Uniform Distribution Theory **1** (2006), no.1, 111–124

uniform distribution theory

OPTIMALLY SMALL SUMSETS IN GROUPS, II. THE HYPERSMALL SUMSETS PROPERTY AND RESTRICTED ADDITION

Alain Plagne

ABSTRACT. This paper continues the work that was started in [*Optimally small sumsets in groups, I. The supersmall sumsets property, the* $\mu_G^{(k)}$ *and the* $\nu_G^{(k)}$ *functions*, Uniform Distribution Theory 1 (2006), 27–43]. Here, we introduce the hypersmall sumsets property and prove that it holds for all Abelian groups. As an application, we establish new upper bounds for the function ξ_G giving the minimal cardinality of a restricted sumset in an arbitrary Abelian group G. We then formulate the conjecture that these bounds are often optimal. Assuming a conjecture by Lev, we show that our conjecture is indeed very close to the truth. In some "generic" cases, we can even prove that it holds true.

Communicated by Georges Grekos

1. Introduction

The groups we consider in this article will all be written additively (and their neutral elements denoted by 0). The notation $|G|$ will denote the cardinality of the group G if it is finite and $+\infty$ otherwise (in which case, an inequality of the form $r \leq |G|$ for some integer r is clearly empty).

In the first part of this work [17], we studied the function $\mu_G^{(k)}(r_1, \ldots, r_k)$, defined as the minimal cardinality of a sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k = \{a_1 + \cdots + a_k, a_1 \in \mathcal{A}_1, \ldots, a_k \in \mathcal{A}_k\}$ with $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset G$ and $|\mathcal{A}_1| = r_1, \ldots, |\mathcal{A}_k| = r_k$, namely

$$\mu_G^{(k)}(r_1, \ldots, r_k) = \min \big\{ |\mathcal{A}_1 + \cdots + \mathcal{A}_k| \text{ such that } \mathcal{A}_1, \ldots, \mathcal{A}_k \subset G \text{ and } |\mathcal{A}_1| = r_1, \ldots, |\mathcal{A}_k| = r_k \big\}$$

2000 Mathematics Subject Classification: 11B75, 20F16, 20D60, 11P99, 20Kxx.
Keywords: group, Abelian, additive number theory, restricted addition, small sumset.

and the still mysterious function $\nu_G^{(k)}$ defined by

$$\nu_G^{(k)}(r_1,\dots,r_k)=\begin{cases}\min\big\{|\mathcal{A}_1+\cdots+\mathcal{A}_k| \text{ such that } \mathcal{A}_1,\dots,\mathcal{A}_k\subset G,\\ \qquad |\mathcal{A}_1|=r_1,\dots,|\mathcal{A}_k|=r_k \text{ and there is an element in}\\ \qquad \mathcal{A}_1+\cdots+\mathcal{A}_k \text{ having a unique representation}\big\},\\ \qquad\qquad \text{if there are any such sets } \mathcal{A}_1,\dots,\mathcal{A}_k\subset G;\\ \infty, \qquad\qquad \text{otherwise.}\end{cases}$$

In [17], among other results, the following general theorem was obtained (see paper [17] for a bibliography on this subject).

Theorem 1. *Let k be a positive integer and G be an arbitrary Abelian group. Then for any integers $r_1,\dots,r_k$ satisfying $1\le r_1,\dots,r_k\le|G|$, we have*

$$\mu_G^{(k)}(r_1,\dots,r_k)=\min_{d\in\mathcal{D}}\left(\left\lceil\frac{r_1}{d}\right\rceil+\cdots+\left\lceil\frac{r_k}{d}\right\rceil-k+1\right)d,$$

where $\mathcal{D}$ is the set of integers that are the cardinality of a finite subgroup of G.

The study of this type of functions is typical of additive number theory. For an introduction to this field, the reader is referred to one of the two classical books [14] or [15], where all the basic tools are extensively presented.

In [17], to study the functions $\mu_G^{(k)}$ and $\nu_G^{(k)}$, we introduced and used what we called the *generalized supersmall sumsets property*. A group G is said to have this property if for any positive integer k, any $1\le r_1,\dots,r_k\le|G|$, there exist subsets $\mathcal{A}_1,\dots,\mathcal{A}_k\subset G$ containing 0, with $|\mathcal{A}_1|=r_1,\dots,|\mathcal{A}_k|=r_k$ and either

(i) $|\mathcal{A}_1+\cdots+\mathcal{A}_k|\le r_1+\cdots+r_k-k$, or

(ii) $|\mathcal{A}_1+\cdots+\mathcal{A}_k|=r_1+\cdots+r_k-k+1$ and the neutral element 0 has the unique representation $0+\cdots+0$ as an element of the sumset $\mathcal{A}_1+\cdots+\mathcal{A}_k$.

Recall that an element $x\in\mathcal{A}_1+\cdots+\mathcal{A}_k$ is said to have r *representations (as an element of the sumset $\mathcal{A}_1+\cdots+\mathcal{A}_k$)* if

$$|\{(a_1,\dots,a_k)\in\mathcal{A}_1\times\cdots\times\mathcal{A}_k,\ x=a_1+\cdots+a_k\}|=r.$$

In [17], we proved among others the following result (this is Theorem 2 of that paper).

Lemma 2. *All solvable groups have the generalized supersmall sumsets property.*

In this article, we will concentrate on situations where we have only two summands (generalizations of the results contained in this paper to a situation with more summands are possible and require only to adapt the arguments developped in the sequel). In this context, we shall speak only of the *supersmall sumsets property*: it holds for G if for any $1\le r,s\le|G|$, there exist subsets $\mathcal{A}$ and $\mathcal{B}\subset G$, containing 0, with $|\mathcal{A}|=r,|\mathcal{B}|=s$ and either

(i) $|\mathcal{A}+\mathcal{B}| \leq r+s-2$, or

(ii) $|\mathcal{A}+\mathcal{B}| = r+s-1$ and 0 has the unique representation $0+0$ as an element of the sumset $\mathcal{A}+\mathcal{B}$.

In the present paper, we are mainly interested in the study of the function $\xi_G(r,s)$, defined as the minimal cardinality of a restricted sumset

$$\mathcal{A}\hat{+}\mathcal{B} = \{a+b,\ a\in\mathcal{A}, b\in\mathcal{B}, a\neq b\}$$

with $\mathcal{A},\mathcal{B}\subset G$ and $|\mathcal{A}|=r, |\mathcal{B}|=s$, namely

$$\xi_G(r,s) = \min\{|\mathcal{A}\hat{+}\mathcal{B}| \text{ such that } \mathcal{A},\mathcal{B}\subset G \text{ and } |\mathcal{A}|=r, |\mathcal{B}|=s\}.$$

This function is certainly much more complicated than $\mu_G = \mu_G^{(2)}$ since the restricted addition $\hat{+}$ is an operation much more difficult to understand than the simple addition $+$. For instance, the proof of the analogue of the Cauchy-Davenport theorem [3, 4], known for a long time as the Erdős-Heilbronn conjecture, was obtained only recently by Dias da Silva and ould Hamidoune [5] and Alon, Nathanson and Ruzsa [1, 2].

Although we may immediately observe that the following upper bound holds true for any group G:

$$\xi_G(r,s) \leq \mu_G(r,s), \tag{1}$$

it seems difficult to compute ξ_G explicitly in general. In particular, it is apparently not so simple to compare $\xi_G(r,s)$ with $\mu_G(r,s)$ and to test the tightness of (1).

Here are however three examples where the exact value of ξ_G can be obtained without too much efforts (for all $1\leq r,s\leq |G|$).

The first – already mentioned – case is the one of $\mathbb{Z}/p\mathbb{Z}$ for which the following result follows from [5, 1, 2]).

Lemma 3. *Let p be a prime number, then for any $1\leq r,s\leq p$, one has*

$$\xi_{\mathbb{Z}/p\mathbb{Z}}(r,s) = \begin{cases} 0, & \text{if } r=s=1,\\ \min(p, r+s-3), & \text{if } r=s>1,\\ \min(p, r+s-2), & \text{if } r\neq s. \end{cases}$$

On recalling that $\mu_{\mathbb{Z}/p\mathbb{Z}}(r,s) = \min(p, r+s-1)$, we observe that

$$\xi_{\mathbb{Z}/p\mathbb{Z}}(r,s) = \mu_{\mathbb{Z}/p\mathbb{Z}}(r,s) - \varepsilon$$

where ε is equal either to 0, 1 or 2.

In the case $G=\mathbb{Z}$, it is immediate (see for instance Lemma 12 below) that

$$\mu_{\mathbb{Z}}(r,s) = r+s-1,$$

while we have the following simple result:

Lemma 4. *Let r and s be positive integers, then*

$$\xi_{\mathbb{Z}}(r,s) = \begin{cases} 0, & \text{if } r = s = 1, \\ r+s-3, & \text{if } r = s > 1, \\ r+s-2, & \text{if } r \neq s. \end{cases}$$

We notice that, depending on whether $r = s > 1$ or not, we have $\xi_{\mathbb{Z}}(r,s) = \mu_{\mathbb{Z}}(r,s) - 2$ or $\mu_{\mathbb{Z}}(r,s) - 1$.

As another example, if we consider the case of a sumset in an elementary 2-group, we have the following result.

Lemma 5. *Let G be an elementary 2-group, then for any $1 \leq r, s \leq |G|$, one has*

$$\xi_G(r,s) = \mu_G(r,s) - 1.$$

For the sake of completeness, Section 2 contains short self-contained proofs of these two easy last results (Lemmas 4 and 5). We note that the second result follows also from [6], where several results on ξ_G are obtained in the case of elementary p-groups, using the polynomial method (introduced in [1, 2]): in particular, it is proved in [6] that if G is an elementary p-group, we have $\mu_G(r,s) - 2 \leq \xi_G(r,s) \leq \mu_G(r,s)$.

In view of everything mentioned above, the following conjecture is tempting.

Conjecture 6. *Let G be an arbitrary Abelian group, then for any $1 \leq r, s \leq |G|$, one has*

$$\mu_G(r,s) - 2 \leq \xi_G(r,s) \leq \mu_G(r,s).$$

In order to study the ξ_G functions for general groups, we introduce what we call the hypersmall sumsets property (a generalized – in the same sense as the one used for the generalized supersmall sumsets property – version of it could also be useful in order to study the generalized functions $\xi_G^{(k)}$). First we introduce a terminology: an element of a sumset $c \in \mathcal{A} + \mathcal{B}$ is a *double* if $c = a + b$ (with $a \in \mathcal{A},\ b \in \mathcal{B}$) implies $a = b$.

We shall say that a group G has the *hypersmall sumsets property* if it has the supersmall sumsets property and if for all positive integers $1 \leq r \leq |G|$, there exists a set $\mathcal{A} \subset G$ containing 0, with $|\mathcal{A}| = r$ and either

(i) $|\mathcal{A} + \mathcal{A}| \leq 2r - 3$, or

(ii) $|\mathcal{A} + \mathcal{A}| = 2r - 2$ and 0 is a double in the sumset $\mathcal{A} + \mathcal{A}$, or

(iii) $|\mathcal{A} + \mathcal{A}| = 2r - 1$, the neutral element 0 is a double in the sumset $\mathcal{A} + \mathcal{A}$ and there is yet another (distinct) double, or

(iv) G admits non-trivial (i.e. $\neq \{0\}$) finite subgroups and for any finite non-trivial minimal subgroup M of G (by which we mean subgroups $M \neq \{0\}$ such that $K < M$, $K \neq M$ implies $K = \{0\}$), one has $r \equiv 1 \pmod{|M|}$.

We notice the following fact: a finite non-trivial minimal subgroup (as appears in condition (iv) of the preceding definition) has to be cyclic of prime order.

Now, suppose that a given group G has the hypersmall sumsets property. An integer r will be said to be *exceptional for* G if we are in case (iv) of the definition, that is, G has finite non-trivial subgroups and for all finite non-trivial minimal subgroups M of G, one has $r \equiv 1 \pmod{|M|}$. Otherwise, if (iv) does not hold that is, if it is not exceptional for G, the integer r will be said to be *regular for* G. This implies that there exists a set $\mathcal{A} \subset G$, with $0 \in \mathcal{A}$ and $|\mathcal{A}| = r$, satisfying either (i), or (ii) or (iii). For instance $1 + p$ is always exceptional in a power of $\mathbb{Z}/p\mathbb{Z}$ (p a prime). We notice that the notion of exceptional integer for a given group G is reminiscent of the one of special pair (introduced in [6]) on which it gives a new and enlightening point of view. We justify the terminology "regular" by the fact that, in general, regular integers (in a given group) correspond to a generic case. For instance, it is immediate to see - using the chinese remainder theorem - that the integer 1 is the unique exceptional integer in a finite Abelian group having a squarefree order.

Notice that we could take a slightly more general definition of the hypersmall sumsets property by asking only for the existence of two sets $\mathcal{A}$ and $\mathcal{B}$ satisfying an analogous property for their sumset $\mathcal{A}+\mathcal{B}$. We will not need this refinement for the present purpose, therefore we do not introduce it in this paper.

Our first theorem of the paper will be the following, which shows why the definition introduced above can be useful.

Theorem 7. *All Abelian groups have the hypersmall sumsets property.*

This theorem will be proved in Section 3. Using Theorem 7, we shall obtain the following general upper bound for ξ_G (it is compatible with our Conjecture 6).

Theorem 8. *Let G be an arbitrary Abelian group. Then for any integers r, s satisfying $1 \leq r, s \leq |G|$, we have*

$$\xi_G(r,s) \leq \min\big(r + s - 2, \mu_G(r,s)\big).$$

Moreover, if r is regular for G, then

$$\xi_G(r,r) \leq \min\big(2r - 3, \mu_G(r,r)\big).$$

This result cannot be improved in general (see the lemmas above) but it is not optimal for all groups G: for instance in the case of elementary 2-groups (using Lemma 5 and Theorem 1), we have for $k > l$ and $1 < t, t' \leq 2^l$:

$$\begin{aligned}\xi_{(\mathbb{Z}/2\mathbb{Z})^k}(2^l+t, 2^l+t') &= 2^{l+1}-1 = \mu_{(\mathbb{Z}/2\mathbb{Z})^k}(2^l+t, 2^l+t')-1 \\ &< \min\big(2^{l+1}+t+t'-3, \mu_{(\mathbb{Z}/2\mathbb{Z})^k}(2^l+t, 2^l+t')\big).\end{aligned}$$

This justifies the discarding of groups with an even component in the following second conjecture – that makes Conjecture 6 more precise (recall that $\mu_G(r,s) \leq r+s-1$) – which may be reasonable.

Conjecture 9. *Let G be an arbitrary Abelian group with no element of order two. Then, there is a small constant c_G such that for any integers r, s satisfying $c_G \leq r, s \leq |G|$,*

- *if $r \neq s$, we have*
$$\xi_G(r,s) = \min\big(r+s-2, \mu_G(r,s)\big),$$
- *if r is exceptional for G, then*
$$\xi_G(r,r) = \min\big(2r-2, \mu_G(r,r)\big),$$
- *if r is regular for G, then*
$$\xi_G(r,r) = \min\big(2r-3, \mu_G(r,r)\big).$$

A condition of the type $r, s \geq c_G$ is necessary to avoid what we could call "small exceptional cases" (as occurs frequently in additive number theory, for instance in Freiman's $3k-3$ or $3k-2$ theorems [9]). In the present context, as mentioned in Section 7 of [6], one has $\xi_{(\mathbb{Z}/3\mathbb{Z})^2}(4,4) = 5$ (and not 6 although 4 is exceptional for $(\mathbb{Z}/3\mathbb{Z})^2$): simply take $\mathcal{A} = \{(0,0),(1,0),(0,1),(1,1)\}$.

The word "small" in Conjecture 9 is voluntarily unprecise. It is not clear that c_G can be chosen independently of G but in any case, this constant should be a $o(|G|)$ as $|G|$ tends to infinity.

We note that for some specific exceptional values of r in some given elementary p-groups, our conjecture is known to hold [7, 8]. With all the above-mentioned other reasons, this supports Conjecture 9.

To go in the direction of this conjecture, it is well possible that a restricted analogue of Kneser's theorem [10, 11] is required in an essential way. However, no such analogue is known and, if true, it seems that proving such a result should be very difficult. Nevertheless, Lev made several interesting conjectures in this respect [12, 13]. Before stating it, we need a definition: we write

$$L_G = |\{g \in G \text{ such that } 2g = 0\}|$$

(this is the cardinality of the subgroup of G consisting of 0 and the elements of order 2).

Conjecture 10 (Lev's Conjecture)**.** *Let G be an Abelian group and $\mathcal{A}, \mathcal{B}$ be two non-empty finite subsets of G such that*

$$|\mathcal{A}\hat{+}\mathcal{B}| < |\mathcal{A}| + |\mathcal{B}| - (L_G + 2)$$

then $\mathcal{A}\hat{+}\mathcal{B} = \mathcal{A} + \mathcal{B}$.

This conjecture is also an indication that computing $\xi_G(r, s)$ in the case of groups with an even order should be slightly more difficult (at least from a technical viewpoint), since in this case $L_G > 1$: in particular, there will exist pairs of sets $\mathcal{A}, \mathcal{B}$ such that $|\mathcal{A}\hat{+}\mathcal{B}| < |\mathcal{A}| + |\mathcal{B}| - 4$ and $\mathcal{A} + \mathcal{B}$ is aperiodic... this implies that it is more constrained to obtain structural information on a small sumset $\mathcal{A}\hat{+}\mathcal{B}$ (as we get from Kneser's theorem [10, 11] in the study of μ_G).

Under Lev's Conjecture 10, we are able to prove - in the forthcoming Theorem 11 - that the upper bounds obtained in Theorem 8 are very close to the truth, a fact which can be interpreted as another indication of the validity of Conjecture 9. Indeed, one third (namely, the "generic case" of regular integers) of Conjecture 9 can be shown to hold true.

Theorem 11. *Assume Lev's Conjecture 10 is true. Let G be an Abelian group with no element of order two. Then, for any integers r, s satisfying $1 \leq r, s \leq |G|$, we have*

$$\xi_G(r, s) \geq \min\big(r + s - 3, \mu_G(r, s)\big).$$

In particular if r is regular for G, we have

$$\xi_G(r, r) = \min\big(2r - 3, \mu_G(r, r)\big).$$

The proof of this result is presented in Section 4.

We plan to continue the present series of papers investigating the general problematic of small sumsets in groups. In particular, in the third part of this series [18], we shall give several other new results on this subject.

2. The proofs of Lemmas 4 and 5

We start with a proof of Lemma 4, a statement which is clearly reminiscent of the following highly classical result (see Chapter 1 of [15]) :

Lemma 12. *Let $\mathcal{A}$ and $\mathcal{B}$ be two non-empty subsets of $\mathbb{Z}$. Then $|\mathcal{A} + \mathcal{B}| \geq |\mathcal{A}| + |\mathcal{B}| - 1$ and equality holds if and only if $\min(|\mathcal{A}|, |\mathcal{B}|) = 1$ or $\mathcal{A}$ and $\mathcal{B}$ are two arithmetic progressions with the same difference.*

This lemma will not be needed in the sequel.

P r o o f o f L e m m a 4. That the values given by the Lemma are upper bounds of $\xi_{\mathbb{Z}}(r,s)$ is trivial by considering the sum of the sets $\mathcal{A}=\{0,\dots,r-1\}$ and $\mathcal{B}=\{0,\dots,s-1\}$.

Let us prove the lower bound. First, we observe that if $a_1<\cdots<a_{|\mathcal{A}|}$ and $b_1<\cdots<b_{|\mathcal{B}|}$ are the ordered elements of two subsets of $\mathbb{Z}$ denoted by $\mathcal{A}$ and $\mathcal{B}$, respectively, then among the following $|\mathcal{A}|+|\mathcal{B}|-1$ distinct elements of $\mathcal{A}+\mathcal{B}$

$$a_1+b_1<a_1+b_2<\cdots<a_1+b_{|\mathcal{B}|}<a_2+b_{|\mathcal{B}|}<\cdots<a_{|\mathcal{A}|}+b_{|\mathcal{B}|} \tag{2}$$

at most two do not belong to $\mathcal{A}\hat{+}\mathcal{B}$ (one at most of the form a_1+b_i for some i between 1 and $|\mathcal{B}|$ and one at most of the form $a_j+b_{|\mathcal{B}|}$ for some j between 1 and $|\mathcal{A}|$). It follows

$$|\mathcal{A}\hat{+}\mathcal{B}|\geq|\mathcal{A}|+|\mathcal{B}|-3.$$

This implies $\xi_{\mathbb{Z}}(r,s)\geq r+s-3$ and proves the Lemma in the case $r=s\neq 1$ (the case $r=s=1$ is immediate).

In the case $r\neq s$, it remains to show that the preceding inequality can be improved into $\xi_{\mathbb{Z}}(r,s)\geq r+s-2$. Indeed assume that $|\mathcal{A}|=r$, $|\mathcal{B}|=s$. We may assume without loss of generality that $r>s$. It follows that $\mathcal{A}\not\subset\mathcal{B}$. We choose some k such that $a_k\notin\mathcal{B}$. Clearly we may also assume that $a_1=b_i$ for some i between 1 and $|\mathcal{B}|$ and $a_j=b_{|\mathcal{B}|}$ for some j between 1 and $|\mathcal{A}|$ otherwise (2) is enough to imply the result. Now we consider the increasing sequence

$$\begin{aligned}a_1+b_1<a_1+b_2<\cdots<a_1+b_{i-1}<a_2+b_{i-1}<\cdots<a_k+b_{i-1}<a_k+b_i\\ <a_k+b_{i+1}<\cdots<a_k+b_{|\mathcal{B}|}<a_{k+1}+b_{|\mathcal{B}|}<\cdots<\cdots<a_{|\mathcal{A}|}+b_{|\mathcal{B}|}.\end{aligned}$$

We check that it has $|\mathcal{A}|+|\mathcal{B}|-1$ distinct elements. Since $a_1=b_i>b_s$ for $1\leq s\leq i-1$ and $a_s>a_1=b_i>b_{i-1}$ for $2\leq s\leq k$ and no b_s is equal to a_k, at most one element in this sequence (in fact exactly one if and only if $k<j$) is possibly not in $\mathcal{A}\hat{+}\mathcal{B}$. It follows that $|\mathcal{A}\hat{+}\mathcal{B}|\geq r+s-2$, as announced. □

P r o o f o f L e m m a 5. In an elementary 2-group G, a double is always equal to zero, while if a sum $a+b$ ($a\in\mathcal{A}$, $b\in\mathcal{B}$ with some subsets $\mathcal{A},\mathcal{B}\subset G$) is equal to 0 then $a=-b=b$ and the sum is a double.

It follows that in an elementary 2-group, we always have $|\mathcal{A}+\mathcal{B}|-1\leq|\mathcal{A}\hat{+}\mathcal{B}|\leq|\mathcal{A}+\mathcal{B}|$ which implies $\mu_G(r,s)-1\leq\xi_G(r,s)\leq\mu_G(r,s)$.

But, since $|\mathcal{A}+\mathcal{B}|$ is unchanged by a translation, we may always assume that $\mu_G(r,s)$ is attained by a pair of sets $(\mathcal{A},\mathcal{B})$ such that $0\in\mathcal{A}\cap\mathcal{B}$. For this pair, we have $|\mathcal{A}\hat{+}\mathcal{B}|=|\mathcal{A}+\mathcal{B}|-1=\mu_G(r,s)-1$. Hence the result. □

3. Theorem 7 and its consequences

In order to prove Theorem 7, we start with a lemma.

Lemma 13. *All finite cyclic groups have the hypersmall sumsets property.*

Proof. First, these groups have the supersmall sumsets property by Lemma 2.

Let now G be a (finite) cyclic group with cardinality n and r be an integer $1 \leq r \leq n$. Assume we are not in the fourth case allowed in the definition of the hypersmall sumsets property: in particular, we must have $r \neq 1$. We now define the set

$$\mathcal{A} = \{0, 1, \ldots, r-1\}$$

and observe that $\mathcal{A} + \mathcal{A} = \{0, \ldots, 2r-2\}$.

In the case $2r-2 \leq n-1$, we have $|\mathcal{A}+\mathcal{A}| = 2r-1$ but 0 and $2r-2 = 2(r-1)$ are two distinct (recall $r \neq 1$) doubles and we are in case (iii) of the definition.

In the case $2r-2 = n$, we have $|\mathcal{A}+\mathcal{A}| = n = 2r-2$ but 0 is a double (with two representations as a double, namely $0+0$ and $(r-1)+(r-1)$). We are in case (ii) of the definition.

Finally, if $2r-2 \geq n+1$, then we are in case (i) of the definition since $|\mathcal{A}+\mathcal{A}| = n \leq 2r-3$. The proof is complete. □

We are now ready to give the proof of Theorem 7.

Proof of Theorem 7. Let G be an arbitrary Abelian group. It verifies the supersmall sumsets property by Lemma 2. It therefore remains only to check the property specific to the hypersmall sumsets property. The proof is decomposed into several steps.

Step 1: The group $\mathbb{Z}$ has the hypersmall sumsets property.

This follows from the fact that for any positive integer r, the sumset $\{0, \ldots, r-1\}+\{0, \ldots, r-1\} = \{0, \ldots, 2r-2\}$ has $2r-1$ elements with two distinct doubles (0 and $2(r-1)$).

Step 2: Every finite cyclic group has the hypersmall sumsets property.

This is the result of Lemma 13.

Step 3: Any finite Abelian group has the hypersmall sumsets property.

Let r be a positive integer. Assume that condition (iv) in the definition of the hypersmall sumsets property is not fulfilled (otherwise we are done): that is, there exists some non-trivial minimal (cyclic of prime order) subgroup M of G such that $r \not\equiv 1 \pmod{|M|}$.

We put

$$\rho = \left\lceil \frac{r}{|M|} \right\rceil$$

and consider the factor group G/M (which is Abelian) in which we apply Lemma 2: this implies the existence of a subset $\mathcal{A}' \subset G/M$ with cardinality ρ such that $0 \in \mathcal{A}'$ and either

(i) $|\mathcal{A}' + \mathcal{A}'| \leq 2\rho - 2$, or

(ii) $|\mathcal{A}' + \mathcal{A}'| = 2\rho - 1$ and 0 has the unique representation $0 + 0$ as an element of $\mathcal{A}' + \mathcal{A}'$.

In fact, we use a slightly more precise version of Lemma 2 which tells us that in the definition of the supersmall sumset property, in the case $r = s$, we can choose $\mathcal{A} = \mathcal{B}$. We do not include a proof of this slight refinement of Lemma 2, since the proof given in [17] can be adapted in an immediate way to contain this.

If we are in case (i), we may select a set $\mathcal{A}$ in G such that $0 \in \mathcal{A}$, $|\mathcal{A}| = r$ and $\mathcal{A} \subset \pi^{-1}(\mathcal{A}')$ (here and in what follows, π denotes the canonical homomorphism of G onto G/M). Therefore,

$$|\mathcal{A} + \mathcal{A}| \leq |\mathcal{A}' + \mathcal{A}'| \times |M| \leq (2\rho - 2)|M|.$$

Since $r \not\equiv 1 \pmod{|M|}$, we have

$$\rho = \left\lceil \frac{r}{|M|} \right\rceil \leq \frac{r + |M| - 2}{|M|}.$$

It follows

$$|\mathcal{A} + \mathcal{A}| \leq \left(2 \cdot \frac{r + |M| - 2}{|M|} - 2 \right) |M| = 2r - 4,$$

which implies the result.

If we are in case (ii), we may apply Lemma 13 (and the proof of it) to the cyclic group of prime order M and find a set $\mathcal{A}_0 \subset M$ containing 0, with cardinality $r - (\rho - 1)|M|$ (a positive integer different from 1 and $\leq |M|$) such that $\mathcal{A}_0$ verifies either (iii), (ii) or (i): we shall write $|\mathcal{A}_0 + \mathcal{A}_0| = 2|\mathcal{A}_0| - \eta$ with $\eta = 1, 2$ or 3 respectively. Now, we define

$$\mathcal{A} = \mathcal{A}_0 \cup \pi^{-1}(\mathcal{A}' \setminus \{0\}).$$

We have $|\mathcal{A}| = (\rho - 1)|M| + |\mathcal{A}_0| = r$ and since $(\mathcal{A} + \mathcal{A}) \cap M$ reduces to $\mathcal{A}_0 + \mathcal{A}_0$ in view of the unicity of the representation of 0 in $\mathcal{A}' + \mathcal{A}' \subset G/M$, we have

$$\begin{aligned} |\mathcal{A} + \mathcal{A}| &= (|\mathcal{A}' + \mathcal{A}'| - 1)|M| + |\mathcal{A}_0 + \mathcal{A}_0| \\ &= (2\rho - 2)|M| + 2|\mathcal{A}_0| - \eta \\ &= 2(\rho - 1)|M| + 2(r - (\rho - 1)|M|) - \eta = 2r - \eta. \end{aligned}$$

We conclude using again the unicity of the representation of 0 in $\mathcal{A}'+\mathcal{A}' \subset G/M$: the properties of doubles in $\mathcal{A}+\mathcal{A}$ which lie in M are inherited from the ones of the doubles in $\mathcal{A}_0+\mathcal{A}_0$ in view of this argument.

Step 4: Any Abelian group has the hypersmall sumsets property.

By Step 3, we can assume that G is infinite. Let r be an arbitrary positive integer. We assume that (iv) does not hold for r in G (otherwise we are done). We choose a subset $\mathcal{S}$ of G having r elements and consider the subgroup H of G generated by $\mathcal{S}$. By definition, this group is finitely generated. By the general structure theorem on finitely generated Abelian groups (see for instance Chapter I.5 in [19]),

- either H contains a subgroup isomorphic to $\mathbb{Z}$ (in which case, the result is immediate by Step 1)
- or H is finite (and satisfies $r \leq |H|$) in which case we conclude using Step 3 as follows. Since G admits non-trivial finite subgroups (e.g. H) but, by assumption, does not satisfy (iv) for the integer r, there is a finite non-trivial minimal subgroup K of G such that $r \not\equiv 1 \pmod{|K|}$. As asserted above, K has to be a cyclic group and we may find a generating element k in it. Now, we consider $\mathcal{S}' = \mathcal{S} \cup \{k\}$ which generates again a finite group (containing K), say H'. By Step 3, H' has the hypersmall sumsets property. Since K is a non-trivial minimal subgroup of H' and $r \not\equiv 1 \pmod{|K|}$, the integer r cannot satisfy (iv) in H' and therefore it satisfies either (i) or (ii) or (iii) in H' and thus in G and we are done.

□

We can now come to the proof of Theorem 8.

Proof of Theorem 8. Consider two integers $1 \leq r, s \leq |G|$. Since G has the supersmall sumsets property (Lemma 2), there are subsets $\mathcal{A}, \mathcal{B} \subset G$, with $|\mathcal{A}| = r$ and $|\mathcal{B}| = s$ such that either $|\mathcal{A}+\mathcal{B}| \leq r+s-2$ or $|\mathcal{A}+\mathcal{B}| = r+s-1$ and 0 has a unique representation $0+0$ (and therefore is a double) in $\mathcal{A}+\mathcal{B}$. In this second case, it follows

$$|\mathcal{A}\hat{+}\mathcal{B}| \leq |\mathcal{A}+\mathcal{B}| - 1 = r+s-2,$$

an inequality which is thus valid in any case. Consequently

$$\xi_G(r,s) \leq r+s-2.$$

In view of the trivial (1), the first inequality in the Theorem follows.

Now, if r is regular for G, we must have a subset $\mathcal{A}$ of G with cardinality r such that either $|\mathcal{A}+\mathcal{A}| \leq 2r-3$, or $|\mathcal{A}+\mathcal{A}| = 2r-2$ and 0 is a double in the

sumset $\mathcal{A}+\mathcal{A}$, or $|\mathcal{A}+\mathcal{A}|=2r-1$ and 0 is a double in the sumset $\mathcal{A}+\mathcal{A}$ and there is yet another (distinct) such double. In all three cases, we have

$$|\mathcal{A}\hat{+}\mathcal{A}|\leq 2r-3.$$

The result follows. □

4. The proof of Theorem 11 using Lev's conjecture

In this section, we present the proof of Theorem 11 which is a good indication of the validity of Conjecture 9.

P r o o f o f T h e o r e m 11. In the special case of Abelian groups G containing no element of order two, one has $L_G=1$. Therefore, Lev's Conjecture 10 reads as follows: let $\mathcal{A},\mathcal{B}$ be two non-empty finite subsets of G such that

$$|\mathcal{A}\hat{+}\mathcal{B}|\leq|\mathcal{A}|+|\mathcal{B}|-4$$

then $\mathcal{A}\hat{+}\mathcal{B}=\mathcal{A}+\mathcal{B}$. In particular, this implies $|\mathcal{A}+\mathcal{B}|=|\mathcal{A}\hat{+}\mathcal{B}|\leq|\mathcal{A}|+|\mathcal{B}|-4$.

If, by contradiction with the conclusion of Theorem 11, we assume that

$$\xi_G(r,s)<\min\big(r+s-3,\mu_G(r,s)\big)=\min\left(r+s-3,\min_{d\in\mathcal{D}}\left(\left\lceil\frac{r}{d}\right\rceil+\left\lceil\frac{s}{d}\right\rceil-1\right)d\right),\tag{3}$$

(where $\mathcal{D}$ stands again - as in our Theorem 1 - for the set of integers that are the cardinality of a finite subgroup of G) then in particular there are $\mathcal{A},\mathcal{B}\subset G$ such that $|\mathcal{A}|=r$, $|\mathcal{B}|=s$ and

$$\xi_G(r,s)=|\mathcal{A}\hat{+}\mathcal{B}|\leq|\mathcal{A}|+|\mathcal{B}|-4.$$

By Lev's Conjecture, we then have $\mathcal{A}\hat{+}\mathcal{B}=\mathcal{A}+\mathcal{B}$ and as mentioned above this implies that $|\mathcal{A}+\mathcal{B}|\leq|\mathcal{A}|+|\mathcal{B}|-4$. Now, the trick (based on Kneser's theorem) which was originally introduced in [16] (and widely reused afterwards) for the study of this type of functions can be used again. Indeed, Kneser's theorem implies that in this case $\mathcal{A}+\mathcal{B}$ is periodic with a period H such that

$$|\mathcal{A}+\mathcal{B}|=|\mathcal{A}+H|+|\mathcal{B}+H|-|H|.$$

This yields

$$\begin{aligned}\xi_G(r,s) = |\mathcal{A}\hat{+}\mathcal{B}| = |\mathcal{A}+\mathcal{B}| &= |\mathcal{A}+H|+|\mathcal{B}+H|-|H| \\ &\geq \left(\left\lceil\frac{r}{|H|}\right\rceil+\left\lceil\frac{s}{|H|}\right\rceil-1\right)|H| \\ &\geq \min_{d\in\mathcal{D}}\left(\left\lceil\frac{r}{d}\right\rceil+\left\lceil\frac{s}{d}\right\rceil-1\right)d \\ &= \mu_G(r,s),\end{aligned}$$

a contradiction with (3). This proves the first assertion of Theorem 11.

The second assertion of the Theorem (case where r is regular) follows from the first one and Theorem 8. □

Acknowledgements. The author thanks an anonymous referee for a careful reading of this paper and several useful remarks.

REFERENCES

[1] ALON, N. – NATHANSON, M.B. – RUZSA, I.Z.: *Adding distinct congruences classes modulo a prime*, Amer. Math. Monthly **102** (1995), 250–255.

[2] ALON, N. – NATHANSON, M.B. – RUZSA, I.Z.: *The polynomial method and restricted sums of congruence classes*, J. Number Theory **56** (1996), 404–417.

[3] CAUCHY, A.-L.: *Recherches sur les nombres*, J. École polytech. **9** (1813), 99–123.

[4] DAVENPORT, H.: *On the addition of residue classes*, J. London Math. Soc. **10** (1935), 30–32.

[5] DIAS DA SILVA, J.A. – HAMIDOUNE, Y.O.: *Cyclic spaces for Grassman derivatives and additive theory*, Bull. London Math. Soc. **26** (1994), 140–146.

[6] ELIAHOU, S. – KERVAIRE, M.: *Sumsets in vector spaces over finite fields*, J. Number Theory **71** (1998), 12–39.

[7] ELIAHOU, S. – KERVAIRE, M.: *Restricted sums of sets of cardinality* $1+p$ *in a vector space over* $\mathbf{F}_p$, Combinatorics (Prague, 1998), Discrete Math. **235** (2001), no. 1-3, 199–213.

[8] ELIAHOU, S. – KERVAIRE, M.: *Restricted sumsets in finite vector spaces: the case* $p=3$, Integers **1** (2001), A2, 19 pp. (electronic).

[9] FREIMAN,G. A.: *Foundations of a Structural Theory of Set Addition* (translated from the Russian), Translations of Mathematical Monographs Vol. **37**, American Mathematical Society, Providence, R. I., 1973.

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

[11] KNESER, M.: *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429–434.

[12] LEV, V.F.: *Restricted set addition in groups I: the classical settings*, J. London Math. Soc. (2) **62** (2000),no. 1, 27–40.

[13] LEV, V.F.: *Restricted set addition in abelian groups: results and conjectures*, J. Théor. Nombres Bordeaux **17** (2005), no. 1, 181–193.
[14] MANN, H. B.: *Addition Theorems: The Addition Theorems of Group Theory and Number Theory*, Interscience Publishers, John Wiley, 1965.
[15] NATHANSON, M. B.: *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics Vol. **165**, Springer Verlag, 1996.
[16] PLAGNE, A.: *Additive number theory sheds extra light on the Hopf-Stiefel $\circ$ function*, Enseign. Math., II. Sér. **49** (2003), no. 1–2, 109–116.
[17] PLAGNE, A.: *Optimally small sumsets in groups I. The supersmall sumsets property, the $\mu_G^{(k)}$ and the $\nu_G^{(k)}$ functions*, Uniform Distribution Theory **1** (2006), 27–43.
[18] PLAGNE, A.: *Optimally small sumsets in groups III. The generalized increasingly small sumsets property and the $\nu_G^{(k)}$ functions*, preprint (2006).
[19] SAMUEL, P.: *Théorie Algébrique des Nombres*, Hermann, Paris, 1967.

Received September 9, 2006
Revised December 29, 2006

Alain Plagne
Centre de Mathématiques Laurent Schwartz
UMR 7640 du CNRS
École polytechnique
91128 Palaiseau cedex
FRANCE
E-mail: plagne@math.polytechnique.fr