Note di Matematica ISSN 1123-2536, e-ISSN 1590-0932
Note Mat. **34** (2014) no. 1, 89–104. doi:10.1285/i15900932v34n1p89

Some inverse problems in group theory

G. A. Freiman
School of Mathematical Sciences, Tel Aviv University,
Tel Aviv 69978, Israel
grisha@post.tau.ac.il

M. Herzog
School of Mathematical Sciences, Tel Aviv University,
Tel Aviv 69978, Israel
herzogm@post.tau.ac.il

P. Longobardi
Dipartimento di Matematica, Universita' di Salerno, Via Giovanni Paolo II, 132
84084 Fisciano (Salerno), Italy
plongobardi@unisa.it

M. Maj
Dipartimento di Matematica, Universita' di Salerno, Via Giovanni Paolo II, 132,
84084 Fisciano (Salerno), Italy
mmaj@unisa.it

Y. V. Stanchescu
Afeka Academic College, Tel Aviv 69107, Israel
and The Open University of Israel, Raanana 43107, Israel
yonis@afeka.ac.il and ionut@openu.ac.il

Abstract. We investigate some inverse problems of small doubling type in nilpotent groups.

Keywords: Inverse problems; small doubling; nilpotent groups; ordered groups.

MSC 2010 classification: Primary 11P70; Secondary 20F05, 20F99, 11B13, 05E15.

1 Introduction

Let G denote an arbitrary group. If S is a subset of G, we define its square S^2 by

$$S^2 = \{x_1 x_2 \mid x_1, x_2 \in S\}.$$

If G is an additive group, we denote by

$$2S = \{x_1 + x_2 \mid x_1, x_2 \in S\}$$

the sumset of S.

We are concerned with the following general problem: let S be a finite subset with k elements of a group G, determine the **structure** of S if

$$|S^2| \leq f(k)$$

for some function f.

Problems of this kind are called **inverse problems**.

In particular, we shall consider problems of the following type: determine the **structure** of S, if $|S^2|$ satisfies the following inequality:

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

for some small $\alpha \geq 1$ and small $|\beta|$.

Such problems are called **inverse problems** of **small doubling** type.

Inverse problems of small doubling type have been first investigated by G. A. Freiman in the additive group of the integers.

It is easy to prove that if S is a finite subset of $\mathbb{Z}$ with k elements, then

$$|2k - 1| \leq |2S| \leq k(k + 1)/2.$$

Moreover $|2S| = 2k - 1$ if and only if S is an arithmetic progression of size k.

In the paper [4] G.A. Freiman proved the following theorem:

Theorem 1.1. *Let S be a finite set of integers with $k \geq 3$ elements and suppose that*

$$|2S| \leq 2k - 1 + b,$$

where $0 \leq b \leq k - 3$. Then S is contained in an arithmetic progression of size $k + b$ and difference q,

$$P = \{a, a + q, a + 2q, \cdots, a + (k + b - 1)q\},$$

where a, q are integers with $q > 0$.

In particular, if

$$|2S| \leq 3k - 4,$$

then S is contained in an arithmetic progression of size $2k - 3$,

$$P = \{a, a + q, a + 2q, \cdots, a + (2k - 4)q\}.$$

This theorem was the beginning of the *"Freiman's structural theory of set addition"*, the foundations for which were led in Freiman's book "Foundations of a structural theory of set addition" (see [6] and also [20]).

In [4] and in [5] Freiman studied also the case $|2S| \leq 3|S| - 3$ and $|2S| \leq 3|S| - 2$. If X is a subset of an abelian semigroup G and Y is a subset of an abelian semigroup G_1, a bijection $\varphi : X \longrightarrow Y$ is called a Freiman isomorphism if for any $a, b, c, d \in X$, $a + b = c + d$ if and only if $\varphi(a) + \varphi(b) = \varphi(c) + \varphi(d)$. X is Freiman isomorphic to Y if there exists a Freiman isomorphism between X and Y.

Freiman proved the following result:

Theorem 1.2. *Let S be a finite set of integers with $k \geq 2$ elements and suppose that*

$$|2S| = 3k - 3.$$

Then one of the following holds:
(i) S is a subset of an arithmetic progression of size at most $2k - 1$;
(ii) S is a bi-arithmetic progression;
(iii) $|S| = 6$ and S is Freiman isomorphic to the set K_6, where

$$K_6 = \{(0,0), (1,0), (2,0), (0,1), (0,2), (1,1)\}.$$

Here, a set of the integers $S = I \cup J$ is called a **bi-arithmetic progression** of length k, with difference d, if both I and J are arithmetic progressions of difference d, $|I| + |J| = k$, and $I + I, I + J, J + J$ are pairwise disjoint.

In [6] Freiman investigated also the exact structure of subsets of the additive group $\mathbb{Z}^d$, for a positive integer d. A complete description of a subset S of the additive group $\mathbb{Z}^2$ with $|S| \geq 4$ and $|2S| < 4|S| - 6$ is due to Y.V. Stanchescu in [24]. A best possible result for the group $\mathbb{Z}^d$ and doubling coefficient $d + \frac{4}{3}$ has been recently obtained in [26].

By now, Freiman's theory had been extended tremendously, in many different direction, see for example [1], [3], [7], [9], [11], [14], [15], [16], [17], [18], [23], [24], [25], [26], the recent survey by T. Sanders [22] and the references contained therein.

In the paper [8], we studied small doubling problems for subsets of an ordered group. We recall that if G is a group and $\leq$ is a total order relation defined on the set G, we say that $(G, \leq)$ is **an ordered group** if for all $a, b, x, y \in G$, the inequality $a \leq b$ implies that $xay \leq xby$, and a group G is **orderable** if there exists an order $\leq$ on G such that $(G, \leq)$ is an ordered group. Obviously the group of integers with the usual ordering is an ordered group. More generally, it is possible to prove that an abelian group is orderable if and only if it is torsion-free (see, for example [2] or [13]).

Extending Freiman's results, we proved in [8] the following theorems.

Theorem 1.3. *Let $(G, \leq)$ be an ordered group and let $S = \{x_1, x_2, \cdots, x_k\}$ be a finite subset of G of size $k \geq 3$, with $x_1 < x_2 \cdots < x_k$. Assume that*

$$t = |S^2| \leq 3k - 4.$$

Then $\langle S \rangle$ is abelian.
Moreover, there exists $g \in G$, $g > 1$, such that $gx_1 = x_1 g$ and S is a subset of

$$\{x_1, x_1 g, x_1 g^2, \cdots, x_1 g^{t-k}\}.$$

Theorem 1.4. *Let $(G, \leq)$ be an ordered group and let $S = \{x_1, x_2, \cdots, x_k\}$ be a finite subset of G of size $k \geq 3$, with $x_1 < x_2 \cdots < x_k$. Assume that*

$$t = |S^2| \leq 3k - 3.$$

Then $\langle S \rangle$ is abelian.

Using results of Freiman and Stanchescu, the following theorem can be deduced from Theorem 1 of [10].

Theorem 1.5. *Let $(G, \leq)$ be an ordered group and let $S = \{x_1, x_2, \cdots, x_k\}$ be a finite subset of G of size $k \geq 3$, with $x_1 < x_2 \cdots < x_k$. Assume that*

$$t = |S^2| \leq 3k - 3.$$

Then $\langle S \rangle$ is abelian and one of the following holds:

(i) S *is a subset of a geometric progression* $\{a, ac, \cdots, ac^{2k-1}\}$;

(ii) S *is a bi-geometric progression, i.e.* $S = \{a, ac, \cdots ac^{i-1}\} \cup \{b, bc, \cdots, bc^{j-1}\}$;

(iii) $k = 6$ *and* $S = \{1, c, c^2, b, b^2, bc\}$.

The aim of this paper is to investigate inverse small doubling problems in torsion-free nilpotent groups.

By a result of A.I. Mal'cev and B.H. Neumann, any torsion-free nilpotent group is orderable (see [19] or [21]). Thus the previous results apply to these groups.

The remainder of the paper is organized as follows.

First, in Section 2, we report some useful results from [12] and [8].

In Section 3, we investigate the structure of subsets S of order k of a torsion-free nilpotent group, with $|S^2| \leq 3k-2$. We study here the case $k=3$, and we report from [12] results concerning the case $k \geq 4$. Notice that, by a result in [10], if S is a subset of a nilpotent torsion-free group, of order bigger that 3, with $|S^2| \leq 3|S|-2$, then $\langle S\rangle$ is nilpotent of class at most 2. Thus the problem reduces to the case when G is nilpotent of class at most 2.

In Section 4 we report results from [12], concerning the structure of subsets S of size k of torsion-free nilpotent groups of class at most 2, which satisfy $k>4$ and $|S^2| = 3k-1$. In [12] the case $k=4$ was left open. Here we complete the result of [12] by proving the following theorem.

Theorem 1.6. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G of size $k=4$ with $\langle S\rangle$ non-abelian. Then $|S^2| = 3k-1 = 11$ if and only if one of the following statements holds:*

(i) There exist $s, t \in S \cap Z(\langle S\rangle), s \neq t$;

(ii) $S = \{a, ac, b, bc, \}$, with $ab = bac^2$;

(iii) $S = \{a, ac^2, b, bc\}$, with $ab = bac$;

(iv) $S = \{a, ac, ac^2, b\}$, with $ab = bac^2$;

(v) $S = \{a, ac, b, x\}$, with $ab = bac$, $ax = xa$, $bx = xb$;

(vi) $S = \{a, ac, ac^2, x\}$, with $ac = ca$ and there exists exactly one $i \in \{0, 1, 2\}$ such that $ac^i x = xac^i$;

(vii) $S = \{a, ac, b, x\}$, with $c > 1$ and either $bx = a^2$, $ab = bac$, $xb = bxc^2$ and $xa = axc$, or $xb = a^2$, $ba = abc$, $ax = xac$ and $bx = xbc^2$.

2 Some general results.

We start by quoting two useful results.

Proposition 2.1. *Let $(G, \leq)$ be an ordered nilpotent group of class 2 and let S be a subset of G satisfying:*

$$S = \{x_1, \cdots, x_k\}, \quad x_1 < x_2 < \cdots < x_k.$$

Write $T = \{x_1, \cdots, x_{k-1}\}$. If

$$x_k x_{k-1} \neq x_{k-1} x_k,$$

then

$$|T^2| \leq |S^2| - 4.$$

Proof. See [12], Lemma 2.1.

QED

Proposition 2.2. *Let $(G, \leq)$ be an ordered group and let T be a finite subset of G of size m. If $b \in G \setminus C_G(T)$, then*

$$|bT \cup Tb| \geq m + 1\ .$$

Proof. See [8], Proposition 2.3.

QED

If G is a torsion-free nilpotent group of class 2, then the following result, concerning the structure of T, holds.

Proposition 2.3. *Let G be a torsion-free nilpotent group of class 2 and let T be a subset of G of size m. Moreover, let $b \in G$ satisfy the following conditions: $bt \neq tb$ for all $t \in T$ and $|bT \cup Tb| = m + 1$. Then $T = \{a, ac, \cdots, ac^{m-1}\}$, with $ba = abc$ (in particular $c \in Z(G)$ and $\langle T \rangle$ is abelian).*

Proof. See [12], Proposition 2.5.

QED

3 Subsets S with $|S^2| \leq 3|S| - 2$.

Let G be a nilpotent torsion-free group. Then, by results of A.I. Mal'cev and B.H. Neumann (see [19] and [21]) , G is orderable.

Let S be a finite subset of G with k elements, and suppose that $|S^2| \leq 3k-2$. If $k = 2$, then $|S^2| = 4 = 3k - 2$ if and only if $\langle S\rangle$ is non-abelian. Hence we may assume that $k \geq 3$.

In this paper we deal with the case $k = 3$. In this case the following proposition holds.

Proposition 3.1. *Let $(G, \leq)$ be a nilpotent ordered group, and let $S \subseteq G$ with $|S| = 3$. Then $|S^2| \leq 7$ if and only if one of the following holds:*

(i) $S \cap Z(\langle S\rangle) \neq \emptyset$;

(ii) $S = \{a, ac, b\}$, with $c > 1, ac = ca$ and either $ab = bac$ or $ba = cab$.

Proof. Write $S = \{x_1, x_2, x_3\}$ with $x_1 < x_2 < x_3$ and suppose that $|S^2| \leq 7$. Moreover, let $T = \{x_1, x_2\}$. It suffices to prove that if $S \cap Z(\langle S\rangle) = \emptyset$, then (ii) holds.

So suppose that $S \cap Z(\langle S\rangle) = \emptyset$. If $|S^2| \leq 6$, then $\langle S\rangle$ is abelian by Theorem 1.4, a contradiction. Hence $|S^2| = 7$. Moreover, we must have either $x_1x_2 \neq x_2x_1$ or $x_2x_3 \neq x_3x_2$.

Suppose, first, that $x_2x_3 \neq x_3x_2$. We must consider the cases: $x_1x_2 \neq x_2x_1$ and $x_1x_2 = x_2x_1$.

If

$$x_1x_2 \neq x_2x_1$$

then $|T^2| = 4$ and it follows from the ordering in S that $x_2x_3, x_3x_2, x_3^2 \notin T$. Since $x_2x_3 \neq x_3x_2$, the elements x_2x_3, x_3x_2, x_3^2 are also distinct from each other and it follows that

$$S^2 = T^2 \dot{\cup} \{x_2x_3, x_3x_2, x_3^2\}.$$

Consider x_1x_3, x_3x_1, and assume, without loss of generality, that $x_1x_3 \leq x_3x_1$. Then $x_1x_3 < x_3x_2, x_2x_3, x_3^2$, implying that $x_1x_3 \in T^2$. Hence either $x_1x_3 = x_2^2$ or $x_1x_3 = x_2x_1$.

If $x_1x_3 = x_3x_1$ and $x_1x_3 = x_2^2$, then $(x_2^2)^{x_1} = x_3x_1 = x_1x_3 = x_2^2$ and $(x_2)^{x_1} = x_2$, a contradiction.

If, on the other hand, $x_1x_3 = x_3x_1$ and $x_1x_3 = x_2x_1$, then $(x_3)^{x_1} = x_3 = {x_2}^{x_1}$, again a contradiction. Hence $x_1x_3 < x_3x_1$.

Moreover, either $x_3x_1 \in T^2$ or $x_3x_1 = x_2x_3$ and $x_1x_3 \in T^2$.

If $x_3x_1 \in T^2$, then the only possibility is that $x_3x_1 = x_2^2$ and $x_1x_3 = x_2x_1$. In this case

$$\langle x_1, x_2, x_3\rangle = \langle x_3, x_3^{x_1}\rangle = \langle x_3\rangle\langle x_1, x_2, x_3\rangle' = \langle x_3\rangle Frat(\langle x_1, x_2, x_3\rangle)$$

since in a nilpotent group the derived subgroup is contained in the Frattini subgroup. Therefore $\langle x_1, x_2, x_3\rangle = \langle x_3\rangle$ is abelian, a contradiction.

Now suppose that $x_3x_1 = x_2x_3$ and $x_1x_3 \in T^2$. In this case, we must have either $x_1x_3 = x_2^2$ or $x_1x_3 = x_2x_1$. If $x_1x_3 = x_2^2$, we get as before the contradiction $\langle x_1, x_2, x_3\rangle = \langle x_2, x_2^{x_3}\rangle = \langle x_2\rangle$, while if $x_1x_3 = x_2x_1$, then $\langle x_1, x_2, x_3\rangle = \langle x_2, x_2^{x_3}, x_2^{x_1}\rangle = \langle x_2\rangle$, again a contradiction.

So we may assume

$$x_1x_2 = x_2x_1.$$

In this case $x_2x_3, x_3x_2, x_1x_3, x_3x_1, x_3^2 \notin \langle x_1, x_2\rangle$, since otherwise we get the contradiction $x_3x_2 = x_2x_3$. Therefore the elements $x_1^2, x_1x_2, x_2^2, x_1x_3, x_2x_3, x_3^2$ are all different. Since $|S^2| = 7$ and $x_2x_3 \neq x_3x_2$, we must have either $x_2x_3 = x_3x_1$ or $x_3x_2 = x_1x_3$. Thus, if we denote $x_1 = a, x_2 = ac, x_3 = b$, then (ii) holds, as required.

Similarly, if instead of $x_2x_3 \neq x_3x_2$ we assume that $x_1x_2 \neq x_2x_1$, then we may also assume that $x_2x_3 = x_3x_2$ and we get the result by considering the order opposite to $\leq$.

Conversely, if $S = \{a, b, c\}$, with $ab = ba$ and $ac = ca$, then

$$S^2 = \{a^2, b^2, c^2, ab, ac, bc, cb\}$$

has order at most 7. If $S = \{a, ac, b\}$, with $ac = ca$ and, for example, $ab = bac$, then

$$S^2 = \{a^2, a^2c, a^2c^2, ab, acb, ba, b^2\}$$

and again $|S^2| \leq 7$.

QED

Now let S be a finite subset with k elements of a nilpotent ordered group, with $k \geq 4$ and assume that $|S^2| \leq 3k - 2$. Then, by Theorem 2 of [10], $\langle S\rangle$ is nilpotent of class 2 at most.

If $\langle S\rangle$ is abelian, then by [10], either $|S| = 4$ and in this case the size of S^2 is always at most 10, or S is Freiman isomorphic to a subset of $\mathbb{Z}$ and the structure of S can be described using Freiman's results in [4] , or S is Freiman isomorphic to a subset of $\mathbb{Z}^2$. In the latter case, the structure of S can be described using results of Freiman and of Stanchescu (see [4] and [24]).

If $\langle S\rangle$ is nilpotent of class exactly 2, then the structure of S follows from the following theorem.

Theorem 3.2. *Let G be a torsion-free nilpotent group of class 2 and let $S \subseteq G$ be non-abelian and of order $k \geq 4$. Then $|S^2| = 3k - 2$ if and only if*

$$S = \{a, ac, \cdots, ac^i, b, bc, bc^2, \cdots, bc^j\},$$

with $1 + i + 1 + j = k$ and $ab = bac$.

Proof. Suppose that $S = \{a, ac, \cdots, ac^i, b, bc, bc^2, \cdots, bc^j\}$, with $1+i+1+j = k$ and $ab = bac$. Write $A = \{a, ac, \cdots, ac^i\}$, $B = \{b, bc, \cdots, bc^j\}$. Then we have: $S = A\dot{\cup}B$, $S^2 = A^2\dot{\cup}B^2\dot{\cup}(AB \cup BA)$, $AB \cup BA = \{ba, bac, \cdots, bac^{i+j+1}\}$, $|A^2| = 2(i + 1) - 1$, $|B^2| = 2(j + 1) - 1$, $|AB \cup BA| = i + j + 2$ and $|S^2| = 2i + 2j + 2 + i + j + 2 = 3k - 2$, as required.

For the converse see the proof of Theorem 2 in [12].

QED

4 Subsets S with $|S^2| \leq 3|S| - 1$.

Let S be a subset of a torsion-free nilpotent group G with $|S| = k$ and $|S^2| \leq 3k - 1$. Let $\leq$ be an order in G such that $(G, \leq)$ is an ordered group. By Theorem 3 of [10], if $k \geq 8$, then $\langle S\rangle$ is nilpotent of class at most 2. Therefore, we first studied the case when G is nilpotent of class 2.

Suppose that S is a subset of a torsion-free nilpotent group G of class 2, with $|S| = k$ and $|S^2| \leq 3k - 1$. In [12] we proved the following result.

Theorem 4.1. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G of size $k \geq 5$, with $\langle S\rangle$ non-abelian. Then $|S^2| = 3k - 1$ if and only if one of the following holds:*

(i)

$$S = \{a, ac, \cdots, ac^{i-1}, b, bc, \cdots, bc^{j-1}\},$$

with $ab = bac^2$ and $i + j = k$;

(ii)

$$S = \{a, ac^2, b, bc, \cdots, bc^j\}, j \geq 2.$$

with $ab = bac$.

If $|S| = 3$, it is easy to show that $|S^2| \leq 8$ if and only if $S = \{x, y, z\}$, with either $xy = yx$ or $xy = z^2$.

In this section we prove Theorem 1.6, concerning the structure of a subset S satisfying $|S| = 4$ and $|S^2| \leq 11$. Thus the description of the structure of S, if S is a subset of size $k \geq 2$ of a torsion-free nilpotent group of class 2 with $|S^2| \leq 3k-1$, is complete.

It is still an open problem to describe S, if S is a subset of any torsion-free nilpotent group with $|S| \leq 7$ and $|S^2| = 3k-1$.

In order to prove Theorem 1.6, we start with the following Lemmas.

Lemma 4.2. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G of size 4, with $\langle S\rangle$ non-abelian and $|S^2| = 11$. Suppose that $S = T \cup \{b\}$, with $\langle T\rangle$ abelian. Then one of the following holds:*

(i) There exist $s, t \in S \cap Z(\langle S\rangle), s \neq t$;

(ii) $S = \{a, ac, ac^2, b\}$, with $ab = bac^2$;

(iii) $S = \{a, ac, b, x\}$, with $ab = bac$, $ax = xa$, $bx = xb$;

(iv) $S = \{a, ac, ac^2, x\}$,

with $ac = ca$ and there exists exactly one $i \in \{0, 1, 2\}$ such that $ac^i x = xac^i$.

Proof. Obviously $b^2 \notin T^2$ and $(bT \cup Tb) \cap T^2 = \emptyset$, since $b \notin C_G(T)$. Therefore $|S^2| = |T^2| + |bT \cup Tb| + 1$. Moreover, since $|T| = 3$ and $b \notin C_G(T)$, it follows by Proposition 2.2 that $|bT \cup Tb| \geq 4$.

If $|bT \cup Tb| \geq 5$, then $|T^2| \leq 5 = 3 \cdot 3 - 4$. Thus, by Theorem 1.3, $T = \{a, ac, ac^2\}$ with $ac = ca$. Hence, in this case, we have $|T^2| = 5$, $|bT \cup Tb| = 5$ and $|bT \cap Tb| = 1$.

If $ac^i b = bac^i$ for some $i \in \{0, 1, 2\}$, then this is true for exactly one i since $|bT \cap Tb| = 1$ and (iv) holds.

If $ac^i b = bac^j$, with $i \neq j$, then $[ac^i, b] = c^{j-i}$. Thus $c^{j-i} \in Z(G)$ and $c \in Z(G)$. In this case $[a, b] = c^v$, for some integer v and $ab = bac^v$. Therefore, as $bT \cup Tb = \{ba, bac, bac^2, bac^v, bac^{v+1}, bac^{v+2}\}$ is of size 5, we get $v = 2$ and S has the structure in (ii).

Now suppose $|bT \cup Tb| = 4$. Then $|T^2| = 6$ and $|bT \cap Tb| = 2$. Moreover, $T \cap C_G(b) \neq \emptyset$, since otherwise $T = \{a, ac, ac^2\}$ by Proposition 2.3 and $|T^2| = 5$, which is not the case. Therefore $0 < |T \cap C_G(b)| \leq 2$. If there exist $s, t \in T \cap C_G(b)$, $s \neq t$, then $s, t \in Z(\langle S\rangle)$, and (i) holds. So assume that there exists exactly one $s \in T$ such that $sb = bs$. Then there exist $x_i, x_j \in T$, $x_i \neq x_j$ such that $bx_i = x_j b$, since $|bT \cap Tb| = 2$. Thus $x_i = b^{-1}x_j b = x_j c$, where $c \in Z(G)$. Obviously $x_i, x_j \neq s$, so denoting $a = x_j$ and $x = s$, we get $T = \{a, ac, x\}$, where $xb = bx$, $ab = bac$, $ax = xa$ and (iii) holds. QED

Lemma 4.3. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G of size 4, with $\langle S\rangle$ non-abelian and $|S^2| = 11$. Suppose that there exists $z \in S \cap Z(\langle S\rangle)$. Then G satisfies the hypothesis of Lemma 4.2.*

Proof. Write $S = T\dot{\cup}\{z\}$. Then $S^2 = T^2 \cup \{z^2\} \cup zT$. Obviously $z^2 \notin zT$. Suppose that $z^2 \in T^2$, implying that $z^2 = x_i x_j$, where $x_i, x_j \in T$. If $x_i = x_j$, then $z = x_i$ since G is torsion-free and $z \in T$, a contradiction. Hence $x_i \neq x_j$, $x_j x_i = x_i x_j$, $\{x_i, x_j, z\}$ is abelian and we have the result.

So we may assume that $\{z^2\} \cap T^2 = \emptyset$.

If $zT \cap T^2 = \emptyset$, then $|T^2| = 11 - 1 - 3 \leq 7$ and by Proposition 3.1 there exist different elements $x_i, x_j \in T$ such that $x_i x_j = x_j x_i$. Thus $\{x_i, x_j, z\}$ is abelian and we have the result.

So we may also assume that $zT \cap T^2 \neq \emptyset$, which implies that

$$zx_i = x_h x_k$$

for some $x_i, x_h, x_k \in T$. If $x_h = x_k$, then $\{x_i, x_h, z\}$ is abelian and we have the result.

So we may assume that

$$T = \{x_i, x_h, x_k\}.$$

We claim that we may suppose that $zx_h \notin T^2$.

Indeed, if that is not the case, then one of the following holds: $zx_h = x_i^2$, or $zx_h = x_k^2$, or $zx_h = x_i x_k$ or $zx_h = x_k x_i$.

In the first case, $\{x_i, x_h, z\}$ is abelian and the result holds. Similarly in the second case $\{z, x_h, x_k\}$ is abelian. If $zx_h = x_i x_k$, then $zx_i = x_h x_k$ implies that $z^2 x_h = zx_i x_k = x_h x_k^2$. Thus $x_k^2 = z^2$ and $z = x_k \in T$, a contradiction. Finally, if $zx_h = x_k x_i$, then we have $zx_h x_k = x_k x_i x_k$. Thus $z^2 x_i = x_k^2 x_i z_1$, for a suitable $z_1 \in Z(G)$, since G has class 2. Therefore $x_k^2 \in Z(G)$ and hence $x_k \in Z(G)$, which implies the result. The proof of our claim is complete.

Arguing similarly, we may suppose that also $zx_k \notin T^2$. Thus $|zT \cap T^2| = 1$ and $|T^2| = 8$. Then, as remarked above, one of the following two cases must hold: either there exist two commuting elements $s, t \in T$ or there exist $x_l, x_m, x_n \in T$ such that $x_l^2 = x_m x_n$. In the first case, $\{s, t, z\}$ is abelian, as required.

Now assume that $x_l^2 = x_m x_n$. If $x_l = x_i$, then $\{x_m, x_n\} = \{x_h, x_k\}$. Thus mod $Z(\langle S\rangle)$ we have $x_i^2 = x_h x_k = x_i z$, hence $x_i \in Z(\langle S\rangle)$, and we have the result. If $x_l \neq x_i$, then $x_l \in \{x_h, x_k\}$ and either x_m or x_n is equal to x_i. Suppose, without loss of generality, that $x_m = x_i$ and $x_l = x_h$. Then $x_n = x_k$ and mod $Z(\langle S\rangle)$ we have $x_i^2 = x_h^2 x_k^2 = x_l^2 x_k^2 = x_i x_k^3$. Thus $[x_i, x_k] = 1$ and $\{x_i, x_k, z\}$ is abelian, as required. QED

Lemma 4.4. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G with $\langle S\rangle$ non-abelian of size* 4 *and $|S^2| = 11$. Suppose that $S = T\dot\cup\{s\}$ and there exists $c \in T \cap Z(\langle T\rangle)$. Then G satisfies the hypothesis of Lemma 4.2.*

Proof. If $[s, c] = 1$, then $c \in Z(\langle S\rangle)\cap S$ and we are done by Lemma 4.3. So assume that $[s, c] \neq 1$. Then $\{s, s^2\}\cap\langle T\rangle = \emptyset$ and $[s, c] \neq 1$, implying that $\{s^2\}\cap T^2 = \emptyset$ and $(\{s^2\} \cup T^2) \cap (sT \cup Ts) = \emptyset$. Moreover, $|sT \cup Ts| \geq 4$ by Proposition 2.2. Then it follows from $S^2 = T^2\dot\cup(sT \cup Ts)\dot\cup\{s^2\}$ that $|T^2| \leq 6 = 3 \cdot 3 - 3$. Hence T is abelian by Theorem 1.4, as required. QED

Lemma 4.5. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G of size 4, with $\langle S\rangle$ non-abelian and $|S^2| = 11$. Suppose that $S = \{a, ac\} \cup \{b, bd\}$, where $ab \neq ba$ and $c, d \in Z(\langle S\rangle)$. Then one of the following holds:*

(i) $S = \{a, ac, b, bc\}$, *with* $ab = bac^2$;

(ii) $S = \{a, ac, b, bc^2\}$, *with* $ab = bac$, *or* $S = \{a, ad^2, b, bd\}$, *with* $ab = bad$.

Proof. Assume, without loss of generality, that $c > 1$ (otherwise change a with $a_1 = ac$ and $a = a_1c^{-1}$) and, similarly, that $d > 1$. Also suppose, without loss of generality, that $ba < ab$.

We have

$$S^2 \supseteq \{a, ac\}^2\dot\cup\{b, bd\}^2\dot\cup\{ba, ab, abc, abd, abcd\}.$$

Clearly $|\{a, ac\}^2\dot\cup\{b, bd\}^2| = 6$ and since $ab \neq ba$, we also have

$$bac, bac^2 \notin \{a, ac\}^2\dot\cup\{b, bd\}^2.$$

First, suppose that $c = d$. Then $ba < ab < abc < abc^2$ and if $bac \in \{ba, ab, abc, abc^2\}$, then $bac = ab$. In this case $S = \{a, ac, b, bc\}$ and by Theorem 3.2 S^2 is of size 10, a contradiction. Hence $bac \notin \{ba, ab, abc, abc^2\}$ and

$$S^2 = \{a, ac\}^2\dot\cup\{b, bc\}^2\dot\cup\{ba, ab, abc, abc^2, bac\}.$$

Then $bac^2 \in \{ba, ab, abc, abc^2, bac\}$ and the only possibility is $bac^2 = ab$. Hence (i) holds.

Now suppose that $c \neq d$ and for example, let $c < d$. We have $ba < ab < abc < abd < abcd$, so

$$S^2 = \{a, ac\}^2\dot\cup\{b, bc\}^2\dot\cup\{ba, ab, abc, abd, abcd\}.$$

Hence the elements bac, bad are in $\{ba, ab, abc, abd, abcd\}$, and from $bac < bad$ we deduce that the only possibility is that $bac = ab$ and $bad = abc$. Thus $bad = bac^2$ and $d = c^2$, yielding (ii). Similarly, if $c > d$, then $c = d^2$, $ab = bad$ and (ii) holds. QED

Lemma 4.6. *Let G be an ordered nilpotent group of class 2 and let S be a subset of G of size 4, with $\langle S\rangle$ non-abelian and $|S^2| = 11$. Write $S = \{x_1, x_2, x_3, x_4\}$, where $x_1 < x_2 < x_3 < x_4$, and suppose that $x_1x_2 = x_2x_1$ and $x_3x_4 = x_4x_3$. Then S satisfies the hypothesis of one of the previous Lemmas.*

Proof. Write $A = \{x_1, x_2\}$, $B = \{x_3, x_4\}$, $Y = x_2\{x_3, x_4\} \cup \{x_3, x_4\}x_2$, $Z = Z(\langle S\rangle)$. The order in S obviously implies that $A^2 \cap B^2 = \emptyset = A^2 \cap Y$. We may also assume $B^2 \cap Y = \emptyset$, since otherwise the conditions of Lemma 4.4 are satisfied, as required. Indeed, if $B^2 \cap Y \neq \emptyset$, then one of the following equalities must hold: $x_2x_4 = x_4x_3$, $x_2x_4 = x_3^2$, $x_4x_2 = x_3^2$ and $x_4x_2 = x_3x_4$. In each of these cases $[x_3, x_2] = 1$ and if $T = \{x_2, x_3, x_4\}$, then $x_3 \in T \cap Z(\langle T\rangle$, as required in Lemma 4.4.

If $x_1Z = x_2Z$ and $x_3Z = x_4Z$, then the conditions of Lemma 4.5 are satisfied, as required. So we may assume, without loss of generality, that

$$x_3Z \neq x_4Z.$$

We claim that we may assume that $x_2\{x_3, x_4\} \cap \{x_3, x_4\}x_2 = \emptyset$. In fact, if $x_2x_3 = x_3x_2$ or $x_2x_4 = x_4x_2$, then we are in the conditions of Lemma 4.4, and if $x_2x_4 = x_3x_2$ then $x_4 = x_2^{-1}x_3x_2 = x_3z$ with $z \in Z$ and we get the contradiction $x_3Z = x_4Z$. Similarly if $x_2x_3 = x_4x_2$. The proof of our claim is complete. It follows that $|Y| = 4$.

Now consider the elements x_1x_4 and x_4x_1. We may suppose that they are different, since otherwise $x_1 \in Z(\langle x_1, x_2, x_4\rangle)$ and the conditions of Lemma 4.4 are satisfied.

Assume, without loss of generality, that $x_1x_4 < x_4x_1$.

We claim that $x_1x_4 \notin Y$. Indeed, if $x_1x_4 = x_2x_3$, then $x_2^{-1}x_1 = x_3x_4^{-1} \in Z$, yielding $x_1Z = x_2Z$ and $x_3Z = x_4Z$, which is not the case. A similar contradiction is reached if $x_1x_4 = x_3x_2$. Since $x_1x_4 < x_4x_1$, we also have $x_1x_4 < x_4x_2$. Thus $x_1x_4 \notin Y$, as claimed.

We may also assume that $x_1x_4 \notin A^2 \cup B^2$, since if for example $x_1x_4 = x_3^2$, then $[x_3, x_1] = 1$ and the conditions of Lemma 4.4 are satisfied.

Taking into account that $|Y| = 4$ and $|A^2| = |B^2| = 3$, we may conclude that

$$S^2 = A^2 \dot\cup B^2 \dot\cup Y \dot\cup \{x_1x_4\}.$$

Now consider the elements x_1x_3 and x_3x_1. As before we may suppose that $x_1x_3 \neq x_3x_1$ and $x_1x_3, x_3x_1 \notin A^2 \cup B^2$. Thus $x_1x_3, x_3x_1 \in Y$. Arguing as before, $x_1x_3 = x_2x_4$ implies that $x_2^{-1}x_1 = x_4x_3^{-1} \in Z$ and $x_3Z = x_4Z$, which is not the case, and a similar contradiction is reached if $x_1x_3 = x_4x_2$, since $x_4x_2Z = x_2x_4Z$. The only possibility which remains is $x_1x_3 = x_3x_2$.

But now consider x_3x_1. Obviously $x_3x_1 < x_3x_2 = x_1x_3$, so $x_3x_1 \neq x_1x_4$, x_2x_3, x_2x_4. Hence $x_3x_1 \notin S^2$, a final contradiction. QED

Now we can prove Theorem 1.6.

Proof of Theorem 1.6. Suppose that $|S| = 4$ and $|S^2| = 11$.

Write $S = \{x_1, x_2, x_3, x_4\}$, $T = \{x_1, x_2, x_3\}$ and $x_1 < x_2 < x_3 < x_4$.

Suppose that $x_3x_4 \neq x_4x_3$. Then by Proposition 2.1 we have $|T^2| \leq 11 - 4 = 7$.

If $|T^2| \leq 6$, then T is abelian by Theorem 1.4, and S has the required structure by Lemma 4.2.

So assume that $|T^2| = 7$ and apply Proposition 3.1. If $T \cap Z(\langle T \rangle) \neq \emptyset$, then S has the required structure by Lemma 4.4. Therefore, we may assume, without loss of generality, that $T = \{a, ac, b\}$, with $c > 1$ and $ab = bac$. Write $x_4 = x$. If $ax = xa$, then $\{a, ac, x\}$ is abelian since $c \in Z(G)$ and again we are in the situation of Lemma 4.2. Hence, suppose that $ax \neq xa$. If $x = bz$ with $z \in Z(G)$, then S has the required structure by Lemma 4.5. So assume that $xZ(G) \neq bZ(G)$. Notice that then if xa, or xac, or ax or acx is in T^2, then the only possibility is that it is equal to b^2. Similarly, if bx or xb is in T^2, then it belongs to the set $\{a^2, a^2c, a^2c^2\}$. Now, if $ax, xa \in T^2$, then $ax = b^2 = xa$, a contradiction. Therefore one of the elements ax, xa is not in T^2. Similarly, one of the elements axc, xac is not in T^2.

Assume, without loss of generality, that $ax \notin T^2$. Assume first that $xa \in T^2$. Then

$$xa = b^2,$$

in which case $xb \neq bx$, since otherwise $b \in C_G(a)$, a contradiction. Moreover $xb, bx \notin T^2$, since otherwise $bxZ(G) = a^2Z(G)$, yielding $b^3Z(G) = bxaZ(G) = a^3Z(G)$ and $ba = ab$, a contradiction. Notice, also, that $xb \neq ax$, since otherwise $xbZ(G) = axZ(G) = xaZ(G)$ and $ab = ba$, a contradiction. Thus

$$S^2 = T^2 \cup \{x^2, bx, xb, ax\},$$

implying that $axc \in T^2$. Hence $axc = b^2 = xa$ and $xac \notin T^2$. It follows that $xac = axc^2 \in \{bx, ax\}$. If $axc^2 = bx$, then $b = ac^2$ and $[a, b] = 1$, a contradiction.

If, on the other hand, $xac = ax$, then $xac^2 = axc = xa$ and $c^2 = 1$, again a contradiction.

Therefore we may assume that $x^2, ax, xa \notin T^2$ and, arguing similarly, axc, $xac \notin T^2$. Hence either $ax = xac$ or $xa = axc$. Since both these equalities could not hold together, if follows that $S^2 = T^2 \cup \{x^2, ax, xa, axc, xac\}$ and $bx, xb \in T^2$. Assume, for example, that $bx \leq xb$. Then it is easy to see that the only possibility is $bx = a^2$, $[b, x] = [a, x]^2$, $xb = a^2c^2$, and (vii) holds.

Now assume that $x_3x_4 = x_4x_3$. Acting similarly, while considering the order opposite to $<$, we may assume that $x_1x_2 = x_2x_1$. Then Lemma 4.6 applies and S has the required structure.

Conversely, suppose that one of (i), (ii), (iii), (iv), (v), (vi), (vii) holds.

First suppose that (i) holds and write $S = \{s, t, a, b\}$, where $s, t \in Z(\langle S\rangle)$ and $ab \neq ba$. Then we have $S^2 = \{s^2, t^2, st, sa, sb, ta, tb, a^2, b^2, ab, ba\}$, and $|S^2| = 11$, as required.

If either (ii) or (iii) or (iv) holds, then it is easy to verify directly that $|S^2| = 11$.

Suppose that (v) holds, and write $T = \{a, ac, b\}$. Then $|T^2| = 7$ and $S^2 = T^2 \dot\cup xT \dot\cup \{x^2\}$. Thus $|S^2| = 7 + 3 + 1 = 11$, as required.

Now suppose that (vi) holds and write $T = \{a, ac, ac^2\}$. Then $|T^2| = 5$, $|xT \cap Tx| = 1$ and $|Tx \cup xT| = 3 + 3 - 1 = 5$. Since $S^2 = T^2 \dot\cup (xT \cup Tx) \dot\cup \{x^2\}$, it follows that $|S^2| = 5 + 5 + 1 = 11$ as required.

Finally suppose that (vii) holds and write $T = \{a, ac, b\}$. Suppose, for example, that $bx = a^2$, $ab = bac$, $xb = bxc^2$ and $xa = axc$. Then $|T^2| = 7$ and $Tx \cup xT = \{bx = a^2, ax, axc = xa, a^2c^2 = xb, axc^2 = xac\}$. Thus $(Tx \cup xT) \cap T^2 = \{a^2, a^2c^2\}$ and $|S^2| = 7 + 5 - 2 + 1 = 11$, as required. QED

References

[1] E. Breuillard, B. Green, T. Tao, The structure of approximate groups, *Publ. Math. Inst. Hautes Études Sci.* **116** (2012), 115-221.

[2] R. Botto Mura and A. Rhemtulla, Orderable groups, *Lecture Notes in Pure and Applied Mathematics*, Marcel Dekker, Inc., New York and Basel, (1977).

[3] J. Cilleruelo, M. Silva, C. Vinuesa, A sumset problem, *J. Comb. Number Theory* **2(1)** (2010), 79–89.

[4] G.A. Freiman, On the addition of finite sets I, *Izv. Vyss. Ucebn. Zaved. Matematika* **6 (13)** (1959), 202-213.

[5] G.A. Freiman, Inverse problems of additive number theory. IV: On the addition of finite sets. II. (Russian) *Elabuž. Gos. Ped. Inst. Učen. Zap.*, **8** (1960), 72-116.

[6] G.A. Freiman, Foundations of a structural theory of set addition, *Translations of mathematical monographs*, **37**, Amer. Math. Soc., (1973), Providence, Rhode Island.

[7] G.A. Freiman, Structure Theory of Set Addition, *Astérisque*, **258** (1999), 1-33.

[8] G.A. Freiman, M. Herzog, P. Longobardi and M. Maj, Small doubling in ordered groups, *J. Austral. Math. Soc.*, **96** (2014), no.3, 316-325.

[9] G. A. 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.

[10] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne and Y.V. Stanchescu, Small doubling in ordered groups: generators and structure, in preparation.

[11] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, and Y.V. Stanchescu, Inverse problems in Additive Number Theory and in Non-Abelian Group Theory, *http://arxiv.org/abs/1303.3053*, 1–31.

[12] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, and Y.V. Stanchescu, Small doubling in nilpotent groups, in preparation.

[13] A.M.W. Glass, Partially ordered groups, *World Scientific Publishing Co., Series in Algebra*, **7**, (1999).

[14] B. Green, What is ... an approximate group?, *Notices Amer. Math. Soc.* **59** (2012), no. 5, 655–656.

[15] N. Gill, H.A. Helfgott, Growth of small generating sets in $SL_n(Z/pZ)$, *Int. Math. Res. Not. IMRN* **18**, (2011), 4226-4251.

[16] H.A. Helfgott, Growth in $SL_3(Z/pZ)$, *J. Eur. Math. Soc. (JEMS)* **13** (2011), no. 3, 761-851.

[17] R. Jin, Detailed Structure for Freiman's 3k-3 Theorem, *arXiv:1308.0741v1 [math.NT] 3 Aug 2013*

[18] V.F. Lev, P.Y. Smeliansky, On addition of two distinct sets of integers, *Acta Arith.* **70** (1995), no. 1, 85–91.

[19] A.I. Mal'cev, On ordered groups, *Izv. Akad. Nauk. SSSR Ser. Mat.* **13** (1948), 473-482.

[20] M.B. Nathanson, Additive Number Theory Inverse Problems and the Geometry of Sumsets, Springer, (1996).

[21] B.H. Neumann, On ordered groups, *Amer. J. Math.* **71** (1949), 1-18.

[22] T. Sanders, The structure theory of set addition revisited, *Bull. Amer. Math. Soc.* **50(1)** (2013), 93-127.

[23] Y.V. Stanchescu, On addition of two distinct sets of integers, *Acta Arith.* **75** (1996), no. 2, 191–194.

[24] Y.V. Stanchescu, On the structure of sets with small doubling property on the plane.I., *Acta Arith.* **83** (1998), no. 2, 127–141.

[25] Y.V. Stanchescu, The structure of d-dimensional sets with small sumset, *J. Number Theory* **130** (2010), no. 2, 289–303.

[26] T.C. Tao, Product set estimates for noncommutative groups, *Combinatorica* **28** (2008), no. 5, 547–594.