ACTA ARITHMETICA
103.2 (2002)

A generalization of Freiman's $3k-3$ Theorem

by

Yahya Ould Hamidoune (Paris) and Alain Plagne (Palaiseau)

1. Introduction. Given two sets of integers $\mathcal{A}$ and $\mathcal{B}$, define as usual the *sumset*

$$\mathcal{A}+\mathcal{B}=\{a+b \mid a\in\mathcal{A},\ b\in\mathcal{B}\}.$$

It is readily seen that

$$|\mathcal{A}+\mathcal{B}|\geq|\mathcal{A}|+|\mathcal{B}|-1. \tag{1}$$

Moreover, equality holds if and only if $|\mathcal{A}|=1$ or $|\mathcal{B}|=1$ or $\mathcal{A}$ and $\mathcal{B}$ are arithmetic progressions with the same difference, that is, of the form

$$\mathcal{A}=\{a+(j-1)d \mid 1\leq j\leq l\}\quad\text{and}\quad\mathcal{B}=\{b+(j-1)d \mid 1\leq j\leq l'\},$$

the integers l and l' being called the *length* of the arithmetic progressions. In what follows, we concentrate our efforts on the case $\mathcal{B}=t.\mathcal{A}$, where we denote (to avoid any ambiguity with the t-fold sumset)

$$t.\mathcal{A}=\{ta \mid a\in\mathcal{A}\}.$$

Freiman [2] (see also [6]) went a step beyond (1) by showing that if $\mathcal{A}$ is a set of integers such that

$$|\mathcal{A}+\mathcal{A}|\leq 3|\mathcal{A}|-4, \tag{2}$$

then $\mathcal{A}$ is a subset of a short arithmetic progression; more precisely there are integers a and d such that

$$\mathcal{A}\subset\{a+(j-1)d \mid 1\leq j\leq l\},$$

where the length l of the arithmetic progression is less than $|\mathcal{A}+\mathcal{A}|-|\mathcal{A}|+1$. This result is called the $3k-4$ Theorem since the early notation of Freiman was $|\mathcal{A}|=k$. The original proof is elementary. In [3] Freiman generalized the $3k-4$ Theorem to the sum of distinct sets. In particular, he proved it for $\mathcal{A}-\mathcal{A}$. Recent works [5, 1] on sum-free sets are based on this last result. In 1993, Steinig found another proof (which appeared recently in [14]) of this generalized result and a short proof of a more general result was proposed

2000 *Mathematics Subject Classification*: Primary 11B75.

by Lev and Smeliansky [12] who reduced the result to Kneser's theorem [11]. The reader is also referred to [13] where all this material is available.

Concerning hypothesis (2), Freiman's $3k-4$ Theorem is optimal as can be seen from the following example: take arbitrary integers a and b such that $b \geq 2a-1$ and consider

$$\mathcal{A} = \{0, \dots, a-1\} \cup \{b, \dots, b+a-1\}.$$

We have $|\mathcal{A}| = 2a$ and $|\mathcal{A}+\mathcal{A}| = 6a-3 = 3|\mathcal{A}|-3$ and $\mathcal{A}$ could not be contained in any arithmetic progression of bounded length (provided b is large enough); therefore the $3k-4$ Theorem does not apply.

Freiman went a bit further by showing a $3k-3$ Theorem (the $3k-3$ Theorem was originally published in [2]). Namely, he characterized the sets of integers $\mathcal{A}$ satisfying $|\mathcal{A}+\mathcal{A}| = 3|\mathcal{A}|-3$. He obtained Theorem 1 below (in the special case $t=1$). The proof, which is in the same vein as the original $3k-4$ proof, is not difficult but rather technical. The reader is also referred to Freiman's book [4] where both the $3k-4$ and the $3k-3$ Theorems are presented.

In this paper, we obtain both a new proof and a generalization of the $3k-3$ Theorem. Our proof is, in spirit, close to that of Lev and Smeliansky. The main difference is that Kneser's theorem is no longer available. Instead, we use the isoperimetric method. This general approach, originally due to one of the authors, is based on intersection properties of critical sets. With this approach, we are able to decompose the proof into elementary, clearly defined steps. In one sense, our proof allows one to understand more precisely why things behave as they do. Let us now motivate the isoperimetric method. This method was introduced by the first author in the context of combinatorial properties of Cayley diagrams [7]. Then it was observed [8, 9] that these results were connected with additive number theory. Since then, the method has proved to be especially suitable for these kinds of problems and some applications have already been given.

We now come to the result we prove in this article. It is clear that, for a set $\mathcal{A}$ of integers, neither $|\mathcal{A}|$ nor $|\mathcal{A}+\mathcal{B}|$ is changed by a translation or an integral dilatation. This allows us to consider instead of $\mathcal{A}$ itself $(\mathcal{A}-\min(\mathcal{A}))/\gcd(\mathcal{A})$ (the notation $\gcd(\mathcal{A})$ is for the greatest common divisor of the elements of $\mathcal{A}$). Consequently, in what follows, without loss of generality, we consider only sets of the form $\mathcal{A} = \{a_1, \dots, a_k\}$ having the following properties: $0 = a_1 < \dots < a_k$ and $\gcd(a_1, \dots, a_k) = 1$. Such sets will be called *normal*.

THEOREM 1. *Let* $\mathcal{A}$ *be a set of positive integers such that* $0 \in \mathcal{A}$ *and* $\gcd(\mathcal{A}) = 1$. *Put* $M = \max(\mathcal{A})$ *and let* t *be any integer. If* $|\mathcal{A}+t.\mathcal{A}| = 3|\mathcal{A}|-3$ *then one of the following happens*:

- $|\mathcal{A}| \geq 1 + \max(\mathcal{A})/2$,
- $t = 1$ *or* -1 *and* $\mathcal{A}$ *is the union of two arithmetic progressions with the same common difference*,
- $t = 1$, M *is even and* $\mathcal{A}$ *is of the form* $\mathcal{A} = \{0, M/2, M, x, x+M/2, 2x\}$ *for some positive integer* $x < M/2$.

It is worth underlining that the case $t = -1$ in this result could be of interest in the context of sum-free sets (see [5, 1]).

2. Some prerequisites. We now introduce the vocabulary needed in this paper. We are given some finite Abelian group G. Let $\mathcal{S}$ be a subset of G such that $0 \in \mathcal{S}$ and $|\mathcal{S}| \geq 2$ and let k be a positive integer. We say that $\mathcal{S}$ is *k-separable* if there exists a set $\mathcal{X}_0 \subset G$ with $|\mathcal{X}_0| \geq k$ and $|\mathcal{X}_0 + \mathcal{S}| \leq |G| - k$. Assume now that $\mathcal{S}$ is k-separable; then the *k-isoperimetric number* is defined as

$$\kappa_k(G, \mathcal{S}) = \min\{|\mathcal{X} + \mathcal{S}| - |\mathcal{X}| \text{ where } \mathcal{X} \text{ is such that } |\mathcal{X}| \geq k \text{ and } |\mathcal{X} + \mathcal{S}| \leq |G| - k\}.$$

A set $\mathcal{X}$ at which this minimum is attained is called a *k-critical* set.

Recall that an arithmetic progression in G is a set of the form

$$\{a + (j-1)d \mid 1 \leq j \leq l\}$$

for some $a, d \in G$.

We begin with an easy well known consequence of Kneser's theorem.

Lemma 1 (folklore). *Let $\mathcal{B}$ be a generating proper subset of a finite Abelian group G such that $0 \in \mathcal{B}$. Then for every non-empty subset $\mathcal{C}$ of G we have*

$$|\mathcal{B} + \mathcal{C}| \geq \min(|G|, |\mathcal{B}|/2 + |\mathcal{C}|).$$

Proof. Suppose $|\mathcal{B} + \mathcal{C}| < |G|$. By Kneser's theorem there is a subgroup K such that

$$|\mathcal{B} + \mathcal{C}| \geq |\mathcal{B} + K| + |\mathcal{C} + K| - |K|. \tag{3}$$

Since K cannot be G (otherwise $\mathcal{B} + \mathcal{C} = G$) and $\mathcal{B}$ is a generating set, $\mathcal{B}$ is not included in K and thus $|\mathcal{B} + K| \geq 2|K|$. Thus $|\mathcal{B}|/2 \leq |\mathcal{B} + K|/2 \leq |\mathcal{B} + K| - |K|$. Since $|\mathcal{C} + K| \geq |\mathcal{C}|$, the conclusion follows from (3). ■

The next result, implicit in [9, 10], will be a key lemma in what follows.

Lemma 2 (cf. [9, 10]). *Let $\mathcal{S}$ be a 2-separable generating subset of some finite Abelian group G such that $0 \in \mathcal{S}$. Assume that $\kappa_2(\mathcal{S}) \leq |\mathcal{S}| - 1$. Then there are 3 possible cases*:

- $|\mathcal{S}| > |G|/2$,
- $\mathcal{S}$ *is an arithmetic progression*,
- *there is a 2-critical subset which is a subgroup.*

This follows immediately from Proposition 6.5 of [10] since the almost-period in case (iii) is a 2-critical subgroup.

We also need the following lemma.

LEMMA 3. *Let $\mathcal{A}$ be a normal set of integers with largest element M. Let $\mathcal{B}$ be a set of integers included in a set of $M+1$ consecutive integers. Denote with a bar reduction modulo M. Then*

$$|\mathcal{A}+\mathcal{B}| \geq 2|\mathcal{B}| - 1 + |(\overline{\mathcal{A}}+\overline{\mathcal{B}}) \setminus \overline{\mathcal{B}}| + c,$$

where c counts the number of elements in $(\overline{\mathcal{A}}+\overline{\mathcal{B}}) \setminus \overline{\mathcal{B}}$ that are the projection of two different elements from $\mathcal{A}+\mathcal{B}$.

Proof. $\mathcal{A}+\mathcal{B}$ contains $\mathcal{B}$ and $M+\mathcal{B}$ and their intersection reduces to at most one element. This gives the term $2|\mathcal{B}|-1$. Next $\mathcal{A}+\mathcal{B}$ contains elements that, when reduced modulo M, do not belong to $\overline{\mathcal{B}}$ (these elements are consequently neither in $\mathcal{B}$ nor in $M+\mathcal{B}$). The number of these elements is $\geq |(\overline{\mathcal{A}}+\overline{\mathcal{B}}) \setminus \overline{\mathcal{B}}| + c$. ∎

3. The proof. We consider a normal set $\mathcal{A}$ such that $|\mathcal{A}| < 1+\max(\mathcal{A})/2$. Write $M = \max(\mathcal{A})$. We may consider only the case $t \in \{-1, 1\}$ since otherwise ($t = 0$ is trivially not possible) consider the partition of $\mathcal{A}$ as $\mathcal{A} = \mathcal{A}_0 \cup \ldots \cup \mathcal{A}_{t-1}$ where $\mathcal{A}_j = \mathcal{A} \cap (j + t.\mathbb{Z})$. Since $0 \in \mathcal{A}$ and $\mathcal{A}$ is normal we get respectively $\mathcal{A}_0 \neq \emptyset$ and $\mathcal{A}_i \neq \emptyset$ for some $1 \leq i \leq t-1$. Then, by (1), $|\mathcal{A}+t.\mathcal{A}| \geq \sum_{\mathcal{A}_j \neq \emptyset} |\mathcal{A}_j + t.\mathcal{A}| \geq \sum_{\mathcal{A}_j \neq \emptyset} (|\mathcal{A}_j| + |\mathcal{A}| - 1) \geq 3|\mathcal{A}| - 2$. So assume

$$t \in \{-1, 1\}$$

and, since there is no ambiguity in these cases, write simply $t\mathcal{A}$ instead of $t.\mathcal{A}$.

We reduce the problem modulo M and obtain a modular set $\overline{\mathcal{A}}$. First, the case where $\overline{\mathcal{A}}$ is an arithmetic progression modulo M is considered; then the generic case is treated. Modular results are then lifted back to natural integers to get the result.

By the assumption of Theorem 1 and Lemma 3, we have

$$|\overline{\mathcal{A}} + t\overline{\mathcal{A}}| \leq 2|\overline{\mathcal{A}}| - 1. \tag{4}$$

We first prove the theorem under the additional assumption that $\overline{\mathcal{A}}$ is an arithmetic progression modulo M. Let d be its difference that we may assume to satisfy $1 \leq d < M/2$ (the case $d = M/2$ leads to a trivial situation that can be handled directly since in this case $|\mathcal{A}| \leq 3$).

If $d = 1$, it is readily seen that $\mathcal{A}$ is the union of two arithmetic progressions and the theorem is proved. Thus, from now on we suppose that $d \neq 1$.

Perform the Euclidean division $M = qd - r$ with $0 \leq r \leq d-1$. Since $\gcd(M, d) = \gcd(r, d)$, we have $\gcd(r, d) \mid \gcd(\mathcal{A}) = 1$ ($\mathcal{A}$ is a normal set) and consequently

$$\gcd(r,d)=1. \tag{5}$$

A partition of $\mathcal{A}$ is thus obtained by writing

$$\mathcal{A}_i=\{a\in\mathcal{A}\mid a\equiv ir \bmod d\}.$$

Now, since $\overline{\mathcal{A}}$ is a modular arithmetic progression, we can write it as $\overline{\mathcal{A}}=\{\alpha_j=\alpha_1+(j-1)d\mid 1\le j\le|\overline{\mathcal{A}}|\}$. We underline the fact that the α_j are of the form $\overline{a}_l$ but there is no reason why $j=l$; in other words, the order induced by the modular arithmetic progression is a priori different from that of $\mathcal{A}$ itself. Two consecutive elements $\overline{b}_s$ and $\overline{b}_{s+1}$ of $\overline{\mathcal{A}}$ (in the order induced by the arithmetic progression) correspond, when lifted back to $\mathcal{A}$, to b_s and b_{s+1} such that $b_{s+1}-b_s\equiv d \bmod M$ and the only possibilities are $b_{s+1}-b_s=d$ or $d-M$. Hence $b_{s+1}-b_s\equiv 0$ or $r \bmod d$. Since $0\in\mathcal{A}$, we infer that there exist two non-negative integers s and t such that the non-void $\mathcal{A}_i$'s correspond exactly to the values of i in the interval $-v\le i\le w$.

If $v=w=0$, then $\mathcal{A}=\mathcal{A}_0$ and $1<d\,|\gcd(\mathcal{A})$, which is impossible. Thus v or w is positive. Without loss of generality we assume $w\ge 1$. We write $|\mathcal{A}_i|=\gamma(i)$ and

$$\mathcal{A}_i=\{b_{i,1}<\ldots<b_{i,\gamma(i)}\}.$$

Now, we observe that

$$\gamma(0),\gamma(1),\ldots,\gamma(w-1)\ge 2. \tag{6}$$

Indeed, this is clearly true for $\gamma(0)$ (because 0 and M belong to $\mathcal{A}$). As observed above, two consecutive elements in $\overline{\mathcal{A}}$ are such that (we return to the preceding notation) $b_{s+1}-b_s=d$ or $d-M$. But the second case implies that $b_{s+1}<b_s-M/2$ and cannot happen twice consecutively (else we would have a negative element in $\mathcal{A}$). Thus the case $b_{s+1}-b_s=d\equiv 0 \bmod d$ happens at least every other time. This proves (6).

We now prove that there are two elements in $\mathcal{A}+t\mathcal{A}$ that have the same value modulo M. Indeed, suppose that this is proved; then by Lemma 3, we get

$$|\mathcal{A}+t\mathcal{A}|\ge 2|\mathcal{A}|-1+|(\overline{\mathcal{A}}+t\overline{\mathcal{A}})\setminus\overline{\mathcal{A}}|+1=3|\mathcal{A}|-2,$$

which cannot happen by hypothesis. The last equality is due to the fact that $|(\overline{\mathcal{A}}+t\overline{\mathcal{A}})\setminus\overline{\mathcal{A}}|=|\overline{\mathcal{A}}|-1=|\mathcal{A}|-2$, a conclusion following directly from the fact that $\overline{\mathcal{A}}$ is an arithmetic progression with difference d and $\gcd(M,d)=1$.

Let us now prove our assertion that there are two elements in $\mathcal{A}+t\mathcal{A}$ that have the same value modulo M. If $\gamma(t)=1$, we have

$$b_{w-1,\gamma(w-1)}=b_{w-1,\gamma(w-1)-1}+d,\qquad b_{w,1}=b_{w-1,\gamma(w-1)}+d-M.$$

Therefore $b_{w,1}+b_{w-1,\gamma(w-1)-1}$ and $2b_{w-1,\gamma(w-1)}$ are different modulo d (and thus different in $\mathbb{Z}$) but coincide modulo M. This proves our assertion if $w=1$. If $t=-1$, just consider $b_{w,1}-b_{w-1,\gamma(w-1)}$ and $b_{w-1,\gamma(w-1)}-b_{w-1,\gamma(w-1)-1}$.

In the case $\gamma(w) = 2$, we get the same result with the two values $b_{w,\gamma(w)} + b_{w-1,\gamma(w-1)}$ and $b_{w,\gamma(w)} + b_{w,1}$.

We are done with the case when $\overline{\mathcal{A}}$ is an arithmetic progression. Assume now that $\overline{\mathcal{A}}$ is not an arithmetic progression (modulo M). It is readily seen from the properties of $|\overline{\mathcal{A}}|$ that $\overline{\mathcal{A}}$ is a 2-separable subset of $\mathbb{Z}/M\mathbb{Z}$ and that

$$\kappa_2(\overline{\mathcal{A}}) \leq |\overline{\mathcal{A}}| - 1. \tag{7}$$

By Lemma 2, since $|\overline{\mathcal{A}}| \leq M/2$ and $\overline{\mathcal{A}}$ is not an arithmetic progression, there is a 2-critical subset that is a subgroup (of $\mathbb{Z}/M\mathbb{Z}$), say H, which is $e\mathbb{Z}/M\mathbb{Z}$ for some $e \mid M$; in particular

$$|H| \geq 2. \tag{8}$$

This implies that

$$|\overline{\mathcal{A}} + H| - |\overline{\mathcal{A}}| \leq |H| - 1, \tag{9}$$

which can be paraphrased by saying that $\overline{\mathcal{A}}$ is almost a union of cosets modulo H (more precisely the total number of "holes" in this union is at most $|H| - 1$).

Define a partition of $\mathcal{A}$ depending on the value of the elements modulo e. That is, write

$$\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1 \cup \ldots \cup \mathcal{A}_u$$

with $u \geq 1$ (since $\gcd(\mathcal{A}) = 1$) and each $\mathcal{A}_i$ being exactly the intersection of $\mathcal{A}$ with an arithmetic progression with difference e. Moreover define $\mathcal{A}_0 = \mathcal{A} \cap e\mathbb{Z}$. We can also find elements $(a_i)_{1 \leq i \leq u}$ in $\mathcal{A}$ such that $\mathcal{A}_i = \mathcal{A} \cap (a_i + e\mathbb{Z})$. Notice that

$$|\overline{\mathcal{A}} + H| = (u+1)|H|.$$

We may now suppose, without loss of generality, that

$$|\mathcal{A}_1|, \ldots, |\mathcal{A}_{u-1}| \geq |\mathcal{A}_u|. \tag{10}$$

Such a partition will be called an *H-tiling.* With the convention (10), we readily see that for any (i,j) except possibly if $(i,j) = (u,u)$ or $(0,0)$,

$$|\mathcal{A}_i| + |\mathcal{A}_j| \geq |H| + 1, \tag{11}$$

since (9) is equivalent to

$$u|H| + 2 \leq \sum_{i=0}^{u} |\mathcal{A}_i|.$$

If we look at what happens in $G = (\mathbb{Z}/M\mathbb{Z})/H$ (which is just $\mathbb{Z}/e\mathbb{Z}$) and denote the reduced set with a double bar, we see that

$$|\overline{\overline{\mathcal{A}}}| = u + 1.$$

Another way to write $\overline{\overline{\mathcal{A}}}$ is $(\overline{\mathcal{A}}+H)/H$. Using this allows us to prove the following Cauchy–Davenport-type result:

$$
\begin{aligned}
(12)\qquad |\overline{\overline{\mathcal{A}}}+t\overline{\overline{\mathcal{A}}}| &= \left|\frac{\overline{\mathcal{A}}+H}{H}+t\,\frac{\overline{\mathcal{A}}+H}{H}\right| = \frac{|\overline{\mathcal{A}}+t\overline{\mathcal{A}}+H|}{|H|}\\
&\geq \left\lceil\frac{\min(\kappa_2(\overline{\mathcal{A}})+|t\overline{\mathcal{A}}+H|, M-1)}{|H|}\right\rceil\\
&= \min\left(\frac{2|\overline{\mathcal{A}}+H|-|H|}{|H|}, \frac{M}{|H|}\right)\\
&= 2|\overline{\overline{\mathcal{A}}}|-1 = 2u+1,
\end{aligned}
$$

where we have used the facts that $|\overline{\mathcal{A}}+H|\geq 2$, M is a multiple of $|H|\geq 2$ (so that $(M-1)/|H|$ cannot be integral), $2|\overline{\mathcal{A}}+H|<M+2|H|$ (and thus $2|\overline{\mathcal{A}}+H|\leq M+|H|$) and (7).

Reasoning modulo e shows immediately that the sets $\mathcal{A}_0+t\mathcal{A}_0, \mathcal{A}_0+t\mathcal{A}_1, \dots, \mathcal{A}_0+t\mathcal{A}_u$ have no common element and are subsets of $\mathcal{A}+t\mathcal{A}$. By (12), we know that there are at least u other elements in $\overline{\overline{\mathcal{A}}}+t\overline{\overline{\mathcal{A}}}$, say

$$\mathcal{A}_{\alpha_1}+t\mathcal{A}_{\beta_1}, \mathcal{A}_{\alpha_2}+t\mathcal{A}_{\beta_2}, \dots, \mathcal{A}_{\alpha_u}+t\mathcal{A}_{\beta_u}.$$

Notice immediately that no α_i can be zero. Synthesizing, we have obtained $2u+1$ couples $(\mathcal{A}_i, t\mathcal{A}_j)$ which have, two by two, no common element in their sum. Thus we obtain the following lower bound:

$$
\begin{aligned}
(13)\quad 3|\mathcal{A}|-3 = |\mathcal{A}+t\mathcal{A}| &\geq \sum_{i=0}^{u}|\mathcal{A}_0+t\mathcal{A}_i| + \sum_{i=1}^{u}|\mathcal{A}_{\alpha_i}+t\mathcal{A}_{\beta_i}|\\
&\geq |\mathcal{A}_0+t\mathcal{A}_0| + \sum_{i=1}^{u-1}|t\mathcal{A}_i\cup(\{M\}+t\mathcal{A}_i)| + |\mathcal{A}_0+t\mathcal{A}_u|\\
&\quad + \sum_{i=1}^{u}(|\mathcal{A}_{\alpha_i}|+|\mathcal{A}_{\beta_i}|-1)\\
&\geq (2|\mathcal{A}_0|-1) + 2\sum_{i=1}^{u-1}|\mathcal{A}_i| + (|\mathcal{A}_0|+|\mathcal{A}_u|-1)\\
&\quad + \sum_{i=1}^{u-1}|H| + (2|\mathcal{A}_u|-1)\\
&\geq 2|\mathcal{A}| + (|\mathcal{A}_0|+(u-1)|H|+|\mathcal{A}_u|)-3\\
&\geq 3|\mathcal{A}|-3,
\end{aligned}
$$

where we have used (1) and the relation (11) in the last inequality to minorize $|\mathcal{A}_{\alpha_i}+t\mathcal{A}_{\beta_i}|$ except in one case (the possible case where $\alpha_i=\beta_i=u$ for some i, say $i = u$). Therefore, in the preceding series of minorizations, all the inequalities are in fact equalities; in particular, by the last majorization, we see that $|\mathcal{A}_i| = |H|$ for any $1 \leq i \leq u-1$. In what follows, when we refer to (13), we mean one of the equalities in the series.

From our preceding series of equalities (13), we get $|\mathcal{A}_0 + t\mathcal{A}_1| = |\mathcal{A}_0| + |t\mathcal{A}_1| - 1$ and thus $\mathcal{A}_0$ and $t\mathcal{A}_1$ (thus also $\mathcal{A}_1$ itself) are arithmetic progressions with the same difference. If $u = 1$, the conclusion follows immediately from $\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1$.

Assume now that $u \geq 2$. From the fact that $\mathcal{A}_0$ and $\mathcal{A}_1$ are both arithmetic progressions with the same difference e and that $0, M \in \mathcal{A}_0$, it follows that $\mathcal{A}_0 = \{0, e, 2e, \ldots, M\}$ and

$$|\mathcal{A}_0| = |H| + 1.$$

Then from (13) we get $|\mathcal{A}_{\alpha_1}| + |\mathcal{A}_{\beta_1}| - 1 = |H|$, which leads readily to

$$|\mathcal{A}_u| = 1.$$

Now we know, by the fact that (13) is an equality, that

$$\mathcal{A} + t\mathcal{A} = \bigcup_{i=0}^{u} (\mathcal{A}_0 + t\mathcal{A}_i) \bigcup_{i=1}^{u} (\mathcal{A}_{\alpha_i} + t\mathcal{A}_{\beta_i}). \tag{14}$$

Moreover, each sum $\mathcal{A}_i + t\mathcal{A}_j$ appearing in this union corresponds to exactly one residue modulo e. In particular, these sets are disjoint. Now, take two non-negative integers $i, j < u$. Since $\mathcal{A}_i + t\mathcal{A}_j \subset \mathcal{A} + t\mathcal{A}$ and this set corresponds to exactly one value modulo e, it is included in one of the $2u + 1$ sets appearing on the right-hand side of (14). But $|\mathcal{A}_i + t\mathcal{A}_j| \geq 2|H| - 1$ and on the other hand, by (13) again, $|\mathcal{A}_{\alpha_i} + t\mathcal{A}_{\beta_i}| \leq |H| < 2|H| - 1$ for any $1 \leq i \leq u$; therefore, each $\mathcal{A}_i + t\mathcal{A}_j$ is contained in some $\mathcal{A}_0 + t\mathcal{A}_k$ $(0 \leq k \leq u)$. If we define $\mathcal{D} = \overline{\mathcal{A}} \setminus \overline{\mathcal{A}}_u \subset \mathbb{Z}/M\mathbb{Z}$, this can be expressed by the following formula:

$$\mathcal{D} + t\mathcal{D} \subset \mathcal{D} \cup (\overline{\mathcal{A}}_u + H).$$

Let us show that

$$\mathcal{D} + t\mathcal{D} = \mathcal{D} \cup (\overline{\mathcal{A}}_u + H). \tag{15}$$

Assuming the contrary and observing that $\mathcal{D} \subset \mathcal{D} + t\mathcal{D}$, we have $\mathcal{D} + t\mathcal{D} = \mathcal{D}$, which would imply that $\mathcal{D}$ is a subgroup, $\mathbb{Z}/v\mathbb{Z}$ say. But in this case we would directly observe that $\mathcal{A}$ is the union of an arithmetic progression (starting from 0 up to M with difference v) and a set of cardinality 1 (namely $\mathcal{A}_u$). This is not possible; assertion (15) holds.

We may also assume that $|H| = 2$ because, in any other case, with i, j as above, $|\mathcal{A}_i + t\mathcal{A}_j| \geq 2|H| - 1 > |H| + 1 \geq |\mathcal{A}_0 + t\mathcal{A}_u|$ contrary to (15). From now on, $|H| = 2$, that is,

$$H = \overline{\{0, M/2\}}.$$

Notice that $\mathcal{D}$ generates G by (15) because $\mathcal{D}+t\mathcal{D}$ contains a generating set (otherwise $\mathcal{D}$ would give a gcd >1 for the elements of $\mathcal{A}$ contrary to the fact that $\mathcal{A}$ is normal). Thus, we are in a position to apply Lemma 1 in $\mathbb{Z}/M\mathbb{Z}$ with $\mathcal{B}=\mathcal{D}$. We obtain

$$\frac{3}{2}u|H| \le |\mathcal{D}+t\mathcal{D}| \le |\mathcal{D}| + |\overline{\mathcal{A}}_u + H| = (u+1)|H|,$$

which gives $u \le 2$ and thus $u=2$. Synthesizing, we finally conclude that $\mathcal{A}$ is of the form

$$\mathcal{A} = \mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{A}_2,$$

with

$$\mathcal{A}_0 = \{0, M/2, M\}, \quad \mathcal{A}_1 = \{x, x+M/2\}, \quad \mathcal{A}_2 = \{y\},$$

where x and y are some integers (the respective classes modulo $M/2$ represented in $\overline{\mathcal{A}}$). If $t=1$, then $\mathcal{A}_1+\mathcal{A}_1=\mathcal{A}_0+\mathcal{A}_2$ and thus $2x=y$, which gives

$$\mathcal{A} = \{0, M/2, M, x, x+M/2, 2x\},$$

which is the third possible conclusion of the theorem. If $t=-1$, it is easily checked that there is no solution, which concludes the proof.

References

[1] J.-M. Deshouillers, G. A. Freiman, V. Sós and M. Temkin, *On the structure of sum-free sets, 2*, Astérisque 258 (1999), 149–161.

[2] G. A. Freiman, *On the addition of finite sets. I*, Izv. Vyssh. Uchebn. Zaved. Mat. 6 (13) (1959), 202–213.

[3] —, *Inverse problems of additive number theory. VI. On the addition of finite sets. III. The method of trigonometric sums*, ibid. 3 (28) (1962), 151–157.

[4] —, *Foundations of a Structural Theory of Set Addition*, Transl. Math. Monographs 37, Amer. Math. Soc., Providence, RI, 1973.

[5] —, *On the structure and the number of sum-free sets*, Astérisque 209 (1992), 195–201.

[6] —, *Structure theory of set addition*, ibid. 258 (1999), 1–33.

[7] Y. O. Hamidoune, *Sur les atomes d'un graphe orienté*, C. R. Acad. Sci. Paris 284 (1977), 1253–1256.

[8] —, *An isoperimetric method in additive theory*, J. Algebra 179 (1996), 622–630.

[9] —, *Subsets with small sums in Abelian groups I: the Vosper property*, European J. Combin. 18 (1997), 541–556.

[10] —, *Some results in additive number theory I: The critical pair theory*, Acta Arith. 96 (2000), 97–119.

[11] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. 58 (1953), 459–484.

[12] V. F. Lev and P. Y. Smeliansky, *On addition of two distinct sets of integers*, Acta Arith. 70 (1995), 85–91.

[13] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[14] J. Steinig, *On Freiman's theorems concerning the sum of two finite sets of integers*, Astérisque 258 (1999), 129–140.

CNRS et Équipe Combinatoire
Université Pierre et Marie Curie
Case 189
4 place Jussieu
75005 Paris, France
E-mail: yha@ccr.jussieu.fr

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

Received on 23.3.2001
and in revised form on 31.8.2001 (4001)