Astérisque

JEAN-MARC DESHOUILLERS
GREGORY A. FREIMAN
VERA SÓS
MIKHAIL TEMKIN

On the structure of sum-free sets, 2

Astérisque, tome 258 (1999), p. 149-161
<http://www.numdam.org/item?id=AST_1999__258__149_0>

Astérisque **258**, 1999, p. 149–161

ON THE STRUCTURE OF SUM-FREE SETS, 2

by

Jean-Marc Deshouillers, Gregory A. Freiman, Vera Sós & Mikhail Temkin

Abstract. — A finite set of positive integers is called sum-free if $\mathbb{A} \cap (\mathbb{A}+\mathbb{A})$ is empty, where $\mathbb{A}+\mathbb{A}$ denotes the set of sums of pairs of non necessarily distinct elements from $\mathbb{A}$. Improving upon a previous result by G.A. Freiman, a precise description of the structure of sum-free sets included in $[1, M]$ with cardinality larger than $0.4M - x$ for $M \geq M_0(x)$ (where x is an arbitrary given number) is given.

1. Introduction

A finite set of positive integers $\mathcal{A}$ is called **sum-free** if $\mathcal{A} \cap (\mathcal{A}+\mathcal{A})$ is empty, where $\mathcal{A}+\mathcal{A}$ denotes the set of sums of pairs of elements from $\mathcal{A}$.

Such sum-free sets have been considered by Cameron and Erdős (cf. [1]), and the first result concerning their structure has been obtained by Freiman (cf. [3]). It is clear that for odd n, the sets $\{1, 3, 5, \ldots, n\}$ and $\{\frac{n+1}{2}, \frac{n+3}{2}, \ldots, n\}$ are sum-free. Freiman showed that when $\mathcal{A}$ is included in $[1, n]$ and its cardinality is at least $5n/12 + 2$, then $\mathcal{A}$ is essentially a subset of the ones we just described. In an unpublished paper, Deshouillers, Freiman and Sós showed the following improvement.

Theorem 1.1. — *Let $\mathcal{A}$ be a sum-free set with minimal element m and maximal element M. Under the assumption that $A = \operatorname{Card}\mathcal{A} > 0.4M + 0.8$, we have either*

(i) : *all the elements of $\mathcal{A}$ are odd,*

(ii) : *the minimal element of $\mathcal{A}$ is at least A, and we have*

$$\operatorname{Card}(\mathcal{A} \cap [1, M/2]) \leq (M - 2A + 3)/4.$$

1991 ***Mathematics Subject Classification.*** — 05 B10, 11 B13.

Key words and phrases. — Sum-free sets, additive number theory, combinatorial number theory, arithmetic progressions.

J.-M. D.: Cette recherche a bénéficié du soutien du CNRS (UMR 9936, Université Bordeaux 1) et de l'Université Victor Segalen Bordeaux 2.

Examples have been produced to show that all the bounds in the theorem are sharp. We are not going to discuss the bound in (ii), but show what may happen if the condition on A is relaxed: let s be a positive integer, and consider

$$\mathcal{A}_1 = \{s, s+1, \dots, 2s-1\} \cap \{4s-1, \dots, 5s-2\},$$

as well as

$$\mathcal{A}_2 = \{2, 3, 7, 8, 12, 13, \dots, 5k-3, 5k-2, \dots, 5s-3, 5s-2\}$$

it is easy to see that $\mathcal{A}_1$ and $\mathcal{A}_2$ are sum-free, that their cardinality, $2s$, is precisely equal to $0.4(5s-2)+0.8$, and that they are very far from satisfying properties (i) or (ii) from Theorem 1.1. A further example, with $A = 0.4M + 0.4$ is

$$\mathcal{A}_3 = \{1, 4, 6, 9, \dots, 5k-4, 5k-1, \dots, 5s-4, 5s-1\}$$

Our aim is to show that when A is not much less than $0.4M$, then the structure of a sum-free set is described by Theorem 1.1, or close to one of the previous examples. More precisely, we have the following

Theorem 1.2. — *Let x be a positive real numbers; there exist real number $M_0(x)$ and $C(x)$ such that for every sum-free set $\mathcal{A}$ with largest element $M \geq M_0(x)$ and cardinality $A \geq 0.4M - x$, at least one of the following properties holds true*

(i) : *all the elements of $\mathcal{A}$ are odd,*
(ii) : *all the elements of $\mathcal{A}$ are congruent to 1 or 4 modulo 5,*
(iii) : *all the elements of $\mathcal{A}$ are congruent to 2 or 3 modulo 5,*
(iv) : *the smallest elements of $\mathcal{A}$ is at least equal to A and we have $|\mathcal{A} \cap [1, M/2]| \leq (M - 2A + 3)/4$*
(v) : *$\mathcal{A}$ is included in $[\frac{M}{5} - C(x), \frac{2M}{5} + C(x)] \cup [\frac{4M}{5} - C(x), M]$.*

The constants $C(x)$ and $M_0(x)$ may be computed explicitly from our proof. However, they are not good enough to lead us to the structure of $\mathcal{A}$ when A is about $0.375M$, where new structures appear.

We may reduce the proof of Theorem 1.2 to the case when $\mathcal{A}$ contains at least one even element. From now on, we take this assumption for granted. The proof will be conducted according to the location of the smallest element m of $\mathcal{A}$: section 4 and 5 are devoted to show that m is around 1 or $M/5$, or that it is at least equal to A; the structure of $\mathcal{A}$ will be deduced from this location in section 6 and 7. Section 3 aims at filling the gap between the content of [3] and a proof of Theorem 1.1, as well as presenting in a simple frame some of the ideas that will be developed later on. In the next section, we present our notation as well as general results.

2. Notation - General results

Letters $\mathcal{A}, \mathcal{B}, \mathcal{C}, \dots$ with or without indices or other diacritical symbols denote finite sets of integers. Their cardinality is represented by $|\mathcal{A}|, |\mathcal{B}|, |\mathcal{C}|, \dots$ or $A, B, C, \dots$ with the same diacritical symbols. For a non empty set $\mathcal{B}$, we further let

$M(\mathcal{B})$: be its maximal element,
$m(\mathcal{B})$: be its minimal element,

$l(\mathcal{B})$: be its length, i.e. $M(\mathcal{B}) - m(\mathcal{B}) + 1$,
$d(\mathcal{B})$: be the gcd of all the differences $(b_i - b_j)$ between pairs of elements of $\mathcal{B}$,
$\mathcal{B}_+ := \mathcal{B} \cap [1, +\infty[$.

The letter $\mathcal{A}$ is restricted to denote a non empty sum-free set of positive integers, and we let

$$\mathcal{A}_0 = \mathcal{A} \cap 2\mathbb{Z},\ \mathcal{A}_1 = \mathcal{A} \cap (2\mathbb{Z}+1),$$

$$\mathcal{A}^- = \mathcal{A} \cap [1, M/2],\ \mathcal{A}^+ = \mathcal{A} \cap [M/2, M],$$

M (resp. m, resp. $M_0, \dots$) denote $M(\mathcal{A})$ (resp. $m(\mathcal{A})$, resp. $M(\mathcal{A}_0)\cdots$).

By x we denote a real number larger than -1. All the constants $C_1, C_2, \dots$ depend on x at most, and their value may change from one section to the other. Further, when we say that a property holds for M sufficiently large, we understand that there exist $M_0(x)$ depending on x at most, such that the considered property holds for M at least equal to $M_0(x)$.

We turn now our attention towards general results that will be used systematically, beginning with section 4.

Definition 2.1. — *A set $\mathcal{A}$ of positive integers is said to satisfy the general assumptions if it is a sum-free set that contains at least one even element and has cardinality $A = 0.4M - x$.*

Proposition 2.1. — *If $\mathcal{A}$ satisfies the general assumptions and M is large enough, we have the following properties*

(i) : *$\mathcal{A}$ contains an odd number,*
(ii) : $d(\mathcal{A}) = 1$,
(iii) : *$\mathcal{A} \cap (\mathcal{A} - \mathcal{A})$ is empty,*
(iv) : $M - m \geq 2A - 2 \Longrightarrow |(\mathcal{A} - \mathcal{A})_+| \geq \frac{3}{2}A - 2$,
(v) : $M - m \leq 2A - 3 \Longrightarrow |(\mathcal{A} - \mathcal{A})_+| \geq (M - m + A - 1)/2$,
(vi) : *for any integers u and v :* $|\mathcal{A} \cap [u, u+v]| \leq (v+m)/2$,
(vii) : *for any integer u :* $|\mathcal{A} \cap [u, u+2m]| \leq m$

Proof

(i) If $\mathcal{A}$ contains only even numbers, then the set $\mathcal{A}/2 = \{a/2 | a \in \mathcal{A}\}$ is a sum-free set that is contained in $[1, M/2]$, and so its cardinality is at most $M/4 + 1$ as can be directly seen (cf. also [4]). But $|\mathcal{A}/2| = |\mathcal{A}| = 0.4M - x$ which is larger than $M/4 + 1$ when M is large enough.

(ii) The number $d(\mathcal{A})$ is defined in such a way that $\mathcal{A}$ is included in an arithmetic progression modulo $d(\mathcal{A})$. Since $\mathcal{A}$ contains an even number (by our general assumption) as well as an odd number (by (i)), we have $d(\mathcal{A}) \neq 2$. On the other hand, we cannot have $d(\mathcal{A}) \geq 3$, otherwise $\mathcal{A}$ would have at most $M/3 + 1$ elements, which would contradict our general assumptions. Thus, $d(\mathcal{A}) = 1$.

(iii) Let $b \in \mathcal{A} \cap (\mathcal{A} - \mathcal{A})$. We can find a_1, a_2, a_3 in $\mathcal{A}$ such that $b = a_1 = a_2 - a_3$. This implies $a_2 = a_1 + a_3$, which is impossible. Thus $\mathcal{A} \cap (\mathcal{A} - \mathcal{A})$ is empty, and our argument shows even that last condition implies that $\mathcal{A}$ is sum-free.

(iv) and (v) are straightforward application of the following result ([2] and [5]):

Lemma 2.1. — *Let $\mathcal{B}$ and $\mathcal{C}$ be to finite sets of integers with $m(\mathcal{B}) = m(\mathcal{C}) = 0$, and let $M(\mathcal{B},\mathcal{C})$ be $max(M(\mathcal{B}), M(\mathcal{C}))$.*
If $M(\mathcal{B},\mathcal{C}) \leq |\mathcal{B}| + |\mathcal{C}| - 3$, then we have $|\mathcal{B}+\mathcal{C}| \geq M(\mathcal{B}) + |\mathcal{C}|$.
If $M(\mathcal{B},\mathcal{C}) \geq |\mathcal{B}| + |\mathcal{C}| - 2$ and $d(\mathcal{B}\cup\mathcal{C}) = 1$, then we have $|\mathcal{B}+\mathcal{C}| \geq M(\mathcal{B}) + |\mathcal{C}| - 3 + min(|\mathcal{B}|, |\mathcal{C}|)$.

(vi) The result is obvious when $v \leq m$, so we way assume $v > m$. We let $\mathcal{B} = \mathcal{A} \cap [u, u+v-m]$ and $\mathcal{C} = \mathcal{A} \cap [u+m, u+v]$. Since $\mathcal{A}$ is sum-free and m is in $\mathcal{A}$, we have $|\mathcal{B}| + |\mathcal{C}| \leq v - m$. Combined with the trivial upper bound $|\mathcal{A}| \leq |\mathcal{B}| + m$ and $|\mathcal{A}| \leq |\mathcal{C}| + m$, this inequality leads us to (vi).
(vii) We apply the same argument as above, leading to $|\mathcal{B}| + |\mathcal{C}| \leq v - m = m$, and further notice that $\mathcal{A}\cap]u, u+2m]$ is the union of $\mathcal{B}$ and $\mathcal{C}$.

The next results are fairly simple.

Lemma 2.2. — *Let $\mathcal{B}$ be a finite set of integers such that $2|\mathcal{B}| > l(\mathcal{B})$. Then $\mathcal{B} - \mathcal{B}$ contains $[1, 2|\mathcal{B}| - l(\mathcal{B}) - 1]$.*

Proof. — We consider a positive integer y which is not the difference of two elements of $\mathcal{B}$. We way assume $\mathcal{B} \subset [1, l(\mathcal{B})]$ and let

$$\begin{array}{ll} \mathcal{B}_1 = \mathcal{B} \cap [1, y] & , \mathcal{B}_2 = \mathcal{B} \cap [y+1, l(\mathcal{B})], \\ \mathcal{B}_3 = \mathcal{B} \cap [1, l(\mathcal{B}) - y] & , \mathcal{B}_4 = \mathcal{B} \cap [l(\mathcal{B}) - y + 1, l(\mathcal{B})]. \end{array}$$

Since y is not difference of two elements of $\mathcal{B}$, the sets $\mathcal{B}_2$ and $\mathcal{B}_3 + y$ are disjoint so that we have

$$|\mathcal{B}_2| + |\mathcal{B}_3| \leq l(\mathcal{B}) - y.$$

This easily leads to

$$2|\mathcal{B}| = |\mathcal{B}_1| + |\mathcal{B}_2| + |\mathcal{B}_3| + |\mathcal{B}_4| \leq y + l(\mathcal{B}) - y + y = l(\mathcal{B}) + y,$$

whence the inequality $y \geq 2|\mathcal{B}| - l(\mathcal{B})$.

Lemma 2.3. — *Let $\mathcal{B} = \{b_1 < b_2 < \cdots < b_B\}$ and $\mathcal{D} = \{d_1 < \cdots < d_D\}$ be to sets of integers such that we have $b_{i+1} - b_i < l(\mathcal{D})$ for $1 \leq i \leq B-1$, and card$\mathcal{D} \geq l(\mathcal{D}) - C$. We have $|\mathcal{B}+\mathcal{D}| \geq (l(\mathcal{B}) + l(\mathcal{D}) + 1)(1 - 3C/l(\mathcal{D}))$*

Proof. — Let $l(\mathcal{D}) = d_D - d_1 + 1$. We show that for any integer $u \in [b_1 + d_1, b_B + d_1[$, the interval $[u, u + l(\mathcal{D})]$ contains at most $2C$ integers which are not in $\mathcal{B} + \mathcal{D}$. We define the integer i such that $b_i + d_1 \leq u < b_{i+1} + d_1$. Since $b_{i+1} - b_i$ is less than $l(\mathcal{D})$, the interval $[u, u + l(\mathcal{D})]$ is included in $[b_i + d_1, b_{i+1} + d_D]$, which contains only elements in $\{b_i, b_{i+1}\} + \mathcal{D}$, with at most $2C$ exception. Since $[b_1 + d_1, b_B + d_D]$ can be covered with at most $(b_B + d_D + b_1 + d_1 + 1)/l(\mathcal{D}) + 1$ intervals of length $l(\mathcal{D})$, we have

$$\begin{array}{rcl} |\mathcal{B}+\mathcal{D}| & \geq & l(\mathcal{B}) + l(\mathcal{D}) + 1 - ((l(\mathcal{B}) + l(\mathcal{D}) + 1)/l(\mathcal{D}) + 1)2C \\ & \geq & (l(\mathcal{B}) + l(\mathcal{D}) + 1)(1 - 3C/l(\mathcal{D})). \end{array}$$

3. Contribution to the proof of Theorem 1.1

Combined with the result of [3], the following proposition leads to a proof of Theorem 1.1.

Proposition 3.1. — *Let $\mathcal{A}$ be a sum-free set of positive elements containing at least one even and one odd numbers, such that*

$$0.4M + 1 \leq A.$$

Then m is either smaller than $0.2M + 1$ or at least equal to $0.25M$.

Proof. — We assume on the contrary that we have

$$0.2M + 1 \leq m \leq 0.25M.$$

This condition implies the chain of inequalities

$$0 < m < M - 3m < (M - m)/2 < 2m < M - 2m < M - m < M.$$

Let $m - \eta$ denote $|\mathcal{A} \cap]M - m, M]|$. Since the interval $]M - m, M]$ is shifted from $]M - 2m, M - m]$ by m which belongs to $\mathcal{A}$, the number of elements in $]M - 2m, M - m]$ is at most η.

The two intervals $]m, M - 3m]$, $]2m, M - 2m]$ being shifted by m, there are at most $M - 4m + 1$ elements from $\mathcal{A}$ in their union.

The interval $]M - 3m, \frac{M-2m}{2}]$ contains $(M - m)/2 - M + 3m$ integers, and so at most $(M - m)/2 - M + 3m$ elements from $\mathcal{A}$.

Let now $\mathcal{B} = \mathcal{A} \cap]\frac{M-m}{2}, 2m[$; then

$$\mathcal{B} + \mathcal{B} \subset (\mathcal{A} + \mathcal{A}) \cap]M - m, 4m[\subset (\mathcal{A} + \mathcal{A}) \cap [M - m, M].$$

Since $\mathcal{A}$ is sum-free, there are at most η elements of $\mathcal{A} + \mathcal{A}$ in $]M - m, M]$, which implies that $|\mathcal{B} + \mathcal{B}|$ is at most η and so $|\mathcal{B}|$ is at most $(\eta + 1)/2$.

Putting all those upper bounds together, we obtain

$$\begin{aligned} A &\leq m - \eta + \eta + M - 4m + 1 + (M - m)/2 - M + 3m + (\eta + 1)/2 \\ &\leq (M - m + 3 + \eta)/2. \end{aligned}$$

Our last step is to obtain an upper bound for η. By Proposition 2.1, we have

$$|(\mathcal{A} - \mathcal{A})_+| > (A - 1 + M - m)/2,$$

and since $\mathcal{A}$ is sum-free, the intersection $\mathcal{A} \cap (\mathcal{A} - \mathcal{A})_+$ is empty. This implies that we have

$$|\mathcal{A}| + |(\mathcal{A} - \mathcal{A})_+| > (3A - 1 + M - m)/2;$$

the total number of elements in $[1, M]$ which are not in $\mathcal{A} \cup (\mathcal{A} - \mathcal{A})_+$ is thus less than

$$M - (3A - 1 + M - m)/2 = (M + m + 1 - 3A)/2,$$

and this is also an upper bound for $|(\mathcal{A} \cup (\mathcal{A} - \mathcal{A})_+) \cap]M - m, M]|$. Since $]M - m, M]$ contains no elements from $(\mathcal{A} - \mathcal{A})_+$, we have $\eta < (M + m + 1 - 3A)/2$, which implies

$$\begin{aligned} A &< (M-m+3)/2+(M+m+1-3A)/4A \\ &\leq (M-m+3)/2+(M+m+1-1.2M-3)/4 \\ &\leq 0.45M-0.25m+1 \\ &\leq 0.4M+0.75<A, \end{aligned}$$

a contradiction which proves the proposition.

4. On the location of m in $[1, M/5]$

Proposition 4.1. — *Under our general assumptions, there exists C such that $m \notin [C, M/5-C]$, when M is large enough.*

Proof. — We assume that $m \in [C, M/5-C]$, and that C has been chosen sufficiently large. We have

$$M-m \geq 4M/5+C \geq 2(2M/5-x)-2 = 2A-2,$$

so that properties (iii) and (iv) from Proposition 2.1 imply

$$|\mathcal{A} \cup (\mathcal{A}-\mathcal{A})_+| = |\mathcal{A}|+|(\mathcal{A}-\mathcal{A})_+| \geq 5A/2-2 = M-C_2.$$

Since $]M-m, M] \cap (\mathcal{A}-\mathcal{A})_+$ is empty, we have

$$|]M-m, M] \cap \mathcal{A}| \geq m-C_2, \tag{4.1}$$

which in turn implies

$$|[1, m[\cap(\mathcal{A}-\mathcal{A})_+| \geq m-C_2. \tag{4.2}$$

On the other hand, we have

$$M \geq |\mathcal{A} \cup (\mathcal{A}-\mathcal{A}_+)| = |\mathcal{A}|+|(\mathcal{A}-\mathcal{A})_+| = 2M/5-x+(\mathcal{A}-\mathcal{A})_+|$$

so that we get

$$m-C_2 \leq |(\mathcal{A}-\mathcal{A})_+| \leq 3M/5+x. \tag{4.3}$$

which will be used later on.

We define the integer k and the sequence $a^{(1)} < \cdots < a^{(k)} \leq M-2m$ to be the set of elements a in $\mathcal{A}$ such that $]a-m, a[$ contains no element from $\mathcal{A}$. We further let $a^{(k+1)} = M-2m+1$, and

$$\mathcal{A}^{(i)} = [a^{(i)}, a^{(i+1)}[\cap\mathcal{A},$$

and $l^{(i)} = M(\mathcal{A}^{(i)}) - m(\mathcal{A}^{(i)}) + 1$, for $i = 1, \ldots, k$. We use (vi) (resp. (vii)) in Proposition 2.1 to get an upper bound for $A^{(i)}$ (resp. $]M-2m, M] \cap \mathcal{A}$), which leads us to

$$2M/5-x = A \leq \sum_{i=1}^{k}(l^{(i)}+m)/2+m. \tag{4.4}$$

Let us consider the set $\mathcal{D} =]M-m, M] \cap \mathcal{A}$. We already noticed in (4.1) that its cardinality is at least $m-C_2$, and Lemma 2.3 leads us to

$$|\mathcal{D}-\mathcal{A}^{(i)}| \geq (1-\frac{4C_2}{m})(l^{(i)}+m-1) \text{for} i = 1, \ldots, k. \tag{4.5}$$

We easily notice that the sets $(\mathcal{D} - \mathcal{A}^{(i)})$ are pairwise disjoint, and disjoint from $(\mathcal{A} - \mathcal{A})_+ \cap [1, m[$. Relation (4.3) in conjunction with (4.2) and (4.5) implies

$$m - C_2 + \sum_{i=1}^{k} (1 - \frac{4C_2}{m})(l^{(i)} + m - 1) \leq 3M/5 + x,$$

and the use of (4.4) leads to

$$m - C_2 + (1 - \frac{4C_2}{m})(2A - 2m) - k \leq 3M/5 + x.$$

Since the $a^{(i)}$ are separated by intervals of length m, we have $km < M$, and we are led to a quadratic inequality

$$m^2 - m(M/5 - C_4) + C_5 M > 0$$

which cannot be fulfilled if $m \in [C, M/5 - C]$, for C sufficiently large.

5. On the location of m in $[M/5, A]$

Proposition 5.1. — *Under our general assumptions, there exists C such that $m \notin [M/5 + C, A[$, when M is large enough.*

We first assume that $m \in]M/3, A[$; in this case, we have $\mathcal{A} \subset]M - 2m, M]$, and relation (vii) in Proposition (2.1) implies $A = |\mathcal{A} \cap]M - 2m, M]| \leq m$, a contradiction.

We now assume that $m \in [M/5 + C, M/3]$, for some sufficiently large C. We then have $M - m \leq 4M/5 - C \leq 2A - 3$, so that relations (iii) and (v) in Proposition (2.1) imply

$$|\mathcal{A} \cup (\mathcal{A} - \mathcal{A})_+| \geq (3M - m + A - 1)/2 = M - (5m - M)/10 - C_1.$$

In the same way as we obtained (4.1), we get

$$|]M - m, M] \cap \mathcal{A}| \geq m - (5m - M)/10 - C_1. \tag{5.1}$$

This relation will be used to get an upper bound for the cardinality of $\mathcal{B} = \mathcal{A} \cap](M - m)/2, M/2]$; we have $\mathcal{B} + \mathcal{B} \subset]M - m, M]$, so that (4.1) implies $|\mathcal{B} + \mathcal{B}| \leq (5m - M)/10 + C_1$, and so we get

$$|\mathcal{B}| \leq (5m - M)/20 + C_2.$$

When we combine this inequality with an easy consequence of relation (vii) in Proposition 2.1, we get

$$|\mathcal{A} \cap (]\frac{M - n}{2}, \frac{M}{2}] \cup]M - 2M, M])| \leq (25m - M)/20 + C_2. \tag{5.2}$$

We consider finally two subcases, according as m is larger than $M/4$ or smaller. If $m \in]M/4, M/3]$, we have the chain of inequalities

$$m \leq (M - m)/2 \leq M - 2m \leq M/2 \leq M - m \leq M,$$

so that (4.2) and a trivial upper bound $[m, (M - m)/2]$ leads to

$$\begin{aligned} A &\leq (25m - M)/20 + C_2 + (M - m)/2 - m + 1 \\ &\leq \tfrac{9M}{20} - \tfrac{m}{4} + C_3 \leq \tfrac{22M}{60} + C_3, \end{aligned}$$

which is less than $\frac{24M}{60} - x = A$, when M is large enough.

We are thus left to consider the case when $m \in]M/5 + C, M/4]$, in which we have the chain of inequalities

$$m \leq (M-m)/2 \leq M/2 \leq M - 2m \leq M.$$

We easily see that the interval $[m+m, (M-m)/2+m]$ covers the interval $[M/2, M-2m]$, so that the number of elements in $\mathcal{A}$ that lie in $[m, (M-m)/2] \cup [M/2, M-2m]$ is at most the number of integers that lie in $[m, (M-m)/2]$. This means that we get as above

$$\begin{aligned} A &\leq \tfrac{9M}{20} - \tfrac{m}{4} + C_3 \\ &\leq (2M)/5 + C_3 - C/4 \end{aligned}$$

which is again a contradiction, when C is large enough.

6. The structure of $\mathcal{A}$ when its minimal value is close to $M/5$

We prove in this section that if the minimal element m of $\mathcal{A}$ is close to $M/5$, in the sense that there exists C such that $M/5 - C < m < M/5 + C$, and $\mathcal{A}$ satisfy our general assumptions, then we are in the case (v) of Theorem 1.2.

Our first step is to show that there exist C_1 and C_2 such hat all elements from $\mathcal{A}$, with at most C_2 exception, lie in $[M/5 - C_1, 2M/5 + C_1] \cup [4M/5 - C_1, M]$. The argument is very similar to that of the previous section, so we just present a sketch of it. We have the chain of inequalities

$$m \leq (M-m)/2 \leq M/2 \leq M - 2m \leq M - m \leq M,$$

and m is about $M/5$, $(M-m)/2$ is about $2M/5$, $M-2m$ is about $3M/5$ and $M-m$ is about $4M/5$.

We may apply (iv) or (v) from Proposition 2.1, getting $|(\mathcal{A} - \mathcal{A})_+| \geq 3M/5 - C_3$. This implies that $|\mathcal{A} \cap]M-m, M]| \geq m - C_4$ so that $|\mathcal{A} \cap]M-2m, M-m]| \leq C_4$, as well as $|\mathcal{A} \cap](M-m)/2, M/2]| \leq C_5$ by using respectively the translation by m and the doubling argument. It remains to take care of $]M/2, M-2m]$. Summing up what we have up to now, we know that at least $M/5 - C_6$ elements of $\mathcal{A}$ are located in $[m, M-3m] \cup]M/2, M-2m]$. By translating by m, we know that there are at most $M/10 + C_7$ elements of $\mathcal{A}$ in $]\frac{M}{2} - m, M-3m] \cup]M/2, M-2m]$, so that there remain at least $M/10 + C_8$ elements of $\mathcal{A}$ in $[m, M/2 - m]$. This implies that $\mathcal{A} + \mathcal{A}$ almost covers $[2m, M-2m]$, so that it almost covers $]M/2, M-2m]$, whence there are at most C_9 elements of $\mathcal{A}$ in $]M/2, M-2m]$, which ends the proof of the first step.

In the second and last step, we show that there is no element of $\mathcal{A}$ in $I =]2M/5 + 2C_2 + 2 - 2C_1, 4M/5 + C_1 - 2C_2 - 2[$. Let indeed y be an element in this set. Since we have $M/5 - C_1 + y < M - 2C_2 + 2$, and $2M/5 + C_1 + y > 4M/5 - C_1 + 2C_2 + 2$ the two intervals $[M/5 - C_1 + y, 2M/5 + C_1 + y]$ and $[4M/5 - C_1, M]$ have at least $2C_2 + 1$ integers in common. Thanks to the first step and the pigeon-hole principle, we know that there exist a_1 and a_2 in $\mathcal{A}$ such that $a_1 + y = a_2$, thus y cannot belong to $\mathcal{A}$, and $\mathcal{A}$ is concentrated in $[m, 2M/5 + C_{10}] \cup [4M/5 - C_{10}, M]$ as we wished to show.

7. Some properties of $\mathcal{A}$ when m is small

We recall our notation, namely

$$\mathcal{A}_0 = \mathcal{A} \cap 2\mathbb{Z},\ \mathcal{A}_1 = \mathcal{A} \cap (2\mathbb{Z}+1),$$

$$\mathcal{A}^- = \mathcal{A} \cap [1, M/2],\ \mathcal{A}^+ = \mathcal{A} \cap [M/2, M],$$

$m = m^- = \min(\mathcal{A})$, $M = M^+ = \max(\mathcal{A})$, $m_0 = \min(\mathcal{A}_0)$.

In his section we prove the following.

Proposition 7.1. — *Let $\mathcal{A}$ satisfy our general assumptions, and be such that $m < M/20$. There exists C such that, when M is large enough, we have*

$$||\mathcal{A}^-| - M/5| \leq C, \tag{7.1}$$

$$m_0 \leq C. \tag{7.2}$$

The proof will be led in three steps, where we prove that (7.1) holds, then that we have the following inequality

$$|\mathcal{A}_0| \geq M/5 - C, \tag{7.3}$$

and finally that (7.2) holds.

7.1. The set $\mathcal{A}$ is balanced between small and large elements. — We first show that $\mathcal{A}^-$ cannot be too large. Indeed, if $|\mathcal{A}^-| > M/5+2$, we may apply Theorem 1.1, and, since $m(\mathcal{A}^-) = m < M/20$, the set $\mathcal{A}^-$ consists only of odd elements, so that $m_0 \geq M/2$. There are at most $m_0/4$ elements from $\mathcal{A}$ in $[1, m_0[$, since they are odd, m_0 is in $\mathcal{A}$, and at most $(M - m_0 + M/20)/2$ elements from $\mathcal{A}$ in $]m_0, M]$, so that $2M/5 - x \leq m_0/4 + (M - m_0 + M/20)/2 + 1$, which implies $M/2 \leq m_0 \leq 9M/20 + C_1$, a contradiction.

We now show that the two simultaneous relations $|\mathcal{A}^+| > M/5 + C_2$ and $d(\mathcal{A}^+) > 1$ lead to a contradiction. We first notice that $\mathcal{A}^+$ contains at least $M/5$ elements, so that $d(\mathcal{A}^+) > 1$ is equivalent to $d(\mathcal{A}^+) = 2$, i.e. $\mathcal{A}^+$ consists only of odd integers, or of even integers. In either case, Lemma 2.2 implies that $(\mathcal{A}^+ - \mathcal{A}^+)$ contains all the non-negative even integers at most equal to $4|\mathcal{A}^+| - M/2$. So we have $m_0 > |\mathcal{A}^+| - M/2 \geq 3M/10$.

Assume that we have $|\mathcal{A}^+| > M/5 + C_2$ and that $\mathcal{A}^+$ consists only of even numbers. We have already shown that all the elements in $\mathcal{A} \cap [1, M/4]$ are odd, so there are at most $M/8$ of them. Thus, $\mathcal{A} \cap]M/4, M/2]$ has at least $|\mathcal{A}^-| - M/8$ elements. By doubling them, we obtain $|\mathcal{A}^-| - M/8$ even numbers in $]M/2, M] \setminus \mathcal{A}$. The total number of even number in $]M/2, M]$, which is about $M/4$, must be at least $|\mathcal{A}^+| + |\mathcal{A}^-| - M/8$, leading to a contradiction with $|\mathcal{A}| = |\mathcal{A}^+| + |\mathcal{A}^-| = 2M/5 - x$.

We now assume that $|\mathcal{A}^+| > M/5 + C_2$ and that $\mathcal{A}^+$ consists of odd numbers, so that $M_0 \leq M/2$. Let u be the number of odd elements less that M_0 which are in $\mathcal{A}$. There are at most $M_0/2 - u$ odd elements in $\mathcal{A} \cap]M_0, 2M_0]$, since $(2a+1) + M_0$ is odd and cannot be in $\mathcal{A}$ when $2a+1$ is in $\mathcal{A}$. In $\mathcal{A}$, there are thus at most $M_0/2 + (M - 2M_0)/2$ odd elements, and the number of even elements in $\mathcal{A}$ is at least $2M/5 - x - (M - M_0)/2$. The largest even element in $\mathcal{A}$ is at least $m_0 + 2(2M/5 -$

$x - (M - M_0)/2) = m_0 + M_0 - M/5 - 2x$, which implies $m_0 \leq M/5 + 2x$, which contradicts the inequality $m_0 \geq 3M/10$ we already obtained.

It remains to show that when $d(\mathcal{A}^+) = 1$, the set $\mathcal{A}^+$ cannot be too large. We apply Lemma 2.1 with $\mathcal{B} = \mathcal{A}^+ - \{m^+\}$ and $\mathcal{C} = \{M^+\} - \mathcal{A}^+$. By Proposition 2.1, we have $m < C_3$, and this implies that $M(\mathcal{B})$ is larger than $2|\mathcal{B}| - C_4$. Either case of Lemma 2.1 leads to $|\mathcal{B}+\mathcal{C}| \geq 3|\mathcal{A}^+| - C_5$, so that we have $|(\mathcal{A}^+ - \mathcal{A}^+)_+| \geq 3|\mathcal{A}^+|/2 - C_6$. But the set $(\mathcal{A}^+ - \mathcal{A}^+)_+$ is included in $[1, M/2]$ and disjoint from $\mathcal{A}^-$, so that we have $3|\mathcal{A}^+|/2 + |\mathcal{A}^-| \leq M/2 + C_7$, or $|\mathcal{A}^+|/2 \leq M/2 + C_7 - |\mathcal{A}| = M/2 + C_7 - 2M/5 + x$, which implies $|\mathcal{A}^+| \leq M/5 + C_8$, or $|\mathcal{A}^-| \geq M/5 - C_9$.

We have so far proved that (7.1) holds.

7.2. The set $\mathcal{A}$ contains many even numbers. — We assume in this subsection that (7.3) does not hold, so that we have $|\mathcal{A}_1| > |\mathcal{A}_0|$.

Since m_0 in the least even element in $\mathcal{A}$, we have $|\mathcal{A} \cap [1, m_0]| \leq m_0/4$, and because $m < C_2$, we have $|\mathcal{A} \cap [m_0, M]| \leq (M - m_0)/2 + C_3$. We thus have

$$2M/5 - x = |\mathcal{A}| \leq m_0/4 + (M - m_0)/2 + C_3, \text{ whence } m_0 \leq 2M/5 + C_4.$$

We may apply he same reasoning to $\mathcal{A}^-$, since we now know that $m_0 < M/2$; using (7.1), we get $m_0 \leq M/5 + C_5$.

By repeating the argument used in previous section, as well as the previous one, we may show, that, up to a constant, $|\mathcal{A} \cap [1, M/4]|$ is about $M/10$, so that $m_0 \leq M/10 + C_6$. We may reduce further the bound on m_0 by the same type of idea, but this would lead us only to $m_0 \leq \varepsilon M$ for any positive ε which is not as strong an inequality as the one we need.

We wish to apply Lemma 2.1 with

$$\mathcal{B} = \{(a_0 - m_0)/2,\ a_0 \in \mathcal{A}_0\} \text{ and } \mathcal{C} = \{(M_1 - a_1)/2, a_1 \in \mathcal{A}_1\}.$$

We have $|\mathcal{B}| = |\mathcal{A}_0|$, $|\mathcal{C}| = |\mathcal{A}_1|$ and

$$\max(M(\mathcal{B}), M(\mathcal{C})) \geq (M - M/10 - C_6)/2 > |\mathcal{A}| - 3 = |\mathcal{B}| + |\mathcal{C}| - 3.$$

Since $\mathcal{B} \cup \mathcal{C}$ contains more than $M/6$ elements and is included in $[0, M/2[$, we have $d(\mathcal{B} \cup \mathcal{C}) = 1$ or 2. We first show that when $d(\mathcal{B} \cup \mathcal{C}) = 2$ then $\mathcal{A}_0$ is large.

When $d(\mathcal{B} \cup \mathcal{C}) = 2$, even elements of $\mathcal{A}$ are either all congruent to 0 modulo 4 or all congruent to 2 modulo 4, and in the same way, odd elements of $\mathcal{A}$ are either all congruent to 1 modulo 4, or all congruent to 3 modulo 4.

If m_0 is congruent to 0 modulo 4, then the set $\{m_0\}+\mathcal{A}_1$ and $\mathcal{A}_1$ are disjoint, in the same class modulo 4 and included in $[1, M+M/10+C_6]$, so that $2|\mathcal{A}_1| \leq 11M/40+C_6$, in contradiction to $|\mathcal{A}_1| > M/5 - C_1$.

If all the even elements are congruent to 2 modulo 4, we are going to use the fact that the sum of two elements in $\mathcal{A}_1$ is also congruent to 2 modulo 4. We first notice that the number of elements in $\mathcal{A}_1$ is at most $M/4$, so that $|\mathcal{A}_0|$ is least $2M/5 - x - M/4 = 3M/20 - x$, which implies that M_0 is at least equal to $3M/5 - x$. The number of odd elements is at most $M_0/8 + (M - M_0)/4 + 1$, which is less than $7M/40 + C$, contradicting our assumption that $|\mathcal{A}_1| > 8M/40 - C_1$.

We now know that $d(\mathcal{B} \cup \mathcal{C}) = 1$, and Lemma 2.1 leads to

$$|(\mathcal{A}_0 - \{m_0\}) + (\{l_1\} - \mathcal{A}_1)| \geq |\mathcal{A}_1| + 2|\mathcal{A}_0| - 3.$$

Since $(\mathcal{A}_0 - \mathcal{A}_1)_+ \cap \mathcal{A}_1 = \varnothing$, we get $|\mathcal{A}_1| + |(\mathcal{A}_0 + \mathcal{A}_1)_+| \leq M/2$, and in the same way $|\mathcal{A}_1| + |(\mathcal{A}_1 + \mathcal{A}_0)_+| \leq M/2$. This leads to

$$M \geq 2|\mathcal{A}_1| + |\mathcal{A}_1 + \mathcal{A}_0| \geq 3|\mathcal{A}_1| + 2|\mathcal{A}_0| - 3 \geq |\mathcal{A}_1| + 4M/5 - 2x - 3,$$

which implies that $|\mathcal{A}_1| \leq M/5 + 2x + 3$, whence (7.3) holds.

7.3. The set $\mathcal{A}$ contains a small even number. — Since we have (7.3), we may apply to the set $\{a_0/2, a_0 \in \mathcal{A}_0\}$ the result we have obtained so far. One of the following cases holds

(i) : $\mathcal{A}_0 \subset 4\mathbb{Z} + 2$,
(ii) : $m_0 > 2M/5 + C_1$,
(iii) : $\mathcal{A}_0 \subset [M/5 - C_1, 2M/5 + C_1] \cup [4M/5 - C_1, M]$,
(iv) : $m_0 < C$,

so that we just have to rule out the first three cases in order to complete the proof of Proposition 7.1.

Case (i) cannot hold because the sets $\{2a_1, a_1 \in \mathcal{A}_1\}$ and $\mathcal{A}_0$ are disjoint, included in $[1, M] \cap (4\mathbb{Z} + 2)$, and the cardinality of their union is $\mathcal{A}$ which is larger than $M/4 + 1$.

Cases (ii) and (iii) cannot hold, because the argument we used at the beginning of (7.2) implies that m_0 is less than $M/10$, up to a constant.

8. End of the proof of Theorem 1.2

Let $\mathcal{A}$ be a sum-free set satisfying our general assumptions. We know that $m \in [1, C] \cup [M/5 - C, M/5 + C] \cup [A, M]$. We have already shown that $m \in [M/5 - C, M/5 + C]$ leads to case (v) in Theorem 1.2. The argument given in [3] for the second case in Theorem 1.1 implies that $m \in [A, M]$ leads to case (iv). It remains to show that $m \leq C$ leads to case (ii) or (iii). We shall make use of Proposition 7.1 and retain in the sequel the notation C for constant implied in (7.1) and (7.2). We let $C_1 = 38C + 60$.

Our first task is to show that we can find a_1 and a_2 in $\mathcal{A} \cap [M/2 - C_1, M/2]$ such that $a_2 = a_1 + m_0/2$. We assume that it is not the case; by this assumption and the fact that m_0 is in $\mathcal{A}$, any interval of length $3m_0/2$ in $[M/2 - C_1, M/2]$ contains at most $m_0/2$ elements from $\mathcal{A}$. We thus have $|\mathcal{A} \cap [M/2 - C_1, M/2]| \leq (C_1/3) + (3m_0/2)$; this implies that $|\mathcal{A} \cap [1, M/2 - C_1]| > 2(M/2 - C_1)/5 + 4$, and we now have a contradiction with Theorem 1.1 applied to $\mathcal{A} \cap [1, M/2 - C_1]$ and the fact that this set contains m_0, a small even integer. So there exist a_1 and a_2 with the prescribed properties.

Let us now define, for $i = 1$ and 2,

$$f_i(t) = \begin{cases} t + a_i & when \quad t \leq M/2 \\ t - a_i & when \quad t > M/2 \end{cases}$$

There exists C_2 such that $||f_i(\mathcal{B})\cap[1,M]|-|\mathcal{B}||\leq C_2$ for any $\mathcal{B}$ in $[1,M]$, and $i\in\{1,2\}$. Since we clearly have

(i) : $f_1(\mathcal{A})\cap\mathcal{A}=f_2(\mathcal{A})\cap\mathcal{A}=\varnothing$,
(ii) : we must have
(iii) : $f_1(\mathcal{A})\cap f_2(\mathcal{A})>M/5-C_3$.

We can find C_4 so that the relations

$$\begin{cases} a_1'\in[C_4,M/2-C_4]\cup[M/2+C_4,M-C_4],\\ f_1(a_1')=f_2(a_2'),\end{cases}$$

imply $|a_1'-a_2'|=m_0/2$. Moreover, for any number t, at most one of $t+m_0/2$ and $t-m_0/2$ belongs to $\mathcal{A}$. All that imply that, with at most C_5 exceptions, all elements in $\mathcal{A}$ can be organized in pairs with common difference $m_0/2$.

The largest such pair is larger than $M-C_6$, for a suitable C_6. Otherwise, there are no more than C_5 elements in $\mathcal{A}\cap[M-C_6,M]$, and so there are more than $2M/5-x-C_5$, i.e. more than $2(M-C_6)/5+2$ elements in $\mathcal{A}\cap[1,M-C_6]$, which is in contradiction with Theorem 1.1 and the fact that $\mathcal{A}$ contains a small even element. Let us call $(M-C_7,M-C_7+m_0/2)$ the largest pair of elements in $\mathcal{A}$.

To each pair $(a,a+m_0/2)$, we associate a triple $(M-C_7-a-m_0/2,M-C_7-a,M-C_7-a+m_0/2)$ of integers that do not belong to $\mathcal{A}$. Since two pairs have no element in common and difference between first and second elements of different pairs is not equal to m, two such triples have no element in common neither. The set $[1,M]\backslash\mathcal{A}$ contains $3M/5$ elements, up to a constant, and there are, again up to a constant, $M/5$ triples, so up a constant number of exceptions, $[1,M]\backslash\mathcal{A}$ is a union of triples.

Let us consider any arithmetic progression modulo $m_0/2$. Up to a constant number of exceptions, the progression is covered by $(M/5)/(m_0/2)$ structures of five consecutive points, the first two belonging to $\mathcal{A}$, and the last three not belonging to $\mathcal{A}$. We consider the set $\mathcal{B}$ of the first element in each pentuple. If $b_1<b_2$ are two elements in $\mathcal{B}$, then b_2-b_1 is the midpoint of a triple of elements that do not belong to $\mathcal{A}$. Since there are $M/5-C_8$ such triples, we have $|(\mathcal{B}-\mathcal{B})_+|=|\mathcal{B}|+C_9$, the reasoning as in [5] imply that $\mathcal{B}$ is located in an arithmetic progression of length at most $|\mathcal{B}|+C_{10}$. Due to the cardinality of $\mathcal{B}$, this progression is modulo $5m_0/2$.

We consider the set $\mathcal{S}$ of the residues modulo $5m_0/2$ of the first and second elements of the pentuples associated to each arithmetic progression modulo $m_0/2$. The set $\mathcal{S}$ consist of m_0 elements. Since $\mathcal{A}$ is sum-free and is equal, up to a constant number of terms, to the numbers in $[1,M]$ which are above the elements of $\mathcal{S}$, the set $\mathcal{S}$ must be sum-free. We are thus left with the characterization of sum-free subsets of $\mathbb{Z}/5L\mathbb{Z}$ which satisfy the following property: each subset $\{u,u+L,u+2L,u+3L,u+4L\}$ contains exactly two elements, and those two elements are consecutive; by this we mean that those two elements are $\{u+iL,u+jL\}$ where (i,j) is one of the pair (0,1),(1,2),(2,3),(3,4),(4,0), and we shall call the first of those two elements the one that corresponds to the first element in the associated pair (i,j). We call $\mathcal{S}_1$ the set of the first elements, and $\mathcal{S}_2$ the set of the second ones. We have $|\mathcal{S}_1|=|\mathcal{S}_2|=L$. Let s and s' be elements in $\mathcal{S}_1$; then $s+L$ and $s'+L$ are in $\mathcal{S}_2$, so that $s+s'$, $s+s'+$

L, $s + s' + 2L$ are not in $\mathcal{S}$ which is sum-free; this implies that $s + s' - 2L$ is in $\mathcal{S}_1$. This implies that $|\mathcal{S}_1 + \mathcal{S}_1| = |\mathcal{S}_1|$, and Kneser's theorem (cf. [4]) implies that $\mathcal{S}_1$ is a coset associated to a subgroup $\mathcal{H}$ of $\mathbb{Z}/5L\mathbb{Z}$ with cardinality L. This implies that $\mathcal{S}_1$, as well as $\mathcal{S}_2$, is the image in $\mathbb{Z}/5L\mathbb{Z}$ of an arithmetic progression modulo 5.

We have thus proved that, up to a constant number of terms, $\mathcal{A}$ is the union of two arithmetic progressions modulo 5. Since $\mathcal{A}$ is sum-free it is easily seen that those two arithmetic progression are either $5\mathbb{Z} + 1$ and $5\mathbb{Z} + 4$, or $5\mathbb{Z} + 2$ and $5\mathbb{Z} + 3$, and that $\mathcal{A}$ is indeed included in the two arithmetic progressions, so that either (ii) or (iii) holds in Theorem 1.2.

References

[1] Cameron P.J. and Erdős P., *On the Number of Sets of Integers With Various Properties*, Proceeding of the first Conference of the CNTA, R.Molin ed., Alberta, April 17-27, 1988.

[2] Freiman G. A., *Inverse problems in additive number theory, VI.* On addition of finite sets, III. The method of trigonometric sums (Russian), Izvestiya Vuzov, Mathem., **3(28)**, 1962, 151–157.

[3] Freiman G.A., *On the structure and the number of sum-free sets*, Astérisque, **209**, 1992, 195–201.

[4] Mann H. B., *Addition Theorems*, Wiley, New-York, 1965, xi+114 p.

[5] Steinig J., *On Freiman's theorems concerning the sum of finite sets of integers*, this volume.

J.-M. Deshouillers, Mathématiques Stochastiques, Université Victor Segalen Bordeaux 2, 33076 Bordeaux, France • *E-mail :* j-m.deshouillers@u-bordeaux2.fr

G.A. Freiman, School of Mathematical Science, Raymond and Beverly Sackler, Faculty of Exact Sciences, Tel Aviv University, 69978 Tel Aviv, Israel • *E-mail :* grisha@math.tau.ac.il

V. Sós, Math. Institute,, Hungarian Academy of Sciences,, Realtanoda u.13-15,, Budapest, Hungary *E-mail :* sos@math-inst.hu

M. Temkin, School of Mathematical Science, Raymond and Beverly Sackler, Faculty of Exact Sciences, Tel Aviv University, 69978 Tel Aviv, Israel