Published on European Journal of Combinatorics
https://doi.org/10.1016/j.ejc.2014.09.004

A SMALL DOUBLING STRUCTURE THEOREM IN A BAUMSLAG-SOLITAR GROUP

G. A. FREIMAN, M. HERZOG, P. LONGOBARDI, M. MAJ, AND Y. V. STANCHESCU

Abstract. We solve a general inverse problem of small doubling type in a monoid, which is a subset of the Baumslag-Solitar group $BS(1,2)$.

1. Introduction

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

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

This paper deals with the following type of problems.

Let X be a finite subset of a group G. Determine the **structure** of X if the following inequality holds:

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

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

Such problems are called **inverse problems** of **small doubling** type. They belong to the *"Freiman's structural theory of set addition",* the foundations for which were led in G. Freiman's book "Foundations of a structural theory of set addition" (see [3]). In this book finite subsets of abelian groups were considered.

By now, Freiman's theory had been extended tremendously. See, for example, Freiman's survey [4] and T. Sanders' recent survey [11].

This paper is a contribution to the current programme aimed at determining the structure of finite subsets of non-abelian groups, with a small doubling property (see, for example, [15] and [8]).

We noticed in [6] (see also [7]) that some inverse problems of small doubling type in the *Baumslag-Solitar* groups are related to similar problems concerning *sums of dilates* in the Additive Number Theory (see Theorem 4).

Keywords: Inverse problems; small doubling; sums of dilates; Baumslag-Solitar groups and monoids.

Mathematics Subject Classification 2010: Primary 11P70; Secondary 20F05, 20F99, 11B13, 05E15.

Since this relation serves as a basis for the proof of our main result, we shall present first a short introduction to the theory of sums of dilates and to the theory of Baumslag-Solitar groups.

We begin with the **theory of sums of dilates**.

Let $A = \{x_1, \dots, x_k\}$ be a finite set of integers and let r be a positive integer. Define

$$r * A = \{rx_1, rx_2, \dots, rx_k\} = \{ra \mid \ a \in A\}.$$

Such sets are called **dilates** and sums of dilates of the form

$$r * A + s * A = \{rx + sy \mid \ x, y \in A\}$$

have been studied recently by several authors.

For example, the following theorem was proved by Cilleruelo et al. in 2010.

Theorem 1. ([2]) *If A is a finite set of integers, then*

$$|A + 2 * A| \geq 3|A| - 2$$

and

$$|A + 2 * A| = 3|A| - 2$$

if and only if A is an arithmetic progression.

In paper [6] we proved the following two new results in this area:

Theorem 2. ([6], Theorem 6) *Let A be a finite set of integers and let r be an integer satisfying $r \geq 3$. Then:*

$$|A + r * A| \geq 4|A| - 4.$$

and

Theorem 3. ([6], Theorem 4) *Let A be a finite set of integers. Suppose that $|A| \geq 3$ and*

$$|A + 2 * A| < 4|A| - 4.$$

Then A is a **subset** *of an arithmetic progression of size $\leq 2|A| - 3$.*

Theorem 3 is an example of an "inverse result" of "sums of dilates" type.

We continue now with the **theory of Baumslag-Solitar groups**.

The Baumslag-Solitar groups $BS(m, n)$ are two-generated groups with one relation, which are defined as follows:

$$BS(m, n) = \langle a, b \mid \ a^m b = ba^n \rangle,$$

where m and n are integers.

Our attention will be concentrated on the Baumslag-Solitar groups

$$BS(1, n) = \langle a, b \mid \ ab = ba^n \rangle.$$

We shall describe now the connection between certain small doubling problems in the Baumslag-Solitar groups $BS(1,n)$ and sums of dilates.

Let S be a finite subset of $BS(1,n)$ of size k and suppose that S is contained in the coset

$$b^r\langle a\rangle$$

of $\langle a\rangle$ in $BS(1,n)$, for some **positive** integer r. Then

$$S=\{b^ra^{x_1},b^ra^{x_2},\ldots,b^ra^{x_k}\},$$

where $A=\{x_1,x_2,\ldots,x_k\}$ is a set of integers. We introduce now the notation

$$S=\{b^ra^x : x\in A\}=b^ra^A.$$

Thus $|S|=|A|$.

Since $BS(1,n)=\langle a,b \mid \ ab=ba^n\rangle$, it follows that

$$a^xb^r=b^ra^{n^rx} \qquad \text{for each} \qquad x\in\mathbb{Z} \quad \text{and} \quad r\in\mathbb{N}.$$

Consequently

$$\begin{aligned}(b^ra^x)(b^pa^y)&=b^r(a^xb^p)a^y=b^r(b^pa^{n^px})a^y\\ &=b^{r+p}a^{n^px+y}\end{aligned}$$

for each $x,y\in\mathbb{Z}$ and for each $r,p\in\mathbb{N}$.

Using this equality and the previous notation, we proved in [6] the following basic result.

Theorem 4. ([6], Theorem 1) *Suppose that*

$$S=b^ra^A\subseteq BS(1,n),\ T=b^pa^B\subseteq BS(1,n)$$

where $r,p\in\mathbb{N}$ and A,B are finite subsets of $\mathbb{Z}$. Then

$$ST=b^{r+p}a^{n^p*A+B}$$

and

$$|ST|=|n^p*A+B|.$$

In particular,

$$S^2=b^{2r}a^{n^r*A+A}$$

and

$$|S^2|=|n^r*A+A|=|A+n^r*A|.$$

We shall now curtail our attention to the Baumslag-Solitar groups $BS(1,2)$, which is defined as follows:

$$BS(1,2)=\langle a,b \mid \ ab=ba^2\rangle.$$

Let S be a finite subset of $BS(1,2)$. It follows by Theorem 4 that if $S\subset b\langle a\rangle$, then

$$|S^2|=|A+2*A|,$$

and if $S \subset b^m\langle a\rangle$ for some positive integer m, then

$$|S^2| = |A + 2^m * A|.$$

Theorems 1, 2, 3 and 4 yield the following results concerning finite subsets of $BS(1,2)$, which will be needed for the proof of our main result (see Theorem 7 and Theorem 9 in Section 2).

Theorem 5. ([6], Theorem 5) *Let $S = ba^A \subseteq BS(1,2)$, where A is a finite set of integers of size k. Then $|S| = k$ and*

$$|S^2| \geq 3k - 2.$$

Moreover, $|S^2| = 3k - 2$ if and only if A is an arithmetic progression.

Furthermore, if $k \geq 3$ and

$$|S^2| = (3k - 2) + h < 4k - 4,$$

then $h \geq 0$ and A is a **subset** *of an arithmetic progression of size $k + h \leq 2k - 3$.*

and

Theorem 6. ([6], Corollary 2) *Let $S = b^m a^A \subseteq BS(1,2)$, where A is a finite set of integers of size k and $m \geq 2$. Then*

$$|S^2| \geq \max(4k - 4, 1) \geq 3k - 2.$$

These results concerning subsets of $BS(1,2)$ were obtained under the assumption that the subsets are contained in **one coset** of $\langle a\rangle$ in $BS(1,2)$.

The aim of **this paper** is to prove a more general result. We would like to determine the structure of an arbitrary subset of $BS(1,2)$, satisfying some small doubling condition. However, this appears to be a difficult problem and we succeeded only in solving it for subsets of the monoid $BS^+(1,2)$, which is a subset of $BS(1,2)$ defined as follows:

$$BS^+(1,2) = \{b^m a^x \in BS(1,2)\},$$

where x is an arbitrary integer and m is a **non-negative integer**. The multiplication in $BS^+(1,2)$ is induced by that of $BS(1,2)$.

The advantage of $BS^+(1,2)$ over $BS(1,2)$ is that all elements of $BS^+(1,2)$ can be uniquely represented by a word of the form $b^m a^n$, which is not the case in $BS(1,2)$.

Using rather complicated arguments, we proved the following **inverse theorem** concerning finite non-abelian subsets S of $BS^+(1,2)$ satisfying the following small doubling condition:

$$|S^2| < \frac{7}{2}|S| - 4.$$

Theorem 7. *Let S be a finite non-abelian subset of $BS^+(1,2)$ and suppose that*

$$|S^2| < \frac{7}{2}|S| - 4.$$

Then

$$S = ba^A,$$

where A is a set of integers of size $|S|$, which is contained in an arithmetic progression of size less than $\frac{3}{2}|S| - 2$.

So, under the above condition, the "arbitrary" subset S of $BS^+(1,2)$ is forced to be, after all, a subset of a single coset $b\langle a\rangle$.

This result is best possible. In fact, there exist non-abelian subsets S of $BS^+(1,2)$ satisfying $|S^2| = \frac{7}{2}|S| - 4$, which are not contained in one coset of $\langle a\rangle$ in $BS^+(1,2)$ (see Example 1 in Section 2).

In this paper we use the following notation. We write $[m,n] = [x \in \mathbb{Z} \mid m \le x \le n\}$. The set $\mathbb{N}$ of natural numbers consists of all **non-negative** integers. The *algebraic sum* of two finite subsets A and B of $\mathbb{Z}$ will be denoted by

$$A + B = \{x + y \mid \ x \in A,\ y \in B\}.$$

In particular, if $y \in \mathbb{Z}$, then $A + y = \{x + y : \ x \in A\}$. Throughout this paper we shall use the well known inequality

$$|A + B| \ge |A| + |B| - 1.$$

Let $A = \{a_0 < a_1 < ... < a_{k-1}\}$ be a finite increasing set of k integers. By the *length* $\ell(A)$ of A we mean the difference

$$\ell(A) = \max(A) - \min(A) = a_{k-1} - a_0$$

between its maximal and minimal elements and

$$h_A = \ell(A) + 1 - |A|$$

denotes the number of *holes* in A, that is $h_A = |\ [a_0, a_{k-1}] \setminus A\ |$. Finally, if $k \ge 2$, then we denote

$$d(A) = g.c.d.(a_1 - a_0, a_2 - a_0, ..., a_{k-1} - a_0).$$

In our proof we need the following result of Lev-Smelianski and Stanchescu:

Theorem 8. ([10] and [12]) *Let A and B be finite subsets of $\mathbb{N}$ such that $0 \in A \cap B$. Define*

$$\delta_{A,B} = \begin{cases} 1, & \text{if } \ell(A) = \ell(B), \\ 0, & \text{if } \ell(A) \ne \ell(B). \end{cases}$$

Then the following statements hold:

(i) *If $\ell(A) = \max(\ell(A), \ell(B)) \ge |A| + |B| - 1 - \delta_{A,B}$ and $d(A) = 1$, then*

$$|A + B| \ge |A| + 2|B| - 2 - \delta_{A,B}.$$

(ii) *If $\max(\ell(A), \ell(B)) \le |A| + |B| - 2 - \delta_{A,B}$, then*

$$|A + B| \ge (|A| + |B| - 1) + \max(h_A, h_B) = \max(\ell(A) + |B|, \ell(B) + |A|).$$

Proof. Assertion (i) is Theorem 2(ii) in [10] and assertion (ii) is Theorem 4 in [12]. □

The next section is devoted to the proof of Theorem 9, which is a more detailed version of Theorem 7.

2. An inverse result for all subsets of $BS^+(1,2)$.

In Theorem 5, we proved an inverse result for finite subsets of the Baumslag-Solitar group $BS(1,2)$, which are contained in the coset $ba^{\mathbb{Z}}$ and satisfy the following inequality:

$$|S^2| < 4|S| - 4.$$

In this section we shall solve, using a more detailed analysis, an inverse problem concerning **all** finite non-abelian subsets S of the corresponding monoid

$$BS^+(1,2) = \{g = b^m a^x \in BS(1,2) \mid \ x, m \in \mathbb{Z}, \ m \geq 0\}, \tag{1}$$

which satisfy the more restrictive small doubling property:

$$|S^2| < \frac{7}{2}|S| - 4.$$

We shall prove the following theorem.

Theorem 9. *If S is a finite non-abelian subset of $BS^+(1,2)$ of size $|S| = k$, then the following statements hold:*

(I) *The size of S^2 satisfies:*

$$|S^2| \geq 3k - 2. \tag{2}$$

(II) *If*

$$|S^2| = (3k - 2) + h < \frac{7}{2}k - 4, \tag{3}$$

then there exists a finite set of integers $A \subseteq \mathbb{Z}$ such that

(a) $S = ba^A$

(b) *The set A is contained in an arithmetic progression of size*

$$k + h < \frac{3}{2}k - 2.$$

Notice that Theorem 9 is a more detailed version of Theorem 7.

Throughout this section we shall use the following **notation**. $BS^+(1,2)$ is the monoid defined in (1), with multiplication induced by that of $BS(1,2)$. Every element $g \in BS^+(1,2)$ can be represented in a *unique way* as a product

$$g = b^m a^x,$$

where $m \in \mathbb{N}$ and $x \in \mathbb{Z}$. It follows that for every two distinct natural numbers $m \neq n$, we have

$$b^m a^{\mathbb{Z}} \cap b^n a^{\mathbb{Z}} = \emptyset. \tag{4}$$

If

$$S \subseteq BS^+(1,2)$$

is a finite subset of $BS^+(1,2)$ of size $k = |S|$, we define a set of natural numbers

$$M_S = M(S) \subseteq \mathbb{N}$$

by the following condition: $m \in M_S$ if and only if there is an integer x such that $b^m a^x \in S$. The set S defines M_S in a unique way and we shall denote it by

$$M_S = \{m_0 < m_1 < ... < m_t\},$$

where $t \geq 0$ and $m_0 \geq 0$. For every $0 \leq i \leq t$, we define

$$S_i = S \cap b^{m_i} a^{\mathbb{Z}}, \; k_i = |S_i|. \tag{5}$$

Every set S_i is non-empty, lies in only one coset of the cyclic subgroup $\langle a \rangle = a^{\mathbb{Z}}$ and there is a finite set of integers $A_i \subseteq \mathbb{Z}$ such that

$$S_i = b^{m_i} a^{A_i} \subseteq b^{m_i} a^{\mathbb{Z}}.$$

The set S can be written as a *disjoint union* of $t+1$ sets

$$S = S_0 \cup S_1 \cup ... \cup S_t, \tag{6}$$

satisfying

$$k_i = |S_i| = |A_i| \geq 1.$$

Before starting the proof of Theorem 9, we wish to show that the result of part (II) of the theorem is **best possible**. That follows from the following example.

Example 1. We shall exhibit a non-abelian subset S of $BS^+(1,2)$ of size k, which satisfies $|S^2| = \frac{7}{2}k - 4$ and which intersects non-trivially two distinct cosets of $\langle a \rangle$.

Notice, that by part (II) of Theorem 9, such situation is impossible if $|S^2| < \frac{7}{2}k - 4$.

Let

$$S = a^{A_0} \cup \{b\} \subset BS^+(1,2),$$

where

$$A_0 = \{0, 1, 2, ..., k-2\} \text{ and } k > 2 \text{ is even.}$$

The set S is clearly non-abelian, and it intersects non-trivially the two distinct cosets $1\langle a \rangle$ and $b\langle a \rangle$ of $\langle a \rangle$ in $BS^+(1,2)$.

Moreover,

$$S^2 = a^{A_0} a^{A_0} \cup b a^{A_0} \cup a^{A_0} b \cup \{b^2\}.$$

and using $a^{A_0} b = b a^{2*A_0}$, we get

$$S^2 = a^{A_0 + A_0} \cup (b a^{A_0} \cup b a^{2*A_0}) \cup \{b^2\} = a^{A_0 + A_0} \cup b a^{A_0 \cup 2*A_0} \cup \{b^2\}.$$

Since

$$a^{A_0 + A_0} \subseteq a^{\mathbb{Z}}, \; b a^{A_0 \cup 2*A_0} \subseteq b a^{\mathbb{Z}}, \; \{b^2\} \subseteq b^2 a^{\mathbb{Z}},$$

it follows by (4) that the three components of S^2 are disjoint in pairs and hence

$$|S^2| = |A_0 + A_0| + |A_0 \cup 2 * A_0| + 1 = (2k-3) + (\frac{3}{2}k - 2) + 1 = \frac{7}{2}k - 4, \qquad (7)$$

as required. □

We continue now with the **proof of part (I)** of Theorem 9.

Proof. By Corollary 3.3 in [5], a **non-abelian** subset S of an orderable group satisfies $|S^2| \geq 3|S| - 2$.

Hence, in order to prove part (I) of Theorem 9, it suffices to prove that the group $BS(1,2)$ is orderable.

As a matter of fact, we shall prove a more general result.

Theorem 10. *For $n \geq 2$, the group*

$$BS(1,n) = \langle a, b \mid \ ab = ba^n \rangle$$

is orderable.

Proof. Recall the definitions of ordered and orderable groups.

Definition 1. Let G be a group and suppose that a total order relation $\leq$ is defined on the set G. We say that $(G,<)$ is an *ordered group* if for all $a, b, x, y \in G$, the inequality $a \leq b$ implies that $xay \leq xby$.

A group G is *orderable*, if there exists a total order relation $\leq$ on the set G, such that $(G,<)$ is an ordered group.

If G is a group, a, b elements of G, we put $a^b = b^{-1}ab$.

The following sufficient condition for a torsion-free group to be orderable was proven by M. I. Kargapolov in [9]:

Theorem 11. *A torsion-free group G has the property that every total order for any subgroup of G can be extended to some total order of G if and only if there exists a normal abelian subgroup A of G such that G/A is abelian and for any $a \in A$ and $b \in G \setminus A$, there exist* **positive** *integers m, n, $m \neq n$, such that $(a^m)^b = a^n$.*

We continue now with the **proof of Theorem 10** . We wish to show that if $n \geq 2$, then the group $BS(1,n)$ satisfies the assumptions of Theorem 11. First of all, it follows from its presentation that it is torsion-free. Next, by Lemma 3.1 in [1], we know that if $n \geq 2$, then

$$BS(1,n) = U \rtimes V,$$

where

$$U = \langle b^{-j}ab^j \mid j \in \mathbb{Z} \rangle \quad \text{and} \quad V = \langle b \rangle.$$

In order to be able to apply Theorem 11 to $BS(1,n)$, it suffices to show that the following two conditions hold:

(i) The group U is abelian;

(ii) For all $x \in U$, we have $x^b = x^n$.

Concerning property (i), it suffices to show that

$$(b^{-i}ab^i)(b^{-j}ab^j) = (b^{-j}ab^j)(b^{-i}ab^i)$$

for all $i, j \in \mathbb{Z}$. We may assume, without loss of generality, that $i > j$ and hence $j - i < 0$.

Since $b^{-1}ab = a^n$, it follows that $b^{-r}ab^r \in \langle a \rangle$ for all positive integers r. Hence

$$(b^{j-i}ab^{i-j})a = a(b^{j-i}ab^{i-j}),$$

which implies that

$$(b^{-i}ab^i)(b^{-j}ab^j) = (b^{-j}ab^j)(b^{-i}ab^i),$$

as required.

Concerning property (ii), it follows from $b^{-1}ab = a^n$ that

$$(b^{-r}ab^r)^b = b^{-r}a^nb^r = (b^{-r}ab^r)^n$$

for all $r \in \mathbb{Z}$. This implies, by property (i), that $x^b = x^n$ for all $x \in U$, as required.

Since conditions (i) and (ii) hold, it follows by Theorem 11 that the group $BS(1, n)$ is orderable. □

In particular, $BS(1, 2)$ is orderable. Thus the proof of part (I) of Theorem 9 is complete.

□

The proof of part (II) of Theorem 9 will follow from Lemmas 1-7 below.

Lemma 1. *Let $S \subseteq BS^+(1, 2)$ be a finite set of size $k = |S|$. Suppose that $t \geq 1$ and there is $0 \leq j \leq t$ such that $k_j = |S_j| \geq 2$. Then S generates a non-abelian group.*

Proof. If $j = 0$ *and* $m_0 = 0$, then $k_0 = |S_0| = |A_0| \geq 2$ implies that $S_0 \neq \{1\}$ and $A_0 \neq \{0\}$. Since $t \geq 1$, it follows that there are three integers m, x, z such that $m \geq 1, x \neq 0$, $a^x \in S_0$ and $b^m a^z \in S_1$. In this case

$$a^x(b^m a^z) = b^m a^{z+2^m x} \neq (b^m a^z)a^x = b^m a^{z+x}$$

and therefore S generates a non-abelian group.

It remains to examine the following two cases:

(i) $j \geq 1$.

(ii) $j = 0$ and $m_0 \geq 1$.

If $j \geq 1$, then $m_j \geq 1$ and $k_j = |S_j| = |b^{m_j} a^{A_j}| \geq 2$ implies that $|A_j| \geq 2$. On the other hand, if $j = 0$ and $m_0 \geq 1$, then $k_0 = |S_0| = |b^{m_0} a^{A_0}| \geq 2$ implies that $|A_0| \geq 2$. In both cases, let $m = m_j$. Then $m \geq 1$ and there are two integers $x \neq y$ such that $\{b^m a^x, b^m a^y\} \subseteq S_j$. We conclude that

$$(b^m a^x)(b^m a^y) = b^{2m} a^{y+2^m x} \neq (b^m a^y)(b^m a^x) = b^{2m} a^{x+2^m y},$$

since $x \neq y$ and $m \geq 1$. The proof of Lemma 1 is complete. □

We shall examine now the case $t = 1$, i.e. we shall study sets S lying in exactly two cosets. Note that inequality (8) in the following Lemma 2 is tight, in view of Example 1 .

Lemma 2. *Let $S \subseteq BS^+(1,2)$ be a finite set of size $k = |S| \geq 2$. Suppose that $S = U \cup V$ with $U = b^m a^M \neq \emptyset$ and $V = b^n a^N \neq \emptyset$, where $0 \leq m < n$ are two integers and $M, N \subseteq \mathbb{Z}$. Then*

$$|S^2| \geq \frac{7}{2}|S| - 4. \tag{8}$$

Proof. Clearly $k = |M| + |N|$ and

$$S^2 = U^2 \cup (UV \cup VU) \cup V^2. \tag{9}$$

Using Theorem 1 we get

$$U^2 = b^{2m} a^{M+2^m * M}, \ V^2 = (b^n a^N)(b^n a^N) = b^{2n} a^{N+2^n * N}, \tag{10}$$

$$UV = (b^m a^M)(b^n a^N) = b^{m+n} a^{N+2^n * M}, \ VU = (b^n a^N)(b^m a^M) = b^{m+n} a^{M+2^m * N}. \tag{11}$$

Since the sets $b^{2m} a^{\mathbb{Z}}$, $b^{m+n} a^{\mathbb{Z}}$ and $b^{2n} a^{\mathbb{Z}}$ are disjoint in pairs, it follows that

$$|S^2| = |U^2| + |(UV \cup VU)| + |V^2|. \tag{12}$$

We shall examine now two complementary cases.

Case 1: $1 \leq m < n$.

We shall estimate $|U^2|$ and $|V^2|$ using either Theorem 5 or Theorem 6. We have

$$|U^2| = |M + 2^m * M| \geq 3|M| - 2, \quad |V^2| = |N + 2^n * N| \geq 3|N| - 2.$$

Using (12) and $|UV| = |N + 2^n * M| \geq |M| + |N| - 1$ we conclude that

$$|S^2| = |U^2| + |UV| + |V^2| \geq 3|M| - 2 + (|M| + |N| - 1) + 3|N| - 2 = 4k - 5 \geq \frac{7}{2}|S| - 4,$$

as required.

Case 2: $0 = m < n$.

In this case S is a disjoint union of two non-empty sets:

$$S = U \cup V, \text{ where } U = a^M, \ V = b^n a^N \text{ and } n \geq 1.$$

We have

$$U^2 = a^{M+M}, \ V^2 = b^{2n} a^{N+2^n * N}, \tag{13}$$

$$UV = b^n a^{N+2^n * M}, \ VU = b^n a^{M+N}. \tag{14}$$

Therefore it follows, either by Theorem 5 or by Theorem 6, that

$$|U^2| = |M + M|, \quad |V^2| = |N + 2^n * N| \geq 3|N| - 2. \tag{15}$$

We also clearly have

$$|UV \cup VU| = |(N + 2^n * M) \cup (M + N)| = |(M \cup 2^n * M) + N| \\ \geq |(M \cup 2^n * M)| + |N| - 1 \geq |M| + |N| - 1. \tag{16}$$

Suppose that $|M| = 1$. Then it follows from (12), (16) and (15) that

$$|S^2| \geq 1 + (1 + |N| - 1) + (3|N| - 2) = 4|N| - 1 \geq 3.5(1 + |N|) - 4 = 3.5|S| - 4,$$

as required. So we may assume that $|M| \geq 2$.

We shall complete the proof by dealing separately with two complementary subcases. Denote

$$\ell = \ell(M) = \max(M) - \min(M), \qquad d = d(M) = \gcd\{x - \min(M) : x \in M\}$$

and define

$$M^* = \frac{1}{d}(M - \min(M)), \qquad \ell^* = \ell(M^*) = \max(M^*) = \frac{\ell}{d}.$$

Case 2.1. Assume that $\ell(M^*) \geq 2|M^*| - 2$.

As shown above, we may assume that $|M| \geq 2$. Suppose that $|M| = 2$. Then $M = \{a_0 < a_1\}$, which implies that $d(M) = a_1 - a_0$ and $M^* = \{0, 1\}$. Thus $\ell(M^*) = 1$ and by our assumptions $1 = \ell(M^*) \geq 2|M^*| - 2 = 2$, a contradiction. Hence we may assume that $|M| \geq 3$, which implies that $k = |M| + |N| \geq 3 + 1 = 4$.

Note that $d(M^*) = 1$. By using Theorem 8(i) for equal summands we get

$$|U^2| = |M + M| = |M^* + M^*| \geq 3|M^*| - 3 = 3|M| - 3. \tag{17}$$

Using (12), (17), (15) and (16), we may conclude that

$$|S^2| = |U^2| + |UV \cup VU| + |V^2| \geq (3|M| - 3) + (|M| + |N| - 1) + (3|N| - 2) = 4k - 6.$$

Since $k \geq 4$, it follows that $|S^2| \geq \frac{7}{2}|S| - 4$, as required.

Case 2.2. Assume that $\ell(M^*) \leq 2|M^*| - 3$.

In this case, we use Theorem 8(ii) for equal summands. Let $h_{M^*} = \ell^* + 1 - |M^*|$ be the number of *holes* in M^*. We get

$$|M + M| = |M^* + M^*| \geq 2|M^*| - 1 + h_{M^*} = |M^*| + \ell^* = |M| + \ell^*. \tag{18}$$

We shall now estimate the size of $M \cap 2^n * M$. Note that all the common elements of $2^n * M$ and M lie in the interval $[\min(M), \max(M)]$ of length ℓ and the set $2^n * M$ is included in an arithmetic progression of difference $2^n d \geq 2d$. Therefore

$$|M \cap (2^n * M)| \leq \frac{\ell}{2d} + 1 = \frac{\ell^*}{2} + 1 \tag{19}$$

and

$$|M \cup (2^n * M)| = |M| + |2^n * M| - |M \cap 2^n * M| \geq 2|M| - \frac{\ell^*}{2} - 1. \tag{20}$$

Using (12), (15), (16), (18) and (20) we conclude that

$$\begin{aligned}|S^2| &= |U^2| + |UV \cup VU| + |V^2| \\ &\geq |M+M| + (|M \cup 2^n * M| + |N| - 1) + (|N + 2^n * N|) \\ &\geq (|M| + \ell^*) + (2|M| - \frac{\ell^*}{2} - 1 + |N| - 1) + (3|N| - 2) \\ &= 3|M| + 4|N| - 4 + \frac{\ell^*}{2} \\ &\geq 3|M| + 4|N| - 4 + \frac{|M^*|-1}{2} = \frac{7}{2}|M| + 4|N| - \frac{9}{2} \geq \frac{7}{2}k - 4,\end{aligned} \tag{21}$$

as required. □

In Lemmas 3, 4, 5 and 6 we shall obtain tight lower bounds for the cardinality of $|S^2|$, assuming that $k_i = |S_i| \geq 2$ for at most one i, $0 \leq i \leq t$.

Recall that by the equations preceeding the statement of Theorem 4, the following equation holds:

$$a^x b^r = b^r a^{2^r x} \tag{22}$$

for each $x \in \mathbb{Z}$ and $r \in \mathbb{N}$.

Lemma 3. *Let $S \subseteq BS^+(1,2)$ be a finite set of size $k = |S|$. Suppose that*

$$S = S_0 \cup S_1 \cup ... \cup S_t, \tag{23}$$

where $t \geq 2$. If $k_0 = |S_0| \geq 2$ and $k_i = |S_i| = 1$ for every $1 \leq i \leq t$, then

$$|S^2| \geq 4k - 5 > \frac{7}{2}k - 4. \tag{24}$$

Example 2. Inequality (24) is tight.
If

$$S = \{1, a\} \cup \{b, b^2, ..., b^t\},$$

then $k = t + 2$ and

$$S^2 = \{1, a, a^2\} \cup \{b, b^2, ..., b^t\} \cup \{ab, ab^2, ..., ab^t\} \cup \{ba, b^2a, ..., b^ta\} \cup \{b^2, b^3, ..., b^{2t}\}.$$

Note that equality (22) implies that

$$\{ab, ab^2, ..., ab^t\} = \{ba^2, b^2a^4, ..., b^ta^{2^t}\}$$

and thus

$$S^2 = \{1, a, a^2\} \cup \bigcup_{j=1}^{t} b^j\{1, a, a^{2^j}\} \cup \{b^{t+1}, b^{t+2}, ..., b^{2t}\}.$$

Using (4), we get $|S^2| = 3(t+1) + t = 4t + 3 = 4k - 5$. □

We continue now with the proof of Lemma 3.

Proof. Clearly $k = k_0 + t \geq 2 + 2 = 4$. Let

$$A_0 = \{y_1 < ... < y_{k_0}\} \subset \mathbb{Z}$$

be a finite set of k_0 integers that defines the set

$$S_0 = b^{m_0} a^{A_0} = \{b^{m_0} a^{y_1}, ..., b^{m_0} a^{y_{k_0}}\}$$

with $k_0 \geq 2$, and let

$$S_i = \{b^{m_i} a^{x_i}\}$$

for every $1 \leq i \leq t$. Recall our assumption that $0 \leq m_0 < m_1 < \cdots < m_t$.

Note that for every $1 \leq i \leq t$ we have $m_i > 0$,

$$S_0 S_i = b^{m_0+m_i}\{a^{x_i+2^{m_i}y_1}, ..., a^{x_i+2^{m_i}y_{k_0}}\},\ |S_0S_i| = k_0$$

and

$$S_i S_0 = b^{m_i+m_0}\{a^{y_1+2^{m_0}x_i}, ..., a^{y_{k_0}+2^{m_0}x_i}\},\ |S_iS_0| = k_0.$$

We claim that

$$|S_0S_i \cup S_iS_0| \geq k_0 + 1. \tag{25}$$

Indeed, if $S_0S_i = S_iS_0$, then

$$\{x_i + 2^{m_i}y_1 < ... < x_i + 2^{m_i}y_{k_0}\} = \{y_1 + 2^{m_0}x_i < ... < y_{k_0} + 2^{m_0}x_i\}$$

and thus

$$(2^{m_0} - 1)x_i = (2^{m_i} - 1)y_1 = ... = (2^{m_i} - 1)y_{k_0},$$

which contradicts $\{y_1 < ... < y_{k_0}\}$, in view of $m_i \geq 1$ and $k_0 \geq 2$.

Note that

$$S_0S_i \cup S_iS_0 \subseteq b^{m_0+m_i}a^{\mathbb{Z}}, \quad S_iS_t \subseteq b^{m_i+m_t}a^{\mathbb{Z}},$$

for every $0 \leq i \leq t$. Moreover, $S_0S_0 = b^{2m_0}a^{A_0+2^{m_0}*A_0}$, so $|S_0S_0| = |A_0 + 2^{m_0} * A_0| \geq 2|A_0| - 1 = 2k_0 - 1$. It follows by (4) that the sets

$$S_0S_0, S_0S_1 \cup S_1S_0, ..., S_0S_t \cup S_tS_0, S_1S_t, ..., S_tS_t$$

are disjoint and included in S^2. Using $t \geq 2$, $k_0 \geq 2$, (25) and $k \geq 4$, we conclude that

$$\begin{aligned}|S^2| &\geq (|S_0S_0| + |S_0S_1 \cup S_1S_0| + ... + |S_0S_t \cup S_tS_0|) + (|S_1S_t| + ... + |S_tS_t|)\\ &\geq (2k_0 - 1) + (k_0 + 1) + ... + (k_0 + 1) + (1 + ... + 1) = (2k_0 - 1) + t(k_0 + 1) + t\\ &= 4k_0 + (t - 2)k_0 + 2t - 1 \geq 4k_0 + 2(t - 2) + 2t - 1 = 4k_0 + 4t - 5 = 4k - 5\\ &> 3.5k - 4, \end{aligned} \tag{26}$$

as required.

□

Lemma 4. *Let $S \subseteq BS^{+}(1,2)$ be a finite set of size $k = |S|$. Suppose that*

$$S = S_0 \cup S_1 \cup ... \cup S_t, \tag{27}$$

where $t \geq 2$. If $k_t = |S_t| \geq 2$ and $k_i = |S_i| = 1$ for every $0 \leq i \leq t-1$, then

$$|S^2| \geq 4k - 5 > \frac{7}{2}k - 4. \tag{28}$$

Example 3. Inequality (28) is tight.
If

$$S = \{1, b, b^2, ..., b^{t-1}\} \cup \{b^t, b^t a\},$$

then $k = t + 2$ and

$$S^2 = \{1, b, b^2, ..., b^{2t-1}\} \cup \{1, b, ..., b^{t-1}\}b^t a \cup b^t a\{1, b, ..., b^{t-1}\} \cup \{b^{2t}, b^{2t}a, b^t a b^t, b^t a b^t a\}.$$

Note that equality (22) implies that

$$b^t a\{1, b, ..., b^{t-1}\} = \{b^t a, b^{t+1}a^2, ..., b^{2t-1}a^{2^{t-1}}\}$$

and

$$\{b^{2t}, b^{2t}a, b^t a b^t, b^t a b^t a\} = \{b^{2t}, b^{2t}a, b^{2t}a^{2^t}, b^{2t}a^{2^t+1}\}.$$

Thus

$$S^2 = \{1, b, b^2, ..., b^{t-1}\} \cup b^t\{1, a\} \cup \bigcup_{j=1}^{t-1} b^{t+j}\{1, a, a^{2^j}\} \cup b^{2t}\{1, a, a^{2^t}, a^{2^t+1}\}$$

and by (4), $|S^2| = t + 2 + 3(t-1) + 4 = 4t + 3 = 4k - 5$. □

We continue now with the proof of Lemma 4.

Proof. Clearly $k = k_t + t \geq 2 + 2 = 4$. Let

$$A_t = \{y_1 < ... < y_{k_t}\} \subseteq \mathbb{Z}$$

be a finite set of $k_t \geq 2$ integers, which defines the set

$$S_t = b^{m_t} a^{A_t} = \{b^{m_t} a^{y_1}, ..., b^{m_t} a^{y_{k_t}}\}$$

and let

$$S_i = \{b^{m_i} a^{x_i}\}$$

for every $0 \leq i \leq t-1$.

Note that for every $0 \leq i \leq t-1$ we have

$$S_t S_i = b^{m_t + m_i}\{a^{x_i + 2^{m_i} y_1}, ..., a^{x_i + 2^{m_i} y_{k_t}}\}, \ |S_t S_i| = k_t$$

and

$$S_i S_t = b^{m_i + m_t}\{a^{y_1 + 2^{m_t} x_i}, ..., a^{y_{k_t} + 2^{m_t} x_i}\}, \ |S_i S_t| = k_t.$$

It follows, like in Lemma 3, that

$$|S_t S_i \cup S_i S_t| \geq k_t + 1 \tag{29}$$

for $1 \leq i \leq t-1$.

Note that $|S_tS_t| \geq 3k_t - 2$, in view of Theorem 6. Using $|S_0S_t| = k_t$, $k_t \geq 2$, (29) and $k \geq 4$, we conclude, like in Lemma 3, that

$$\begin{aligned}|S^2| &\geq (|S_0S_0| + ... + |S_0S_t|) + (|S_1S_t \cup S_tS_1| + ... + |S_{t-1}S_t \cup S_tS_{t-1}| + |S_tS_t|) \\ &\geq (1 + ... + 1 + k_t) + ((t-1)(k_t+1) + (3k_t - 2)) = 4k_t + (t-1)k_t + 2t - 3 \\ &\geq 4k_t + 4t - 5 = 4k - 5 > \frac{7}{2}k - 4, \end{aligned} \tag{30}$$

as required. □

Lemma 5. *Let $S \subseteq BS^+(1,2)$ be a finite non-abelian set of size $k = |S| \geq 2$. Suppose that*

$$S = S_0 \cup S_1 \cup ... \cup S_t \tag{31}$$

where $|S_i| = 1$ for all i and

$$S_i = \{s_i\}, \quad s_i = b^{m_i}a^{x_i}.$$

Denote $T = S \setminus \{s_0\}$. If the subgroup $\langle T \rangle$ is abelian, then

$$|S^2| \geq 4k - 4. \tag{32}$$

Proof. Recall that $M_S = \{m_0 < m_1 < \cdots < m_t\}$, where $m_0 \geq 0$. We notice first that $T \neq \emptyset$ since $k \geq 2$. Moreover, we claim that the sets T^2, $s_0T \cup Ts_0$ and $\{s_0^2\}$ are disjoint. Indeed, we have:

(i) $s_0^2 \notin T^2$, since $s_0^2 = (b^{m_0}a^{x_0})^2 = b^{2m_0}a^{x_0+2^{m_0}x_0}$ and $T^2 \subseteq \{b^m a^x : \ m \geq 2m_1\}$.

(ii) $s_0^2 \notin (s_0T \cup Ts_0)$, because $s_0 \notin T$.

(iii) $s_0 \notin \langle T \rangle$, because $\langle T \rangle$ is abelian and $\langle S \rangle$ is non-abelian. This implies that $s_0T \cup Ts_0$ does not intersect the set T^2.

Notice also that $|T| = t$ and if $s_i, s_j \in T$, then $s_is_j = b^{m_i+m_j}a^{2^{m_j}x_i + x_j}$, which implies that $|T^2| \geq |M_S \setminus \{m_0\} + M_S \setminus \{m_0\}| \geq 2|M_S \setminus \{m_0\}| - 1 = 2t - 1$.

In order to complete the proof of Lemma 5, it suffices to show that the sets s_0T and Ts_0 are disjoint. Indeed, if that is the case, then

$$\begin{aligned}|S^2| &\geq |T^2| + |s_0T \cup Ts_0| + |\{s_0^2\}| \\ &= |T^2| + |s_0T| + |Ts_0| + |\{s_0^2\}| \\ &\geq (2t-1) + t + t + 1 = 4t = 4|S| - 4,\end{aligned}$$

as required.

So suppose, by way of contradiction, that

$$s_0T \cap Ts_0 \neq \emptyset. \tag{33}$$

Note that

$$s_0T = \{s_0s_1, \ldots, s_0s_t\} = \{b^{m_0+m_1}a^{x_1+2^{m_1}x_0}, \ldots, b^{m_0+m_t}a^{x_t+2^{m_t}x_0}\},$$

and

$$Ts_0 = \{s_1s_0, \ldots, s_ts_0\} = \{b^{m_0+m_1}a^{x_0+2^{m_0}x_1}, \ldots, b^{m_0+m_t}a^{x_0+2^{m_0}x_t}\}.$$

Therefore (33) implies that there is $1 \leq i \leq t$ such that

$$s_0 s_i = b^{m_0+m_i} a^{x_i+2^{m_i}x_0} = s_i s_0 = b^{m_0+m_i} a^{x_0+2^{m_0}x_i}$$

and thus

$$(2^{m_i} - 1)x_0 = (2^{m_0} - 1)x_i. \tag{34}$$

Choose an arbitrary $1 \leq j \leq t$. Since $\langle T \rangle$ is abelian, it follows that

$$s_j s_i = b^{m_j+m_i} a^{x_i+2^{m_i}x_j} = s_i s_j = b^{m_j+m_i} a^{x_j+2^{m_j}x_i},$$

yielding

$$(2^{m_i} - 1)x_j = (2^{m_j} - 1)x_i.$$

Hence

$$x_i = \frac{2^{m_i} - 1}{2^{m_j} - 1} x_j$$

and from (34) we get

$$(2^{m_i} - 1)x_0 = (2^{m_0} - 1)\frac{2^{m_i} - 1}{2^{m_j} - 1} x_j.$$

That means that $(2^{m_j} - 1)x_0 = (2^{m_0} - 1)x_j$ and thus

$$s_0 s_j = b^{m_0+m_j} a^{x_j+2^{m_j}x_0} = b^{m_0+m_j} a^{x_0+2^{m_0}x_j} = s_j s_0.$$

It follows that s_0 commutes with every element of T, which contradicts our assumptions that $\langle T \rangle$ is abelian and $\langle S \rangle$ is non-abelian. The proof of Lemma 5 is complete. $\square$

Lemma 6. *Let $S \subseteq BS^+(1,2)$ be a finite set of cardinality $k = |S| \geq 2$. Suppose that S is a disjoint union*

$$S = V_1 \cup V_2 \cup ... \cup V_t, \tag{35}$$

of t subsets

$$V_i = \{s_i\}, s_i = b^{m_i} a^{x_i},$$

of size $|V_i| = 1$. If S is a non-abelian set and $1 \leq m_1 < m_2 < .. < m_t$, then

$$|S^2| \geq 4k - 4. \tag{36}$$

Example 4. Inequality (36) is tight.

If $S = \{b, b^2, ..., b^{t-1}\} \cup \{b^t a\}$, then $k = t$ and S^2 is the union of four disjoint sets:

$$\{b^2, b^3, ..., b^{2t-2}\},$$

$$\{b, b^2, ..., b^{t-1}\}b^t a = \{b^{t+1}a, b^{t+2}a, ..., b^{2t-1}a\},$$

$$b^t a\{b, b^2, ..., b^{t-1}\} = \{b^{t+1}a^2, b^{t+2}a^4, ..., b^{2t-1}a^{2^{t-1}}\}$$

and $\{b^t a b^t a\} = \{b^{2t} a^{2^t+1}\}$. Therefore

$$|S^2| = (2t - 3) + (t - 1) + (t - 1) + 1 = 4k - 4.$$

□

We continue now with the proof of Lemma 6.

Proof. If a set S satisfies all the assumptions of Lemma 6, then we say that S is an *elementary set*.

Clearly $t = k \geq 2$ and we proceed by induction on t. If $t = 2$, then $S = \{s_1, s_2\}$ and since $s_1s_2 \neq s_2s_1$ and $s_1^2 \neq s_2^2$, it follows that $|S^2| = 4 = 4|S| - 4$, as required.

For the inductive step, let $t \geq 3$ be an integer, and assume that Lemma 6 holds for each elementary set $T \subseteq BS^+(1, 2)$ of size $2 \leq |T| \leq t - 1$. Denote

$$S' = S \setminus \{s_1\}.$$

In view of Lemma 5, we may assume that $\langle S' \rangle$ is non-abelian.

We shall continue by examining two complementary cases.

Case 1: $s_1s_2 = s_2s_1$.

Choose $n \geq 2$ *maximal* such that the set $S^* := \{s_1, s_2, ..., s_n\}$ is abelian. Note that $n < t$, because S in a non-abelian set, and $s_{n+1} \notin \langle S^* \rangle$. Moreover, $s_1s_{n+1} \notin S'^2$, since otherwise $s_1s_{n+1} = s_us_v$ for some $2 \leq u, v \leq t$ and hence $b^{m_1+m_{n+1}} = b^{m_u+m_v}$, implying that $m_1 < m_u, m_v < m_{n+1}$, whence $1 < u, v < n + 1$ and $s_{n+1} \in \langle S^* \rangle$, a contradiction. Similarly $s_{n+1}s_1 \notin S'^2$.

We claim that it suffices to show that s_{n+1} does not commute with s_1.

Indeed, if $s_1s_{n+1} \neq s_{n+1}s_1$, then (36) follows from

$$\{s_1^2, s_1s_2, s_1s_{n+1}, s_{n+1}s_1\} \subseteq S^2 \setminus S'^2$$

and from the induction hypothesis for S':

$$|S^2| \geq |S'^2| + |\{s_1^2, s_1s_2, s_1s_{n+1}, s_{n+1}s_1\}| \geq (4|S'| - 4) + 4 = 4|S| - 4.$$

We shall complete the proof by showing that if

$$s_1s_{n+1} = s_{n+1}s_1, \tag{37}$$

then

$$s_js_{n+1} = s_{n+1}s_j,$$

for every $1 \leq j \leq n$, which contradicts the maximality of n.

Our argument is similar to that used in the proof of Lemma 5. Denote $m = m_{n+1}$, $x = x_{n+1}$ and

$$s_{n+1} = b^m a^x.$$

We first note that (37) implies that

$$\begin{aligned} s_1s_{n+1} &= (b^{m_1}a^{x_1})(b^m a^x) = b^{m_1+m}a^{x+2^m x_1} \\ &= s_{n+1}s_1 = (b^m a^x)(b^{m_1}a^{x_1}) = b^{m+m_1}a^{x_1+2^{m_1}x} \end{aligned}$$

and thus

$$(2^{m_1} - 1)x = (2^m - 1)x_1. \tag{38}$$

Choose an arbitrary $1 \leq j \leq n$. Using

$$s_1 s_j = s_j s_1$$

we get, like in the proof of Lemma 5, that

$$x_1 = \frac{2^{m_1} - 1}{2^{m_j} - 1} x_j.$$

It follows by (38) that

$$(2^{m_1} - 1)x = (2^m - 1)\frac{2^{m_1} - 1}{2^{m_j} - 1} x_j$$

and since $m_1 \geq 1$, we may conclude that

$$(2^{m_j} - 1)x = (2^m - 1)x_j.$$

Thus $s_j s_{n+1} = s_{n+1} s_j$, a contradiction.

Case 2: $s_1 s_2 \neq s_2 s_1$.

We *claim* that

$$\text{either} \quad s_1 s_3 \neq s_2^2 \quad \text{or} \quad s_3 s_1 \neq s_2^2. \tag{39}$$

Indeed, if $s_1 s_3 = s_2^2$ and $s_3 s_1 = s_2^2$, then $s_1 s_3 = s_3 s_1$ and hence $s_1 s_2^2 = s_2^2 s_1$. Since by Theorem 10 $BS(1,2)$ is an orderable group, this equality implies by B.H.Neumann's result (see Lemma 2.2 in [5]) that $s_1 s_2 = s_2 s_1$, a contradiction. The proof of our claim is complete.

Thus

$$|\{s_1 s_3, s_3 s_1\} \setminus \{s_2^2\}| \geq 1.$$

Since

$$\{s_1^2, s_1 s_2, s_2 s_1\} \subseteq S^2 \setminus S'^2$$

and

$$\{s_1 s_3, s_3 s_1\} \setminus \{s_2^2\} \subseteq S^2 \setminus S'^2,$$

it follows by the induction hypothesis for S', that

$$|S^2| \geq |S'^2| + |\{s_1^2, s_1 s_2, s_2 s_1, s_1 s_3, s_3 s_1\} \setminus S'^2| \geq (4|S'| - 4) + 4 = 4|S| - 4.$$

The proof of Lemma 6 is complete.

□

The following lemma is the main step in the proof of part (II) of Theorem 9. We use an inductive argument analogous to that used for the proof of Lemma 2.2 in [13] (see also Lemma 3 in [14]).

Lemma 7. *Let $S \subseteq BS^+(1,2)$ be a finite set of size $k = |S| \geq 2$. Suppose that*

$$S = S_0 \cup S_1 \cup \ldots \cup S_t, \tag{40}$$

where $t \geq 1$. If S is a non-abelian set, then

$$|S^2| \geq \frac{7}{2}k - 4. \tag{41}$$

Proof. We use induction on $t \geq 1$. Observe that when $t = 1$, Lemma 7 follows from Lemma 2.

For the inductive step, let $t \geq 2$ be an integer, and assume that Lemma 7 holds for any non-abelian finite set $T \subseteq BS^+(1,2)$ which lies in u distinct cosets of $\langle a \rangle = a^{\mathbb{Z}}$, where $2 \leq u < t$.

Denote

$$S^* = S \setminus S_t, \quad k^* = |S^*| = k - k_t.$$

Notice that if S^* generates a non-abelian group, then our inductive hypothesis implies that

$$|(S^*)^2| \geq \frac{7}{2}k^* - 4,$$

and it suffices to show that

$$|S_t^2 \cup S_t S_{t-1} \cup S_{t-1} S_t| \geq \frac{7}{2}k_t, \tag{42}$$

since inequality (41) then follows from

$$|S^2| \geq |(S^*)^2| + |S_t^2 \cup S_t S_{t-1} \cup S_{t-1} S_t| \geq (\frac{7}{2}k^* - 4) + \frac{7}{2}k_t = \frac{7}{2}k - 4. \tag{43}$$

The proof of Lemma 7 will now be completed by examining four complementary cases.

Case 1: Assume that either $k_t \geq 2$ or $k_{t-1} \geq 2$.

Recall that $0 \leq m_0 < m_1 < ... < m_t$ and hence $t \geq 2$ implies that $m_t \geq 2$. Thus, using Theorem 6, we get

$$|S_t^2| \geq \max\{4k_t - 4, 1\} \geq 3k_t - 2.$$

We shall examine now four subcases.

(**i**) If $k_t + 2k_{t-1} \geq 6$, then (42) is true in view of:

$$|S_t^2 \cup S_t S_{t-1} \cup S_{t-1} S_t| \geq |S_t^2| + |S_t S_{t-1}| \geq (3k_t - 2) + (k_t + k_{t-1} - 1) = 4k_t + k_{t-1} - 3 \geq \frac{7}{2}k_t.$$

If there is $0 \leq j \leq t-1$ such that $k_j = |S_j| \geq 2$, then S^* generates a non-abelian group (in view of Lemma 1) and we may apply the induction hypothesis. Thus Lemma 7 follows from (42) and (43).

If $k_j = 1$ for all $0 \leq j \leq t-1$, then $k_t \geq 6 - 2k_{t-1} = 4$, in view of (**i**). In this case, Lemma 7 follows from Lemma 4.

So we may assume that Case (**i**) does not hold and in particular

$$k_t + 2k_{t-1} \leq 5.$$

Hence one of the following cases must hold: (**ii**) $k_t = 3, k_{t-1} = 1$, (**iii**) $k_t = 2, k_{t-1} = 1$ or (**iv**) $k_t = 1, k_{t-1} = 2$.

(ii) If $k_t = 3$ and $k_{t-1} = 1$, then Theorem 6 implies that $|S_t^2| \geq 4k_t - 4$ and therefore inequality (42) follows from:

$$|S_t^2 \cup S_tS_{t-1} \cup S_{t-1}S_t| \geq |S_t^2| + |S_tS_{t-1}| \geq (4k_t - 4) + (k_t + k_{t-1} - 1) = 5k_t - 4 > \frac{7}{2}k_t.$$

If there is $0 \leq j \leq t-1$ such that $k_j = |S_j| \geq 2$, then S^* generates a non-abelian group (in view of Lemma 1) and we may apply the induction hypothesis. Thus Lemma 7 follows from (42) and (43).

If $k_j = 1$ for all $0 \leq j \leq t-1$, then Lemma 7 follows from Lemma 4, in view of $k_t = 3$.

(iii) If $k_t = 2$ and $k_{t-1} = 1$, then we can write

$$S_{t-1} = \{b^ua^x\}, \quad S_t = \{b^va^y, b^va^z\},$$

where $1 \leq u = m_{t-1} < v = m_t$ and $y < z$ are integers. Using the identity $a^xb^m = b^ma^{2^mx}$, we get

$$S_{t-1}S_t = b^{u+v}\{a^{2^vx+y}, a^{2^vx+z}\} \quad \text{and} \quad S_tS_{t-1} = b^{u+v}\{a^{2^uy+x}, a^{2^uz+x}\}.$$

Note that $S_{t-1}S_t \neq S_tS_{t-1}$. Indeed, if $S_{t-1}S_t = S_tS_{t-1}$, then $2^vx + y = 2^uy + x$ and $2^vx + z = 2^uz + x$. Thus $(2^u - 1)y = (2^v - 1)x = (2^u - 1)z$, which contradicts $y < z$, in view of $u \geq 1$. Therefore either Theorem 5 or Theorem 6 implies (42):

$$|S_t^2 \cup S_tS_{t-1} \cup S_{t-1}S_t| = |S_t^2| + |S_tS_{t-1} \cup S_{t-1}S_t| \geq (3k_t - 2) + 3 = 4 + 3 = \frac{7}{2}k_t.$$

If there is $0 \leq j \leq t-1$ such that $k_j = |S_j| \geq 2$, then S^* generates a non-abelian group (in view of Lemma 1) and we may apply the induction hypothesis. Thus, Lemma 7 follows from (42) and (43).

If $k_j = 1$ for all $0 \leq j \leq t-1$, then Lemma 7 follows from Lemma 4, in view of $k_t = 2$.

(iv) If $k_t = 1$ and $k_{t-1} = 2$, then we can write

$$S_{t-1} = \{b^ua^y, b^ua^z\}, \ S_t = \{b^va^x\},$$

where $1 \leq u = m_{t-1} < v = m_t$, x, y, z are integers and $y < z$. Using the identity $a^xb^m = b^ma^{2^mx}$, we get

$$S_{t-1}S_t = b^{u+v}\{a^{2^vy+x}, a^{2^vz+x}\} \quad \text{and} \quad S_tS_{t-1} = b^{u+v}\{a^{2^ux+y}, a^{2^ux+z}\}.$$

Note that $S_{t-1}S_t \neq S_tS_{t-1}$. Indeed, if $S_{t-1}S_t = S_tS_{t-1}$, then $2^vy + x = 2^ux + y$ and $2^vz + x = 2^ux + z$. Thus $(2^v - 1)y = (2^u - 1)x = (2^v - 1)z$, which contradicts $y < z$, in view of $v \geq 1$. Therefore (42) holds:

$$|S_t^2 \cup S_tS_{t-1} \cup S_{t-1}S_t| = |S_t^2| + |S_tS_{t-1} \cup S_{t-1}S_t| \geq 1 + 3 > \frac{7}{2}k_t.$$

Since $k_{t-1} = 2$, Lemma 1 implies that S^* generates a non-abelian group and we may apply the induction hypothesis. Thus Lemma 7 follows from (42) and (43).

The proof in **Case 1** is complete.

Case 2: Assume that $k_t = k_{t-1} = ... = k_1 = 1$ and $k_0 \geq 2$.

In this case, Lemma 7 follows from Lemma 3.

Case 3: Assume that $k_t = k_{t-1} = 1$ and there is $1 \leq j \leq t-2$ such that $k_j \geq 2$ and $k_i = 1$ for every $i \in \{j+1, ..., t\}$.

Let

$$S_j = b^{m_j} a^{A_j} = \{b^{m_j} a^{y_1}, ..., b^{m_j} a^{y_{k_j}}\}$$

and let $S_i = \{b^{m_i} a^{x_i}\}$ for every $i \in \{j+1, ..., t\}$. Clearly $|S_j S_i| = |S_i S_j| = k_j$ and using the reasoning in the proof of Lemma 3, we get

$$|S_j S_i \cup S_i S_j| \geq k_j + 1 \tag{44}$$

for every $i \in \{j+1, ..., t\}$.

Note that $k_j \geq 2$, so by Lemma 1 the set

$$S_j^* = S_0 \cup S_1 \cup ... \cup S_j$$

is non-abelian. By applying the inductive hypothesis to S_j^* and in view of (44), we obtain

$$\begin{aligned}
|S^2| &\geq |S_j^* S_j^*| + \sum_{u=j+1}^{t} |S_j S_u \cup S_u S_j| + \sum_{u=j+1}^{t} |S_u S_t| \\
&\geq (\frac{7}{2}|S_j^*| - 4) + (k_j + 1)(t-j) + (t-j) \\
&= (\frac{7}{2}|S_j^*| - 4) + (k_j + 2)(t-j) \geq (\frac{7}{2}|S_j^*| - 4) + 4(t-j) \\
&= (\frac{7}{2}|S_j^*| - 4) + 4(k - |S_j^*|) = 4k - 4 - \frac{1}{2}|S_j^*| > \frac{7}{2}k - 4,
\end{aligned}$$

as required.

Case 4: Assume that $k_i = 1$ for every $0 \leq i \leq t$.

If the set $S' = S \setminus \{s_0\}$ is abelian, then Lemma 5 implies that

$$|S^2| \geq 4|S| - 4 > \frac{7}{2}k - 4,$$

as required. Therefore, we may assume that $S' = S_1 \cup S_2 \cup ... \cup S_t$ is non-abelian. Since $t \geq 2$, it follows that $k = t + 1 \geq 3$ and Lemma 6 implies that

$$|S'^2| \geq 4|S'| - 4.$$

Moreover,$\{s_0^2, s_0 s_1\} \subseteq S^2 \setminus S'^2$.

We distinguish now between two complementary cases.

(a) If $k = |S| \geq 4$, then

$$|S^2| \geq |S'^2| + 2 \geq 4(k-1) - 4 + 2 = 4k - 6 \geq \frac{7}{2}k - 4,$$

as required.

(b) If $k = 3$, then $S = \{s_0, s_1, s_2\}$, $S' = \{s_1, s_2\}$, $s_1 s_2 \neq s_2 s_1$, $|S'^2| = 4$ and

$$S^2 = \{s_0^2, s_0 s_1, s_1 s_0, s_0 s_2, s_2 s_0\} \cup S'^2.$$

We *claim* that

$$\text{either} \quad s_0 s_2 \neq s_1^2 \quad \text{or} \quad s_2 s_0 \neq s_1^2.$$

Indeed, if $s_0 s_2 = s_1^2$ and $s_2 s_0 = s_1^2$, then $s_0 s_2 = s_2 s_0$ and hence $s_1^2 s_2 = s_2 s_1^2$. Since by Theorem 10 $BS(1,2)$ is an orderable group, this equality implies by B.H.Neumann's result (see Lemma 2.2 in [5]) that $s_1 s_2 = s_2 s_1$, a contradiction.

We conclude that

$$|S^2| \geq |\{s_0^2, s_0 s_1, s_0 s_2, s_2 s_0\} \setminus S'^2| + |S'^2| \geq 3 + 4 = 7 > \frac{7}{2}|S| - 4.$$

The proof of Lemma 7 is complete.

□

We are finally ready for the **proof of part (II)** of Theorem 9.

Let S be a finite set satisfying the assumptions of part (II) of Theorem 9. The inequality

$$|S^2| < \frac{7}{2}k - 4$$

and Lemma 7 imply that

$$S = S_0 = b^{m_0} a^{A_0},$$

where $m_0 \geq 0$.

The set S is non-abelian, so $m_0 \geq 1$. If $m_0 \geq 2$, then Theorem 6 implies that $|S^2| \geq 4k - 4 > \frac{7}{2}k - 4$, which contradicts our hypothesis. Therefore

$$S = S_0 = ba^A$$

and Theorem 5 is applicable.

Hence, if

$$|S^2| = (3k-2) + h < \frac{7}{2}k - 4,$$

then $h < \frac{1}{2}k - 2$ and Theorem 5 implies that A is contained in an arithmetic progression of size $k + h < k + (\frac{1}{2}k - 2) = \frac{3}{2}k - 2$. The proof of part (II) of Theorem 9 is complete.

Hence also the proof of Theorem 9 is complete.

References

[1] O. Bogopolski, Abstract commensurators of solvable Baumslag-Solitar groups, *Communications of Algebra*, **40(7)** (2012), 2494-2502.

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

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

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

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

[6] 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.

[7] 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.

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

[9] M. I. Kargapolov, Completely orderable groups, *Algebra i Logica (2)*, **1** (1962), 16-21.

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

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

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

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

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

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

Gregory A. Freiman

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
Email address: grisha@post.tau.ac.il

Marcel Herzog

School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel
Email address: herzogm@post.tau.ac.il

Patrizia Longobardi

Dipartimento di Matematica, Universita' di Salerno, 84084 Fisciano (Salerno), Italy
Email address: plongobardi@unisa.it

Mercede Maj

Dipartimento di Matematica, Universita' di Salerno, 84084 Fisciano (Salerno), Italy
Email address: mmaj@unisa.it

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