A LOWER BOUND FOR THE SIZE OF A MINKOWSKI SUM OF DILATES

Y. O. HAMIDOUNE AND J. RUÉ

Abstract. Let A be a finite nonempty set of integers. An asymptotic estimate of several dilates sum size was obtained by Bukh. The unique known exact bound concerns the sum $|A+k\cdot A|$, where k is a prime and $|A|$ is large. In its full generality, this bound is due to Cilleruelo, Serra and the first author.

Let k be an odd prime and assume that $|A|>8k^k$. A corollary to our main result states that $|2\cdot A+k\cdot A|\geq (k+2)|A|-k^2-k+2$. Notice that $|2\cdot P+k\cdot P|=(k+2)|P|-2k$, if P is an arithmetic progression.

1. Introduction

Let $A,\ B$ be finite nonempty sets of real numbers. The *Minkowski sum* of A and B is defined as

$$A+B=\{a+b\ :\ a\in A \text{ and } b\in B\}.$$

The inequality $|A+B|\geq |A|+|B|-1$ is an easy exercise, that we shall use without any reference. For a real number r, the *r-dilate* of A is the set $r\cdot A=\{ra : a\in A\}$. Lower bounds for the size of dilates sums appeared in different contexts. Łaba and Konyagin [**?**] investigated the sum $A+\lambda\cdot A$ (where λ is a transcendental number) in connection with well-distributed planar sets distances. Dilates sums also appeared in the proofs of sum-product results in finite fields by Garaev [**?**], and by Katz and Shen [**?**]. The sum of two dilates appeared in the work of Nathanson, O'Bryant, Orosz, Ruzsa and Silva on binary linear forms [**?**]. Also, they were used by Bukh [**?**] in connection with a problem of Ruzsa.

From now on, we assume that A is a nonempty set of integers. Dilates sum of the form $A+3\cdot A$ were investigated independently by Bukh [**?**] and by Cilleruelo, Silva and Vinuesa [**?**]. More recently, the authors of [**?**] proved that for an odd prime k, $|A+k\cdot A|\geq (1+k)|A|-(k+1)^2/4$ for $|A|$ sufficiently large. Let $m_1,\cdots,m_j$ be integers with $\gcd(m_1,\ldots,m_j)=1$, Bukh proved in [**?**] that

$$|m_1\cdot A+\cdots+m_j\cdot A|\geq (|m_1|+\cdots+|m_j|)|A|-o\left(|A|\right).$$

Bukh's result suggests the following:

Conjecture 1.1. For a set of integers Z with $\gcd(Z)=1$ and for every nonempty set of integers A, there is an absolute constant c such that

$$\left|\sum_{m\in Z} m\cdot A\right|\geq \left(\sum_{m\in Z}|m|\right)|A|-c.$$

In the present work, we prove the above conjecture for $Z = \{2, k\}$, where k is an odd prime. For simplicity, we will not consider negative dilates, but the reader will certainly observe that our approach works in this case.

In section 2, we present some easy and known lemmas that we need. In section 3, we prove some intermediary results needed in our induction arguments. One of the results of this section states that $|n \cdot A + m \cdot A| \geq 4|A| - 4$, where m and n are coprime integers. This result is a counterpart of a lemma by Nathanson [**?**] stating that $|A+2\cdot A| \geq 3|A|-2$. Let k be an odd prime. By a k-component of a set $X \subset \mathbb{Z}$, we shall mean the nonempty intersection of X with some congruence class modulo k. In section 4, we investigate the marginal set $(2\cdot C+k\cdot A)\setminus(2\cdot C+k\cdot C)$, where C is a k-component of A. In section 5, we prove that $|2\cdot A+k\cdot A| \geq (k+2)|A|-4k^{k-1}$.

Assuming that $0 \in A$, $\gcd(A) = 1$, $|A| > 8k^k$ and that A has a k-component containing at most $k-1$ nonempty k^2-component, we show that

$$|2 \cdot A + k \cdot A| > (k+2)|A|.$$

Readers interested in the description of sets reaching equality could quite likely use this result, since it shows that the objective function $|2 \cdot A + k \cdot A|$ achieves its minimum on structured sets, for $|A|$ large. Let X be a finite set of integers with $|X| > 8k^k$. We conclude Section 5 by an easy consequence of our main result, stating that $|2 \cdot X + k \cdot X| \geq (k+2)|X| - k^2 - k + 2$. As an exercise, the reader could prove that $|2 \cdot P + k \cdot P| = (k+2)|P| - 2k$, if P is an arithmetic progression. Observe that for $k = 3$, our bound differs at most by 4 from the best possible one.

2. Preliminaries and terminology

In this paper, we consider sums of dilates of a finite set of integers. The next known lemma shows that the size of a dilates sum remains invariant if we replace A by an affine transform of it.

Lemma 2.1. [**?**] *Let A be a finite set of integers and let r, s, u, v be non-zero integers. Then*

- $|r \cdot (A + v) + s \cdot (A + v)| = |r \cdot A + s \cdot A|$,
- $|r \cdot (u \cdot A) + s \cdot (u \cdot A)| = |r \cdot A + s \cdot A|$.

Proof. We have clearly

$$\begin{aligned} |r \cdot (A + v) + s \cdot (A + v)| &= |r \cdot A + s \cdot A + (rv + sv)| \\ &= |r \cdot A + s \cdot A|. \end{aligned}$$

as $|A+w| = |A|$. We also have

$$\begin{aligned} |r\cdot(u\cdot A)+s\cdot(u\cdot A)| &= |(ru)\cdot A+(su)\cdot A| \\ &= |u\cdot(r\cdot A)+u\cdot(s\cdot A)| \\ &= |r\cdot A+s\cdot A|. \end{aligned}$$

□

Let A be a finite set of integers. The intersection of A with a congruence class modulo n will be called a *n-component*. By a *decomposition* modulo n, we mean a partition of A into its n-components. The number of n-components of A will be denoted by $c_n(A)$. We shall say that A is *n-full* if $c_n(A) = n$. The set A is *n-semi-full* if every n-component C of A satisfies $c_{n^2}(C) = n$.

Lemma 2.2. *If A is n-full, then $\gcd(A)$ is coprime to n. Moreover, $\frac{1}{\gcd(A)}\cdot A$ is n-full.*

Proof. There is an $u \in A$ such that $u \equiv 1 \pmod n$. As $\gcd(A)$ divides u, then $\gcd(\gcd(A), n)$ divides both u and n, hence it divides 1. Since $\gcd(A)$ is invertible modulo n, $c_n\left(\frac{1}{\gcd(A)}\cdot A\right) = c_n(A)$. □

3. Tools

Lemma 3.1. *Let A and B be finite sets of integers and let m, n be coprime integers. Let $\mathcal{C}$ denote the set of m-components of A. Then $n\cdot A+m\cdot B = \bigcup_{C\in\mathcal{C}} n\cdot C+m\cdot B$ is a decomposition modulo m.*

Proof. Clearly $n\cdot C+m\cdot B \equiv n\cdot C \pmod m$, for any $C \in \mathcal{C}$. The result follows now since $n\cdot C$ and $n\cdot C'$ are necessarily incongruent modulo m, for distinct components $C, C' \in \mathcal{C}$. □

The next proposition is basic in our approach.

Proposition 3.2. *Let A and B be finite sets of integers and let m, n be coprime integers. Then $|n\cdot A+m\cdot B| \geq c_n(B)|A| + c_m(A)|B| - c_m(A)c_n(B)$.*

Proof. Let $\mathcal{A}$ be the set m-components of A and let $\mathcal{B}$ be the set n-components of B. We claim that if $M_1, M_2 \in \mathcal{A}$ and $N_1, N_2 \in \mathcal{B}$ such that $(M_1, N_1) \neq (M_2, N_2)$, then $(n\cdot M_1+m\cdot N_1)\cap(n\cdot M_2+m\cdot N_2) = \emptyset$. Suppose the contrary and take $a_i \in M_i$ and $b_i \in N_i$, $1 \leq i \leq 2$ with $na_1+mb_1 = na_2+mb_2$. Thus, $n(a_1-a_2) = m(b_1-b_2)$. Since m is coprime to n, we have $b_1-b_2 \equiv 0 \pmod n$ and $a_1-a_2 \equiv 0 \pmod m$. In particular, $M_1 = M_2$ and $N_1 = N_2$, a contradiction.

Therefore, using Lemma 3.1 we have

$$|n\cdot A+m\cdot B| = \left|\bigcup_{M\in\mathcal{A};\ N\in\mathcal{B}} n\cdot M+m\cdot N\right| \geq \sum_{M\in\mathcal{A};\ N\in\mathcal{B}} |M|+|N|-1$$
$$= c_n(B)|A|+c_m(A)|B|-c_m(A)c_n(B).$$

□

Corollary 3.3. *Let $2\leq n<m$ be coprime integers. Let A be a finite set of integers. Then $|n\cdot A+m\cdot A|\geq 4|A|-4$.*

Proof. The result holds clearly if $|A|=1$. Assume that $|A|\geq 2$. Without loss of generality, $0\in A$. Put $B=\frac{1}{\gcd(A)}\cdot A$. Put $r=c_m(B)$ and $s=c_n(B)$. Without loss of generality we may assume that $r\geq s$. Observe that $2\leq r\leq |A|$. By Lemma 2.1 and Proposition 3.2, we have

$$\begin{aligned}|n\cdot A+m\cdot A| &= |n\cdot B+m\cdot B|\\ &\geq 4|B|-4+(r+s-4)|B|-rs+4\\ &\geq 4|B|-4+(r+s-4)r-rs+4\\ &\geq 4|B|-4+(r-2)^2\geq 4|A|-4.\end{aligned}$$

□

Corollary 3.4. *Let m be an odd integer. If A is a m-full finite set of integers, then $|2\cdot A+m\cdot A|\geq (m+2)|A|-2m$. If A is m-semi-full set of integers, then $|2\cdot A+m\cdot A|\geq (m+2)|A|-2mc_m(A)$.*

Proof. Without loss of generality we can assume that $c_2(A)=2$. Then, the first part is a direct consequence of Proposition 3.2. For the second part, take the m-decomposition of A, namely $A=\bigcup_{i\in I}A_i$. Take an arbitrary element $i\in I$. Since A is m-semi-full, A_i can be affinely transformed into an m-full subset. By the first part of this corollary, $|2\cdot A_i+m\cdot A_i|\geq (m+2)|A_i|-2m$. By Lemma 3.1, $2\cdot A_i+m\cdot A_i$ and $2\cdot A_j+m\cdot A_j$ belong to different congruence classes modulo m for $i\neq j$. By Lemma 3.1, $|2\cdot A+m\cdot A|\geq \sum_{i\in I}|2\cdot A_i+m\cdot A_i|\geq \sum_{i\in I}(m+2)|A_i|-2m=(m+2)|A|-2mc_m(A)$. □

4. Marginal sets

Let A be a finite set of integers and let C be a component of A. The *C-marginal* set is defined as

$$M_C=(2\cdot C+k\cdot A)\setminus(2\cdot C+k\cdot C).$$

We start by proving a bound for marginal sets sizes in the semi-full case.

Let A be a finite set of integers and let $\mathcal{C}$ be the set of k-components of A. We formulate the next lemma.

Lemma 4.1. $\sum_{C\in\mathcal{C}} |M_C| \geq (|\mathcal{C}|-1)|\mathcal{C}|$.

Proof. For any component $C \in \mathcal{C}$, we shall write ${M_C}^- = \{x \in M_C : x < \min(2\cdot C + k\cdot C)\}$ and ${M_C}^+ = \{x \in M_C : x > \max(2\cdot C + k\cdot C)\}$. We shall denote by Γ the directed graph of the order relation $x < y$ defined on the set $L = \{\min(C) : C \in \mathcal{C}\}$. Recall that for a given element $x \in L$, $\Gamma^-(x) = \{y \in L : y < x\}$. Clearly

$$2\cdot\min(C) + k\cdot\Gamma^-(\min(C)) \subset M_C^-.$$

In particular, $|\Gamma^-(\min(C))| \leq |M_C^-|$. Therefore,

$$\sum_{C\in\mathcal{C}} |M_C^-| \geq \sum_{C\in\mathcal{C}} |\Gamma^-(\min(C))| = (|\mathcal{C}|-1)|\mathcal{C}|/2,$$

since $\sum_{C\in\mathcal{C}} |\Gamma^-(\min(C))|$ is the total number of arcs in the order relation, which is obviously $(|\mathcal{C}|-1)|\mathcal{C}|/2$. Similar arguments show that $\sum_{C\in\mathcal{C}} |M_C^+| \geq (|\mathcal{C}|-1)|\mathcal{C}|/2$. The lemma follows then from the relation $\sum_{C\in\mathcal{C}} |M_C| \geq \sum_{C\in\mathcal{C}} |M_C^-| + \sum_{C\in\mathcal{C}} |M_C^+|$. □

We continue relating the size of M_C and C. Sets with the property $|M_C| \geq |C|$ are satisfactory for induction proofs, as we shall see in the next section. For a subset X of an abelian group G, we write $\pi(X) = \{x \in G : x + X = X\}$. We recall that $|\pi(X)|$ is a divisor of $|X|$.

Lemma 4.2. *Let k be an odd prime and let A be a finite set of integers with $0 \in A$ and $\gcd(A) = 1$. Let C be a non-k-semi-full component of A and let $C' \neq C$ be another k-component of A. Then $|M_C| \geq |C'|$. Moreover, $|M_C| \geq |C|$ if one of the following conditions holds:*

- *There is another component with size not less than $|C|$.*
- *C is non-2-full.*

Proof. Let $\phi : \mathbb{Z} \to \mathbb{Z}/k^2\mathbb{Z}$ be the projection. Since $|\pi(\phi(C))|$ divides k^2 and $|\phi(C)|$ and since $|\phi(C)| < k$, we have necessarily $\pi(\phi(C)) = \{0\}$. Since all elements of $k\cdot C$ are equal modulo k^2, if $\phi(2\cdot C + k\cdot C) = \phi(2\cdot C + k\cdot C')$, we have $\phi(k\cdot C) = \phi(k\cdot C')$, and hence $C \equiv C'$ modulo k. It follows that $C = C'$, a contradiction.

Thus, M_C contains $2\cdot C_0 + k\cdot C'$, where C_0 is some k^2-component of C, and hence $|M_C| \geq |C'|$. Assume now that C is non-2-full. Pick either an odd v (using $\gcd(A) = 1$) if C contains only even numbers or $v = 0 \in A$ if C contains only odd numbers. Clearly, $2\cdot C + kv$ is a subset of M_C. □

5. Large sets of integers

The next result is our first step.

Theorem 5.1. *Let k be an odd prime. If A is a finite set of integers, then*

$$|2\cdot A+k\cdot A|\geq (k+2)|A|-4k^{k-1}.$$

Proof. Without loss of generality, we may take $0\in A$ and $\gcd(A)=1$. We shall prove by induction that for all $2\leq s\leq k$, we have

$$|2\cdot A+k\cdot A|\geq (s+2)|A|-4k^{s-1}.$$

For $s=2$, this bound is weaker than the one obtained by Corollary 3.3.

Assume now that $2<s\leq k$ and that the result holds for $s-1$. Take a k-decomposition of A, namely $A=\bigcup_{i\in I}A_i$. We shall write $M_i=M_{A_i}$. Put $F=\{i\in I: A_i \text{ is } k-\text{semi-full}\}$ and $E=I\setminus F$. Notice that $|E|+|F|=|I|\leq k$.

Assume first that

$$\sum_{i\in E}|M_i|\geq \sum_{i\in E}|A_i|.$$

By Lemma 3.1, $2\cdot A_i+k\cdot A$ and $2\cdot A_j+k\cdot A$ belong to different congruence classes modulo k, for $i\neq j$. By Corollary 3.4, for every $i\in F$, $|2\cdot A_i+k\cdot A_i|\geq (k+2)|A_i|-2k$. Using the last relations, the induction hypothesis applied for every $i\in E$, we have

$$\begin{aligned}
|2\cdot A+k\cdot A|\geq & \sum_{i\in E}(|2\cdot A_i+k\cdot A_i|+|M_i|)+\sum_{i\in F}|2\cdot A_i+k\cdot A_i|\\
\geq & \sum_{i\in E}((s+1)|A_i|-4k^{s-2})+\sum_{i\in E}|A_i|+\sum_{i\in F}((k+2)|A_i|-2k)\\
\geq & \sum_{i\in I}(s+2)|A_i|-4|I|k^{s-2}+2k|F|\left(2k^{s-3}-1\right)\\
\geq & (s+2)|A|-4k^{s-1},
\end{aligned}$$

and the result holds.

Assume now that

$$\sum_{i\in E}|M_i|<\sum_{i\in E}|A_i|.$$

In particular, we have $|E|\geq 1$. We must have $|E|=1$, otherwise we take a derangement (permutation without fixed element) σ of E. By Lemma 4.2, $|M_i|\geq |A_{\sigma(i)}|$, for every i. We get a contradiction by summing over all $i\in E$. Put $E=\{e\}$ and take $f\in F$. Observe that there must be at least two k-components, as $0\in A$ and $\gcd(A)=1$. Applying and affine transformation to both A_e and A_f we can apply Proposition 3.2, getting $|2\cdot A_f+k\cdot A_e|\geq k|A_f|+2|A_e|-2k$.

The idea here is to estimate the component of $2\cdot A+k\cdot A$ containing $2\cdot A_f+k\cdot A_f$, using the sum $2\cdot A_f+k\cdot A_e$. By Lemma 4.2, A_e is 2-full, $|A_e|>|A_f|$ and $|M_e|\geq |A_f|$.

Using Lemma 3.1 and the previous considerations we have

$$\begin{aligned}
|2\cdot A+k\cdot A| \geq & |2\cdot A_e+k\cdot A_e|+|M_e|+|2\cdot A_f+k\cdot A_e|+\sum_{i\in F\setminus f}|2\cdot A_i+k\cdot A_i| \\
\geq & (s+1)|A_e|-4k^{s-2}+|A_f|+k|A_f|+2|A_e|-2k+\sum_{i\in F\setminus f}((k+2)|A_i|-2k) \\
> & (s+2)|A_e|-4k^{s-2}+\sum_{i\in F}((s+2)|A_i|-2k) \\
\geq & (s+2)|A|-4k^{s-1}+2|F|k(2k^{s-3}-1) \\
\geq & (s+2)|A|-4k^{s-1}.
\end{aligned}$$

□

Our main result is the following one:

Theorem 5.2. *Let k be an odd prime. Let A be a finite set of integers with $0\in A$, $\gcd(A)=1$ and $|A|>8k^k$. If A has a k-component involving at most $k-1$ distinct k^2-components, then*

$$|2\cdot A+k\cdot A|>(k+2)|A|.$$

Proof. Let $\mathcal{C}$ denote the set of k-components of A and let C be a non-k-semi-full component of A. Take a k-component N with a maximal cardinality. Clearly $|N|>8k^{k-1}$. Assume first that $|M_C|\geq|N|$. By Theorem 5.1 and Lemma 3.1,

$$\begin{aligned}
|2\cdot A+k\cdot A| \geq & |2\cdot C+k\cdot C|+|M_C|+|2\cdot(A\setminus C)+k\cdot(A\setminus C)| \\
> & (k+2)|C|-4k^{k-1}+8k^{k-1}+(k+2)|A\setminus C|-4k^{k-1} \\
= & (k+2)|A|,
\end{aligned}$$

Assume now that $|M_C|<|N|$ and put $c=c_k(A)$. By Lemma 4.2, $C=N$ and C is 2-full. Hence C is the unique non-k-semi-full component of A. Take now a k-semi-full component of A, say T and put $A'=A\setminus(C\cup T)$. By Lemma 4.2 $|M_C|\geq|T|$. Applying a convenient affine transformation, by Proposition 3.2 $|2\cdot T+k\cdot C|\geq k|T|+2|C|-2k$.

Thus using Corollary 3.4 and Lemma 3.1 we have

$$\begin{aligned}
|2\cdot A+k\cdot A| \geq & |2\cdot C+k\cdot C|+|T|+|2\cdot T+k\cdot C|+(k+2)|A'|-2(c-2)k \\
\geq & (k+2)|C|-4k^{k-1}+|C|+(k+2)|T|-2k+(k+2)|A'|-2(c-2)k \\
> & (k+2)|A|+4k^{k-1}-2k(k-1)>(k+2)|A|,
\end{aligned}$$

and the result holds. □

We can now prove the following lower bound on $|2\cdot A+k\cdot A|$:

Corollary 5.3. *Let k be an odd prime. If A is a finite set of integers with $|A| > 8k^k$, then*

$$|2 \cdot A + k \cdot A| \geq (k+2)|A| - k^2 - k + 2.$$

Proof. By Lemma 2.1, we may take $0 \in A$ and $\gcd(A) = 1$. By Corollary 3.4, the result holds if A is k-full. Assume that A is non-k-full and let $\mathcal{C}$ denote the set of k-components of A. By Theorem 5.2, we may assume that A is k-semi-full. By Corollary 3.4, Lemma 3.1 and Lemma 4.1 we have

$$\begin{aligned} |2 \cdot A + k \cdot A| &= \sum_{C \in \mathcal{C}} |2 \cdot C + k \cdot C| + |M_C| \\ &\geq \sum_{C \in \mathcal{C}} ((k+2)|C| - 2k) + c_k(A)(c_k(A) - 1) \\ &= (k+2)|A| - c_k(A)(2k - c_k(A) + 1) \end{aligned}$$

Therefore $|2 \cdot A + k \cdot A| \geq (k+2)|A| - k^2 - k + 2$, and the result holds. □

Acknowledgement: the authors thank the referee, whose suggestions and advices helped to improve the presentation of the article.

References

[1] B. Bukh. Non-trivial solutions to a linear equation in integers. *Acta Arithmetica*, 131:41–55, 2008.
[2] B. Bukh. Sums of dilates. *Combinatorics, Probability and Computing*, 17:627–639, 2008.
[3] J. Cilleruelo, Y. O. Hamidoune, and O. Serra. On sums of dilates. *Combinatorics, Probability and Computing*, 18:871–880, 2009.
[4] J. Cilleruelo, M. Silva, and C. Vinuesa. A sumset problem. *Journal of Combinatorics and Number Theory*, 2, 2010.
[5] M. Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. *International Mathematics Research Notices*. Vol. 2007 : article ID rnm035, 11 pages, 2007.
[6] N. Hawk Katz and C.-Y. Shen. A slight improvement to Garaev's sum product estimate. *Proceedings of the American Mathematical Society*, 136:2499–2504, 2008.
[7] I. Łaba and S. Konyagin. Distance sets of well-distributed planar sets for polygonal norms. *Israel Journal of Mathematics*, 152:157–179, 2006.
[8] M. B. Nathanson. Inverse problems for linear forms over finite sets of integers. Available on-line at arXiv: 0708.2304v2.
[9] M. B. Nathanson, K. O'Bryant, B. Orosz, I. Ruzsa, and M. Silva. Binary linear forms over finite sets of integers. *Acta Arithmetica*, 129:341–361, 2007.

UPMC, Université Paris 06, 4 Place Jussieu, 75005 Paris, France.
E-mail address: hamidoune@math.jussieu.fr

LIX, École Polytechnique , 91128 Palaiseau-Cedex, France.
E-mail address: rue1982@lix.polytechnique.fr