A SUMSET PROBLEM

JAVIER CILLERUELO, MANUEL SILVA AND CARLOS VINUESA

Abstract. We study the sumset $A + k \cdot A$ for the first non trivial case, $k = 3$, where $k \cdot A = \{k \cdot a,\ a \in A\}$. We prove that $|A + 3 \cdot A| \geq 4|A| - 4$ and that the equality holds only for $A = \{0, 1, 3\}$, $A = \{0, 1, 4\}$, $A = 3 \cdot \{0, \ldots, n\} \cup (3 \cdot \{0, \ldots, n\} + 1)$ and all the affine transforms of these sets.

1. Introduction

Throughout this paper, the sets considered have integer elements, unless the contrary is said.

We address here the question of how large is the sumset $A + k \cdot A$ where $k \cdot A = \{k \cdot a,\ a \in A\}$ and A is finite. It is well known that $|A + A| \geq 2|A| - 1$ and that equality only holds when A is an arithmetic progression. Nathanson proved in [1] that $|A + 2 \cdot A| \geq 3|A| - 2$ for any set A. It is easy to check that for any arithmetic progression with k or more elements, we have $|A + k \cdot A| = (k+1)|A| - k$, so it might be expected that arithmetic progressions are extremal cases for this problem, as when $k = 1$. Indeed this is the case for $k = 2$ as we will prove in section §2.

Theorem 1.1. *For any set A we have $|A + 2 \cdot A| \geq 3|A| - 2$. Furthermore, if $|A + 2 \cdot A| = 3|A| - 2$, then A is an arithmetic progression or a singleton.*

Then, what for $k = 3$? In a recent paper, Bukh [2] has proved that $|A + 3 \cdot A| \geq 4|A| - O(1)$ for any set A. Our main theorem gives, using a different argument, a sharp lower bound and a complete description of the extremal sets. We observe that these sets are not arithmetic progressions, as in cases $k = 1, 2$.

Theorem 1.2. *For any set A we have $|A + 3 \cdot A| \geq 4|A| - 4$. Furthermore if $|A + 3 \cdot A| = 4|A| - 4$ then $A = 3 \cdot \{0, \ldots, n\} \cup (3 \cdot \{0, \ldots, n\} + 1)$ or $A = \{0, 1, 3\}$ or $A = \{0, 1, 4\}$ or A is an affine transform of one of these sets.*

The general sums of dilated sets, $\lambda_1 \cdot A + \cdots + \lambda_k \cdot A$, have been studied by Bukh in [2]. The main theorem there says that for coprime integers $\lambda_1, \ldots, \lambda_k$,

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

In particular it gives $|A + k \cdot A| \geq (k+1)|A| - o(|A|)$. As we will prove in section §5, there exist arbitrarily large sets A such that $|A + k \cdot A| = (k+1)|A| - \left\lceil \frac{k^2+2k}{4} \right\rceil$. We conjecture that this lower bound is sharp for large $|A|$.

2. Case $k = 2$ and preliminary lemmas

The next lemma is folklore, and we give it without proof.

Lemma 1. For arbitrary non-empty sets A, B we have

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

ii) Furthermore, if equality holds, then A and B are arithmetic progressions with the same difference unless one of them is a singleton.

---

*2000 Mathematics Subject Classification:*11B75 .

We generalize this lemma for any k. For that, it is natural to divide A into residue classes $\pmod k$. We define $\hat{A}$ as the projection of A into $\mathbb{Z}/k\mathbb{Z}$.

Lemma 2. For arbitrary non-empty sets B and $A = \bigcup_{i\in\hat{A}}(k\cdot A_i + i)$ we have

i) $|A + k\cdot B| = \sum_{i\in\hat{A}} |A_i + B|$
ii) $|A + k\cdot B| \geq |A| + |\hat{A}|(|B| - 1)$.
iii) Furthermore, if equality holds in ii), then either $|B| = 1$ or $|A_i| = 1$ for all $i \in \hat{A}$ or B and all the sets A_i with more than one element are arithmetic progressions with the same difference.

Proof. For i) $|A + k\cdot B| = |\cup_{i\in\hat{A}}(k\cdot A_i + i + k\cdot B)| = \sum_{i\in\hat{A}} |k\cdot(A_i + B) + i| = \sum_{i\in\hat{A}} |A_i + B|$. To prove ii) we use i) and Lemma 1-i). To prove iii) we observe that Lemma 1-ii) implies that A_i and B are arithmetic progressions with the same difference except for the degenerate cases. □

Next we prove theorem 1.1 as a direct application of Lemma 2.

Proof. Proof of theorem 1.1 If $|A| = 1$ then $|A + 2\cdot A| = 3|A| - 2$, and these sets are described in Theorem 1.1, so the inverse part is also proved.

So we assume $|A| \geq 2$. If $|\hat{A}| = 1$ then we can write $A = 2\cdot A_i + i$ for some $i \in \{0, 1\}$ and $|A + 2\cdot A| = |2\cdot A_i + i + 4\cdot A_i + 2i| = |A_i + 2\cdot A_i|$. Now, if $|\hat{A}_i| = 1$, we can repeat this process and it's clear that finally we will reach a set A' with $|\hat{A}'| = 2$, that only differs from A on a translation and a dilation, and so, such that $|A + 2\cdot A| = |A' + 2\cdot A'|$.

Then we can also assume that $|\hat{A}| = 2$ and Lemma 2-ii) implies that $|A + 2\cdot A| \geq |A| + 2(|A| - 1) = 3|A| - 2$. For the inverse part, if the equality holds, Lemma 2-iii) implies that either $|A| = 1$ or $|A_0| = |A_1| = 1$ or A is an arithmetic progression. We finish by observing that $|A| = 1$ is impossible since we assumed $|A| \geq 2$ and $|A_0| = |A_1| = 1$ implies that $|A| = 2$, so it is an arithmetic progression. □

For the case $k = 3$ we will need some preliminary lemmas.

Lemma 3. If $A = 3\cdot A_0 \cup (3\cdot A_1 + 1)$, then

i) $|A + 3\cdot A| \geq |A_0 + 3\cdot A_0| + |A_1 + 3\cdot A_1| + 2$.
ii) $|A + 3\cdot A| \geq |A_0 + 3\cdot A_1| + |A_1 + 3\cdot A_0| + 2$.

Proof. To prove i) we write

$$\begin{aligned}|A + 3\cdot A| &= |A_0 + A| + |A_1 + A| \\ &= |(A_0 + 3\cdot A_0) \cup (A_0 + 3\cdot A_1 + 1)| + |(A_1 + 3\cdot A_0) \cup (A_1 + 3\cdot A_1 + 1)| \\ &= |A_0 + 3\cdot A_0| + |A_1 + 3\cdot A_1 + 1| \\ &+ |(A_0 + 3\cdot A_1 + 1) \setminus (A_0 + 3\cdot A_0)| + |(A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)|\end{aligned}$$

Then we only need to check that the last line above is at least 2. If $|A_0| = 1$ and $|A_1| = 1$, we write $A_0 = \{a_0\}$ and $A_1 = \{a_1\}$. Then $a_0 + 3a_1 + 1 \neq a_0 + 3a_0$ and $a_1 + 3a_0 \neq a_1 + 3a_1 + 1$ because they are different modulo 3, so we have two extra elements. If not, let m_i and M_i be the minimum and the maximum of A_i, $i = 0, 1$, and we know that for at least one i, $m_i \neq M_i$.

If $M_0 \leq M_1$ then $M_0 + 3M_1 + 1 \in (A_0 + 3\cdot A_1 + 1) \setminus (A_0 + 3\cdot A_0)$ because $M_0 + 3M_1 + 1$ is greater than $M_0 + 3M_0$, which is the maximum of $A_0 + 3\cdot A_0$. On the other hand, if $M_0 > M_1$, then $M_1 + 3M_0 \in (A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)$.

If $m_0 \leq m_1$ then $m_1 + 3m_0 \in (A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)$ and if $m_0 > m_1$ then $m_0 + 3m_1 + 1 \in (A_0 + 3\cdot A_1 + 1) \setminus (A_0 + 3\cdot A_0)$.

We obtain one extra element in each case. To see that they are distinct, observe that if $M_0 + 3M_1 + 1 = m_0 + 3m_1 + 1$, then we must have $M_0 = m_0$ and $M_1 = m_1$, a contradiction. The same thing happens if $M_1 + 3M_0 = m_1 + 3m_0$. The proof of ii) is similar. □

Lemma 4. If $A = 3\cdot A_0 \cup (3\cdot A_1 + 1)$, then

i) If $|\hat{A}_0| = 2$, we have $|A_0 + A| \geq 2|A| - 2$.
ii)
- If $|\hat{A}_0| \leq 2$ and $|A_0 + 3\cdot A_0| \geq 4|A_0| - 4$, we have $|A_0 + A| \geq 4|A_0| + |A_1| - 4$.

- If $|\hat{A}_1| \le 2$ and $|A_1 + 3\cdot A_1| \ge 4|A_1| - 4$, we have $|A_1 + A| \ge 4|A_1| + |A_0| - 4$.

Proof. For i), let $\hat{A}_0 = \{u, u+1\}$. We can write $A_0 = A_0^u \cup A_0^{u+1}$, where $A_0^u = \{x \in A_0,\ x \equiv u \pmod 3\}$. Then

$$\begin{aligned}|A_0 + A| &= |(A_0 + 3\cdot A_0) \cup (A_0 + 3\cdot A_1 + 1)|\\ &= |(A_0^u + 3\cdot A_0) \cup (A_0^{u+1} + 3\cdot A_0) \cup (A_0^u + 3\cdot A_1 + 1) \cup (A_0^{u+1} + 3\cdot A_1 + 1)|\\ &\ge |A_0^u + 3\cdot A_0| + |A_0^u + 3\cdot A_1 + 1| + |A_0^{u+1} + 3\cdot A_1 + 1|\\ &\ge |A_0^u| + |A_0| - 1 + |A_1| + |A_0^{u+1}| + |A_1| - 1 = 2|A| - 2,\end{aligned}$$

where we have twice used Lemma 1-i).

For part ii), we again write $A_0 = A_0^u \cup A_0^{u+1}$ if $|\hat{A}_0| = 2$, or $A_0 = A_0^{u+1}$ if $|\hat{A}_0| = 1$. Then

$$\begin{aligned}|A_0 + A| &= |(A_0 + 3\cdot A_0) \cup (A_0 + 3\cdot A_1 + 1)| \ge |(A_0 + 3\cdot A_0) \cup (A_0^{u+1} + 3\cdot A_1 + 1)|\\ &= |A_0 + 3\cdot A_0| + |A_0^{u+1} + 3\cdot A_1 + 1| \ge 4|A_0| - 4 + |A_1|.\end{aligned}$$

The same argument works for A_1 instead of A_0. □

Lemma 5.

i) If $|A| = 2$ then $|A + 3\cdot A| = 4|A| - 4 = 4$.

ii) If $|A| = 3$ then $|A + 3\cdot A| \ge 4|A| - 4$. Furthermore, if $|A| = 3$ and $|A + 3\cdot A| = 4|A| - 4$ then A is an affine transform of $\{0, 1, 3\}$ or $\{0, 1, 4\}$.

Proof. i) Since affine transforms don't affect the size of $|A + 3\cdot A|$, we can write $A = \{0, 1\}$. Then $A + 3\cdot A = \{0, 1, 3, 4\}$.

ii) Now, we know that $A' = \{0, 1, a\}$, where $a > 1$ is a real number, is a dilation of A and we have that

$$A' + 3\cdot A' = \{0, 1, a, 3, 4, 3 + a, 3a, 3a + 1, 4a\}.$$

If $A' + 3\cdot A'$ has 8 or less elements then there is some repeated element in the sumset. The possible repetitions come from $a = 3,\ a = 4,\ 4 = 3a,\ 3 + a = 3a$ which provide the sets $\{0, 1, 3\}$, $\{0, 1, 4\}$, $\{0, 3, 4\}$, $\{0, 2, 3\}$. □

3. Proof of Theorem 1.2: the inequality

We will prove first the lower bound for $|A+3\cdot A|$ and next the inverse problem which is more involved. We distinguish three cases according to the different values of $|\hat{A}|$.

If $|\hat{A}| = 3$ then (by Lemma 2-ii)) we have that $|A + 3\cdot A| \ge 4|A| - 3$, a better lower bound than that we want to prove in Theorem 1.2.

If $|\hat{A}| = 1$ then we have that $A = 3\cdot A' + i$ and then $|A+3\cdot A| = |A'+3\cdot A'|$. If $|A| > 1$ we repeat the process until we obtain a set A' with $|\hat{A}'| > 1$. If $|A| = 1$ then $4|A| - 4 = 0$ and the theorem is trivial.

So we can now assume that $|\hat{A}| = 2$, $A = (3\cdot A_i + i) \cup (3\cdot A_{i+1} + i + 1)$. We can assume that $|\hat{A}_i| \le |\hat{A}_{i+1}|$. If not the set $B = -A$ could be written as $B = (3\cdot B_j + j) \cup (3\cdot B_{j+1} + j + 1)$ where $B_j = -A_{i+1} - 1,\ B_{j+1} = -A_i - 1,\ j = 2 - i$, and in this case we would have $|\hat{B}_j| \le |\hat{B}_{j+1}|$. Finally, by translation we can assume

- $A = 3\cdot A_0 \cup (3\cdot A_1 + 1)$
- $\min A_0 = 0$
- $|\hat{A}_0| \le |\hat{A}_1|$.

Assuming all this, we prove $|A+3\cdot A| \ge 4|A| - 4$ by induction on $|A|$. It is clear for $|A| = 1$. Suppose we have proved it for any set with fewer elements than A, in particular for A_0 and A_1. We distinguishing three cases:

Case $|\hat{A}_0| = |\hat{A}_1| = 3$. We use Lemma 3-i) and Lemma 2-ii) to obtain

$$|A + 3\cdot A| \ge |A_0 + 3\cdot A_0| + |A_1 + 3\cdot A_1| + 2 \ge 4|A_0| - 3 + 4|A_1| - 3 + 2 = 4|A| - 4.$$

Case $|\hat{A}_1| = 3,\ |\hat{A}_0| < 3$. We apply Lemma 4-ii) (using the induction hypothesis) and Lemma 2-ii) to obtain

$$|A + 3\cdot A| = |A_0 + A| + |A_1 + A| \geq |A_0 + A| + |A_1 + 3\cdot A_1| \geq$$
$$4|A_0| + |A_1| - 4 + 4|A_1| - 3 = 4|A| - 4 + |A_1| - 3 \geq 4|A| - 4.$$

In the last inequality we have used that $|A_1| \geq |\hat{A}_1| = 3$.

Case $|\hat{A}_1| < 3$. We apply Lemma 4-ii) to A_0 and A_1 (again, using the induction hypothesis) to obtain

$$|A + 3\cdot A| = |A_0 + A| + |A_1 + A| \geq 4|A_0| + |A_1| - 4 + 4|A_1| + |A_0| - 4 = 4|A| - 4 + |A| - 4.$$

If $|A| \geq 4$ this gives the bound. If not, we use Lemma 5. This completes the proof.

4. Proof of Theorem 1.2: the cases of equality

As in the previous section we can assume $A = 3\cdot A_0 \cup (3\cdot A_1 + 1)$, $|\hat{A}_0| \leq |\hat{A}_1|$ and $\min A_0 = 0$.

Case $|\hat{A}_0| = |\hat{A}_1| = 3$. We use Lemma 3-i) and 3-ii) and Lemma 2-ii) to obtain

$$\begin{aligned} 4|A| - 4 = |A + 3\cdot A| &\geq |A_0 + 3\cdot A_0| + |A_1 + 3\cdot A_1| + 2 \\ &\geq |A_0| + 3|A_0| - 3 + |A_1| + 3|A_1| - 3 + 2 = 4|A| - 4. \end{aligned}$$

and

$$\begin{aligned} 4|A| - 4 = |A + 3\cdot A| &\geq |A_0 + 3\cdot A_1| + |A_1 + 3\cdot A_0| + 2 \\ &\geq |A_0| + 3|A_1| - 3 + |A_1| + 3|A_0| - 3 + 2 = 4|A| - 4. \end{aligned}$$

Then, the inequalities are, indeed, equalities. So $|A_0 + 3\cdot A_0| = |A_0| + 3|A_0| - 3$, $|A_1 + 3\cdot A_1| = |A_1| + 3|A_1| - 3$, $|A_0 + 3\cdot A_1| = |A_0| + 3|A_1| - 3$ and $|A_1 + 3\cdot A_0| = |A_1| + 3|A_0| - 3$. Now we apply Lemma 2-iii) to conclude that (since $|A_0| \geq |\hat{A}_0| = 3$ and $|A_1| \geq |\hat{A}_1| = 3$)

a) either $A_0 = \{x_0, x_1, x_2\}$ and $A_1 = \{y_0, y_1, y_2\}$ with $x_i, y_i \equiv i \pmod 3$
b) or A_0 and A_1 are arithmetic progressions with the same difference, d.

a) In this subcase, $|A| = 6$ and $4|A| - 4 = 20$, and we know by Lemma 2-i) that $20 = |A + 3\cdot A| = |A_0 + A| + |A_1 + A|$. Then, $|A_0 + A| \leq 10$ or $|A_1 + A| \leq 10$. We suppose that $|A_0 + A| \leq 10$ (the other case is identical) and, because $A_0 = \{x_0, x_1, x_2\}$ with $x_i \equiv i \pmod 3$, we have

$$\begin{aligned} 10 &\geq |(A_0 + 3\cdot A_0) \cup (A_0 + 3\cdot A_1 + 1)| \\ &= |(x_0 + 3\cdot A_0) \cup (x_2 + 3\cdot A_1 + 1)| \\ &+ |(x_1 + 3\cdot A_0) \cup (x_0 + 3\cdot A_1 + 1)| \\ &+ |(x_2 + 3\cdot A_0) \cup (x_1 + 3\cdot A_1 + 1)| \\ &= \left| A_0 \cup \left(A_1 + \frac{x_2 - x_0 + 1}{3} \right) \right| \\ &+ \left| A_0 \cup \left(A_1 + \frac{x_0 - x_1 + 1}{3} \right) \right| \\ &+ \left| A_0 \cup \left(A_1 + \frac{x_1 - x_2 + 1}{3} \right) \right| \end{aligned}$$

and we can observe that each addend give us at least 4 elements unless the two members of the union are equal (in this case we have only 3). But because the sum of the three is less or equal than 10, we must have at least two equalities, like for example:

$$A_0 = A_1 + \frac{x_2 - x_0 + 1}{3} \text{ and } A_0 = A_1 + \frac{x_0 - x_1 + 1}{3}.$$

Then, we have $x_2 - x_0 = x_0 - x_1$, so A_0 is an arithmetic progression and also A_1 is an arithmetic progression with the same difference, since it is a translation of A_0. The other possibilities are identical.

b) So A_0 and A_1 are arithmetic progressions with difference d, and because $0 = \min A_0$ we can write $A_0 = d\cdot[0, n_0-1]$, $A_1 = d\cdot[0, n_1-1]+e$. Since $n_0, n_1 \geq 3$, we have that $[0, n_i-1]+3\cdot[0, n_j-1] = [0, 3n_j + n_i - 4]$ for any $i, j \in \{0, 1\}$. Thus

$$\begin{aligned}
&|A + 3\cdot A| = |A_0 + A| + |A_1 + A| \\
&= |d\cdot([0, n_0-1] + 3\cdot[0, n_0-1]) \cup d\cdot([0, n_0-1] + 3\cdot[0, n_1-1]) + 3e + 1| \\
&+|(d\cdot([0, n_1-1] + 3\cdot[0, n_0-1]) + e) \cup (d\cdot([0, n_1-1] + 3\cdot[0, n_1-1]) + 4e + 1)| \\
&= |d\cdot[0, 4n_0-4] \cup (d\cdot[0, 3n_1 + n_0 - 4] + 3e + 1)| \\
&+|d\cdot[0, 4n_1-4] \cup (d\cdot[0, 3n_0 + n_1 - 4] - 3e - 1)|.
\end{aligned}$$

If $n_1 > n_0$ then

$$|A + 3\cdot A| \geq 3n_1 + n_0 - 3 + 4n_1 - 3 = 4(n_0 + n_1) + 3(n_1 - n_0) - 6 \geq 4|A| - 3,$$

which is a contradiction. So $n_1 \leq n_0$. For the same reason (interchanging n_0 and n_1) we have that $n_0 \leq n_1$ and then $n_0 = n_1$. Now we can write

$$\begin{aligned}
|A + 3\cdot A| &= |d\cdot[0, 4n_0-4] \cup (d\cdot[0, 4n_0-4] + 3e + 1)| \\
&+ |d\cdot[0, 4n_0-4] \cup (d\cdot[0, 4n_0-4] - 3e - 1)|.
\end{aligned}$$

If $3e + 1 \not\equiv 0 \pmod d$ then the unions are disjoint and we have $4|A| - 4 = |A + 3\cdot A| = 2(4n_0 - 3) + 2(4n_0 - 3) = 8|A| - 12$. That implies that $|A| = 2$ and this is impossible since $|A| = |A_0| + |A_1| \geq |\hat{A}_0| + |\hat{A}_1| = 6$. If $3e + 1 \equiv 0 \pmod d$ we write $3e + 1 = de'$ and then

$$\begin{aligned}
|A + 3\cdot A| &= |[0, 4n_0-4] \cup ([0, 4n_0-4] + e')| \\
&+ |[0, 4n_0-4] \cup ([0, 4n_0-4] - e')|.
\end{aligned}$$

If $|e'| \geq 2$ then the cardinality of each union is greater than or equal to $4n_0 - 1$, and $|A + 3\cdot A| \geq 4n_0 - 1 + 4n_0 - 1 = 4|A| - 2$. So, since $e' \neq 0$ then $e' = \pm 1$, so $3e + 1 = \pm d$ and $A = 3\cdot A_0 \cup 3\cdot A_1 + 1 = d\cdot(3\cdot[0, n_0-1] \cup 3\cdot[0, n_0-1] \pm 1)$. These sets are contained in Theorem 1.2.

Case $|\hat{A}_0| = 2,\ |\hat{A}_1| = 3$**.** We write

$$|A_1 + A| = |(A_1 + 3\cdot A_0) \cup (A_1 + 3\cdot A_1 + 1)| = |A_1 + 3\cdot A_1| + |(A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)|.$$

Lemma 2-i), Lemma 4-ii) and the equality above imply that

$$\begin{aligned}
|A + 3\cdot A| &= |A_0 + A| + |A_1 + A| \\
&\geq 4|A_0| + |A_1| - 4 + 4|A_1| - 3 + (|A_1 + 3\cdot A_1| - 4|A_1| + 3) \\
&+ |(A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)|.
\end{aligned}$$

Then

$$4|A| - 4 \geq 4|A| - 4 + (|A_1| - 3) + (|A_1 + 3\cdot A_1| - 4|A_1| + 3) + |(A_1 + 3\cdot A_0) \setminus (A_1 + 3\cdot A_1 + 1)|.$$

Using that $|A_1| \geq |\hat{A}_1| = 3$ and Lemma 2-ii) we see that the three last addends are non negative. But the inequality implies that all of them are indeed 0. Then,

i) $|A_1| = 3$.
ii) By Lemma 2-iii),
   a) either $A_1 = \{y_0, y_1, y_2\}$ with $y_i \equiv i \pmod 3$
   b) or A_1 is an arithmetic progression, say $A_1 = d\cdot[0, 2] + e$.
iii) $3\cdot A_0 \subset A_1 - A_1 + 3\cdot A_1 + 1$ (because $A_1 + 3\cdot A_0 \subset A_1 + 3\cdot A_1 + 1$).

Now we claim that also $|A_0| = 3$. To see that we will obtain a lower and upper bound.

To prove $|A_0| \leq 3$ we use Lemma 2-i), Lemma 4-ii), Lemma 2-ii) and the fact that $|A_1| = 3$ to have

$$\begin{aligned} |A + 3 \cdot A| &= |A_0 + A| + |A_1 + A| \geq |A_0 + A| + |A_1 + 3 \cdot A_0| \geq \\ & 4|A_0| + |A_1| - 4 + |A_1| + 3(|A_0| - 1) = 4|A| - 4 + 3|A_0| - 9. \end{aligned}$$

Since we have assumed that $|A + 3 \cdot A| = 4|A| - 4$ then $|A_0| \leq 3$.

To prove $|A_0| \geq 3$ we use Lemma 2-i), Lemma 4-i) and Lemma 5-ii) (for a set A of three elements that covers the three classes modulo 3 we must have $|A + 3 \cdot A| = 9$) to obtain

$$4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 2|A| - 2 + |A_1 + 3 \cdot A_1| = 2|A| - 2 + 9,$$

so $|A| \geq 11/2$. And since $|A_1| = 3$ we have that $|A_0| \geq 5/2$, so $|A_0| \geq 3$.
So we have proved that $|A| = 6$.

Next we will see that if we are in case ii)-a), that is if $A_1 = \{y_0, y_1, y_2\}$ with $y_i \equiv i \pmod 3$, then A_1 is an arithmetic progression. As in a) of the case $|\hat{A}_0| = |\hat{A}_1| = 3$ we have, $20 = 4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A|$. Again, one of them is less or equal than 10. If $|A_1 + A| \leq 10$ then we proceed exactly as we did in that case and we have that A_1 is an arithmetic progression. If $|A_0 + A| \leq 10$ then $A_0 = \{x_0, y_0, x_1\}$ or $A_0 = \{x_0, y_0, x_2\}$ where $x_i \equiv y_i \equiv i \pmod 3$ except for translations. In the first case $10 \geq |A_0 + A| = |(A_0 + 3 \cdot A_0) \cup (A_0 + 3 \cdot A_1 + 1)| \geq |(x_0 + 3 \cdot A_0) \cup (y_0 + 3 \cdot A_0)| + |(x_0 + 3 \cdot A_1 + 1) \cup (y_0 + 3 \cdot A_1 + 1)| + |x_1 + 3 \cdot A_1 + 1| \geq 4 + 4 + 3 = 11$, which is a contradiction. The second case is similar.

Thus, the only possibility is ii)-b), that is, A_1 is an arithmetic progression, say $A_1 = d \cdot [0, 2] + e$, and then $A_1 + 3 \cdot A_1 + 1 - A_1 = d \cdot [-2, 8] + 3e + 1$, so by iii) we have that

$$3 \cdot A_0 \subset d \cdot [-2, 8] + 3e + 1. \tag{4.1}$$

Inclusion (4.1) implies that $(d, 3) = 1$.

Suppose $d \equiv 1 \pmod 3$. Then $3 \cdot A_0 \subset d \cdot \{-1, 2, 5, 8\} + 3e + 1$. In this case $A = d \cdot (S \cup \{0, 3, 6\}) + 3e + 1$, where $S = \{-1, 2, 8\}$ or $S = \{-1, 5, 8\}$. Observe that these sets are the only subsets of three elements of $\{-1, 2, 5, 8\}$ satisfying that $|\widehat{\tfrac{1}{3}(S + 1)}| = 2$. Since the problem is invariant by translations and dilations we only have to check the sets $A = \{-1, 0, 2, 3, 6, 8\}$ and $A = \{-1, 0, 3, 5, 6, 8\}$.

If $d \equiv 2 \pmod 3$ the sets we have to check are $A = \{-2, 0, 1, 3, 6, 7\}$ and $A = \{-2, 0, 3, 4, 6, 7\}$. The four sets described satisfy $|A + 3 \cdot A| = 24 \neq 4|A| - 4$.

Case $|\hat{A}_0| = 1,\ |\hat{A}_1| = 3$**.** Since $|\hat{A}_0| = 1$ we have $|A_0 + A| = |(A_0 + 3 \cdot A_0) \cup (A_0 + 3 \cdot A_1 + 1)| = |A_0 + 3 \cdot A_0| + |A_0 + 3 \cdot A_1| \geq 4|A_0| - 4 + |A_0| + |A_1| - 1 = 5|A_0| + |A_1| - 5$. Also we have that $|A_1 + A| \geq |A_1 + 3 \cdot A_1| \geq 4|A_1| - 3$. Then

$$4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 5|A_0| + |A_1| - 5 + 4|A_1| - 3 = 5|A| - 8,$$

thus $|A| \leq 4$. But since $|\hat{A}_0| = 1$ and $|\hat{A}_1| = 3$ we have that $|A_0| = 1$ and $|A_1| = 3$. In this case we get $|A_0 + A| = |A_0 + 3 \cdot A_0| + |A_0 + 3 \cdot A_1| = 1 + |A_1| = 4$. Then

$$12 = 4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 4 + 4|A_1| - 3 = 13$$

and we get a contradiction.

Case $|\hat{A}_0| = 2,\ |\hat{A}_1| = 2$**.** We can write, as in the proof of Lemma 4, $A_0 = A_0^u \cup A_0^{u+1}$ and $A_1 = A_1^v \cup A_1^{v+1}$, where $A_i^j = \{x \in A_i,\ x \equiv j \pmod 3\}$.

$$|A_0 + A| \geq |A_0 + 3 \cdot A_0| + |A_0^{u+1} + 3 \cdot A_1 + 1| \geq 4|A_0| - 4 + |A_1|.$$

Similary $|A_1 + A| \geq 4|A_1| - 4 + |A_0|$. Then $4|A| - 4 = |A + 3 \cdot A| = |A_0 + A| + |A_1 + A| \geq 4|A_0| - 4 + |A_1| + 4|A_1| - 4 + |A_0| = 5|A| - 8$ and thus $|A| \leq 4$. Since $|\hat{A}_0| = |\hat{A}_1| = 2$ we have that $|A_0| = |A_1| = 2$.

Then we write $A_0 = \{a_0, b_0\}$, $A_1 = \{a_1, b_1\}$ with $b_i \equiv a_i + 1 \pmod 3$, $i = 0, 1$, and then

$$\begin{aligned}|A_0 + A| &= |a_0 + 3\cdot A_0| + |(b_0 + 3\cdot A_0) \cup (a_0 + 1 + 3\cdot A_1)| + |b_0 + 1 + 3\cdot A_1| \\ &\geq 4 + |3\cdot A_0 \cup (a_0 - b_0 + 1 + 3\cdot A_1)|, \\ |A_1 + A| &= |a_1 + 3\cdot A_0| + |(b_1 + 3\cdot A_0) \cup (a_1 + 1 + 3\cdot A_1)| + |b_1 + 1 + 3\cdot A_1| \\ &\geq 4 + |3\cdot A_0 \cup (a_1 - b_1 + 1 + 3\cdot A_1)|.\end{aligned}$$

Then

$$\begin{aligned}12 &= 4|A| - 4 = |A + 3\cdot A| = |A_0 + A| + |A_1 + A| \\ &\geq 8 + |3\cdot A_0 \cup (a_0 - b_0 + 1 + 3\cdot A_1)| + |3\cdot A_0 \cup (a_1 - b_1 + 1 + 3\cdot A_1)|.\end{aligned}$$

We claim that $3\cdot A_0 = a_1 - b_1 + 1 + 3\cdot A_1$. If not we would obtain more than 2 elements in the last sum and we get a contradiction. Then $3\cdot A_0 = \{3a_1 + a_1 - b_1 + 1, 3b_1 + a_1 - b_1 + 1\} = \{4a_1 - b_1 + 1, a_1 + 2b_1 + 1\}$, so we obtain a set A like those described in Theorem 1.2,

$$\begin{aligned}A &= 3\cdot A_0 \cup (3\cdot A_1 + 1) = \{4a_1 - b_1, a_1 + 2b_1, 3a_1, 3b_1\} + 1 \\ &= 3b_1 + 1 + (a_1 - b_1)\cdot\{0, 1, 3, 4\}.\end{aligned}$$

Case $|\hat{A}_0| = 1$, $|\hat{A}_1| = 2$. In this case we have

$$|A_0 + A| = |A_0 + 3\cdot A_0| + |A_0 + 3\cdot A_1| \geq 4|A_0| - 4 + |A_0| + |A_1| - 1 = 5|A_0| + |A_1| - 5$$

and we apply Lemma 4-ii) to obtain $|A_1 + A| \geq 4|A_1| + |A_0| - 4$. Then

$$4(|A_0| + |A_1|) - 4 = |A + 3\cdot A| = |A_0 + A| + |A_1 + A| \geq 5|A_0| + |A_1| - 5 + 4|A_1| + |A_0| - 4,$$

so $5 \geq 2|A_0| + |A_1|$. Since $|\hat{A}_1| = 2$ then $|A_1| \geq 2$ and $|A_0| \leq 3/2$; so $|A_0| = 1$. But in this case we have that $|A_0 + A| = |A|$ and $|A_1 + A| \geq 4|A_1| - 3$. Then $4|A_1| = 4|A| - 4 \geq |A| + 4|A_1| - 3$, so $|A| \leq 3$. Indeed, since $|\hat{A}_1| = 2$ and $|\hat{A}_0| = 1$ we have that $|A| = 3$. These cases are analyzed in Lemma 5.

Case $|\hat{A}_0| = 1$, $|\hat{A}_1| = 1$. As above we have $|A_0 + A| \geq 5|A_0| + |A_1| - 5$ and also we have $|A_1 + A| \geq 5|A_1| + |A_0| - 5$. Then $4|A| - 4 = |A + 3\cdot A| = |A_0 + A| + |A_1 + A| \geq 6|A| - 10$, so $|A| \leq 3$ and again Lemma 5 makes the work for us.

5. Small sumsets $A + k\cdot A$

Now we show some constructions that give a small sumset, $A + k\cdot A$, for general $k \in \mathbb{N}$.

Proposition 5.1. *For any $k \in \mathbb{Z}_{>0}$*

i) *there exist arbitrarily large sets A such that*

$$|A + k\cdot A| = (k+1)|A| - \left\lceil \frac{k^2 + 2k}{4} \right\rceil$$

ii) *there exists a set A such that*

$$|A + k\cdot A| = (k+1)|A| - \frac{k^3 + 6k^2 + 9k + \delta_k}{27}$$

where

$$\delta_k = \begin{cases} 3k + 8 & \text{if } k \equiv 1 \pmod 3 \\ 4 & \text{if } k \equiv 2 \pmod 3 \\ 0 & \text{if } k \equiv 0 \pmod 3 \end{cases}.$$

Note: We conjecture that, for a fixed k, the constructions given in i) are the best possible, in the sense that for a large set A we always have $|A + k\cdot A| \geq (k+1)|A| - \left\lceil \frac{k^2+2k}{4} \right\rceil$. But the construction given in ii) says that there are small sets that make the lower bound smaller.

Proof. Following the examples we obtained in the inverse problem for k=3, we consider sets that are unions of arithmetic progressions of difference k. We write

$$A = \bigcup_{i \in I} (k \cdot [0, m-1] + i)$$

where I is an interval, $I = [0, |I| - 1] \subseteq [0, k-1]$. Then $|A| = |I|m$. As in Lemma 2, we have (with $A_i = [0, m-1]$ for all i)

$$|A + k \cdot A| = \sum_{i \in I} |A_i + A|.$$

and

$$A_i + A = [0, m-1] + \bigcup_{i \in I} (k \cdot [0, m-1] + i) = [0, m-1] + k \cdot [0, m-1] + I.$$

Now, we try to find the sets of this shape that give us the smallest sumset, $A + k \cdot A$.

i) If $m \geq k$

$$A_i + A = [0, (k+1)(m-1) + |I| - 1]$$

so

$$|A + k \cdot A| = |I|((k+1)(m-1) + |I|) = (k+1)|A| - |I|(k+1-|I|).$$

We want to maximize $|I|(k+1-|I|)$ in order to get an A with small sumset. If we think on $|I|$ as a real number we can look at the derivative to see that this happens when $|I| = \frac{k+1}{2}$. If k is odd everything works and if k is even we take $|I| = \frac{k}{2}$ or $|I| = \frac{k+2}{2}$ and in any case we have the formula of the proposition.

ii) If $m < k$ (we are thinking that $k > 1$ and $m > 0$ but if $k = 1$ we know we can take for example any A with $|A| = 1$ and $|A + A| = 2|A| - 1$ as the formula of ii) says). Then $A_i + A$ is the union of m intervals of lenght $m + |I| - 1$ starting on $0, k, 2k, \ldots$ and $(m-1)k$. If we don't want this intervals to overlap, then we must impose $m + |I| - 1 \leq k$, i. e. $|I| \leq k + 1 - m$. Then

$$|A_i + A| = (m + |I| - 1)m$$

and

$$|A + k \cdot A| = |I|m(m + |I| - 1) = (k+1)|A| - m|I|(k + 2 - m - |I|).$$

We want to maximize $m|I|(k+2-m-|I|)$. If we think on m and $|I|$ as real numbers, we can look at the gradient to conclude that the maximum occurs for $m = |I| = \frac{k+2}{3}$. If $k \equiv 1$ (3), everything works and we have $|A + k \cdot A| = (k+1)|A| - \left(\frac{k+2}{3}\right)^3$ as in ii) of the theorem. If $k \equiv 2$ (3), we can take $m = |I| = \frac{k+1}{3}$ or one of them equal to $\frac{k+1}{3}$ and the other to $\frac{k+4}{3}$ and we have $|A + k \cdot A| = (k+1)|A| - \left(\frac{k+1}{3}\right)^2 \left(\frac{k+4}{3}\right)$. Finally, if $k \equiv 0$ (3), we take $m = |I| = \frac{k+3}{3}$ or one equal to $\frac{k+3}{3}$ and the other to $\frac{k}{3}$ and we have $|A + k \cdot A| = (k+1)|A| - \left(\frac{k+3}{3}\right)^2 \left(\frac{k}{3}\right)$. This proves ii).

□

References

[1] Melvin B. Nathanson, *Inverse problems for linear forms over finite sets of integers*, arXiv:0708.2304v2 [math.NT] 21 Aug 2007.

[2] Boris Bukh, *Sums of dilates*, arXiv:0711.1610v1 [math.NT] 11 Nov 2007.

Departamento de Matemáticas. Universidad Autónoma de Madrid. 28049 Madrid
E-mail address: `franciscojavier.cilleruelo@uam.es`

Department of Mathematics, New University of Lisbon, Lisbon, Portugal
E-mail address: `mnasilva@gmail.com`

Departamento de Matemáticas. Universidad Autónoma de Madrid. 28049 Madrid
E-mail address: `c.vinuesa@uam.es`