Combinatorics, Probability and Computing (2009) 18, 871–880. © Cambridge University Press 2009
doi:10.1017/S0963548309990307 First published online 9 July 2009

On Sums of Dilates

JAVIER CILLERUELO[1]†, YAHYA O. HAMIDOUNE[2]
and ORIOL SERRA[3]

[1]Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049-Madrid, Spain
(e-mail: franciscojavier.cilleruelo@uam.es)

[2]UPMC Université Paris 06, E. Combinatoire, Case 189, 4 Place Jussieu, 75005 Paris, France
(e-mail: hamidoune@math.jussieu.fr)

[3]Universitat Politécnica de Catalunya, Jordi Girona, 1, E-08034 Barcelona, Spain
(e-mail: oserra@ma4.upc.edu)

Received 27 February 2009; revised 26 May 2009

For k prime and A a finite set of integers with $|A| \geqslant 3(k-1)^2(k-1)!$ we prove that $|A + k \cdot A| \geqslant (k+1)|A| - \lceil k(k+2)/4 \rceil$ where $k \cdot A = \{ka : a \in A\}$. We also describe the sets for which equality holds.

1. Introduction

Let k be a positive integer and let $A \subset \mathbb{Z}$. We let $k \cdot A = \{ka : a \in A\}$ denote the k-dilation of A, and let $kA = A + \cdots + A$ (k-times) be the k-fold sumset of A. We observe that $A + k \cdot A \subset A + kA = (k+1)A$ and that, in general, $A + k \cdot A$ is much smaller than $(k+1)A$. It is well known that $|(k+1)A| \geqslant (k+1)|A| - k$, and that equality holds only if A is an arithmetic progression. Indeed, if A is an arithmetic progression with $|A| \geqslant k$, one can check that $A + k \cdot A = (k+1)A$. So it is a natural problem to study lower bounds for $|A + k \cdot A|$ as well as the description of the extremal cases.

The case $k = 1$ is trivial since $|A + A| \geqslant 2|A| - 1$ and equality holds for arithmetic progressions. The case $k = 2$ (see [3]) is also easy since we can split $A = A_1 \cup A_2$ into the two classes (mod 2), and then $|A + 2 \cdot A| = |A_1 + 2 \cdot A| + |A_2 + 2 \cdot A| \geqslant |A_1| + |2 \cdot A| - 1 + |A_2| + |2 \cdot A| - 1 = 3|A| - 2$. (If A contains only one class we write $A = 2 \cdot A' + i$ and then

† Supported by Project MTM2008-03880 from MYCIT (Spain) and the joint Madrid Region-UAM project TENU3 (CCG08-UAM/ESP-3906).

$|A+2\cdot A|=|A'+2\cdot A'|$.) It is shown in [2] that $|A+2\cdot A|=3|A|-2$ only when A is an arithmetic progression.

The cases $k\geqslant 3$ are much more involved. Nathanson [3] proved that $|A+k\cdot A|\geqslant \lfloor \frac{7}{2}|A|-\frac{5}{2}\rfloor$ for $k\geqslant 3$ and Bukh [1] proved that $|A+3\cdot A|\geqslant 4|A|-C$ for some constant C. Cilleruelo, Silva and Vinuesa [2] obtained the sharp bound and the description of the extremal cases for $k=3$.

Theorem 1.1 ([2]). *For any set of integers A we have $|A+3\cdot A|\geqslant 4|A|-4$. Furthermore, if $|A+3\cdot A|=4|A|-4$, then $A=3\cdot\{0,\dots,n\}+\{0,1\}$, or $A=\{0,1,3\}$, or $A=\{0,1,4\}$ or A is an affine transformation of any of these sets.*

They proposed the following conjecture.

Conjecture (Cilleruelo, Silva and Vinuesa [2]). *For every positive integer k and a finite set of integers A with sufficiently large cardinality, we have*

$$|A+k\cdot A|\geqslant (k+1)|A|-\lceil k(k+2)/4\rceil.$$

Bukh's main theorem [1] states that, for $(\lambda_1,\dots,\lambda_t)\in\mathbb{Z}^t$ with $\gcd(\lambda_1,\dots,\lambda_t)=1$,

$$|\lambda_1\cdot A+\cdots+\lambda_t\cdot A|\geqslant (|\lambda_1|+\cdots+|\lambda_t|)|A|-o(|A|).$$

This general result implies $|A+k\cdot A|\geqslant (k+1)|A|-o(|A|)$ in our problem. The existence of a simple proof for $|A+k\cdot A|\geqslant (k+1)|A|-C_k$ for $k\geqslant 4$ is implicitly asked by Bukh in [1].

When k is prime we give a positive answer to the above questions by proving a precise version of the conjecture above. In addition we characterize the extremal sets A for the lower bound in that conjecture. Since $|A+k\cdot A|$ is invariant under affine transformations, we will assume without loss of generality that $0\in A$ and $\gcd(A)=1$.

Theorem 1.2. *Let k be a prime and let A be a subset of $\mathbb{Z}$ with $\min A=0$, $\gcd(A)=1$ and $|A|\geqslant 3|\hat{A}|^2(k-1)!$, where $\hat{A}$ is the projection of A in $\mathbb{Z}/k\mathbb{Z}$. Then*

$$|A+k\cdot A|\geqslant (k+1)|A|-|\hat{A}|(k+1-|\hat{A}|). \tag{1.1}$$

Furthermore, if $|\hat{A}|<k$, equality holds in (1.1) *only if*

$$A=k\cdot\{0,1,\dots,n\}+\{0,1,\dots,|\hat{A}|-1\} \tag{1.2}$$

for some n, while if $|\hat{A}|=k$, equality holds in (1.1) *only if A is an arithmetic progression.*

If $|\hat{A}|=k$, one can obtain

$$|A+k\cdot A|\geqslant (k+1)|A|-k,$$

under the weaker hypothesis $|A|>k$, and equality holds only when A is an arithmetic progression. This case is contained in Corollary 2.2 below.

The next corollary follows from Theorem 1.2 and Corollary 2.2.

Corollary 1.3. *Let k be an odd prime and let A be a subset of $\mathbb{Z}$ with $|A| \geqslant 3(k-1)^2(k-1)!$. Then*

$$|A + k \cdot A| \geqslant (k+1)|A| - \lceil k(k+2)/4 \rceil. \tag{1.3}$$

Moreover, up to affine transformations, equality holds in (1.3) *only if*

$$A = k \cdot \{0, 1, \ldots, n\} + \{0, 1, \ldots, (k-1)/2\} \tag{1.4}$$

for some n.

Theorem 1.2 implies in particular that, for k prime and any set A, we have $|A + k \cdot A| \geqslant (k+1)|A| - C_k$ for a suitable constant C_k. Indeed, Lemma 4.1 below shows that inequality holds with $C_k = 3(k-1)!$.

Small sets are more difficult to deal with. For example, if $k = 3$, Theorem 1.2 covers Theorem 1.1 only when $|A| \geqslant 24$. Smaller sets have to be analysed more carefully, as was done in [2] with a particular approach. Actually the lower bound (1.1) does not hold for an arbitrary set. In [2] it is shown that there exist small sets A for which $|A + k \cdot A| \leqslant (k+1)|A| - P(k)$, where P is a cubic polynomial.

The paper is organized as follows. We first give some notation and preliminary results in Section 2. We then show in Section 3 that, for the class of so-called k-full sets, which actually contain the extremal ones, Theorem 1.2 is relatively easy to prove. In Section 4 we give a universal weaker lower bound for the cardinality of $A + k \cdot A$, and we use it to show in the final section that, for sufficiently large sets which are not k-full, we get a better lower bound for $|A + k \cdot A|$ than that of Theorem 1.2, thus completing its proof.

2. Notation and preliminary results

For two finite non-empty sets of integers A and B, it is well known that $|A + B| \geqslant |A| + |B| - 1$, and that equality holds only if either $\min\{|A|, |B|\} = 1$ or both A and B are arithmetic progressions with the same common difference. We next give a generalization of the above inequality for $|A + k \cdot B|$.

A maximal subset of $X \subset \mathbb{Z}$ of congruent elements modulo k will be called a *k-component* of X.

Lemma 2.1. *For arbitrary non-empty sets of integers A and B with $|B| > 1$, we have*

$$|A + k \cdot B| \geqslant |A| + |\hat{A}|(|B| - 1),$$

where $\hat{A}$ denotes the natural projection of A onto $\mathbb{Z}/k\mathbb{Z}$.

Furthermore, if equality holds and A has a k-component C with $|C| > 1$, then both C and $k \cdot B$ are arithmetic progressions with the same difference.

Proof. Observe that $A + k \cdot B$ is the disjoint union $\cup_{i \in \hat{A}}(A_i + k \cdot B)$, where A_i are the distinct k-components of A. Write $A_i = k \cdot X_i + u_i$. We have

$$\begin{aligned} |A + k \cdot B| &= |\cup_{i \in \hat{A}} (k \cdot X_i + u_i + k \cdot B)| \\ &= \sum_{i \in \hat{A}} |X_i + B| \geqslant \sum_{i \in \hat{A}} (|X_i| + |B| - 1) = |A| + |\hat{A}|(|B| - 1). \end{aligned}$$

To prove the second part of the statement, suppose that equality holds and let $C = A_r = k \cdot X_r + u_r$. Then $|X_r + B| = |X_r| + |B| - 1$, which implies that both X_r and B are arithmetic progressions with the same difference and the same is true of A_r and $k \cdot B$. □

Lemma 2.1 easily handles the case when $|\hat{A}| = k$, as described in the next corollary.

Corollary 2.2. *Let A be a set of integers with $|\hat{A}| = k$ and $|A| > k$. Then we have*

$$|A + k \cdot A| \geqslant (k+1)|A| - k,$$

and equality holds only if A is an arithmetic progression.

Proof. The inequality follows from Lemma 2.1. For the inverse part, we observe that $|A_r| \geqslant 2$ for some r, and Lemma 2.1 implies that the set $k \cdot A$ must be an arithmetic progression. Hence A must be an arithmetic progression as well. □

Throughout the paper we use the following notation. For a set A we let $\hat{A}$ denote the natural projection of A on $\mathbb{Z}/k\mathbb{Z}$. We simply write $\hat{a}$ if $A = \{a\}$. We write $j = |\hat{A}|$ and $A_1, \ldots, A_j$ for the distinct classes of A modulo k. We also write $A_i = k \cdot X_i + u_i,\ i = 1, \ldots, j$ for some distinct u_i modulo k. Thus,

$$A = \bigcup_{i=1}^{j} A_i = \bigcup_{i=1}^{j} (k \cdot X_i + u_i).$$

Unless explicitly stated, we will always assume that $|A_1| \geqslant |A_2| \geqslant \cdots \geqslant |A_j|$. Also, we write

$$F = \{i :\ |\hat{X}_i| = k\}, \qquad A_F = \bigcup_{i \in F} A_i,$$

$$E = \{i :\ 0 < |\hat{X}_i| < k\}, \qquad A_E = \bigcup_{i \in E} A_i.$$

Let

$$\Delta_{rs} = (A_r + k \cdot A) \setminus (A_r + k \cdot A_s),$$

so that

$$|A_r + k \cdot A| = |A_r + k \cdot A_s| + |\Delta_{rs}| = |X_r + k \cdot X_s| + |\Delta_{rs}|. \tag{2.5}$$

Lemma 2.3. *For each subset $I \subset \{1, 2, \ldots, j\}$ and each $r \in \{1, 2, \ldots, j\}$, we have:*
(i) $\sum_{i \in I} |\Delta_{ii}| \geqslant |I|(|I| - 1)$,
(ii) $\sum_{i \in I} |\Delta_{ri}| \geqslant |I|(|I| - 1)$,

Proof. Let

$$\Delta_{rs}^{+} = (A_r + k \cdot A) \setminus (-\infty, \max(A_r + k \cdot A_s)],$$

and

$$\Delta_{rs}^{-} = (A_r + k \cdot A) \setminus [\min(A_r + k \cdot A_s), \infty),$$

so that

$$|\Delta_{rs}| \geqslant |\Delta_{rs}^+| + |\Delta_{rs}^-|.$$

Let $\Gamma^+(s) = \{h : \max(A_s) < \max(A_h)\}$ and $\Gamma^-(s) = \{h : \min(A_s) > \min(A_h)\}$. Clearly $\max(A_r + k \cdot A_s) < \max(A_r + k \cdot A_h)$, for every $h \in \Gamma^+(s)$. Since, for distinct h, the elements on the right-hand side of the last inequality belong to distinct congruence classes modulo k^2, we have $|\Delta_{rs}^+| \geqslant |\Gamma^+(s)|$. By replacing A by $-A$, we obtain $|\Delta_{rs}^-| \geqslant |\Gamma^-(s)|$.

Observe that $|\Gamma^+(u)| > |\Gamma^+(v)|$ if $\max(A_u) < \max(A_v)$. In particular, the numbers $|\Gamma^+(u)|$, $u = 1, \ldots, j$ are pairwise distinct. Since $|\Gamma^+(u)| \leqslant j - 1$, it follows that

$$\{|\Gamma^+(u)| : u = 1, 2, \ldots, j\} = \{0, 1, \ldots, j - 1\}.$$

By replacing A by $-A$, we get $\{|\Gamma^-(u)| : u = 1, 2, \ldots, j\} = \{0, 1, \ldots, j - 1\}$ as well. Therefore,

$$\sum_{i \in I} |\Delta_{ii}| \geqslant \sum_{i \in I} |\Delta_{ii}^+| + \sum_{i \in I} |\Delta_{ii}^-| \geqslant \sum_{i \in I} |\Gamma^+(i)| + \sum_{i \in I} |\Gamma^-(i)| \geqslant |I|(|I| - 1),$$

which proves (i). Similarly,

$$\sum_{i \in I} |\Delta_{ri}| \geqslant \sum_{i \in I} |\Gamma^+(i)| + \sum_{i \in I} |\Gamma^-(i)| \geqslant |I|(|I| - 1),$$

and (ii) follows. □

Lemma 2.4. *Let k be a prime and assume the notation above. Then:*

(i) *if $i \in E$ then $|\Delta_{ii}| \geqslant |A_s|$ for any $s \neq i$,*
(ii) $\sum_{i \in E} |\Delta_{ii}| \geqslant (|E| - 1)|A_1| + |A_2|$.

Proof. (i) Suppose that $\hat{X}_i + x = \hat{X}_i + y$ for distinct $x, y \in \mathbb{Z}/k\mathbb{Z}$. Then $\hat{X}_i = \hat{X}_i + (y - x) = \hat{X}_i + 2(y - x) = \cdots = \hat{X}_i + (k - 1)(y - x)$, which implies $\hat{X}_i = \mathbb{Z}/k\mathbb{Z}$, as k is prime. Hence, if $i \in E$ and $s \neq i$ then $\hat{X}_i + \hat{u}_s \neq \hat{X}_i + \hat{u}_i$. Thus $|(\hat{X}_i + \hat{u}_s) \setminus (\hat{X}_i + \hat{u}_i)| \geqslant 1$. Now we have

$$\begin{aligned} |\Delta_{ii}| &= |(A_i + k \cdot A) \setminus (A_i + k \cdot A_i)| \geqslant |(k \cdot X_i + u_i + k \cdot A_s) \setminus (k \cdot X_i + u_i + k \cdot A_i)| \\ &= |(X_i + A_s) \setminus (X_i + A_i)| = |(X_i + k \cdot X_s + u_s) \setminus (X_i + k \cdot X_i + u_i)| \\ &\geqslant |X_s||(\hat{X}_i + \hat{u}_s) \setminus (\hat{X}_i + \hat{u}_i)| \geqslant |X_s| = |A_s|. \end{aligned}$$

(ii) We observe that (i) implies that $|\Delta_{ii}| \geqslant |A_1|$ for all $i \in E$ except for $i = 1$, when $1 \in E$. In that case we have $|\Delta_{11}| \geqslant |A_2|$. □

3. Full sets

We say that a set A is *k-full* if $|\hat{X}_i| = k$ for each $i = 1, 2, \ldots, j$. The following lemma proves Theorem 1.2 for *k-full* sets and all k with a weaker condition on their cardinality. Since Corollary 2.2 proves Theorem 1.2 for $j = k$, we can assume that $j < k$.

Lemma 3.1. *Let A be a finite k-full set of integers with* $\min(A) = 0$, $\gcd(A) = 1$, $|A| > jk$ *and* $j < k$. *Then*

$$|A + k \cdot A| \geqslant (k + 1)|A| - j(k - j + 1).$$

Moreover, equality holds if and only if

$$A = k \cdot \{0, 1, \dots, n\} + \{0, 1, \dots, j-1\}$$

for some n.

Proof. We apply (2.5) and Lemma 2.1 to get, for each $s = 1, \dots, j$,

$$\begin{aligned} |A + k \cdot A| &= \sum_{i=1}^{j} |A_i + k \cdot A| = \sum_{i=1}^{j} \big(|X_i + k \cdot X_s| + |\Delta_{is}|\big) \\ &\geqslant \sum_{i=1}^{j} \big(|X_i| + k(|X_s| - 1) + |\Delta_{is}|\big) \geqslant |A| + kj|X_s| - kj + \sum_{i=1}^{j} |\Delta_{is}|. \end{aligned} \tag{3.1}$$

If we sum over all $s = 1, \dots, j$ and divide by j, we obtain

$$\begin{aligned} |A + k \cdot A| &\geqslant (k+1)|A| - kj + \frac{1}{j} \sum_{s=1}^{j} \sum_{i=1}^{j} |\Delta_{is}| \\ &= (k+1)|A| - kj + \frac{1}{j} \sum_{i=1}^{j} \sum_{s=1}^{j} |\Delta_{is}| \\ &\geqslant (k+1)|A| - j(k+1-j), \end{aligned} \tag{3.2}$$

due to Lemma 2.3(ii). This proves the lower bound.

For the inverse part of the lemma and only until the end of this proof, we next order the k-components $A_1, A_2, \dots, A_j$ of A in such a way that $0 = m_1 < m_2 < \cdots < m_j$, where $m_i = \min(A_i)$ (so we do not assume they are decreasing in cardinality).

Suppose that equality holds in (1.1). Since there is equality in (3.1), we have $|X_i + k \cdot X_s| = |X_i| + k(|X_s| - 1)$ for all i, s. Since $|A| > jk$, we have $|X_i| > k$ for some i, so that one of the k-components of this X_i has at least two elements. Lemma 2.1 implies that all X_s are arithmetic progressions with the same difference d. So, for $i = 1, \dots, j$ we have

$$A_i = (kd) \cdot \{0, 1, \dots, n_i\} + m_i$$

for some $n_i \geqslant k - 1$, where $m_i = \min(A_i)$ and $|A| = \sum_{i=1}^{j} (n_i + 1)$.

Observe that, since $n_i \geqslant k - 1$, we have

$$\begin{aligned} A_i + k \cdot A_r &= m_i + (kd) \cdot \{0, 1, \dots n_i\} + k \cdot (m_r + (kd) \cdot \{0, 1, \dots, n_r\}) \\ &= m_i + km_r + (kd) \cdot (\{0, 1, \dots, n_i\} + k \cdot \{0, 1, \dots, n_r\}) \\ &= m_i + km_r + (kd) \cdot \{0, 1, \dots, n_i + kn_r\}, \end{aligned} \tag{3.3}$$

so that $A_i + k \cdot A_r$ is an arithmetic progression for each i and r.

First we will prove that $m_r \equiv 0 \pmod{d}$ for all r. Otherwise, if we write R_0 for those r with $m_r \equiv 0 \pmod{d}$ (which contains m_1) and R_1 for those r with $m_r \not\equiv 0 \pmod{d}$ (which is also

non-empty by assumption), we have

$$\begin{aligned}
|A + k\cdot A| &= \sum_{i=1}^{j} |A_i + k\cdot A| = \sum_{i=1}^{j} \Big|\bigcup_r (A_i + k\cdot A_r)\Big| \\
&= \sum_{i=1}^{j} \Big|\bigcup_r \big(m_i + km_r + (kd)\cdot\{0,1,\dots,n_i + kn_r\}\big)\Big| \\
&= \sum_{i=1}^{j} \Big|\bigcup_r \big(m_r + d\cdot\{0,1,\dots,n_i + kn_r\}\big)\Big| \\
&= \sum_{i=1}^{j} \Bigg(\Big|\bigcup_{r\in R_0} \big(d\cdot\{0,\dots,kn_r + n_i\} + m_r\big)\Big| \\
&\qquad + \Big|\bigcup_{r\in R_1} \big(d\cdot\{0,\dots,kn_r + n_i\} + m_r\big)\Big|\Bigg) \\
&\geqslant \sum_{i=1}^{j} \Big(n_i + 1 + k\max_{r\in R_0} n_r\Big) + \sum_{i=1}^{j} \Big(n_i + 1 + k\max_{r\in R_1} n_r\Big) \\
&= 2|A| + kj\Big(\max_{r\in R_0} n_r + \max_{r\in R_1} n_r\Big) \geqslant 2|A| + kj\Big(k - 1 + \max_r n_r\Big) \\
&= 2|A| + kj\Big(k - 2 + \max_r (n_r + 1)\Big) \geqslant 2|A| + kj\Big(k - 2 + \frac{|A|}{j}\Big) \\
&\geqslant (2+k)|A| > (k+1)|A|,
\end{aligned}$$

and equality (1.1) cannot hold.

Now, since $\gcd(A) = 1$, we have that $d = 1$. It follows, by (3.3), that

$$A_i + k\cdot A = \bigcup_{r=1}^{j} (A_i + k\cdot A_r) = \bigcup_{r=1}^{j} \big(m_i + km_r + k\cdot\{0,1,\dots,kn_r + n_i\}\big). \tag{3.4}$$

By using the notation from the proof of Lemma 2.3, for each i and for each $r \geqslant 2$, the set $\Delta_{ir}^- = (A_i + k\cdot A) \setminus [\min(A_i + k\cdot A_r), \infty)$ clearly contains $m_i + km_1, m_i + km_2, \dots, m_i + km_{r-1}$. It follows that

$$\sum_{r=1}^{j} |\Delta_{ir}^-| \geqslant \sum_{r=2}^{j} (r-1) = j(j-1)/2.$$

By the analogous argument on $-A$ we also have $\sum_{r=1}^{j} |\Delta_{ir}^+| \geqslant j(j-1)/2$.

Since there is equality in (3.2), we have $\sum_{s=1}^{j} \Delta_{is} = j(j-1)$ for each i. It follows that $\sum_{r=1}^{j} |\Delta_{ir}^-| = \sum_{r=1}^{j} |\Delta_{ir}^+| = j(j-1)/2$. Hence

$$\Delta_{ir}^- = m_i + k\cdot\{m_1, m_2, \dots, m_{r-1}\},\ r = 2, 3, \dots, j. \tag{3.5}$$

We claim that $m_{r-1} + 1 = m_r$ for each $2 \leqslant r \leqslant j$. Suppose, on the contrary, that $m_{r-1} + 1 < m_r$ (we have assumed that $0 = m_1 < \cdots < m_j$). Then $m_i + k(m_{r-1} + 1) < \min(A_i + k\cdot A_r)$. On

the other hand, by (3.4), we have $m_i + k(m_{r-1}+1) \in m_i + km_r + k\cdot\{0,1,\dots,kn_r+n_i\} \subset A_i + k\cdot A$. Thus $m_i + k(m_{r-1}+1) \in \Delta^-_{ir}$, which is a contradiction because $\max \Delta^-_{ir} = m_i + km_{r-1} < m_i + k(m_{r-1}+1)$.

Since $m_1 = 0$, we conclude that $m_r = r-1$ for $r = 1,\dots,j$. Thus $[0, j-1] \subset A$.

By applying the above argument to $-A + \max(A)$, we conclude that the set A also contains the interval $[\max(A)-(j-1), \max(A)]$. Since each A_i is an arithmetic progression of difference k and $j < k$, we must have $\max(A) - (j-1) \equiv 0 \pmod k$ and $n_1 = \cdots = n_j$. This completes the proof. □

4. A general lower bound

In this section we give a weaker lower bound for $|A + k\cdot A|$ valid for every finite set A of integers and k prime.

Lemma 4.1. *Let k be a prime and let A be a finite non-empty subset of $\mathbb{Z}$. We have*

$$|A + k\cdot A| \geqslant (k+1)|A| - 3(k-1)!. \tag{4.1}$$

Proof. Let t be the largest integer such that, for every finite set X of integers,

$$|X + k\cdot X| \geqslant (t+1)|X| - 3(t-1)!.$$

Suppose that $t < k$ and let A be a critical set, verifying $|A + k\cdot A| < (t+2)|A| - 3t!$. Without loss of generality we may assume that $0 \in A_1$ and $\gcd(A) = 1$. In particular $j = |\hat{A}| \geqslant 2$.

Lemma 2.1 gives $|A + k\cdot A| \geqslant (j+1)|A| - j$. Therefore $t \geqslant j$.

We have

$$|A + k\cdot A| = \sum_{i\in F} |A_i + k\cdot A| + \sum_{i\in E} |A_i + k\cdot A|. \tag{4.2}$$

We have

$$\begin{aligned}
\sum_{i\in F} |A_i + k\cdot A| &\geqslant \sum_{i\in F} |A_i + k\cdot A_1| \\
&= \sum_{i\in F} |X_i + k\cdot X_1| \\
\text{(by Lemma 2.1)} \quad &\geqslant \sum_{i\in F} (|X_i| + k(|X_1|-1)) \\
&= \sum_{i\in F} (|A_i| + k(|A_1|-1)) \\
\text{(since } t \leqslant k-1) \quad &\geqslant |A_F| + (t+1)|F|(|A_1|-1) \\
\text{(since } t|A_1||F| \geqslant t|A_F|) \quad &\geqslant (t+1)|A_F| + |F||A_1| - (t+1)|F|.
\end{aligned} \tag{4.3}$$

On the other hand, by (2.5), Lemma 2.4(ii) and the assumption on t,

$$\begin{aligned}\sum_{i\in E}|A_i + k\cdot A| &= \sum_{i\in E}(|A_i + k\cdot A_i| + |\Delta_{ii}|)\\ &\geqslant \sum_{i\in E}\big((t+1)|A_i| - 3(t-1)!\big) + \sum_{i\in E}|\Delta_{ii}|\\ &\geqslant (t+1)|A_E| - 3|E|(t-1)! + (|E|-1)|A_1| + |A_2|. \end{aligned} \tag{4.4}$$

By substitution of (4.3) and (4.4) in (4.2), we get

$$\begin{aligned}|A + k\cdot A| &\geqslant (t+1)|A| + (|F| + |E| - 1)|A_1| + |A_2| - (t+1)|F| - 3|E|(t-1)!\\ &\geqslant (t+2)|A| - (t+1)|F| - 3|E|(t-1)!,\end{aligned}$$

since $(|F| + |E| - 1)|A_1| + |A_2| = (j-1)|A_1| + |A_2| \geqslant |A_1| + |A_2| + \cdots + |A_j| = |A|$. Finally, since $|E| + |F| = j \leqslant t$, we have

$$\begin{aligned}3|E|(t-1)! + (t+1)|F| &\leqslant 3(t-|F|)(t-1)! + (t+1)|F|\\ &\leqslant 3t! + |F|(t+1-3(t-1)!) \leqslant 3t!,\end{aligned}$$

which contradicts our choice of A. This contradiction proves the statement. □

5. Proof of Theorem 1.2

Suppose now that $|A| \geqslant 3j^2(k-1)!$. By Lemma 3.1 and Corollary 2.2 we may assume $E \neq \emptyset$ and $j < k$.

Case 1. There exists $s \geqslant 2$ with $s \in E$.
By (2.5), Lemma 4.1 and Lemma 2.4(i), we obtain

$$\begin{aligned}|A + k\cdot A| &= |A_s + k\cdot A| + \sum_{i\neq s}|A_i + k\cdot A|\\ &\geqslant |X_s + k\cdot X_s| + |\Delta_{ss}| + \sum_{i\neq s}|X_i + k\cdot X_i|\\ &\geqslant (k+1)|A_s| - 3(k-1)! + |A_1| + \sum_{i\neq s}((k+1)|A_i| - 3(k-1)!)\\ &\geqslant (k+1)|A| - 3j(k-1)! + \frac{|A|}{j}\\ &\geqslant (k+1)|A|,\end{aligned}$$

since $|A| \geqslant 3j^2(k-1)!$.

Case 2. $E = \{1\}$.
In this case, since $|\hat{X}_2| = k$, Lemma 2.1 implies that

$$|X_2 + k\cdot X_1| \geqslant |X_2| + k(|X_1| - 1) = |A_2| + k|A_1| - k. \tag{5.1}$$

We observe also (by Lemma 2.4(i)) that $|\Delta_{11}| \geqslant |A_2|$.

Then, by (2.5), Lemma 4.1, Lemma 2.4(i) and (5.1), we have

$$\begin{aligned}
|A + k\cdot A| &= |A_1 + k\cdot A| + |A_2 + k\cdot A| + \sum_{i\geqslant 3} |A_i + k\cdot A| \\
&\geqslant |X_1 + k\cdot X_1| + |\Delta_{11}| + |X_2 + k\cdot X_1| + \sum_{3\leqslant i\leqslant j} |X_i + k\cdot X_i| \\
&\geqslant (k+1)|A_1| - 3(k-1)! + |A_2| + (|A_2| + k|A_1| - k) \\
&\qquad + \sum_{3\leqslant i\leqslant j} ((k+1)|A_i| - 3(k-1)!) \\
&\geqslant |A_1| + (k+1)|A| - 3(j-1)(k-1)! - k \\
&\geqslant \frac{|A|}{j} + (k+1)|A| - 3j(k-1)! \\
&\geqslant (k+1)|A|,
\end{aligned}$$

since $|A| \geqslant 3j^2(k-1)!$.

This completes the proof.

Acknowledgements

The authors wish to thank an anonymous referee for very helpful remarks, and particularly for the suggested simplification of the proof of Lemma 3.1.

References

[1] Bukh, B. (2008) Sums of dilates. *Combin. Probab. Comput.* **17** 627–639.
[2] Cilleruelo, J., Silva, M. and Vinuesa, C. A sumset problem. Preprint.
[3] Nathanson, M. B. Inverse problems for linear forms over finite sets of integers. Available from: `arXiv:0708.2304`.