n = 6$ and $d = 2$, and we have $|S^2| = 15 + 2 = 3|S| - 1$, as required; if (vii) holds, then $n = 5$ and $d = 4$, and we have $|S^2| \leq 10 + 4 = 3|S| - 1$, as required; finally if (viii) holds, then $n \in \{3, 4\}$, $d \leq 4$ and in any case $|S^2| \leq 3|S| - 1$ as required. □

Acknowledgments

This work was supported by the “National Group for Algebraic and Geometric Structures, and their Applications” (GNSAGA - INdAM), Italy.

The first author wish to thank the Department of Mathematics of the University of Salerno for its hospitality and support, while this investigation was carried out.

REFERENCES

- [1] Y. Bilu, Structure of sets with small sumset, Structure theory of set addition, *Astérisque*, **258** (1999) 77–108.
- [2] L. V. Brailovsky and G. A. Freiman, On a product of finite subsets in a torsion-free group, *J. Algebra*, **130** (1990) 462–476.
- [3] E. Breuillard, B. Green and T. Tao, Small doubling in groups, Erdős Centennial, *Bolyai Soc. Math. Studies*, **25** (2013) 129151.
- [4] K. J. Böröczky, P. P. Pálffy and O. Serra, On the cardinality of sumsets in torsion-free groups, *Bull. Lond. Math. Soc.*, **44** (2012) 1034–1041.
- [5] J.-M. Deshouillers, F. Hennecart and A. Plagne, On small sumsets in $(\mathbb{Z}/2\mathbb{Z})^p$, *Combinatorica*, **24** (2004) 53–68.
- [6] G. A. Freiman, On the addition of finite sets. I., *Izv. Vysš. Učebn. Zaved. Matematika*, **6** (1959) 202–213.
- [7] G. A. Freiman, Inverse problems of additive number theory. IV: On the addition of finite sets. II, Elabuž, *Gos. Ped. Inst. Učen. Zap.*, **8** (1960) 72–116.
- [8] G. A. Freiman, Foundations of a structural theory of set addition, Translations of mathematical monographs, **37**, American Mathematical Society, Providence, R. I., 1973.
- [9] G. A. Freiman, Structure Theory of Set Addition, *Astérisque*, **258** (1999) 1–33.
- [10] G. Freiman, M. Herzog, P. Longobardi and M. Maj, Small doubling in ordered groups, *J. Aust. Math. Soc.*, **96** (2014) 316–325.
- [11] G. Freiman, M. Herzog, P. Longobardi, M. Maj and Y. V. Stanchescu, Direct and inverse problems in additive number theory and in non-abelian group theory, *European J. Combin.*, **40** (2014) 42–54.
- [12] G. Freiman, M. Herzog, P. Longobardi, M. Maj and Y. V. Stanchescu, Some inverse problems in group theory, *Note Mat.*, **34** (2014) 89–104.
- [13] G. Freiman, M. Herzog, P. Longobardi, M. Maj and Y. V. Stanchescu, A small doubling structure theorem in a Baumslag-Solitar group, *European J. Combin.*, **44** (2015) 106–124.
- [14] G. Freiman, M. Herzog, P. Longobardi, M. Maj and Y. V. Stanchescu, Small doubling in nilpotent groups of class 2, *European J. Combin.*, **67** (2018) 87–95.
- [15] G. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne, D. J. S. Robinson and Y. V. Stanchescu, On the structure of subsets of an orderable group with some small doubling properties, *J. Algebra*, **445** (2016) 307–326.
- [16] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne and Y. V. Stanchescu, Small doubling in ordered groups: Generators and structure, *Groups Geom. Dyn.*, **11** (2017) 585–612.
- [17] G. A. Freiman and B. M. Schein, *Group and semigroup theoretic considerations inspired by inverse problems of the additive number theory*, Semigroups, theory and applications (Oberwolfach, 1986), 121140, Lecture Notes in Math., Springer, Berlin, 1988.
- [18] B. Green, What is ... an approximate group?, *Notices Amer. Math. Soc.*, **59** (2012) 655–656.
- [19] B. Green and I. Z. Ruzsa, Freiman’s theorem in an arbitrary abelian group, *J. London Math. Soc.*, **75** (2007) 163–175.
- [20] Y. O. Hamidoune, An application of connectivity theory in graphs to factorizations of elements in groups, *European J. Combin.*, **2** (1981) 349–355.
- [21] Y. O. Hamidoune, The isoperimetric method, Combinatorial number theory additive group theory, *Adv. Courses Math. CRM Barcelona*, Birkhauser Verlag, Basel, (2009) 241-252.
- [22] Y. O. Hamidoune and A. Plagne, A generalization of Freiman’s $3k - 3$ Theorem, *Acta Arith.*, **103** (2002) 147–156.

- [23] Y. O. Hamidoune and A. Plagne, A multiple set version of the $3k - 3$ theorem, *Rev. Mat. Iberoam.*, **21** (2005) 133–161.
- [24] M. Herzog, P. Longobardi and M. Maj, *Some results on products of finite subsets in groups*, C. M. Campbell, M. R. Quick, E. F. Robertson and C. M. Roney-Dougal, London Mathematical Society Lecture Note Series, **422** (2015), Groups St. Andrews, Cambridge University Press, 2013 286–305.
- [25] J. H. B. Kemperman, On complexes in a semigroup, *Indag. Math.*, **18** (1956) 247–254.
- [26] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.*, **58** (1953) 459–484.
- [27] V. F. Lev and P. Y. Smeliansky, On addition of two distinct sets of integers, *Acta Arith.*, **70** (1995) 85–91.
- [28] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.
- [29] D. J. S. Robinson, *A course in theory of groups*, 2nd ed., Springer, 1996.
- [30] I. Z. Ruzsa, An analog of Freiman’s theorem in groups, *Astérisque*, **258** (1999) 323–326.
- [31] T. Sanders, The structure theory of set addition revisited, *Bull. Amer. Math. Soc.*, **501** (2013) 93–127.
- [32] Y. V. Stanchescu, On addition of two distinct sets of integers, *Acta Arith.*, **75** (1996) 191–194.
- [33] Y. V. Stanchescu, On the structure of sets with small doubling property on the plane. I, *Acta Arith.*, **83** (1998) 127–141.
- [34] Y. V. Stanchescu, The structure of d -dimensional sets with small sumset, *J. Number Theory*, **130** (2010) 289–303.
- [35] T. Tao and Van H. Vu, Additive combinatorics, *Cambridge studies in advanced mathematics*, Cambridge University Press, Cambridge, **105** 2006.
- [36] T. Tao, Product set estimates for non-commutative groups, *Combinatorica*, **28** (2008) 547–594.

Leonid A. Kurdachenko

Department of Algebra and Geometry, School of Mathematics and Mechanics, University of Dnipro, Gagarin prospect 72, Dnipro 10, 49010 Ukraine

Email: lkurdachenko@i.ua

Patrizia Longobardi

Dipartimento di Matematica, Università di Salerno, via Giovanni Paolo II, 132, 84084 Fisciano (Salerno), Italy

Email: plongobardi@unisa.it

Mercede Maj

Dipartimento di Matematica, Università di Salerno, via Giovanni Paolo II, 132, 84084 Fisciano (Salerno), Italy

Email: mmaj@unisa.it