ON SUMS OF DILATES

JAVIER CILLERUELO, YAHYA O. HAMIDOUNE, AND ORIOL SERRA

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

1. Introduction

Let k be a positive integer and let $A \subset \mathbb{Z}$. We denote by $k\cdot A = \{ka,\ a\in A\}$ the k–dilation of A and by $kA = A+\cdots+A$ (k–times) 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 $|(k+1)A| \geq (k+1)|A|-k$ and that the equality holds only if A is an arithmetic progression. Indeed, if A is an arithmetic progression with $|A|\geq k$ 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 $|A+A|\geq 2|A|-1$ and the equality holds for arithmetic progressions. The case $k=2$ (see [3]) is also easy since we can split $A=A_1\cup A_2$ in the two classes $\pmod 2$ and then $|A+2\cdot A| = |A_1+2\cdot A|+|A_2+2\cdot A| \geq |A_1|+|2\cdot A|-1+|A_2|+|2\cdot A|-1 = 3|A|-2$. (If A contains only a class we write $A=2\cdot A'+i$ and then $|A+2\cdot A| = |A'+2\cdot A'|$). It is shown in [2] that $|A+2\cdot A|=3|A|-2$ only when A is an arithmetic progression.

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

Theorem 1 ([2])**.** *For any set of integers A we have $|A+3\cdot A|\geq 4|A|-4$. 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–Vinuesa [2])**.** *For all positive integer k and a finite set of integers A with sufficiently large cardinality we have*

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

2000 *Mathematics Subject Classification.* 11B60, 11B34, 20D60.

J. C. was supported by Project MTM2008-03880 from MYCIT (Spain) and the joint Madrid Region-UAM project TENU3 (CCG08-UAM/ESP-3906).

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

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

This general result implies $|A + k \cdot A| \geq (k+1)|A| - o(|A|)$ in our problem. The existence of a simple proof for $|A + k \cdot A| \geq (k+1)|A| - C_k$ for $k \geq 4$ 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 Conjecture above. In addition we characterize the extremal sets A for the lower bound in that conjecture. Since $|A + k \cdot A|$ is invariant by affine transformations we will assume without loss of generality that $0 \in A$ and $\gcd(A) = 1$.

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

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

Furthermore if $|\hat{A}| < k$ equality holds in (1) only if

$$A = k \cdot \{0, 1, \ldots, n\} + \{0, 1, \ldots, |\hat{A}| - 1\} \tag{2}$$

for some n, while if $|\hat{A}| = k$, equality holds in (1) only if A is an arithmetic progression.

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

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

under the weaker hypothesis $|A| > k$ and equality holds only when A is an arithmetic progression. This case is contained in Corollary 5 below.

The following Corollary follows from Theorem 2.

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

$$|A + k \cdot A| \geq (k+1)|A| - \lceil k(k+2)/4 \rceil. \tag{3}$$

Moreover, up to affine transformations, equality holds in (3) only if

$$A = k \cdot \{0, 1, \ldots, n\} + \{0, 1, \ldots, (k-1)/2\} \tag{4}$$

for some n.

Theorem 2 implies in particular that, for k prime and any set A, we have $|A + k \cdot A| \geq (k+1)|A| - C_k$ for a suitable constant C_k. Indeed, Lemma 9 below shows that the inequality holds with $C_k = 3(k-1)!$.

Small sets are more difficult to deal with. For example, in case $k = 3$, Theorem 2 covers Theorem 1 only when $|A| \geq 24$. Smaller sets have to be analyzed more carefully as it was done in [2] with a distinct approach. Actually the lower bound (1) does not hold for an arbitrary set. In [2] it is shown that there exist small sets A for which $|A + k \cdot A| \leq (k+1)|A| - P(k)$ 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 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 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 the one in Theorem 2 thus completing its proof.

2. Notation and preliminary results

For two finite nonempty sets of integers A and B it is well known that $|A + B| \geq |A|+|B|-1$, 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 4. *For arbitrary nonempty sets of integers A and B with $|B| > 1$, we have*

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

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

Furthermore if the 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

$$|A+k\cdot B| = |\cup_{i\in\hat{A}}(k\cdot X_i+u_i+k\cdot B)| = \sum_{i\in\hat{A}}|X_i+B| \geq \sum_{i\in\hat{A}}(|X_i|+|B|-1) = |A|+|\hat{A}|(|B|-1).$$

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 $k \cdot B$. $\square$

Lemma 4 easily handles the case when $|\hat{A}| = k$ as described in next Corollary.

Corollary 5. *Let A be a set of integers with $|\hat{A}| = k$ and $|A| > k$. Then we have*

$$|A + k \cdot A| \geq (k + 1)|A| - k$$

and the equality holds only if A is an arithmetic progression.

Proof. The inequality follows from Lemma 4. For the inverse part, we observe that $|A_r| \geq 2$ for some r, and Lemma 4 implies that the set $k \cdot A$ must be an arithmetic progression. Hence A must be an arithmetic progression as well. $\square$

Throughout the paper we use the following notation. For a set A we write $j = |\hat{A}|$, where $\hat{A}$ is the natural projection of A on $\mathbb{Z}/k\mathbb{Z}$ and $A_1, \ldots, A_j$ for the distinct classes 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,

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

We will always assume that $|A_1| \geq |A_2| \geq \cdots \geq |A_j|$. Also we write

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

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

Denote by

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

so that

$$|A_r + k \cdot A| = |A_r + k \cdot A_s| + |\Delta_{rs}| = |X_r + k \cdot X_s| + |\Delta_{rs}|. \tag{5}$$

Lemma 6. *For each subset $I \subset \{1, 2, \ldots, j\}$ and each $r \in \{1, 2, \ldots, j\}$, we have*

i) $\sum_{i \in I} |\Delta_{ii}| \geq |I|(|I| - 1)$,
ii) $\sum_{i \in I} |\Delta_{ri}| \geq |I|(|I| - 1)$,

Proof. Let

$$\Delta^+_{r,s} = (A_r + k \cdot A) \setminus (-\infty, \max(A_r + k \cdot A_s)],$$

and

$$\Delta^-_{r,s} = (A_r + k \cdot A) \setminus [\min(A_r + k \cdot A_s), \infty),$$

so that

$$|\Delta_{r,s}| \geq |\Delta^+_{r,s}| + |\Delta^-_{r,s}|.$$

Denote by $\Gamma^+(s) = \{h : \max(A_s) < \max(A_h)\}$ 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 in the right–hand side of the last inequality belong to distinct congruence classes modulo k^2, we have $|\Delta^+_{rs}| \geq |\Gamma^+(s)|$. By replacing A by $-A$, we obtain $|\Delta^-_{rs}| \geq |\Gamma^-(s)|$.

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 $|\Gamma^+(u)| \leq j - 1$ it follows that

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

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

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

which proves (i). Similarly

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

and (ii) follows. □

Lemma 7. *Let k be a prime and we assume the notation above. Then*

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

Proof. i) Suppose that $\hat{X}_i+x=\hat{X}_i+y$ for distinct $x,y\in\mathbb{Z}_k$. 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 $\hat{X}_i=\mathbb{Z}_k$. Hence, if $i\in E$ and $s\neq i$ then $\hat{X}_i+\hat{u}_s\neq\hat{X}_i+\hat{u}_i$. Thus $|(\hat{X}_i+\hat{u}_s)\setminus(\hat{X}_i+\hat{u}_i)|\geq 1$. Now we have

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

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

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 2 for *k–full* sets and all k with no condition on their cardinality. Since Corollary 5 proves Theorem 2 for $j=k$, we can assume that $j<k$.

Lemma 8. *Let A be a finite k–full set of integers with* $\min(A)=0$ *and $j<k$. Then*

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

Moreover, equality holds if and only if

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

for some n.

Proof. We apply (5) and Lemma 4 to get, for each $s=1,\ldots,j$,

$$\begin{aligned}
|A+k\cdot A| &= \sum_{i=1}^{j}|A_i+k\cdot A|\\
&= \sum_{i=1}^{j}(|X_i+k\cdot X_s|+|\Delta_{is}|)\\
&\geq \sum_{i=1}^{j}(|X_i|+k(|X_s|-1)+|\Delta_{is}|) \qquad (6)\\
&\geq |A|+kj|X_s|-kj+\sum_{i=1}^{j}|\Delta_{is}|.
\end{aligned}$$

If we sum in all $s=1,\ldots,j$ and divide by j we obtain

$$\begin{aligned}
|A+kA| &\geq (k+1)|A|-kj+\frac{1}{j}\sum_{s=1}^{j}\sum_{i=1}^{j}|\Delta_{is}|\\
&= (k+1)|A|-kj+\frac{1}{j}\sum_{i=1}^{j}\sum_{s=1}^{j}|\Delta_{is}| \qquad (7)\\
&\geq (k+1)|A|-j(k+1-j),
\end{aligned}$$

due to Lemma 6. This proves the lower bound.

For the inverse part of the Lemma and only till 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). Since there is equality in (6), we have $|X_i + k \cdot X_s| = |X_i| + k(|X_s| - 1)$ for all i, s and, since $|X_i| \geq k$ for all $i = 1, \dots, j$, Lemma 4 implies that all X_i 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 $n_i \geq k - 1$ where $m_i = \min(A_i)$ and $|A| = \sum_{i=1}^{j} (n_i + 1)$.

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

$$\begin{aligned} A_i + k \cdot A_r &= m_i + (kd) \cdot \{0, 1, \dots n_i\} + k \cdot (m_r + (kd) \cdot \{0, 1, \dots, n_r\}) \\ &= m_i + km_r + (kd) \cdot (\{0, 1, \dots, n_i\} + k \cdot \{0, 1, \dots, n_r\}) \\ &= m_i + km_r + (kd) \cdot \{0, 1, \dots, n_i + kn_r\}, \end{aligned} \tag{8}$$

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 nonempty by assumption) we have

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

and the equality (1) can not hold.

Now, since $gcd(A) = 1$ we have that $d = 1$. It follows, by (8), that

$$A_i + k \cdot A = \bigcup_{r=1}^{j} \left(A_i + k \cdot A_r \right) = \bigcup_{r=1}^{j} \left(m_i + km_r + k \cdot \{0, 1, \dots, kn_r + n_i\} \right). \tag{9}$$

By using the notation from the proof of Lemma 6, for each i and for each $r \geq 2$, the set $\Delta_{i,r}^- = (A_i + k \cdot A) \setminus [\min(A_i + k \cdot A_r), \infty)$ clearly contains $m_i + km_1, m_i + km_2, \ldots, m_i + km_{r-1}$. It follows that

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

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

Since there is equality in (7) 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

$$\Delta_{ir}^- = m_i + k \cdot \{m_1, m_2, \ldots, m_{r-1}\},\ r = 2, 3, \ldots, j. \tag{10}$$

We claim that $m_{r-1} + 1 = m_r$ for any $2 \leq r \leq j$. 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 (9), we have $m_i + k(m_{r-1} + 1) \in m_i + km_r + k \cdot \{0, 1, \ldots, kn_r + n_i\} \subset A_i + k \cdot A$. 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 $r = 1, \ldots, j$.

Putting this in (9) we have

$$|A_i + k \cdot A| \geq \left| \bigcup_{r=1}^{j} (r - 1 + \{0, \ldots, kn_r + n_i\}) \right| = n_i + 1 + kn_l + l - 1, \tag{11}$$

where $kn_l + l - 1 = \max_r(kn_r + r - 1)$. Since

$$n_l \geq \begin{cases} n_r & \text{for } r \leq l \\ n_r + 1 & \text{for } r > l, \end{cases} \tag{12}$$

we have

$$jn_l \geq n_1 + \cdots + n_l + (n_{l+1} + 1) + \cdots + (n_j + 1) = |A| - l. \tag{13}$$

By (11) we have

$$|A + k \cdot A| = \sum_{i=1}^{j} |A_i + k \cdot A| \geq |A| + j(kn_l + l - 1) \geq (k+1)|A| - l(k-j) - j.$$

Since we have assumed that $|A + k \cdot A| = (k+1)|A| - j(k+1-j)$, we have that $l = j$. Furthermore we can see that all the inequalities, included those of (13) and (12), are equalities, so $n_1 = \cdots = n_j$.

Hence, $A_i = k \cdot \{0, \ldots, n\} + i - 1$ for $i = 1, \ldots, j$ and we can write

$$A = \bigcup_{i=1}^{r} A_i = \{0, 1, \ldots, j-1\} + k \cdot \{0, 1, \ldots, n\},$$

for some $n \geq k - 1$. This completes the proof. $\square$

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 9. *Let k be a prime and let A be a finite nonempty subset of $\mathbb{Z}$. We have*

$$|A + k \cdot A| \geq (k+1)|A| - 3(k-1)! \tag{14}$$

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

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

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

Lemma 4 gives $|A + k \cdot A| \geq (j+1)|A| - j$. Therefore $t \geq j+1$.

We have

$$|A + k \cdot A| = \sum_{i \in F} |A_i + k \cdot A| + \sum_{i \in E} |A_i + k \cdot A|. \tag{15}$$

We have

$$\begin{aligned}
\sum_{i \in F} |A_i + k \cdot A| &\geq \sum_{i \in F} |A_i + k \cdot A_1| \\
&= \sum_{i \in F} |X_i + k \cdot X_1| \\
(\textit{by} \quad \textit{Lemma} \quad 4) \qquad &\geq \sum_{i \in F} (|X_i| + k(|X_1| - 1)) \\
&= \sum_{i \in F} (|A_i| + k(|A_1| - 1)) \\
(\textit{since} \quad t \leq k-1) \qquad &\geq |A_F| + (t+1)|F|(|A_1| - 1) \\
(\textit{since} \quad t|A_1||F| \geq t|A_F|) \qquad &\geq (t+1)|A_F| + |F||A_1| - (t+1)|F|. \qquad (16)
\end{aligned}$$

On the other hand, by (5), induction hypothesis and Lemma 7-*ii)*,

$$\begin{aligned}
\sum_{i \in E} |A_i + k \cdot A| &= \sum_{i \in E} (|A_i + k \cdot A_i| + |\Delta_{ii}|) \\
&\geq \sum_{i \in E} ((t+1)|A_i| - 3(t-1)!) + \sum_{i \in E} \Delta_{ii} \\
&\geq (t+1)|A_E| - 3|E|(t-1)! + (|E| - 1)|A_1| + |A_2|. \qquad (17)
\end{aligned}$$

By substitution of (16) and (17) in (15) we get

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

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

$$3|E|(t-1)! + (t+1)|F| \leq 3(t - |F|)(t-1)! + (t+1)|F| \leq 3t! + |F|(t+1-3(t-1)!) \leq 3t!,$$

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

5. Proof of theorem 2

Suppose now that $|A| \geq 3j^2(k-1)!$. By Lemma 8 and Corollary 5 we may assume $E \neq \emptyset$ and $j < k$.

Case 1: There is $s \geq 2$ with $s \in E$.

By (5), Lemma 9 and Lemma 7-*i)*, we obtain

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

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

Case 2: $E = \{1\}$.

In this case, since $|\hat{X}_2| = k$, Lemma 4 implies that

$$|X_2 + k\cdot X_1| \geq |X_2| + k(|X_1| - 1) = |A_2| + k|A_1| - k. \tag{18}$$

We observe also (by Lemma 7-*i)*) that $|\Delta_{11}| \geq |A_2|$.

Then, by (5), Lemma 9, Lemma 7-*i)* and (18) we have

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

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

This completes the proof.

References

[1] B. Bukh, *Sums of Dilates.* Combinatorics, Probability and Computing, vol. 17, 2008
[2] J. Cilleruelo, M. Silva and C. Vinuesa, *A sumset problem*, preprint.
[3] M. B. Nathanson, *Inverse problems for linear forms over finite sets of integers*, arXiv:0708.2304.

Instituto de Ciencias Matemáticas (CSIC-UAM-UC3M-UCM) and Departamento de Matemáticas, Universidad Autónoma de Madrid, 28049-Madrid, Spain

E-mail address: francisco.javier.cilleruelo@uam.es

UPMC Univ Paris 06, E. Combinatoire, Case 189, 4 Place Jussieu, 75005 Paris, France.

E-mail address: hamidoune@math.jussieu.fr

Universitat Politécnica de Catalunya, Jordi Girona, 1, E-08034 Barcelona, Spain.

E-mail address: oserra@ma4.upc.edu