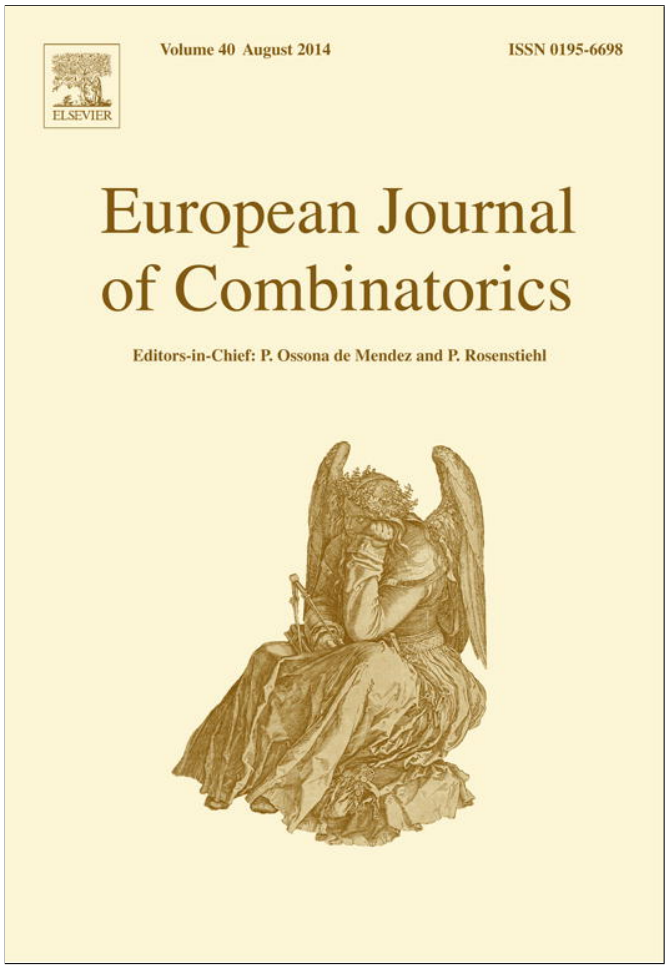

European Journal of Combinatorics 40 (2014) 42–54

Contents lists available at ScienceDirect

European Journal of Combinatorics

journal homepage: www.elsevier.com/locate/ejc

Direct and inverse problems in additive number theory and in non-abelian group theory

G.A. Freiman [a], M. Herzog [a], P. Longobardi [b], M. Maj [b], Y.V. Stanchescu [c,d]

[a] School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

[b] Dipartimento di Matematica, Universita' di Salerno, 84084 Fisciano (Salerno), Italy

[c] Afeka Academic College, Tel Aviv 69107, Israel

[d] The Open University of Israel, Raanana 43107, Israel

ARTICLE INFO

Article history:
Received 17 September 2013
Accepted 6 February 2014
Available online 12 March 2014

ABSTRACT

We obtain new direct and inverse results for Minkowski sums of dilates and we apply them to solve certain direct and inverse problems in Baumslag–Solitar groups, assuming appropriate small doubling properties.

1. Introduction

The aim of this paper is threefold:

(a) Finding new direct and inverse results in the additive number theory concerning Minkowski sums of dilates.
(b) Finding a connection between the above results and some direct and inverse problems in the theory of Baumslag–Solitar (non-abelian) groups.
(c) Solving certain inverse problems in Baumslag–Solitar groups, assuming appropriate small doubling properties.

We start with our first topic (a), concerning the additive number theory. In this paper $\mathbb{Z}$ denotes the rational integers, $\mathbb{N}$ denotes the *non-negative* elements of $\mathbb{Z}$ and the size of a finite set A will be

E-mail addresses: grisha@post.tau.ac.il (G.A. Freiman), herzogm@post.tau.ac.il (M. Herzog), plongobardi@unisa.it (P. Longobardi), mmaj@unisa.it (M. Maj), yonis@afeka.ac.il, ionut@openu.ac.il (Y.V. Stanchescu).

http://dx.doi.org/10.1016/j.ejc.2014.02.001
0195-6698/

denoted by $|A|$. Subsets of $\mathbb{Z}$ of the form

$$r * A = \{rx : x \in A\},$$

where r is a positive integer and A is a *finite* subset of $\mathbb{Z}$, are called *r-dilates*.

Minkowski sums of dilates are defined as follows:

$$r_1 * A + \cdots + r_s * A = \{r_1x_1 + \cdots + r_sx_s : x_i \in A,\ 1 \le i \le s\}.$$

These sums have been recently studied in different situations by Bukh, Cilleruelo, Hamidoune, Ljujić, Nathanson, Plagne, Pontiveros, Rué, Serra, Silva and Vinuesa (see [2–4,9,10,12–15]). In particular, they examined sums of two dilates of the form

$$A + r * A = \{a + rb \mid a, b \in A\}$$

and solved various direct and inverse problems concerning their sizes.

For example, it was shown in [9,4] that

$$|A + 2 * A| \ge 3|A| - 2,$$

which represents a direct result. Moreover, they solved the following inverse problem: what is the *structure* of the set A if

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

Their answer was that in such case A must be an arithmetic progression.

Inverse problems of this type, where the exact bound is assumed, will be called *ordinary inverse problems*. The term *extended inverse problem* will refer to inverse problems in which a small diversion from the exact bound is allowed, still enabling us to reach a definite conclusion concerning the structure of A.

As an example of an extended inverse problem, consider the following question: what is the structure of the set A if $|A| \ge 3$ and

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

Our answer to this question is:

(A) *If* $|A| \ge 3$ *and* $|A + 2 * A| < 4|A| - 4$, *then* A *is a* subset *of an arithmetic progression* P *of size* $|P| \le |A + 2 * A| - 2|A| + 2 \le 2|A| - 3$ (see Theorem 4, Section 3).

The above mentioned authors and others studied also the sums $A + r * A$ for $r \ge 3$. In this direction we proved the following new (direct) result:

(B) *If* $r \ge 3$, *then* $|A + r * A| \ge 4|A| - 4$ (see Theorem 5, Section 4).

This very useful result yields a *uniform* bound for all sets A and for $r \ge 3$. In the literature, most bounds of this type are asymptotic.

It is worthwhile to notice that in Corollary 3.3 of [10] Hamidoune and Rué proved that $|n * A + m * A| \ge 4|A| - 4$. But they assume that $2 \le n < m$, with n and m coprime. As far as we can see, our result does not follow from their corollary.

We continue now with the second topic (b), dealing with a connection, noticed by us, between results concerning sums of dilates and some problems in the theory of Baumslag–Solitar groups.

If S and T are subsets of a group G, their *product* is defined as follows:

$$ST = \{st \mid s \in S,\ t \in T\}.$$

In particular, $S^2 = \{s_1s_2 \mid s_1, s_2 \in S\}$ and if $b \in G$, then $bS = \{bs \mid s \in S\}$.

For integers m and n, the general Baumslag–Solitar group $BS(m, n)$ is a group with two generators a, b and one defining relation $b^{-1}a^mb = a^n$:

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

We shall concentrate on the Baumslag–Solitar groups

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

Let S be a finite subset of $BS(1, n)$ of size k_1 contained in the coset $b^r\langle a\rangle$ for some $r \in \mathbb{N}$ and let T be a finite subset of $BS(1, n)$ of size k_2 contained in the coset $b^p\langle a\rangle$ for some $p \in \mathbb{N}$. Then

$$S = \{b^r a^{x_0}, b^r a^{x_1}, \ldots, b^r a^{x_{k_1-1}}\},$$

where $A = \{x_0, x_1, \ldots, x_{k_1-1}\}$ is a subset of $\mathbb{Z}$. We introduce now the notation

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

Thus $|S| = |A|$.

Similarly, $T = b^p a^B$ for some subset $B = \{y_0, y_1, \ldots, y_{k_2-1}\}$ of $\mathbb{Z}$. Since $ab = ba^n$, it follows that $a^{-1}b = ba^{-n}$ and

$$a^x b^y = b^y a^{n^y x} \quad \text{for each } x \in \mathbb{Z} \text{ and } y \in \mathbb{N}. \tag{1}$$

In particular,

$$a^x b = ba^{nx} \quad \text{for each } x \in \mathbb{Z}.$$

Eq. (1) implies that

$$(b^r a^x)(b^p a^y) = b^r (a^x b^p) a^y = b^r (b^p a^{n^p x}) a^y = b^{r+p} a^{n^p x + y}$$

for each $x, y \in \mathbb{Z}$ and for each $r, p \in \mathbb{N}$. Therefore the *product set*

$$ST = \{vw \mid v \in S,\ w \in T\}$$

can be written as

$$\begin{aligned} ST &= \{(b^r a^{x_i})(b^p a^{y_j}) \mid i \in \{0, 1, \ldots, k_1 - 1\}, j \in \{0, 1, \ldots, k_2 - 1\}\} \\ &= \{b^{r+p} a^{n^p x_i + y_j} \mid i \in \{0, 1, \ldots, k_1 - 1\}, j \in \{0, 1, \ldots, k_2 - 1\}\} = b^{r+p} a^{n^p * A + B} \end{aligned} \tag{2}$$

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

We have proved the following *basic* theorem.

Theorem 1. *Suppose that*

$$S = b^r a^A \subseteq BS(1, n), \qquad T = b^p a^B \subseteq BS(1, n)$$

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

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

This result will serve us as the major means for investigating $|ST|$, and in particular $|S^2|$, using information about sizes of sums of dilates.

We skip now to our third topic (c), dealing with inverse problems in Baumslag–Solitar groups. By means of Theorem 1 and the results mentioned in topic (a), we proved the following statements, where the previous notation is used.

(C) *If* $S = ba^A \subseteq BS(1,2)$, *then* $|S^2| = |2 * A + A|$. *Hence* $|S^2| \geq 3|S| - 2$ *and if* $|S^2| = 3|S| - 2$, *then* A is *an arithmetic progression* (see Theorem 2(a), Section 2).
(D) *If* $S = ba^A \subseteq BS(1,2)$ *and* $|S^2| < 4|S| - 4$, *then* A *is a* subset *of an arithmetic progression of size* $|S^2| - 2|S| + 2 \leq 2|S| - 3$ (see Theorem 6, Section 5).
(E) *If* $S = ba^A \subseteq BS(1,r)$ *with* $r \geq 3$, *then* $|S^2| \geq 4|S| - 4$ (see Corollary 1, Section 6).
(F) *If* $S = b^m a^A \subseteq BS(1,2)$ *with* $m \geq 2$ *an integer, then* $|S^2| \geq 4|S| - 4$ (see Corollary 2, Section 6).

For more results concerning S^2, when $S = ba^A \subseteq BS(1,n)$, see Section 2.

Conditions of type $|S^2| < 4|S| - 4$ are called *small doubling properties*. In [7], we used methods of [19,20] in order to determine the structure of *arbitrary* finite non-abelian subsets S *of the monoid*

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

satisfying the small doubling property

$$|S^2| < 3.5|S| - 4.$$

The monoid $BS^+(1,2)$ is a subset of $BS(1,2)$, which is closed with respect to multiplication.

In this paper, Section 2 is devoted to results which follow immediately from our Theorem 1 and from known results about the sizes of sums of dilates. In Sections 3 and 4 we prove our basic Theorems 4 and 5 concerning the sizes of sums of dilates. Finally, in Sections 5 and 6 we use these theorems in order to solve inverse problems in Baumslag–Solitar groups.

Our paper is a pilot study in the following more general direction. Let G be an infinite non-abelian group of certain type and let S denote a finite *non-abelian* subset (i.e. $\langle S \rangle$ is non-abelian) of G of order k (k-subset in short). It is natural to ask the following questions:

Q.1. Find $m_G(k)$, the minimal possible value of $|S^2|$ for non-abelian k-subsets S of G.
Q.2. What can we say about the detailed structure of *extremal* k*-subsets* of G, i.e. finite non-abelian subsets S of G of size k, satisfying

$$|S^2| = m_G(k)?$$

Q.3. More generally, what can we say about the detailed structure of non-abelian k-subsets S of G, satisfying some *small doubling property*, say,

$$m_G(k) \leq |S^2| < c_0 k + d_0,$$

where c_0 is a small constant greater than 1 and d_0 is some small constant.

As mentioned above, we tried to answer these questions in the case of $G = BS(1,n)$ and in particular for $G = BS(1,2)$. We hope that our work will lead to similar studies for other classes of non-abelian groups.

This paper is a contribution to the current programme of extending the Freiman-type theory, concerning the structure of subsets of $\mathbb{Z}$ with a small doubling property (see [5,16]), to subsets S of non-abelian groups with a small doubling property (see, for example, [6,8,21,1] and references therein).

Preliminaries

In this paper we use the following notation. The *algebraic sum* of two finite subsets A and B of $\mathbb{Z}$ will be denoted by

$$A + B = \{a + b \mid a \in A,\ b \in B\}.$$

In particular, if $b \in \mathbb{Z}$, then $A + b = \{a + b :\ a \in A\}$. The sum $2A = A + A$ is called the *sumset* of A. Throughout this paper we shall use the well known inequality

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

Let $A = \{a_0 < a_1 < \cdots < a_{k-1}\}$ 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 $h_A = |\{a_0, a_0 + 1, a_0 + 2, \dots, a_{k-1}\} \setminus A|$. Finally, if $k \geq 2$, then we denote

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

We shall use several times the following results of Lev–Smeliansky in [11] and of Stanchescu in [18]:

Theorem LSS. *Let A and B be finite subsets of $\mathbb{N}$ such that $0 \in A \cap B$. Define*

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

Then the following statements hold:

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

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

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

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

Proof. Assertion (i) is Theorem 2(ii) from [11]. Assertion (ii) is Theorem 4 from [18]. □

2. Extremal sets contained in one coset of $BS(1, n)$

In this section we consider finite subsets S of

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

which are contained in the coset $b\langle a \rangle$ of $\langle a \rangle$ in $BS(1, n)$. In other words, if $|S| = k$, then

$$S = b\{a^{x_0}, a^{x_1}, \dots, a^{x_{k-1}}\} = ba^A,$$

where $A = \{x_0, x_1, \dots, x_{k-1}\} \subseteq \mathbb{Z}$.

In view of Theorem 1, Questions Q.1 and Q.2 concerning such S belong to the Additive Number Theory: find a tight lower bound for the size of the Minkowski sum $n*A+A$ and describe the structure of extremal sets A.

For $n = 2$ and $n = 3$, the answer to Questions Q.1 and Q.2 are known. Using Theorems 1.1 and 1.2 in [4] and Theorem 1, we get the following group-theoretical results:

Theorem 2. *Let $A \subseteq \mathbb{Z}$ be a finite set of integers. Then the following statements hold.*

(a) *If $S = ba^A \subseteq BS(1, 2)$, then $|S^2| \geq 3|S| - 2$. Moreover, equality holds if and only if A is an arithmetic progression.*

(b) *If $S = ba^A \subseteq BS(1, 3)$, then*

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

Moreover, equality holds if and only if either one of the following holds:

$$A = \{0, 1, 3\}, \qquad A = \{0, 1, 4\}, \qquad A = 3 * \{0, \dots, n\} \cup (3 * \{0, \dots, n\} + 1)$$

or A is an affine transform of one of these sets.

Proof. (a) It follows from Theorem 1.1 in [4] that $|A + 2 * A| \geq 3|A| - 2$ and $|A + 2 * A| = 3|A| - 2$ if and only if A is an arithmetic progression. Since $|S^2| = |A + 2 * A|$ by Theorem 1, we get (a).

(b) It follows from Theorem 1.2 in [4] that $|A + 3 * A| \geq 4|A| - 4$ and $|A + 3 * A| = 4|A| - 4$ if and only if either one of the following holds:

$$A = \{0, 1, 3\}, \qquad A = \{0, 1, 4\}, \qquad A = 3 * \{0, \dots, n\} \cup (3 * \{0, \dots, n\} + 1)$$

or A is an affine transform of one of these sets. Since $|S^2| = |A + 3 * A|$ by Theorem 1, we get (b). □

For $n \geq 4$, Theorem 1 and known results concerning sums of dilates yield the following partial results.

Theorem 3. *Let $A \subseteq \mathbb{Z}$ be a finite set of integers and let $S = ba^A$ be a subset of $BS(1, n)$. Then:*

(a) *If $S \subseteq BS(1, 4)$ and $|S| \geq 5$, then $|S^2| \geq 5|S| - 6$.*
(b) *If $S \subseteq BS(1, n)$, then $|S^2| \geq (n + 1)|S| - o(|S|)$.*
(c) *If p is an odd prime number, $S \subseteq BS(1, p)$ and $|S| \geq 3(p - 1)^2(p - 1)!$, then*

$$|S^2| \geq (p + 1)|S| - \lceil p(p + 2)/4 \rceil.$$

Moreover, equality holds if and only if $A = p * \{0, \ldots, m\} + \{0, \ldots, \frac{p-1}{2}\}$ for some m.

Proof. Using Theorem 1, we get $|S^2| = |n * A + A|$.
Inequality (a) follows from $|S^2| = |4 * A + A|$ and Theorem 3 in [17].
Inequality (b) follows from $|S^2| = |n * A + A|$ and Theorem 1.2 in [2].
Assertion (c) follows from $|S^2| = |p * A + A|$ and Corollary 1.3 in [3]. □

3. An extended inverse result for $|A + 2 * A|$

In this section we extend Theorem 1.1 in [4], which states that $|A + 2 * A| \geq 3|A| - 2$ for any finite subset A of $\mathbb{Z}$ and $|A + 2 * A| = 3|A| - 2$ implies that A is an arithmetic progression. In Theorem 4 below, we prove the following extended inverse result in the Additive Number Theory: if A is a finite subset of $\mathbb{Z}$ of size $|A| \geq 3$ satisfying $|A + 2 * A| < 4|A| - 4$, then A is *contained* in an arithmetic progression of size at most $2|A| - 3$. Our proof is independent of Theorem 1.1 in [4]. This result will be used in the next section.

Theorem 4. *Let $A = \{a_0 < a_1 < a_2 < \cdots < a_{k-1}\} \subset \mathbb{Z}$ be a finite set of integers of size $k = |A| \geq 1$. Then the following statements hold.*

(a) *If $1 \leq k \leq 2$, then $|A + 2 * A| = 3k - 2$ and A is an arithmetic progression of size k.*
(b) *If $k \geq 3$, assume that*

$$|A + 2 * A| = (3k - 2) + h < 4k - 4. \tag{3}$$

Then

$$h \geq 0, \quad |A + 2 * A| \geq 3k - 2$$

and the set A is a subset *of an arithmetic progression*

$$P = \{a_0, a_0 + d, a_0 + 2d, \ldots, a_0 + (l - 1)d\}$$

such that

$$|P| \leq k + h = |A + 2 * A| - 2k + 2 \leq 2k - 3. \tag{4}$$

(c) *If $k \geq 1$ and $|A + 2 * A| = 3k - 2$, then A is an arithmetic progression*

$$A = \{a_0, a_0 + d, a_0 + 2d, \ldots, a_0 + (k - 1)d\}.$$

Proof. (a) If $k = 1$, then $|A + 2 * A| = 1 = 3k - 2$ and A is an arithmetic progression of size k. If $k = 2$ and $A = \{a < b\}$, then

$$A + 2 * A = \{3a,\ a + 2b,\ b + 2a,\ 3b\}.$$

Since $a \neq b$, it follows that $|A + 2 * A| = 4 = 3k - 2$ and A is an arithmetic progression of size k. The proof of (a) is complete.

(b) We assume now that $k \geq 3$ and (3) holds. Suppose, first, that A is *normal*, i.e.

$$\min(A) = a_0 = 0 \quad \text{and} \quad d = d(A) = gcd(A) = 1. \tag{5}$$

Thus $\ell(A) = a_{k-1}$.

We split the set A into a disjoint union

$$A = A_0 \cup A_1,$$

where $A_0 \subseteq 2\mathbb{Z}$ and $A_1 \subseteq 2\mathbb{Z}+1$. Since $0 = a_0 \in A_0$ and $d(A) = 1$, it follows that $A_0 \neq \emptyset$ and $A_1 \neq \emptyset$. Therefore

$$m = |A_0| \geq 1, \qquad n = |A_1| \geq 1 \quad \text{and} \quad k = m + n.$$

We denote

$$A_0 = \{0 = 2x_0 < 2x_1 < \cdots < 2x_{m-1}\}, \qquad A_0^* = \frac{1}{2}A_0 = \{0 < x_1 < \cdots < x_{m-1}\},$$
$$A_1 = \{2y_0 + 1 < 2y_1 + 1 < \cdots < 2y_{n-1} + 1\},$$

and

$$A_1^* = \frac{1}{2}(A_1 - 1) - y_0 = \{0 < y_1 - y_0 < y_2 - y_0 < \cdots < y_{n-1} - y_0\}.$$

Thus

$$\ell(A_0^*) = x_{m-1} < a_{k-1} = \ell(A) \quad \text{and also} \quad \ell(A_1^*) = y_{n-1} - y_0 < a_{k-1} = \ell(A).$$

The set $A + 2 * A$ is the union of two disjoint subsets $A_0 + 2 * A \subseteq 2\mathbb{Z}$ and $A_1 + 2 * A \subseteq 2\mathbb{Z} + 1$ and therefore

$$|A + 2 * A| = |A_0 + 2 * A| + |A_1 + 2 * A| = |A_0^* + A| + |A_1^* + A|. \tag{6}$$

We continue our proof with two claims.

Claim 1.

$$\ell(A) \leq k + \max(m, n) - 2 \leq 2k - 3. \tag{7}$$

For the proof of Claim 1 we shall use Theorem LSS(i). Since $\ell(A) > \ell(A_0^*), \ell(A_1^*)$, we have $\delta_{A,A_0^*} = \delta_{A,A_1^*} = 0$.

Suppose, first, that $m \leq n$. If the claim is false, then

$$\ell(A) \geq k + n - 1 = |A| + |A_1^*| - 1 \geq k + m - 1 = |A| + |A_0^*| - 1$$

and since $d(A) = 1$, Theorem LSS(i) yields the following inequalities:

$$|A_0^* + A| \geq k + 2|A_0^*| - 2 = k + 2m - 2 \quad \text{and} \quad |A_1^* + A| \geq k + 2|A_1^*| - 2 = k + 2n - 2. \tag{8}$$

Using (6) and (8), we get that $|A + 2 * A| \geq 4k - 4$, which contradicts our hypothesis (3).

Similarly, if $n \leq m$ and

$$\ell(A) \geq k + m - 1 \geq k + n - 1,$$

then $d(A) = 1$ and Theorem LSS(i) imply again the inequalities (8), which together with (6) yield $|A + 2 * A| \geq 4k - 4$, a contradiction.

Hence $\ell(A) \leq k + \max(m, n) - 2$. Since $k = m + n$ and $m, n \geq 1$, it follows that $\max(m, n) \leq k - 1$ and hence $\ell(A) \leq k + \max(m, n) - 2 \leq 2k - 3$. The proof of Claim 1 is complete.

Next we state and prove Claim 2.

Claim 2.

$$|A + 2 * A| \geq (3k - 2) + h_A. \tag{9}$$

Recall that $h_A = \ell(A) + 1 - |A|$. For the proof of Claim 2 we shall use Claim 1 and Theorem LSS(ii). We distinguish between two cases.

Case 1: Suppose that $m \leq n$ and hence, by (7), $\ell(A) \leq k + n - 2$.

Thus it follows by Theorem LSS(ii) that

$$|A_1^* + A| \geq (n + k - 1) + h_A$$

and therefore

$$\begin{aligned}|A+2*A| &= |A_0^*+A|+|A_1^*+A| \\ &\geq (|A_0^*|+|A|-1)+|A_1^*+A| \geq (m+k-1)+(n+k-1)+h_A \\ &= (3k-2)+h_A.\end{aligned}$$

Case 2: Suppose that $n < m$ and hence, by (7), $\ell(A) \leq k+m-2$.
Thus it follows by Theorem LSS(ii) that

$$|A_0^*+A| \geq (m+k-1)+h_A$$

and therefore

$$|A+2*A| = |A_0^*+A|+|A_1^*+A| \geq (m+k-1)+h_A+(n+k-1) = (3k-2)+h_A.$$

In both cases we obtain that h_A, the total number of holes in the normal set A, satisfies

$$0 \leq h_A \leq |A+2*A|-(3k-2) = h \leq k-3.$$

Hence

$$h \geq h_A \geq 0 \quad \text{and} \quad |A+2*A| \geq (3k-2).$$

Moreover, the set A is contained in the arithmetic progression

$$P = \{a_0, a_0+1, a_0+2, \ldots, a_{k-1}\} = \{0, 1, 2, \ldots, a_{k-1}\}$$

of size

$$a_{k-1}+1 = k+h_A \leq k+h \leq 2k-3. \tag{10}$$

It follows that Theorem 4(b) holds for *normal* sets A satisfying (5) and (3).
Let now A be an *arbitrary* finite set of $k = |A| \geq 3$ integers satisfying the inequality (3). We define

$$B = \frac{1}{d(A)}(A-a_0) = \left\{\frac{1}{d(A)}(x-a_0) : x \in A\right\}.$$

Note that $|B| = |A| = k$, $\min(B) = 0$, $d(B) = 1$ and

$$|B+2*B| = |A+2*A| = (3k-2)+h < 4k-4.$$

Therefore B is a normal set satisfying inequality (3) of Theorem 4 and as shown above

$$0 \leq h_B \leq |B+2*B|-(3k-2) = |A+2*A|-(3k-2) = h \leq k-3.$$

Hence also in the general case we get

$$h \geq 0 \quad \text{and} \quad |A+2*A| \geq (3k-2).$$

Moreover, it follows from (10) applied to B that B is contained in the arithmetic progression

$$P = \{0, 1, 2, \ldots, b_{k-1}\}$$

with

$$b_{k-1} = \max(B) \leq k+h-1 \leq 2k-4.$$

Thus $A = d(A)B + a_0$ is contained in an arithmetic progression

$$\{a_0, a_0+d, a_0+2d, \ldots, a_0+(k+h-1)d\}$$

of size $k+h \leq 2k-3$, where d denotes $d(A)$. The proof of (b) is complete.

(c) If $1 \leq k \leq 2$, then our claim follows from (a). So suppose that $k \geq 3$. Then $h = 0$ and by (4) in (b), A is a subset of an arithmetic progression of size k at most. But A is a set of size k, so A is equal to the arithmetic progression. The proof of (c), and hence also of Theorem 4, is now complete. □

4. A new lower bound for $|A + r * A|$

In this section we obtain a new tight lower bound for $|A + r * A|$, provided that $r \geq 3$.

Theorem 5. *Let $A = \{a_0 < a_1 < a_2 < \cdots < a_{k-1}\} \subset \mathbb{Z}$ be a finite set of integers of size $|A| = k \geq 1$. Then for every integer $r \geq 3$ we have*

$$|A + r * A| \geq \max(4k - 4, 1) \geq 3k - 2. \tag{11}$$

Remark. If $r = 3$, then Theorem 5 follows from Theorem 1.2 in [4]. If $r \geq 4$, then the results of [2,3] are asymptotically stronger than (11), but we need a lower bound valid for *every* k. Our proof is independent of [4].

Proof. If $k = 1$, then $|A + r * A| = 1 = \max(4k - 4, 1) = 3k - 2$ and the theorem holds.

If $k = 2$, then $A = \{a < b\}$ and $r > 1$ implies that $a + rb \neq b + ra$. Hence

$$\begin{aligned} |A + r * A| &= |\{a, b\} + \{ra, rb\}| = |\{(r + 1)a, b + ra, a + rb, (r + 1)b\}| \\ &= 4 = 4k - 4 = 3k - 2, \end{aligned}$$

so the theorem holds also for $k = 2$. Therefore we shall assume, from now on, that $k \geq 3$. Thus, since $k > 1$, we need only to prove that

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

We assume first that A is *normal*, i.e.

$$\min(A) = a_0 = 0 \quad \text{and} \quad d = d(A) = gcd(A) = 1. \tag{12}$$

We split the set A into a disjoint union of s non-empty subsets, each of which being contained in a *distinct* residue class modulo r:

$$A = A_1 \cup A_2 \cup \cdots \cup A_s,$$

where

$$A_i \subseteq x_i + r\mathbb{Z}, \quad |A_i| \geq 1 \quad \text{and} \quad x_i = \min A_i.$$

Note that $k \geq 3$, $d(A) = 1$ and $\min(A) = a_0 = 0$, so $s \geq 2$.

We clearly have

$$|A + r * A| = \sum_{i=1}^{s} |A_i + r * A| \geq \sum_{i=1}^{s} (|A_i| + |A| - 1) = |A| + s(|A| - 1).$$

If $s \geq 3$, then we get $|A + r * A| \geq 4|A| - 3$ and Theorem 5 follows.

Hence we may assume that $s = 2$ and $A = A_1 \cup A_2$, where A_1 and A_2 are non-empty subsets of A contained in disjoint residue classes modulo r. Let

$$k_1 = |A_1| \quad \text{and} \quad k_2 = |A_2|.$$

Then $k = k_1 + k_2$ and we may assume, without loss of generality, that

$$k_1 \geq k_2.$$

Hence $2k_1 \geq k$ and $k_1 \geq 2$.

Recall that if S is a finite subset of $\mathbb{Z}$, then $\ell(S)$, the length of S, is defined by $\ell(S) = \max(S) - \min(S)$. For $i = 1, 2$ we define

$$A_i^* = \frac{1}{r}(A_i - \min(A_i)) = \left\{ \frac{1}{r}(x - x_i) : x \in A_i \right\},$$

where $x_i = \min A_i$. Clearly $|A_i^*| = |A_i|$ and we have

$$|A_i + r * A| = |A_i^* + A|.$$

Thus

$$|A + r * A| = |A_1 + r * A| + |A_2 + r * A| = |A_1^* + A| + |A_2^* + A|.$$

Note also that

$$\ell(A_i) \geq r(k_i - 1) \quad \text{and} \quad \ell(A_i^*) = \frac{1}{r}\ell(A_i),$$

so

$$k_i - 1 \leq \ell(A_i^*) = \frac{1}{r}\ell(A_i) \leq \ell(A_i) \leq \ell(A).$$

Moreover, $\ell(A_i) > \ell(A_i^*)$ if and only if $k_i > 1$, so $\ell(A_1) > \ell(A_1^*)$ since $k_1 \geq 2$.

Clearly we must have either $k_1 = k - 1 > k_2 = 1$ or $k_1 \geq k_2 > 1$. We shall examine these two cases separately.

Case 1: Suppose that $k_1 = k - 1 > k_2 = 1$. We have $k = k_1 + 1$ and $\ell(A) \geq \ell(A_1) > \ell(A_1^*)$. Moreover,

$$\ell(A) \geq \ell(A_1) \geq r(k_1 - 1) \geq 3k_1 - 3.$$

We distinguish now between two complementary subcases.
(i) Suppose that $\ell(A) \geq k + k_1 - 1 = 2k_1$. Then, since $d(A) = 1$, Theorem LSS(i) implies that

$$|A + A_1^*| \geq k + 2k_1 - 2.$$

(ii) Suppose that $\ell(A) \leq k + k_1 - 2 = 2k_1 - 1$. Then, since $k_1 \geq 2$, Theorem LSS(ii) implies that

$$|A + A_1^*| \geq \ell(A) + |A_1| \geq 3k_1 - 3 + k_1 = 4k_1 - 3 \geq 3k_1 - 1 = k + 2k_1 - 2.$$

Thus in both cases we have

$$|A + r * A| = |A_1^* + A| + |A_2^* + A| \geq (k + 2k_1 - 2) + k = 4k - 4,$$

as required.

Case 2: Suppose that $k_1 \geq k_2 > 1$. Then

$$\ell(A) > \ell(A_1^*), \quad \ell(A) > \ell(A_2^*)$$

and

$$\ell(A) \geq \ell(A_i) \geq r(k_i - 1) \geq 3k_i - 3$$

for $i = 1, 2$.

We distinguish now between three complementary subcases, depending on the value of $\ell(A)$ with respect to $k + k_1 - 1$ and $k + k_2 - 1$.
(i) Suppose that $\ell(A) \geq k + k_1 - 1$. Then also $\ell(A) \geq k + k_2 - 1$ and since $d(A) = 1$, Theorem LSS(i) implies that

$$|A + A_1^*| \geq k + 2k_1 - 2, \qquad |A + A_2^*| \geq k + 2k_2 - 2.$$

Hence

$$\begin{aligned} |A + r * A| &= |A_1^* + A| + |A_2^* + A| \geq (k + 2k_1 - 2) + (k + 2k_2 - 2) \\ &= 4k_1 + 4k_2 - 4 = 4k - 4, \end{aligned}$$

as required.
(ii) Suppose that $k + k_2 - 1 \leq \ell(A) \leq k + k_1 - 2$. Then

$$k_1 \geq k_2 + 1$$

and since $d(A) = 1$, Theorem LSS(i) and (ii) imply that

$$|A + A_1^*| \geq \ell(A) + |A_1^*| \geq 3k_1 - 3 + k_1 = 4k_1 - 3 \quad \text{and} \quad |A + A_2^*| \geq k + 2k_2 - 2.$$

Hence

$$|A + r * A| = |A_1^* + A| + |A_2^* + A| \geq 5k_1 + 3k_2 - 5 \geq 4k_1 + 4k_2 - 4 = 4k - 4,$$

as required.
(iii) Suppose that $\ell(A) \leq k + k_2 - 2$. Then $3k_1 - 3 \leq \ell(A) \leq k_1 + 2k_2 - 2$, yielding $2k_1 \leq 2k_2 + 1$. Since $k_1 \geq k_2$, it follows that

$$k_1 = k_2 \geq 2$$

and

$$3k_i - 3 \leq r(k_i - 1) \leq \ell(A_i) \leq \ell(A) \leq k + k_2 - 2 = 3k_1 - 2 = 3k_2 - 2.$$

We claim that $\ell(A) = 3k_1 - 2$. Indeed, if $\ell(A) = 3k_1 - 3$, then $\ell(A_1) = \ell(A_2) = \ell(A) = a_{k-1}$. But $a_{k-1} \notin A_i$ for some i and hence $\ell(A_i) < a_{k-1}$, a contradiction. This proves our claim.

Recall that $\ell(A) > \ell(A_1^*)$ and $\ell(A) > \ell(A_2^*)$. Since $\ell(A) = 3k_1 - 2 = k + (k_i - 2) = |A| + |A_i^*| - 2$ for $i = 1, 2$, it follows, by Theorem LSS(ii), that

$$|A + r * A| = |A_1^* + A| + |A_2^* + A| \geq \ell(A) + k_1 + \ell(A) + k_2 = 2(3k_1 - 2) + k = 4k - 4,$$

as required. Our proof in Case 2 is complete.

So Theorem 5 holds for *normal* sets A. Let A be now an *arbitrary* finite set of $k = |A| \geq 3$ integers. We define

$$B = \frac{1}{d(A)}(A - a_0) = \left\{ \frac{1}{d(A)}(x - a_0) : x \in A \right\}.$$

Note that $|B| = |A| = k$, $\min(B) = 0$, $d(B) = 1$ and $|A + r * A| = |B + r * B|$. For the normal set B we have proved that $|B + r * B| \geq 4|B| - 4$. It follows that

$$|A + r * A| = |B + r * B| \geq 4|B| - 4 = 4|A| - 4,$$

as required. The proof of Theorem 5 is complete. □

5. An extended inverse result for subsets of $b\langle a\rangle$ in $BS(1, 2)$

In this section we shall apply Theorem 4 in order to obtain an extended inverse result in Group Theory.

Recall that $BS(1, 2) = \langle a, b \mid ab = ba^2\rangle$. In Theorem 2(a) we obtained the following ordinary inverse group-theoretical result:

If $A \subseteq \mathbb{Z}$ is a finite set of integers and $S = ba^A \subset BS(1, 2)$, then

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

Moreover, equality holds if and only if A is an arithmetic progression.

Theorem 4, together with Theorem 1, allows us to solve the corresponding extended inverse group-theoretical problem.

Theorem 6. *Let $A \subseteq \mathbb{Z}$ be a finite set of integers of size $k = |A| \geq 1$. If $S = ba^A$ is a finite subset of the group $BS(1, 2)$, then $|S| = k$ and*

$$|S^2| \geq 3k - 2. \tag{13}$$

Moreover, if $k \geq 3$ and

$$|S^2| = (3k - 2) + h < 4|S| - 4, \tag{14}$$

then $h \geq 0$ and S is a subset *of a geometric progression*

$$S \subseteq \{ba^u, ba^{u+d}, ba^{u+2d}, \ldots, ba^{u+(k+h-1)d}\}$$

of size $k + h \leq 2k - 3$, where $u = \min(A)$ and $d = d(A)$.

Furthermore, if either $1 \le k \le 2$ *or* $k \ge 3$ *and* $h = 0$, *then* S *is the geometric progression*

$$S = \{ba^u, ba^{u+d}, ba^{u+2d}, \dots, ba^{u+(k-1)d}\}.$$

Proof. Clearly $|S| = |A| = k$ and by Theorem 1, $|S^2| = |2 * A + A|$. Hence it follows by Theorem 4 that $|S^2| \ge 3k - 2$, proving (13).

If $k \ge 3$, then (14) implies, again by Theorem 1, that

$$|A + 2 * A| = (3k - 2) + h < 4k - 4.$$

Hence it follows by Theorem 4, that $h \ge 0$ and A is a subset of an arithmetic progression

$$P = \{u, u + d, u + 2d, \dots, u + (k + h - 1)d\}$$

of size $k + h \le 2k - 3$, where $u = \min(A)$ and $d = d(A)$. Hence

$$S \subseteq \{ba^u, ba^{u+d}, ba^{u+2d}, \dots, ba^{u+(k+h-1)d}\}.$$

Finally, if either $1 \le k \le 2$ or $k \ge 3$ and $h = 0$, then, by Theorem 4, A *is* an arithmetic progression and hence S *is* the required geometric progression. □

6. Other results concerning $BS(1, n)$

We conclude this paper with two applications of Theorem 5. The first application is concerned with subsets of $BS(1, r)$.

Corollary 1. *Let* $S \subseteq BS(1, r)$ *be a finite set of size* $k = |S| \ge 1$ *and suppose that* $r \ge 3$ *and*

$$S = ba^A,$$

where $A \subseteq \mathbb{Z}$ *is a finite set of integers.*

Then

$$|S^2| = |A + r * A| \ge \max(4k - 4, 1) \ge 3k - 2. \tag{15}$$

Proof. By Theorem 1, $|S^2| = |A + r * A|$ and hence, by Theorem 5, $|S^2| \ge \max(4k - 4, 1) \ge 3k - 2$, as required. □

The final application deals with subsets of $BS(1, 2)$ of type $S = b^m a^A$ for $m \ge 2$.

Corollary 2. *Let* $S \subseteq BS(1, 2)$ *be a finite set of size* $k = |S| \ge 1$ *and suppose that*

$$S = b^m a^A,$$

where $m \ge 2$ *is an integer and* $A \subseteq \mathbb{Z}$ *is a finite set of integers.*

Then

$$S^2 = b^{2m} a^{A + 2^m * A} \tag{16}$$

and

$$|S^2| = |A + 2^m * A| \ge \max(4k - 4, 1) \ge 3k - 2. \tag{17}$$

Proof. By Theorem 1, $|S^2| = |A + 2^m * A|$. Since $2^m > 3$, it follows by Theorem 5 that $|S^2| \ge \max(4k - 4, 1) \ge 3k - 2$, as required. □

Acknowledgments

The authors are grateful to the referees for their constructive remarks.

References

[1] E. Breuillard, B. Green, T. Tao, The structure of approximate groups, Publ. Math. Inst. Hautes Études Sci. 116 (2012) 115–221.
[2] B. Bukh, Sums of dilates, Combin. Probab. Comput. 17 (5) (2008) 627–639.
[3] J. Cilleruelo, Y.O. Hamidoune, O. Serra, On sums of dilates, Combin. Probab. Comput. 18 (6) (2009) 871–880.
[4] J. Cilleruelo, M. Silva, C. Vinuesa, A sumset problem, J. Combin. Number Theory 2 (1) (2010) 79–89.
[5] G.A. Freiman, Foundations of A Structural Theory of Set Addition, in: Translations of Mathematical Monographs, vol. 37, Amer. Math. Soc., Providence, Rhode Island, 1973.
[6] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, Small doubling in ordered groups, J. Aust. Math. Soc. (2014) in print.
[7] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, Y.V. Stanchescu, A small doubling structure theorem in a Baumslag–Solitar group (see Theorem 7 in: Inverse problems in Additive Number Theory and in Non-Abelian Group Theory, 2013, pp. 1–31. arXiv:1303.3053v1). submitted for publication.
[8] B. Green, What is . . . an approximate group? Notices Amer. Math. Soc. 59 (5) (2012) 655–656.
[9] Y.O. Hamidoune, A. Plagne, A generalization of Freiman's $3k-3$ theorem, Acta Arith. 103 (2) (2002) 147–156.
[10] Y.O. Hamidoune, J. Rué, A lower bound for the size of a Minkowski sum of dilates, Combin. Probab. Comput. 20 (2) (2011) 249–256.
[11] V.F. Lev, P.Y. Smeliansky, On addition of two distinct sets of integers, Acta Arith. 70 (1) (1995) 85–91.
[12] Z. Ljujić, A lower bound for the size of a sum of dilates, J. Combin. Number Theory 5 (1) (2013) 31–51.
[13] M.B. Nathanson, Inverse problems for linear forms over finite sets of integers, J. Ramanujan Math. Soc. 23 (2) (2008) 151–165.
[14] A. Plagne, Sum of dilates in groups of prime order, Combin. Probab. Comput. 20 (6) (2011) 867–873.
[15] G.F. Pontiveros, Sums of dilates in $\mathbb{Z}_p$, 2012. arXiv:1203.2659v2.
[16] I.Z. Ruzsa, Generalized arithmetical progressions and sumsets, Acta Math. Hungar. 65 (4) (1994) 379–388.
[17] D. Shan-Shan, C. Hui-Qin, S. Zhi-Wei, On a sumset problem for integers, 2010. arXiv:1011.5438.
[18] Y.V. Stanchescu, On addition of two distinct sets of integers, Acta Arith. 75 (2) (1996) 191–194.
[19] Y.V. Stanchescu, On the structure of sets with small doubling property on the plane. I., Acta Arith. 83 (2) (1998) 127–141.
[20] Y.V. Stanchescu, The structure of d-dimensional sets with small sumset, J. Number Theory 130 (2) (2010) 289–303.
[21] T.C. Tao, Product set estimates for noncommutative groups, Combinatorica 28 (5) (2008) 547–594.