Functiones et Approximatio
XXXVII.2 (2007), 377–397

OPTIMALLY SMALL SUMSETS IN GROUPS III. THE GENERALIZED INCREASINGLY SMALL SUMSETS PROPERTY AND THE $\nu_G^{(k)}$ FUNCTIONS

Alain Plagne

À Jean-Marc Deshouillers,
à l'occasion de son $1^5+2^4+3^3+4^2$-ième anniversaire

Abstract: In this third part of our work, we go back to the study of the $\nu_G^{(k)}$ functions (introduced in the first one), which count the minimal cardinality of a sumset containing an element with a single representation. An upper bound for these functions is obtained in the case $k=2$ using what we call the generalized increasingly small sumsets property, which is proved to hold for all Abelian groups. Moreover, we show that our bound cannot be improved in general.
Keywords: additive number theory, small sumsets, supersmall sumsets, Abelian groups, initial segment.

1. Introduction

This is the third part of a work started in [12, 13] on small sumsets in groups, a subject taking place in the context of additive number theory (see [9] and [10] for two classical introductions). In what follows, we start with a short summary of what we did in our previous papers. Concerning precise motivations and for a more complete history and references on the subject, we refer to the first two parts [12, 13].

In the first part [12], the author introduced the generalized supersmall sumsets property: a group G (written additively) was said to have this property if for any positive integer k, any $1 \leqslant r_1, \dots, r_k \leqslant |G|$ (where $|G|$ denotes the cardinality of the group G if it is finite or $+\infty$ if G is infinite, in which case, a constraint like $r_1 \leqslant |G|$ is trivially empty), 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

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

2000 Mathematics Subject Classification: 11B75, 20D60, 11P99, 20Kxx.

We recall that a (Minkowski) sumset is defined as follows

$$\mathcal{A}_1 + \cdots + \mathcal{A}_k = \{a_1 + \cdots + a_k,\ a_1 \in \mathcal{A}_1, \ldots, a_k \in \mathcal{A}_k\}.$$

It was proved in [12] that this property holds for all solvable groups. As an application of this problematic (and using Kneser's theorem [6, 7] in the way introduced for this problem in [11]), we obtained a formula (see (2) below) for the functions

$$\mu_G^{(k)}(r_1, \ldots, r_k) = \min\{|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \text{ such that } \mathcal{A}_1, \ldots, \mathcal{A}_k \subset G \text{ and } |\mathcal{A}_1| = r_1, \ldots, |\mathcal{A}_k| = r_k\}, \quad (1)$$

defined as the minimal cardinality of a sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ with $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset G$ and $|\mathcal{A}_1| = r_1, \ldots, |\mathcal{A}_k| = r_k$ and, second, bounds for the $\nu_G^{(k)}(r_1, \ldots, r_k)$ functions, which have a slightly more complex definition, namely

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

Not only the definition of these functions are more complex, but also their behaviours. The reader is referred to [12] for the precise bounds that were obtained there for $\nu_G^{(k)}(r_1, \ldots, r_k)$.

In the second part [13], a more sophisticated tool – which builds on the supersmall sumsets property – called the hypersmall sumsets property was introduced. It was shown that all Abelian groups have this property which was then applied to the computation of the $\xi_G(r, s)$ functions defined as the minimal cardinality of a restricted sumset $\mathcal{A}\hat{+}\mathcal{B}$ where $|\mathcal{A}| = r$, $|\mathcal{B}| = s$ and $\mathcal{A}\hat{+}\mathcal{B}$ denotes $\{a + b,\ a \in \mathcal{A}, b \in \mathcal{B}, a \neq b\}$. Using this new tool, we could prove that for any Abelian group G and for any integers $1 \leqslant r, s \leqslant |G|$, we have

$$\xi_G(r, s) \leqslant \min\big(r + s - 2, \mu_G(r, s)\big);$$

if $r = s$, we also proved that, in most cases (that we called regular), we could improve this upper bound into

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

Finally, a conjecture was stated on the precise values taken by $\xi_G(r, s)$, which, in some cases, was shown to hold, assuming a conjecture by Lev [8] dealing with a counterpart to Kneser's theorem [6, 7] in the frame of restricted addition.

In this paper, we keep the notation adopted in the first two parts of this work [12, 13]: let G be a group, k be a positive integer and $r_1, \ldots, r_k$ be k positive

integers $\leqslant |G|$. All the groups we shall deal with in this article will be written additively and their neutral element denoted by 0.

While the function $\mu_G^{(k)}(r_1,\dots,r_k)$ is proved [12] – when G is an arbitrary Abelian group – to be equal to

$$\mu_G^{(k)}(r_1,\dots,r_k)=\min_{d\in\mathcal{D}}\left(\left\lceil\frac{r_1}{d}\right\rceil+\cdots+\left\lceil\frac{r_k}{d}\right\rceil-k+1\right)d, \tag{2}$$

where $\mathcal{D}$ is the set of integers that are the cardinality of a finite subgroup of G, the function $\nu_G^{(k)}(r_1,\dots,r_k)$ (see the definition above) has a more erratic behaviour to which we go back in the present article. In [12], we obtained several results on this function, notably the following lower bound (which was obtained as a consequence of the Kemperman-Scherk theorem [4, 5, 15]).

Theorem 1. *Let G be an Abelian group. As soon as $r_1+\cdots+r_k\geqslant |G|+k$, we have*

$$\nu_G^{(k)}(r_1,\dots,r_k)=\infty.$$

Moreover, if $r_1+\cdots+r_k\leqslant |G|+k-1$, we have

$$\nu_G^{(k)}(r_1,\dots,r_k)\geqslant r_1+\cdots+r_k-k+1.$$

This lower bound cannot in general be improved since we could prove explicitly the value of $\nu_G^{(k)}(r_1,\dots,r_k)$ to be equal to this lower bound in some specific cases. Let us for instance reformulate (in an apparently more general form) a result we obtained in [12].

Theorem 2. *Let G be a group and $1\leqslant r_1,\dots,r_k\leqslant |G|$ be integers. If G is an Abelian group containing either a subgroup isomorphic to $\mathbb{Z}$ or a cyclic subgroup H such that $r_1+\cdots+r_k\leqslant |H|+k-1$, then*

$$\nu_G^{(k)}(r_1,\dots,r_k)=r_1+\cdots+r_k-k+1.$$

We also gave lots of other situations where the same value $r_1+\cdots+r_k-k+1$ is attained (this was our Theorem 9 in [12]). However, we noticed that, in general, $\nu_G^{(k)}(r_1,\dots,r_k)$ is different from $r_1+\cdots+r_k-k+1$ by observing the following two very simple examples (valid in the case $k=2$):

(1) $G=(\mathbb{Z}/2\mathbb{Z})^2$ and $r_1=r_2=2$ for which $\nu^{(2)}_{(\mathbb{Z}/2\mathbb{Z})^2}(2,2)=4$,

(2) $G=(\mathbb{Z}/3\mathbb{Z})^2$, $r_1=2$ and $r_2=3$ where $\nu^{(2)}_{(\mathbb{Z}/3\mathbb{Z})^2}(2,3)=5$.

In the present work, we restart from this point. Our aim is to investigate upper bounds for the $\nu_G^{(k)}(r_1,\dots,r_k)$ functions in the case where G is an Abelian group.

2. New results

To start with and for the sake of completeness, we first state the following proposition which presents a new (but commonplace) situation in which the lower bound of Theorem 1 is attained.

Theorem 3. *Let G be an Abelian group. If*

$$\mu_G^{(k)}(r_1,\dots,r_k) = r_1+\cdots+r_k-k+1$$

then

$$\nu_G^{(k)}(r_1,\dots,r_k) = r_1+\cdots+r_k-k+1.$$

Indeed, since G has the generalized supersmall sumsets property (in view of Theorem 2 of [12] and because G is Abelian) we must be either in case (i) or in case (ii) of the definition of this property (see the introduction). But in view of the value of $\mu_G(r_1,\dots,r_k)$ we cannot be in case (i). This implies that we are in case (ii) and the result follows.

Then, we study upper bounds on $\nu_G^{(k)}(r_1,\dots,r_k)$. It turns out that what is needed in such a study is a property of increasingness of the generalized supersmall sumsets property. Having this remark in mind, the introduction of a rather technical refinement of this property becomes quite natural: we say that a group G has the *generalized increasingly small sumsets property* if for any positive integer k, any $1\leqslant r_1,\dots,r_k\leqslant |G|$, any $1\leqslant r'_1,\dots,r'_k\leqslant |G|$ such that $r_i\leqslant r'_i$ (for all $1\leqslant i\leqslant k$), there exist subsets $\mathcal{A}_1,\dots,\mathcal{A}_k,\mathcal{A}'_1,\dots,\mathcal{A}'_k\subset G$, containing 0, such that $|\mathcal{A}_1|=r_1,\dots,|\mathcal{A}_k|=r_k,|\mathcal{A}'_1|=r'_1,\dots,|\mathcal{A}'_k|=r'_k$, satisfying $\mathcal{A}_i\subset\mathcal{A}'_i$ for all $1\leqslant i\leqslant k$ and such that

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

(ii) or $|\mathcal{A}_1+\cdots+\mathcal{A}_k| = r_1+\cdots+r_k-k+1$ and there is an element α in $\mathcal{A}_1+\cdots+\mathcal{A}_k$ which has a unique representation $\alpha=\alpha_1+\cdots+\alpha_k$ (with $\alpha_1\in\mathcal{A}_1,\dots,\alpha_k\in\mathcal{A}_k$) as an element of the sumset $\mathcal{A}_1+\cdots+\mathcal{A}_k$,

and

(i') either $|\mathcal{A}'_1+\cdots+\mathcal{A}'_k|\leqslant r'_1+\cdots+r'_k-k$,

(ii') or $|\mathcal{A}'_1+\cdots+\mathcal{A}'_k| = r'_1+\cdots+r'_k-k+1$ and there is an element α' in $\mathcal{A}'_1+\cdots+\mathcal{A}'_k$ which has a unique representation $\alpha'=\alpha'_1+\cdots+\alpha'_k$ (with $\alpha'_1\in\mathcal{A}'_1,\dots,\alpha'_k\in\mathcal{A}'_k$) as an element of the sumset $\mathcal{A}'_1+\cdots+\mathcal{A}'_k$.

For the sake of completeness, we recall the following definition: we say that an element $x\in\mathcal{A}_1+\cdots+\mathcal{A}_k$ has r *representations (as an element of the sumset* $\mathcal{A}_1+\cdots+\mathcal{A}_k$*)* if

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

We notice that, by definition, a group which has the generalized increasingly small sumsets property has also the generalized supersmall sumsets property (simply take $r'_i=r_i$ for all index i). In fact, the generalized supersmall sumsets property appears like a "diagonal" case compared to the generalized increasingly small sumsets property which can be seen as a "polar" version of it.

We already knew that every solvable group has the generalized supersmall sumsets property (Theorem 2 in [12]). Here, we first obtain the following result.

Theorem 4. *Every Abelian group has the generalized increasingly small sumsets property.*

The proof of Theorem 4 will be given in Section 3.

In view of what we just mentioned, this result implies in particular the special case of Abelian groups in Theorem 2 of [12]. In fact, the method for proving Theorem 4 (a rather "direct" method in the spirit of that one used in [3]) will be different from the method used in [12] (a mainly "inductive" method). It follows that Theorem 4 gives a second proof that every Abelian group has the generalized supersmall sumsets property.

To go further and discuss the application of Theorem 4 to $\nu_G^{(k)}$, let us now introduce another definition. For G a group, k a positive integer and $r_1, \dots, r_k \in \mathbb{N}$ satisfying $r_1, \dots, r_k \leqslant |G|$, we write $\mathcal{D}$ for the set of integers that are the cardinality of a finite subgroup of G. We shall denote by $\delta_G^{(k)}(r_1, \dots, r_k)$ the (well-defined) quantity

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

Notice that $\delta_G^{(k)}(r_1, \dots, r_k) \leqslant \mu_G^{(k)}(r_1, \dots, r_k)$.

Having this notation at our disposal, we are ready to apply the increasingly small sumsets property to obtain an upper bound on $\nu_G^{(k)}$ in the case of two arguments ($k = 2$).

Theorem 5. *Let G be an arbitrary Abelian group and $\mathcal{D}$ stands for the set of integers that are the cardinality of a finite subgroup of G. For any $1 \leqslant r, s \leqslant |G|$, we have*

$$\nu_G^{(2)}(r, s) \leqslant \mu_G^{(2)}(r, s) + \delta_G^{(2)}(r, s).$$

We notice that in particular, this implies

$$\mu_G^{(2)}(r, s) \leqslant \nu_G^{(2)}(r, s) \leqslant 2\mu_G^{(2)}(r, s).$$

The proof of Theorem 5 will be presented in Section 4.

One of the interests of this result follows from the fact that it is in general best possible. Indeed, our next result shows a family of situations where it is an equality.

Theorem 6. *Let p be an arbitrary prime. We have*

$$\nu_{(\mathbb{Z}/p\mathbb{Z})^2}^{(2)}(p, p) = 2p, \quad \mu_{(\mathbb{Z}/p\mathbb{Z})^2}^{(2)}(p, p) = p \quad \text{and} \quad \delta_{(\mathbb{Z}/p\mathbb{Z})^2}^{(2)}(p, p) = p.$$

We shall give two proofs of this result in Section 5. First, a long but down-to--earth proof will be explained: it uses only simple but specific to $\mathbb{Z}/p\mathbb{Z}$ tools and leaves open possibilities to further developments (in particular, other values of $\nu_{(\mathbb{Z}/p\mathbb{Z})^2}^{(2)}$ can be obtained by a similar method). Second, a more sophisticated proof based on Kemperman's theorem, which is much shorter (in fact, its length and

complexity are hidden by the use of Kemperman's theorem). The author thanks an anonymous referee for suggesting such another proof.

Developping Theorem 5 into several directions, including for instance the case $k > 2$, should be a good subject to which we plan to come back in a near future. Other applications of Theorem 4 should also be of interest.

3. Proof of Theorem 4

We start by introducing some terminology in the case where we consider a finite product of finite cyclic groups,

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z},$$

where $n_1, \ldots, n_s$ are given integers such that $n_i \geqslant 2$ $(1 \leqslant i \leqslant s)$. In what follows, an element of G will be written as an s-tuple $(x_1, \ldots, x_s)$ where each x_i is an integer between 0 and $n_i - 1$, for $1 \leqslant i \leqslant s$.

We may now order the elements of G lexicographically, that is

$$(y_1, \ldots, y_s) \succ (x_1, \ldots, x_s)$$

if and only if there is some integer i $(1 \leqslant i \leqslant s)$ such that $y_i > x_i$ and $y_j = x_j$ for all $1 \leqslant j < i$.

We shall denote by G_i the subgroup of G given by

$$G_i = \{0\} \times \cdots \times \{0\} \times \mathbb{Z}/n_i\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

where i is any integer satisfying $1 \leqslant i \leqslant s$.

We notice that every integer m less than $n = n_1 \cdots n_s$ can be written in a unique way as a sum

$$m = \alpha_1(m)n_2 \cdots n_s + \alpha_2(m)n_3 \cdots n_s + \cdots + \alpha_{s-1}(m)n_s + \alpha_s(m), \qquad (3)$$

where each $\alpha_i(m)$ is an integer (a digit) verifying $0 \leqslant \alpha_i(m) \leqslant n_i - 1$ (for $1 \leqslant i \leqslant s$). We write $m = [\alpha_1(m), \alpha_2(m), \ldots, \alpha_{s-1}(m), \alpha_s(m)]_{n_1,\ldots,n_s}$, that is as a list of digits (in basis $(n_1, \ldots, n_s)$). When there is no ambiguity, we shall write α_i instead of $\alpha_i(m)$.

We can check the following compatibility fact: $l < m$ (that is,

$$[\alpha_1(l), \alpha_2(l), \ldots, \alpha_{s-1}(l), \alpha_s(l)]_{n_1,\ldots,n_s} < [\alpha_1(m), \alpha_2(m), \ldots, \alpha_{s-1}(m), \alpha_s(m)]_{n_1,\ldots,n_s})$$

if and only if

$$(\alpha_1(l), \alpha_2(l), \ldots, \alpha_{s-1}(l), \alpha_s(l)) \prec (\alpha_1(m), \alpha_2(m), \ldots, \alpha_{s-1}(m), \alpha_s(m))$$

in G.

For a non-negative integer $m \leqslant |G|$, we finally denote by $\mathfrak{I}_m$ the subset of G composed of its elements which are lexicographically less than $(\alpha_1(m), \alpha_2(m), \ldots, \alpha_{s-1}(m), \alpha_s(m))$. In other words, we observe the following explicit description (still using the notation of (3) but forgetting the reference to m in the α_i's) of $\mathfrak{I}_m$:

$$\begin{aligned}\mathfrak{I}_m = &\big(\{(i,0,\ldots,0) \text{ for } 0 \leqslant i \leqslant \alpha_1 - 1\} + G_2\big)\\ &\cup \big(\{(\alpha_1, i, 0, \ldots, 0) \text{ for } 0 \leqslant i \leqslant \alpha_2 - 1\} + G_3\big)\\ &\cup \ldots \cup \big(\{(\alpha_1, \alpha_2, \ldots, \alpha_{s-2}, i, 0) \text{ for } 0 \leqslant i \leqslant \alpha_{s-1} - 1\} + G_s\big)\\ &\cup \big(\{(\alpha_1, \alpha_2, \ldots, \alpha_{s-1}, i) \text{ for } 0 \leqslant i \leqslant \alpha_s - 1\}\big).\end{aligned}$$

We shall write

$$I^{(k)}_{\alpha_1,\ldots,\alpha_k} = \{(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, i, 0, \ldots, 0) \text{ for } 0 \leqslant i \leqslant \alpha_k - 1\}$$

so that

$$\mathfrak{I}_m = \big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big(I^{(2)}_{\alpha_1,\alpha_2} + G_3\big) \cup \ldots \cup \big(I^{(s-1)}_{\alpha_1,\ldots,\alpha_{s-1}} + G_s\big) \cup I^{(s)}_{\alpha_1,\ldots,\alpha_{s-1},\alpha_s}. \quad (4)$$

In [3], such sets are called *initial segments* and we shall keep this terminology in our present purpose. The element

$$(\alpha_1, \alpha_2, \ldots, \alpha_{s-1}, \alpha_s - 1)$$

will be called the *extremity* of the initial segment $\mathfrak{I}_m$.

Two facts are worth noticing. First, the set $\mathfrak{I}_m$ in the form (4) is a disjoint union of $\big(I^{(1)}_{\alpha_1} + G_2\big)$, $\big(I^{(2)}_{\alpha_1,\alpha_2} + G_3\big), \ldots, \big(I^{(s-1)}_{\alpha_1,\ldots,\alpha_{s-1}} + G_s\big)$ and $I^{(s)}_{\alpha_1,\ldots,\alpha_{s-1},\alpha_s}$. Second, given an initial segment, the integers $\alpha_1, \ldots, \alpha_{s-1}, \alpha_s$ used in a decomposition of the form (4) are unique. For instance, α_1 is the greatest first coordinate of any element in the set, α_2 is the greatest second coordinate of any element in the set having α_1 as its first coordinate, and so on...

We also emphasize the following basic fact that the set

$$\big(I^{(k)}_{\alpha_1,\ldots,\alpha_k} + G_{k+1}\big) \cup \ldots \cup \big(I^{(s-1)}_{\alpha_1,\ldots,\alpha_{s-1}} + G_s\big) \cup I^{(s)}_{\alpha_1,\ldots,\alpha_{s-1},\alpha_s}$$

is composed of elements which are of the form $(\alpha_1, \ldots, \alpha_{k-1}, y_k, \ldots, y_s)$, where $(y_k, \ldots, y_s) \in \mathbb{Z}/n_k\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$ describes an initial segment of $\mathbb{Z}/n_k\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$. More precisely, we have the following lemma.

Lemma 1. *Let $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$ and k be an integer, $2 \leqslant k \leqslant s$. For any subset J of $G_k \subset G$ and any $\alpha_1 \in \mathbb{Z}/n_1\mathbb{Z}, \ldots, \alpha_{k-1} \in \mathbb{Z}/n_{k-1}\mathbb{Z}$, the following assertions are equivalent:*

(i) *J is an initial segment included in G_k,*

(ii) *the set*

$$\big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big(I^{(2)}_{\alpha_1,\alpha_2} + G_3\big) \cup \ldots \cup \big(I^{(k-1)}_{\alpha_1,\ldots,\alpha_{k-1}} + G_k\big) \cup (\alpha_1, \ldots, \alpha_{k-1}, 0, \ldots, 0) + J$$

is an initial segment of G.

Proof. An initial segment J included in G_k is of the form

$$\begin{aligned} J = &\big(\{(0,\dots,0,i,0,\dots,0) \text{ for } 0 \leqslant i \leqslant \alpha_k - 1\} + G_{k+1}\big) \\ &\cup \big(\{(0,\dots,0,\alpha_k,i,0,\dots,0) \text{ for } 0 \leqslant i \leqslant \alpha_{k+1} - 1\} + G_{k+2}\big) \\ &\cup \dots \cup \big(\{(0,\dots,0,\alpha_k,\alpha_{k+1},\dots,\alpha_{s-1},i) \text{ for } 0 \leqslant i \leqslant \alpha_s - 1\}\big), \end{aligned}$$

where the non-zero coordinates start at the k-th place. It follows that

$$\begin{aligned} &(\alpha_1,\dots,\alpha_{k-1},0,\dots,0) + J \\ &= \big(\{(\alpha_1,\dots,\alpha_{k-1},i,0,\dots,0) \text{ for } 0 \leqslant i \leqslant \alpha_k - 1\} + G_{k+1}\big) \\ &\quad \cup \big(\{(\alpha_1,\dots,\alpha_{k-1},\alpha_k,i,0,\dots,0) \text{ for } 0 \leqslant i \leqslant \alpha_{k+1} - 1\} + G_{k+2}\big) \\ &\quad \cup \dots \cup \big(\{(\alpha_1,\dots,\alpha_{k-1},\alpha_k,\alpha_{k+1},\dots,\alpha_{s-1},i) \text{ for } 0 \leqslant i \leqslant \alpha_s - 1\}\big) \\ &= \big(I^{(k)}_{\alpha_1,\dots,\alpha_k} + G_{k+1}\big) \cup \big(I^{(k+1)}_{\alpha_1,\dots,\alpha_{k+1}} + G_{k+2}\big) \cup \dots \cup I^{(s)}_{\alpha_1,\dots,\alpha_{s-1},\alpha_s}, \end{aligned}$$

which implies that

$$\big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big(I^{(2)}_{\alpha_1,\alpha_2} + G_3\big) \cup \dots \cup \big(I^{(k-1)}_{\alpha_1,\dots,\alpha_{k-1}} + G_k\big) \cup (\alpha_1,\dots,\alpha_{k-1},0,\dots,0) + J$$

is an initial segment of G. So (i) implies (ii).

The proof of the converse statement is of the same kind. Let $K \subset G$ be the following set

$$K = \big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big(I^{(2)}_{\alpha_1,\alpha_2} + G_3\big) \cup \dots \cup \big(I^{(k-1)}_{\alpha_1,\dots,\alpha_{k-1}} + G_k\big) \cup (\alpha_1,\dots,\alpha_{k-1},0,\dots,0) + J.$$

Since $J \subset G_k$, this union is a disjoint union (this can be seen in an analogous way as what was done for showing that (4) is a disjoint union). If K is an initial segment, it is also of the form

$$K = \big(I^{(1)}_{\beta_1} + G_2\big) \cup \big(I^{(2)}_{\beta_1,\beta_2} + G_3\big) \cup \dots \cup \big(I^{(s-1)}_{\beta_1,\dots,\beta_{s-1}} + G_s\big) \cup I^{(s)}_{\beta_1,\dots,\beta_{s-1},\beta_s},$$

for some integers $\beta_1,\dots,\beta_s$. We readily see that these two ways of writing K as a disjoint union imply that $\beta_1 = \alpha_1,\dots,\beta_{k-1} = \alpha_{k-1}$. This follows from the fact that α_1 and β_1 are both the greatest first coordinate of any element in K, α_2 and β_2 are both the greatest second coordinate of any element in K having $\alpha_1 = \beta_1$ as its first coordinate, and so on...

It follows, after simplification, that

$$(\alpha_1,\dots,\alpha_{k-1},0,\dots,0) + J = \big(I^{(k)}_{\alpha_1,\dots,\alpha_k} + G_{k+1}\big) \cup \dots \cup \big(I^{(s-1)}_{\alpha_1,\dots,\alpha_{s-1}} + G_s\big) \cup I^{(s)}_{\alpha_1,\dots,\alpha_{s-1},\alpha_s}.$$

Translating everything by $-(\alpha_1,\dots,\alpha_{k-1},0,\dots,0)$ gives

$$J = \big(I^{(k)}_{0,\dots,0} + G_{k+1}\big) \cup \dots \cup \big(I^{(s-1)}_{0,\dots,0,\alpha_k,\dots,\alpha_{s-1}} + G_s\big) \cup I^{(s)}_{0,\dots,0,\alpha_k,\dots,\alpha_{s-1},\alpha_s},$$

an initial segment contained in G_k. ∎

We now define the function

$$\phi_G : \begin{cases} \{0,\dots,n-1\} \to \mathcal{P}(G) \\ \qquad m \qquad\quad \to \mathfrak{I}_m, \end{cases}$$

where $\mathcal{P}(G)$ denotes the set of all subsets of G, and prove the following lemma.

Lemma 2. *Let G be a finite product of finite cyclic groups, then ϕ_G is an increasing function and $|\phi_G(m)| = m$.*

Proof. Consider $l < m$, then as noted above

$$(\alpha_1(l), \alpha_2(l), \dots, \alpha_{s-1}(l), \alpha_s(l)) \prec (\alpha_1(m), \alpha_2(m), \dots, \alpha_{s-1}(m), \alpha_s(m)).$$

The increasingness of ϕ_G then follows from the very definitions of $\mathfrak{I}_l$ and $\mathfrak{I}_m$.

Using for instance the description (4) above and keeping our notation, we immediately notice that

$$|\mathfrak{I}_m| = \alpha_1|G_2| + \cdots + \alpha_{s-1}|G_s| + \alpha_s = \alpha_1 n_2 \cdots n_s + \cdots + \alpha_{s-1} n_s + \alpha_s = m. \quad \blacksquare$$

Here is now our main lemma in the direction of Theorem 4.

Lemma 3. *Let G be a finite product of finite cyclic groups. Let u and v be two positive integers $< |G|$, then $\phi_G(u) + \phi_G(v)$ is either equal to $\phi_G(t)$ for some integer $t \leqslant u + v - 2$ or equal to $\phi_G(u + v - 1)$, in which case, the extremity of $\phi_G(u + v - 1)$ has a unique representation as an element of the sumset $\phi_G(u) + \phi_G(v)$, namely as the sum of the extremities of $\phi_G(u)$ and $\phi_G(v)$, respectively.*

Proof. The proof is by induction on the number of factors s appearing in the decomposition

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}.$$

We may still assume that $n_1, \dots, n_s \geqslant 2$.

If $s = 1$, then the result is immediate since

$$\begin{aligned} \phi_G(u) + \phi_G(v) &= \{0, \dots, u-1\} + \{0, \dots, v-1\} \\ &= \begin{cases} \{0, \dots, u+v-2\} = \phi_G(u+v-1) & \text{if } u + v \leqslant n_1 + 1, \\ \{0, \dots, n_1 - 1\} = \phi_G(n_1) & \text{if } u + v \geqslant n_1 + 2. \end{cases} \end{aligned}$$

We note that in the first case the extremity of $\phi_G(u) + \phi_G(v)$, namely $u + v - 2$, has the unique representation $(u-1)+(v-1)$, that is, as the sum of the respective extremities of $\phi_G(u)$ and $\phi_G(v)$.

Assume now the result to be true for some integer $s-1$ and consider the case of a group G which is a product of s cyclic groups. We compute $\phi_G(u) + \phi_G(v)$ using the description (4), the remarks thereafter and Lemma 1 (in the case $k = 2$). We therefore write

$$\mathfrak{I}_u = \left(I_{\alpha_1}^{(1)} + G_2\right) \cup \left((\alpha_1, 0, \dots, 0) + \mathfrak{I}'_u\right)$$

and analogously

$$\mathfrak{I}_v = \left(I_{\beta_1}^{(1)} + G_2\right) \cup \left((\beta_1, 0, \dots, 0) + \mathfrak{I}'_v\right),$$

where $\mathfrak{I}'_u$ and $\mathfrak{I}'_v$ are initial segments of G included in G_2.

We consider several cases.

Case 1. If $\alpha_1 = \beta_1 = 0$, then $\mathcal{I}_u = \mathcal{I}'_u$ and $\mathcal{I}_v = \mathcal{I}'_v$ and everything happens in the subgroup G_2 of G, which is a product of $s-1$ finite cyclic groups. Therefore the result follows from the induction hypothesis.

Case 2. If $\alpha_1 \neq 0$, $\beta_1 = 0$. We must have $\mathcal{I}'_v \neq \emptyset$. We compute

$$\begin{aligned}\mathcal{I}_u + \mathcal{I}_v &= \Big(\big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big((\alpha_1, 0, \ldots, 0) + \mathcal{I}'_u\big)\Big) + \mathcal{I}'_v \\ &= \big(I^{(1)}_{\alpha_1} + G_2 + \mathcal{I}'_v\big) \cup \big((\alpha_1, 0, \ldots, 0) + \mathcal{I}'_u + \mathcal{I}'_v\big) \\ &= \big(I^{(1)}_{\alpha_1} + G_2\big) \cup \Big((\alpha_1, 0, \ldots, 0) + \big(\mathcal{I}'_u + \mathcal{I}'_v\big)\Big)\end{aligned}$$

since $\mathcal{I}'_v \subset G_2$ implies $G_2 + \mathcal{I}'_v = G_2$.

By the induction hypothesis, since G_2 is isomorphic to a product of $s-1$ finite cyclic groups and $\mathcal{I}'_u, \mathcal{I}'_v$ are initial segments contained in it, the sumset $\mathcal{I}'_u + \mathcal{I}'_v$ is an initial segment in G_2 satisfying $|\mathcal{I}'_u + \mathcal{I}'_v| \leqslant |\mathcal{I}'_u| + |\mathcal{I}'_v| - 1$. Therefore, by Lemma 1,

$$\mathcal{I}_u + \mathcal{I}_v = \big(I^{(1)}_{\alpha_1} + G_2\big) \cup \Big((\alpha_1, 0, \ldots, 0) + \big(\mathcal{I}'_u + \mathcal{I}'_v\big)\Big)$$

is an initial segment of G.

As regards the cardinality, we have

$$|\mathcal{I}_u + \mathcal{I}_v| = \alpha_1|G_2| + |\mathcal{I}'_u + \mathcal{I}'_v| \leqslant \alpha_1|G_2| + |\mathcal{I}'_u| + |\mathcal{I}'_v| - 1,$$

by the induction hypothesis. Since $\alpha_1|G_2| + |\mathcal{I}'_u| = |\mathcal{I}_u|$ and $|\mathcal{I}'_v| = |\mathcal{I}_v|$, we have $|\mathcal{I}_u + \mathcal{I}_v| \leqslant |\mathcal{I}_u| + |\mathcal{I}_v| - 1$.

If this is an equality, we must have $|\mathcal{I}'_u + \mathcal{I}'_v| = |\mathcal{I}'_u| + |\mathcal{I}'_v| - 1$. But then, the induction hypothesis implies that the extremity of $\mathcal{I}'_u + \mathcal{I}'_v$ has a single representation (which is the sum of the extremities of $\mathcal{I}'_u$ and $\mathcal{I}'_v$, respectively). It can then be immediately deduced that the extremity of $\mathcal{I}_u + \mathcal{I}_v$, which coincides with $(\alpha_1, 0, \ldots, 0)$ plus the extremity of $\mathcal{I}'_u + \mathcal{I}'_v$ can be uniquely written as the sum of the extremity of $\mathcal{I}_u$ (which is $(\alpha_1, 0, \ldots, 0)$ plus the extremity of $\mathcal{I}'_u$) and the extremity of $\mathcal{I}_v$.

Case 3. The case $\alpha_1 = 0$, $\beta_1 \neq 0$ can be treated symetrically in exactly the same way.

From now on, we therefore assume that neither α_1 nor β_1 is equal to zero.

Case 4. If $\mathcal{I}'_u = \mathcal{I}'_v = \emptyset$, then we have $|\mathcal{I}_u| = \alpha_1|G_2|$ and $|\mathcal{I}_v| = \beta_1|G_2|$ (in this case $\alpha_1, \beta_1 > 0$). We compute

$$\begin{aligned}\mathcal{I}_u + \mathcal{I}_v &= \big(I^{(1)}_{\alpha_1} + G_2\big) + \big(I^{(1)}_{\beta_1} + G_2\big) \\ &= \big(I^{(1)}_{\alpha_1} + I^{(1)}_{\beta_1} + G_2\big) \\ &= \begin{cases} \big(I^{(1)}_{\alpha_1+\beta_1-1} + G_2\big) & \text{if } \alpha_1 + \beta_1 \leqslant n_1 + 1, \\ G & \text{otherwise.} \end{cases}\end{aligned}$$

In both cases, $\mathcal{I}_u + \mathcal{I}_v$ is therefore an initial segment of cardinality

$$|\mathcal{I}_u + \mathcal{I}_v| \leqslant (\alpha_1 + \beta_1 - 1)|G_2| = |\mathcal{I}_u| + |\mathcal{I}_v| - |G_2| \leqslant |\mathcal{I}_u| + |\mathcal{I}_v| - 2,$$

which proves the result in this case.

Case 5. If $\mathcal{I}'_v = \emptyset$ and $\mathcal{I}'_u \neq \emptyset$, we compute (using $\mathcal{I}'_u \subset G_2$)

$$\begin{aligned}
\mathcal{I}_u + \mathcal{I}_v &= \Big(\big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big((\alpha_1, 0, \dots, 0) + \mathcal{I}'_u\big)\Big) + \big(I^{(1)}_{\beta_1} + G_2\big) \\
&= \big(I^{(1)}_{\alpha_1} + I^{(1)}_{\beta_1} + G_2\big) \cup \Big((\alpha_1, 0, \dots, 0) + \big(I^{(1)}_{\beta_1} + G_2\big)\Big) \\
&= \begin{cases} \big(I^{(1)}_{\alpha_1+\beta_1} + G_2\big) & \text{if } \alpha_1 + \beta_1 \leqslant n_1, \\ G & \text{otherwise.} \end{cases}
\end{aligned}$$

In both cases, $\mathcal{I}_u + \mathcal{I}_v$ is therefore an initial segment of cardinality

$$|\mathcal{I}_u + \mathcal{I}_v| \leqslant (\alpha_1 + \beta_1)|G_2| = (|\mathcal{I}_u| - |\mathcal{I}'_u|) + |\mathcal{I}_v| \leqslant |\mathcal{I}_u| + |\mathcal{I}_v| - 1.$$

If equality holds here, then we must have both $|\mathcal{I}'_u| = 1$ and $\alpha_1 + \beta_1 \leqslant n_1$. It follows that the extremity of $\mathcal{I}_u + \mathcal{I}_v$ which coincides exactly with $(\alpha_1, 0, \dots, 0)$ plus the extremity of $\mathcal{I}'_u + \big(I^{(1)}_{\beta_1} + G_2\big)$ has a single representation (since $\mathcal{I}'_u$ has one element). It can be checked easily that this unique representation has the right form of the sum of the two extremities of $\mathcal{I}_u$ and $\mathcal{I}_v$, respectively.

Case 6. The case $\mathcal{I}'_v \neq \emptyset$ and $\mathcal{I}'_u = \emptyset$ is treated in a similar way as Case 5.

Case 7. Assume finally that we are in the generic case, $\alpha_1, \beta_1 \neq 0$, $\mathcal{I}'_u, \mathcal{I}'_v \neq \emptyset$. In this case

$$\begin{aligned}
&\mathcal{I}_u + \mathcal{I}_v \\
&= \Big(\big(I^{(1)}_{\alpha_1} + G_2\big) \cup \big((\alpha_1, 0, \dots, 0) + \mathcal{I}'_u\big)\Big) + \Big(\big(I^{(1)}_{\beta_1} + G_2\big) \cup \big((\beta_1, 0, \dots, 0) + \mathcal{I}'_v\big)\Big) \\
&= \big(I^{(1)}_{\alpha_1} + I^{(1)}_{\beta_1} + G_2\big) \cup \Big(I^{(1)}_{\beta_1} + G_2 + \big((\alpha_1, 0, \dots, 0) + \mathcal{I}'_u\big)\Big) \\
&\qquad \cup \Big(I^{(1)}_{\alpha_1} + G_2 + \big((\beta_1, 0, \dots, 0) + \mathcal{I}'_v\big)\Big) \cup \big((\alpha_1 + \beta_1, 0, \dots, 0) + \mathcal{I}'_u + \mathcal{I}'_v\big) \\
&= \big(I^{(1)}_{\alpha_1} + I^{(1)}_{\beta_1} + G_2\big) \cup \big(I^{(1)}_{\beta_1} + G_2 + (\alpha_1, 0, \dots, 0)\big) \\
&\qquad \cup \big(I^{(1)}_{\alpha_1} + G_2 + (\beta_1, 0, \dots, 0)\big) \cup \big((\alpha_1 + \beta_1, 0, \dots, 0) + \mathcal{I}'_u + \mathcal{I}'_v\big) \\
&= \big(I^{(1)}_{\alpha_1} + I^{(1)}_{\beta_1} + G_2\big) \cup \big((\alpha_1 + \beta_1 - 1, 0, \dots, 0) + G_2\big) \\
&\qquad \cup \big((\alpha_1 + \beta_1, 0, \dots, 0) + \mathcal{I}'_u + \mathcal{I}'_v\big) \\
&= \begin{cases} \big(I^{(1)}_{\alpha_1+\beta_1} + G_2\big) \cup \big((\alpha_1 + \beta_1, 0, \dots, 0) + \mathcal{I}'_u + \mathcal{I}'_v\big) & \text{if } \alpha_1 + \beta_1 \leqslant n_1 - 1, \\ G & \text{otherwise.} \end{cases}
\end{aligned}$$

So, in both cases, $\mathcal{I}_u + \mathcal{I}_v$ is always an initial segment.

If $\alpha_1 + \beta_1 \geqslant n_1$, we obtain

$$|\mathcal{I}_u + \mathcal{I}_v| = |G| \leqslant (\alpha_1 + \beta_1)|G_2| = |\mathcal{I}_u| + |\mathcal{I}_v| - |\mathcal{I}'_u| - |\mathcal{I}'_v| \leqslant |\mathcal{I}_u| + |\mathcal{I}_v| - 2$$

and the result follows.

If $\alpha_1 + \beta_1 \leqslant n_1 - 1$, we obtain

$$|\mathcal{I}_u + \mathcal{I}_v| \leqslant (\alpha_1 + \beta_1)|G_2| + |\mathcal{I}'_u + \mathcal{I}'_v| \leqslant (\alpha_1 + \beta_1)|G_2| + |\mathcal{I}'_u| + |\mathcal{I}'_v| - 1 = |\mathcal{I}_u| + |\mathcal{I}_v| - 1$$

where we have used the induction hypothesis in order to bound from above the quantity $|\mathcal{I}'_u + \mathcal{I}'_v|$. The case of equality follows analogously to what has been done for Cases 2 or 5, because the extremity of $\mathcal{I}_u + \mathcal{I}_v$ coincides with $(\alpha_1 + \beta_1, 0, \ldots, 0)$ plus the extremity of $\mathcal{I}'_u + \mathcal{I}'_v$ which must have a single representation. Again, it follows that the unique representation of the extremity of $\mathcal{I}_u + \mathcal{I}_v$ has the right form of the sum of the two extremities of $\mathcal{I}_u$ and $\mathcal{I}_v$, respectively. ■

We can now pass to an arbitrary number of variables.

Lemma 4. *Let G be a finite product of finite cyclic groups. Let k be an integer, $k \geqslant 2$, and $u_1, u_2, \ldots, u_k$ be k positive integers $< |G|$, then $\phi_G(u_1) + \phi_G(u_2) + \cdots + \phi_G(u_k)$ is either equal to $\phi_G(t)$ for some integer $t \leqslant u_1 + \cdots + u_k - k$ or equal to $\phi_G(u_1 + \cdots + u_k - k + 1)$, in which case, the extremity of this sumset has a single representation, namely as the sum of the extremities of $\phi_G(u_1), \phi_G(u_2), \ldots,$ and $\phi_G(u_k)$, respectively.*

Proof. The proof is by induction on k.

If $k = 2$ then the result follows from the preceding Lemma 3.

Assume the result to be true for some integer $k - 1 \geqslant 2$ and consider k positive integers $u_1, u_2, \ldots, u_k < |G|$. We study the sumset $\phi_G(u_1) + \phi_G(u_2) + \cdots + \phi_G(u_k)$. By the induction hypothesis

$$\phi_G(u_1) + \phi_G(u_2) + \cdots + \phi_G(u_{k-1}) = \phi_G(t')$$

for some $t' \leqslant u_1 + \cdots + u_{k-1} - (k-1) + 1 = u_1 + \cdots + u_{k-1} - k + 2$.

Using this and Lemma 3, we conclude that

$$\phi_G(u_1) + \phi_G(u_2) + \cdots + \phi_G(u_k) = \phi_G(t') + \phi_G(u_k) = \phi_G(t) \tag{5}$$

where $t \leqslant t' + u_k - 1$. It follows

$$t \leqslant t' + u_k - 1 \leqslant u_1 + \cdots + u_{k-1} - k + 2 + u_k - 1 = u_1 + \cdots + u_{k-1} + u_k - k + 1. \tag{6}$$

It remains to examine the case of equality. It $t = u_1 + \cdots + u_{k-1} + u_k - k + 1$, then we must have equalities everywhere in (6). Each of these equalities implies unicity of the representation (in the right form) of its extremity in the corresponding sumset. This implies the same result for the sumset $\phi_G(u_1) + \phi_G(u_2) +$

$\cdots + \phi_G(u_k)$. More precisely, first, the first equality in (6) shows that the extremity of $\phi_G(u_1 + \cdots + u_k - k + 1)$ can be written uniquely as the sum of the extremity of $\phi_G(u_1 + \cdots + u_{k-1} - k + 2)$ and of $\phi_G(u_k)$, respectively. Now, in view of the second equality in (6) and the induction hypothesis, the extremity of $\phi_G(u_1 + \cdots + u_{k-1} - k + 2)$ can be uniquely written as the sum of the extremities of $\phi_G(u_1), \ldots, \phi_G(u_{k-1})$. And the conclusion follows. ■

We can now complete the proof of Theorem 4 in a way reminiscent to [12, 13].

Proof of Theorem 4.

Step 1. The group $\mathbb{Z}$ has the generalized increasingly small sumsets property.

Indeed, for any positive integer k, any $1 \leqslant r_1, \ldots, r_k \leqslant |G|$, any $1 \leqslant r'_1, \ldots, r'_k \leqslant |G|$ such that $r_i \leqslant r'_i$ (for all $1 \leqslant i \leqslant k$), we define $\mathcal{A}_i = \{0, \ldots, r_i - 1\}$ and $\mathcal{A}'_i = \{0, \ldots, r'_i - 1\}$ (for $1 \leqslant i \leqslant k$). We have $\mathcal{A}_i \subset \mathcal{A}'_i$ for each index i. We compute that $\mathcal{A}_1 + \cdots + \mathcal{A}_k = \{0, \ldots, r_1 + \cdots + r_k - k\}$ has cardinality $r_1 + \cdots + r_k - k + 1$ and that $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k = \{0, \ldots, r'_1 + \cdots + r'_k - k\}$ has cardinality $r'_1 + \cdots + r'_k - k + 1$. Moreover, it is immediately seen that the element $r_1 + \cdots + r_k - k$ has a unique representation as an element of the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ (namely $(r_1 - 1) + \cdots + (r_k - 1)$), and that the element $r_1 + \cdots + r_k - k$ has a unique representation as an element of the sumset $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k$.

Step 2. Every finite Abelian group has the generalized increasingly small sumsets property.

Let G be a finite Abelian group. The structure of such a group is well known (see for instance Chapter I.5 of [14]). We may therefore assume that

$$G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$$

for some integers $n_1, \ldots, n_s \geqslant 2$.

Let k be any positive integer and $1 \leqslant r_1, \ldots, r_k \leqslant |G|$, $1 \leqslant r'_1, \ldots, r'_k \leqslant |G|$ such that $r_i \leqslant r'_i$ (for all $1 \leqslant i \leqslant k$).

We define $\mathcal{A}_i = \phi_G(r_i), \mathcal{A}'_i = \phi_G(r'_i)$ for all $1 \leqslant i \leqslant k$. By Lemma 2, since ϕ_G is increasing and $r_i \leqslant r'_i$, we have $\mathcal{A}_i \subset \mathcal{A}'_i$. By Lemma 4, $\mathcal{A}_1 + \cdots + \mathcal{A}_k = \phi_G(t)$ and $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k = \phi_G(t')$ with $t \leqslant r_1 + \cdots + r_k - k + 1$ and $t' \leqslant r'_1 + \cdots + r'_k - k + 1$.

This implies, by Lemma 2 again,

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = |\phi_G(t)| = t \leqslant r_1 + \cdots + r_k - k + 1.$$

If equality holds, this yields $t = r_1 + \cdots + r_k - k + 1$, in which case, Lemma 4 implies that there is an element (namely the extremity of the sumset) in $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ which has a single representation.

Since an analogous fact can be shown on the sumset $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k$, we have proved that G has the generalized increasingly small sumsets property.

Step 3. Any Abelian group has the generalized increasingly small sumsets property.

If this group, say G, is finite, the result follows from Step 2. Otherwise, for any positive integer k and integers $r_1, \dots, r_k, r'_1, \dots, r'_k \geqslant 1$ with $r'_i \geqslant r_i$ for each index $1 \leqslant i \leqslant k$, we choose $\max(r'_1, \dots, r'_k)$ arbitrary elements in G. Let H be the subgroup of G generated by these elements. The group H is by definition finitely generated. But, by the general structure theorem on finitely generated Abelian groups (see for instance Chapter I.5 of [14] again), either H is finite in which case the result follows by Step 2, or H contains a subgroup isomorphic to $\mathbb{Z}$ in which case the result follows by the result of Step 1 (and the fact that it is enough to prove the result in an infinite subgroup, see Lemma 1 of [12] for an analogous remark).

The proof is complete. ∎

4. Proof of Theorem 5

In this proof, we write simply $\delta = \delta_G^{(2)}(r,s)$. Recall that

$$\mu_G^{(2)}(r,s) = \left(\left\lceil \frac{r}{\delta} \right\rceil + \left\lceil \frac{s}{\delta} \right\rceil - 1 \right) \delta.$$

Let H be a subgroup of cardinality δ. We define, for $i = 1, 2$,

$$\rho_i = \left\lceil \frac{r_i}{|H|} \right\rceil = \left\lceil \frac{r_i}{\delta} \right\rceil.$$

The notation π will stand again for the canonical homomorphism $G \to G/H$.

We apply the increasingly small sumsets property (Theorem 4) in (the Abelian group) G/H with $r_1 = \rho_1, r_2 = \rho_2$ and $r'_1 = \rho_1 + 1, r'_2 = \rho_2$. This gives us sets $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}'_1, \mathcal{B}'_2 \subset G/H$ of respective cardinalities ρ_1, ρ_2 and $\rho_1 + 1, \rho_2$ such that $\mathcal{B}_1 \subset \mathcal{B}'_1$, $\mathcal{B}_2 = \mathcal{B}'_2$ satisfying in particular

$$|\mathcal{B}_1 + \mathcal{B}_2| \leqslant \rho_1 + \rho_2 - 1$$

and

$$|\mathcal{B}'_1 + \mathcal{B}'_2| \leqslant \rho_1 + \rho_2.$$

Now, using π^{-1} in the way introduced in [11], we can obtain sets $\mathcal{A}_1, \mathcal{A}_2$, $\mathcal{A}'_1, \mathcal{A}'_2 \subset G$ with respective cardinalities $r, s, r + \delta, s$ such that

$$\mathcal{A}_i \subset \pi^{-1}(\mathcal{B}_i), \quad \mathcal{A}'_i \subset \pi^{-1}(\mathcal{B}'_i) \qquad (\text{for } i = 1, 2)$$

such that $\mathcal{A}_1 \subset \mathcal{A}'_1$ and $\mathcal{A}_2 \subset \mathcal{A}'_2$ (so $\mathcal{A}'_2 = \mathcal{A}_2$).

It follows that

$$|\mathcal{A}_1 + \mathcal{A}_2| \leqslant |\mathcal{B}_1 + \mathcal{B}_2| \times |H| \leqslant (\rho_1 + \rho_2 - 1)\delta = \mu_G^{(2)}(r,s)$$

and

$$|\mathcal{A}_1' + \mathcal{A}_2'| \leqslant |\mathcal{B}_1' + \mathcal{B}_2'| \times |H| \leqslant (\rho_1 + \rho_2)\delta.$$

Since by definition $|\mathcal{A}_1 + \mathcal{A}_2| \geqslant \mu_G^{(2)}(r,s)$, we deduce from the first inequality that

$$|\mathcal{A}_1 + \mathcal{A}_2| = \mu_G^{(2)}(r,s). \tag{7}$$

We also have, by the second one,

$$|\mathcal{A}_1' + \mathcal{A}_2'| \leqslant (\rho_1 + \rho_2)\delta = \mu_G^{(2)}(r,s) + \delta, \tag{8}$$

while, on the other hand, we notice that

$$|\mathcal{A}_1' + \mathcal{A}_2'| \geqslant \mu_G^{(2)}(r+\delta, s). \tag{9}$$

But since (using for instance (2))

$$\mu_G^{(2)}(r+\delta,s) = \min_{d\in\mathcal{D}} \left(\left\lceil \frac{r+\delta}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d$$

we have

$$\mu_G^{(2)}(r+\delta,s) > \mu_G^{(2)}(r,s). \tag{10}$$

Indeed, if $d \in \mathcal{D}$ is such that $d \leqslant \delta$ then

$$\begin{aligned} \left(\left\lceil \frac{r+\delta}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d &\geqslant \left(\left\lceil \frac{r}{d} \right\rceil + 1 + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \\ &> \left(\left\lceil \frac{r}{\delta} \right\rceil + \left\lceil \frac{s}{\delta} \right\rceil - 1 \right) \delta; \end{aligned}$$

while if it satisfies $d \geqslant \delta$ then

$$\begin{aligned} \left(\left\lceil \frac{r+\delta}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d &\geqslant \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d \\ &> \left(\left\lceil \frac{r}{\delta} \right\rceil + \left\lceil \frac{s}{\delta} \right\rceil - 1 \right) \delta \end{aligned}$$

in view of the maximality condition in the very definition of $\delta = \delta_G^{(2)}(r,s)$.

It follows from (7), (10), (9) and (8) that

$$|\mathcal{A}_1 + \mathcal{A}_2| = \mu_G^{(2)}(r,s) < |\mathcal{A}_1' + \mathcal{A}_2'| \leqslant \mu_G^{(2)}(r,s) + \delta.$$

Let $\mathcal{A}_1' \setminus \mathcal{A}_1 = \{a_1, \dots, a_\delta\}$. For $i = 1, \dots, \delta$, we define $\mathcal{A}_1^{(i)} = \mathcal{A}_1 \cup \{a_1, \dots, a_i\}$ and put $\mathcal{A}_1^{(0)} = \mathcal{A}_1$. We have $|\mathcal{A}_1^{(0)} + \mathcal{A}_2| = |\mathcal{A}_1 + \mathcal{A}_2|$, $|\mathcal{A}_1^{(i)} + \mathcal{A}_2| \geqslant |\mathcal{A}_1^{(i-1)} + \mathcal{A}_2|$ for all integers $1 \leqslant i \leqslant \delta$ and $|\mathcal{A}_1^{(\delta)} + \mathcal{A}_2| = |\mathcal{A}_1' + \mathcal{A}_2| > |\mathcal{A}_1 + \mathcal{A}_2|$. In particular there is a value of i_0 $(1 \leqslant i_0 \leqslant \delta)$ such that $|\mathcal{A}_1^{(i_0)} + \mathcal{A}_2| > |\mathcal{A}_1^{(i_0-1)} + \mathcal{A}_2|$.

This means that there is an element s in $\mathcal{A}_1^{(i_0)}+\mathcal{A}_2$ which is not in $\mathcal{A}_1^{(i_0-1)}+\mathcal{A}_2$. This imposes that the element s is of the form $a_{i_0}+b$ where $b\in\mathcal{A}_2$. This relation shows immediately that s has a unique representation as an element of $\mathcal{A}_1^{(i_0)}+\mathcal{A}_2$ since b is then uniquely defined ($b=s-a_{i_0}$).

To sum up, we have found a set $\mathcal{A}_1^{(i_0)}$ of cardinality $r+i_0$, containing $\mathcal{A}_1$ such that $\mathcal{A}_1^{(i_0)}+\mathcal{A}_2$ possesses an element having a single representation. Select now a subset $\mathcal{A}_1''$ of $\mathcal{A}_1^{(i_0)}$, with cardinality r and containing a_{i_0}. The element s still belongs to $\mathcal{A}_1''+\mathcal{A}_2$ and still has a single representation as an element of this sumset. We then conclude

$$\nu_G^{(2)}(r,s)=\nu_G^{(2)}(|\mathcal{A}_1''|,|\mathcal{A}_2'|)\leqslant|\mathcal{A}_1''+\mathcal{A}_2'|\leqslant|\mathcal{A}_1'+\mathcal{A}_2'|\leqslant\mu_G^{(2)}(r,s)+\delta,$$

as promised by the statement of Theorem 5.

5. Proof of Theorem 6

That $\delta^{(2)}_{(\mathbb{Z}/p\mathbb{Z})^2}(p,p)=p$ can be seen immediately while the assertion that $\mu^{(2)}_{(\mathbb{Z}/p\mathbb{Z})^2}(p,p)=p$ follows in a straightforward way from the formula already used several times (see (2) again for instance).

It remains to prove

$$\nu^{(2)}_{(\mathbb{Z}/p\mathbb{Z})^2}(p,p)=2p.$$

If we consider the two subsets of $(\mathbb{Z}/p\mathbb{Z})^2$ having each p elements

$$\mathcal{A}=\{0\}\times\mathbb{Z}/p\mathbb{Z}\quad\text{ and }\quad\mathcal{B}=\{0\}\times(\mathbb{Z}/p\mathbb{Z}\setminus\{0\})\cup\{(1,0)\},$$

we check that $\mathcal{A}+\mathcal{B}=\{0,1\}\times\mathbb{Z}/p\mathbb{Z}$ and that for instance the element $(1,0)$ has a single representation in $\mathcal{A}+\mathcal{B}$ (given by $(1,0)=(0,0)+(1,0)$). It follows $\nu^{(2)}_{(\mathbb{Z}/p\mathbb{Z})^2}(p,p)\leqslant 2p$.

We now come to prove the lower bound $\nu^{(2)}_{(\mathbb{Z}/p\mathbb{Z})^2}(p,p)\geqslant 2p$ which is the main part of the proof of Theorem 6.

We assume that $\mathcal{A}$ and $\mathcal{B}$ are two subsets of $(\mathbb{Z}/p\mathbb{Z})^2$ that have p elements each and that their sumset possesses an element with a single representation. We show that $|\mathcal{A}+\mathcal{B}|\geqslant 2p$.

If $\mathcal{A}$ or $\mathcal{B}$, say $\mathcal{A}$ (without loss of generality), is a coset modulo a subgroup, say H, $|\mathcal{A}+\mathcal{B}|=c|H|$ where c is the number of H-cosets met by $\mathcal{B}$. If c is equal to 1, then $\mathcal{A}$ and $\mathcal{B}$ are both a single coset and clearly no element of $\mathcal{A}+\mathcal{B}$ can have a single representation. This implies $c\geqslant 2$ and $|\mathcal{A}+\mathcal{B}|\geqslant 2|H|=2p$.

From now on, we may assume that neither $\mathcal{A}$ nor $\mathcal{B}$ is a coset modulo a subgroup.

Moreover, we proceed by contradiction, assuming that $|\mathcal{A}+\mathcal{B}|\leqslant 2p-1$. We derive two proofs of this contradiction.

5.1. First proof. We see $(\mathbb{Z}/p\mathbb{Z})^2$ as a two-dimensional vector space over the field $\mathbb{Z}/p\mathbb{Z}$. Let us consider any basis (e_1, e_2) of $(\mathbb{Z}/p\mathbb{Z})^2$ and decompose $\mathcal{A}$ as a disjoint union in the following way (with respect to the second coordinate in this basis):

$$\mathcal{A} = \big(\mathcal{A}_0 \times \{0\}\big) \cup \big(\mathcal{A}_1 \times \{1\}\big) \cup \ldots \cup \big(\mathcal{A}_{p-1} \times \{p-1\}\big)$$

and $\mathcal{B}$ in the same fashion

$$\mathcal{B} = \big(\mathcal{B}_0 \times \{0\}\big) \cup \big(\mathcal{B}_1 \times \{1\}\big) \cup \ldots \cup \big(\mathcal{B}_{p-1} \times \{p-1\}\big)$$

where all these (possibly empty) sets $\mathcal{A}_i$'s and $\mathcal{B}_i$'s are in $\mathbb{Z}/p\mathbb{Z}$. In other words, this means that, for instance, $\mathcal{A}_i$ is the set of residues $j \in \mathbb{Z}/p\mathbb{Z}$ such that $je_1 + ie_2 \in \mathcal{A}$. Since $|\mathcal{A}| = |\mathcal{B}| = p$, we have

$$|\mathcal{A}_0| + |\mathcal{A}_1| + \cdots + |\mathcal{A}_{p-1}| = |\mathcal{B}_0| + |\mathcal{B}_1| + \cdots + |\mathcal{B}_{p-1}| = p. \tag{11}$$

By our previous assumption that neither $\mathcal{A}$ nor $\mathcal{B}$ is a coset, this implies that all the sets $\mathcal{A}_0, \mathcal{A}_1, \ldots, \mathcal{A}_{p-1}, \mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_{p-1}$ have a cardinality less than or equal to $p-1$.

We shall soon show that all of the $\mathcal{A}_i$'s and all of the $\mathcal{B}_i$'s are non-empty which, by (11), is equivalent to the fact that all these sets possess exactly one element.

Assuming this result to hold (the proof will be given in a few lines), we now prove our result. Indeed one obtains that, in particular, $\mathcal{A}$ is of the form

$$\mathcal{A} = \{a_i e_1 + ie_2, \quad i = 0, 1, \ldots, p-1\},$$

for some elements $a_0, \ldots, a_{p-1}$ of $\mathbb{Z}/p\mathbb{Z}$. By symmetry of the two coordinates, the a_i's must all by distinct. If we summarize: given any basis of $(\mathbb{Z}/p\mathbb{Z})^2$, the elements of $\mathcal{A}$ are (when expressed in this basis) of the form (a_i, i) (for $i = 0, 1, \ldots, p-1$) where the a_i's are distinct.

Apply this result in the canonical basis (ϵ_1, ϵ_2): the elements of $\mathcal{A}$ are of the form $(a_i, i)_{(\epsilon_1, \epsilon_2)}$ (for $i = 0, 1, \ldots, p-1$) where the a_i's are distinct. Now, for each fixed $j = 0, 1, \ldots, p-1$, the pair $(\epsilon_1, \epsilon_2 + j\epsilon_1)$ is a basis of $(\mathbb{Z}/p\mathbb{Z})^2$. The coordinates of the elements of $\mathcal{A}$ in the new basis $(\epsilon_1, \epsilon_2 + j\epsilon_1)$ are $(a_i - ji, i)$. It follows that when i describes $0, 1, \ldots, p-1$, the elements $a_i - ji$ are all distinct. So in particular for all $j \in \mathbb{Z}/p\mathbb{Z}$ one has $a_1 - j \neq a_2 - 2j$. But this is clearly false for $j = a_2 - a_1$, a contradiction from which the result follows.

It therefore only remains to prove that all of the $\mathcal{A}_i$'s and all of the $\mathcal{B}_i$'s are non-empty or, equivalently, that all of these sets have cardinality 1. Indeed, if we assume the contrary, we may put

$$\alpha = \max_{0 \leqslant i \leqslant p-1} \{|\mathcal{A}_i|, |\mathcal{B}_i|\} \geqslant 2,$$

say, without loss of generality (by translation), $\alpha = |\mathcal{A}_0| \geqslant 2$. We denote

$$a = |\{0 \leqslant i \leqslant p-1 : \mathcal{A}_i \neq \emptyset\}|$$

and

$$b = |\{0 \leqslant i \leqslant p-1 : \mathcal{B}_i \neq \emptyset\}|.$$

We shall write $\mathcal{B}_{\beta_i}$'s $(1 \leqslant i \leqslant b)$ for the non-empty of the $\mathcal{B}_i$'s. Since neither $\mathcal{A}$ nor $\mathcal{B}$ is a coset, we must have $a, b \geqslant 2$. With $|\mathcal{A}_0| \geqslant 2$ and (11), this implies in particular

$$p \geqslant 3.$$

We also immediately notice that we must have

$$\min(a,b)\alpha > p, \tag{12}$$

since for instance

$$a\alpha \geqslant \sum_{0 \leqslant i \leqslant p-1,\ \mathcal{A}_i \neq \emptyset} |\mathcal{A}_i| = \sum_{0 \leqslant i \leqslant p-1} |\mathcal{A}_i| = p,$$

using then (to get the strict inequality) the fact that $a \geqslant 2$, $\alpha \geqslant 2$ and p is a prime (the proof of the lower bound for $b\alpha$ is similar). Now, by the Cauchy-Davenport theorem [1, 2], if we define

$$\begin{aligned}\mathcal{S} = \{0 \leqslant i \leqslant p-1 :\ & \text{there exist two integers } 0 \leqslant k, l \leqslant p-1 \text{ such that} \\ & k + l \equiv i \pmod{p} \text{ and } \mathcal{A}_k + \mathcal{B}_l \neq \emptyset\},\end{aligned}$$

we have

$$s = |\mathcal{S}| \geqslant \min(p, a+b-1). \tag{13}$$

We notice that, since $a, b \geqslant 2$ and $p \geqslant 3$, we have

$$s \geqslant 3. \tag{14}$$

With this notation, the sumset $\mathcal{A}+\mathcal{B}$ must contain the disjoint union (still expressed with respect to the basis (e_1, e_2)) composed of the following s terms

$$\begin{aligned}&\big((\mathcal{A}_0 + \mathcal{B}_{\beta_1}) \times \{\beta_1\}\big) \cup \ldots \cup \big((\mathcal{A}_0 + \mathcal{B}_{\beta_b}) \times \{\beta_b\}\big) \cup \big((\mathcal{A}_{\gamma_1} + \mathcal{B}_{\delta_1}) \times \{\eta_1\}\big) \\ &\qquad \cup \ldots \cup \big((\mathcal{A}_{\gamma_{s-b}} + \mathcal{B}_{\delta_{s-b}}) \times \{\eta_{s-b}\}\big)\end{aligned}$$

for some $0 \leqslant \gamma_i, \delta_i, \eta_i \leqslant p-1$ (for $1 \leqslant i \leqslant s-b$) such that, if $1 \leqslant i \leqslant s-b$, one has $\gamma_i \neq 0$, $\eta_i \equiv \gamma_i + \delta_i \pmod{p}$ and no β_i (for $1 \leqslant i \leqslant b$) is equal to an η_i (for $1 \leqslant i \leqslant s-b$). Using again the Cauchy-Davenport theorem (for each term in this disjoint union), we obtain

$$\begin{aligned}|\mathcal{A}+\mathcal{B}| &\geqslant |\mathcal{A}_0 + \mathcal{B}_{\beta_1}| + \cdots + |\mathcal{A}_0 + \mathcal{B}_{\beta_b}| + |\mathcal{A}_{\gamma_1} + \mathcal{B}_{\delta_1}| + \cdots + |\mathcal{A}_{\gamma_{s-b}} + \mathcal{B}_{\delta_{s-b}}| \\ &\geqslant \min(p, |\mathcal{A}_0| + |\mathcal{B}_{\beta_1}| - 1) + \cdots + \min(p, |\mathcal{A}_0| + |\mathcal{B}_{\beta_b}| - 1) \\ &\quad + \min(p, |\mathcal{A}_{\gamma_1}| + |\mathcal{B}_{\delta_1}| - 1) + \cdots + \min(p, |\mathcal{A}_{\gamma_{s-b}}| + |\mathcal{B}_{\delta_{s-b}}| - 1).\end{aligned} \tag{15}$$

Assume first that none of the s terms in this sum is equal to p. We obtain

$$\begin{aligned}|\mathcal{A}+\mathcal{B}| &\geqslant (|\mathcal{A}_0|+|\mathcal{B}_{\beta_1}|-1)+\cdots+(|\mathcal{A}_0|+|\mathcal{B}_{\beta_b}|-1)+(|\mathcal{A}_{\gamma_1}|+|\mathcal{B}_{\delta_1}|-1)\\ &\quad+\cdots+(|\mathcal{A}_{\gamma_{s-b}}|+|\mathcal{B}_{\delta_{s-b}}|-1)\\ &\geqslant b(\alpha-1)+(|\mathcal{B}_{\beta_1}|+\cdots+|\mathcal{B}_{\beta_b}|)+(s-b)\\ &= b(\alpha-2)+p+s\\ &\geqslant p+s.\end{aligned}$$

From this inequality, we first conclude that $s \leqslant |\mathcal{A}+\mathcal{B}|-p \leqslant p-1$ and, by (13), this implies $s \geqslant a+b-1$. Reinjecting, we now obtain

$$2p-1 \geqslant |\mathcal{A}+\mathcal{B}| \geqslant b(\alpha-2)+p+s \geqslant b(\alpha-1)+a+p-1.$$

It follows that

$$p \geqslant b(\alpha-1)+a \geqslant \alpha\min(a,b),$$

which contradicts (12).

We may thus assume that at least one of the s terms in (15) is equal to p. In fact since $|\mathcal{A}+\mathcal{B}|$ is assumed to be at most $2p-1$, there must be exactly one such term in (15). This term must be one of the b first terms because otherwise inequality (15) would lead to the following contradiction

$$\begin{aligned}2p-1 \geqslant |\mathcal{A}+\mathcal{B}| &\geqslant (|\mathcal{A}_0|+|\mathcal{B}_{\beta_1}|-1)+\cdots+(|\mathcal{A}_0|+|\mathcal{B}_{\beta_b}|-1)+p+(s-b-1)\\ &= b(\alpha-1)+(|\mathcal{B}_{\beta_1}|+\cdots+|\mathcal{B}_{\beta_b}|)+p+(s-b-1)\\ &= b(\alpha-2)+2p+s-1\\ &\geqslant 2p+2,\end{aligned}$$

by (14).

Consequently, without loss of generality, we may assume that $|\mathcal{A}_0+\mathcal{B}_{\beta_b}| = p$. Inequality (15) then gives

$$\begin{aligned}2p-1 \geqslant |\mathcal{A}+\mathcal{B}| &\geqslant (|\mathcal{A}_0|+|\mathcal{B}_{\beta_1}|-1)+\cdots+(|\mathcal{A}_0|+|\mathcal{B}_{\beta_{b-1}}|-1)+p+(s-b)\\ &= (b-1)(\alpha-1)+(|\mathcal{B}_{\beta_1}|+\cdots+|\mathcal{B}_{\beta_{b-1}}|)+p+(s-b)\\ &= (b-1)(\alpha-1)+(p-|\mathcal{B}_{\beta_b}|)+p+(s-b)\\ &\geqslant 2p+(b-1)(\alpha-1)-\alpha+(s-b),\end{aligned}$$

in view of $|\mathcal{B}_{\beta_b}| \leqslant \alpha$. It follows that

$$2p-1 \geqslant 2p-1+(b-2)(\alpha-1)+(s-b),$$

which implies

$$(b-2)(\alpha-1)+(s-b) \leqslant 0.$$

Since both terms on the left-hand side of this inequality are non-negative and $\alpha > 1$, this yields $b = 2$, $s = b$ and thus $s = 2$, a contradiction with (14).

5.2. Second proof. The inequality $\nu^{(2)}_{(\mathbb{Z}/p\mathbb{Z})^2}(p,p) \geqslant 2p-1$ follows from Theorem 1. Therefore we assume that $|\mathcal{A}+\mathcal{B}| = 2p-1$.

We notice that $\mathcal{A}+\mathcal{B}$ cannot be periodic since p does not divide $|\mathcal{A}+\mathcal{B}|$. By Kemperman's theorem [5], since $|\mathcal{A}+\mathcal{B}| = |\mathcal{A}|+|\mathcal{B}|-1$, we infer that $\mathcal{A}+\mathcal{B}$ is either an arithmetic progression or a quasi-periodic set. The first possibility is excluded since an arithmetic progression cannot have more than p elements. It follows that there is a non-zero subgroup H in $(\mathbb{Z}/p\mathbb{Z})^2$ such that $\mathcal{A}+\mathcal{B}$ is a union of H-cosets and a subset H_0 included in yet another H-coset. We must have $|H| = p$. We infer that $\mathcal{A}+\mathcal{B}$ is included in two H-cosets. We conclude that either $\mathcal{A}$ or $\mathcal{B}$ is a coset (otherwise, $\mathcal{A}$ and $\mathcal{B}$ meet at least two H-coset which implies by the Cauchy-Davenport theorem that $\mathcal{A}+\mathcal{B}$ meets at least three H-cosets). But this is a contradiction.

References

[1] A.-L. Cauchy, Recherches sur les nombres, J. École polytech. 9 (1813), 99–123.

[2] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935), 30–32.

[3] S. Eliahou, M. Kervaire, A. Plagne, Optimally small sumsets in finite abelian groups, J. Number Theory 101 (2003), 338–348.

[4] J. H. B. Kemperman, On complexes in a semi-group, Indag. Math. 18 (1956), 247–254.

[5] J. H. B. Kemperman, On small sumsets in an abelian group, Acta Math. 103 (1960), 63–88.

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

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

[8] V. F. Lev, Restricted set addition in Abelian groups: results and conjectures, J. Théor. Nombres Bordeaux 17 (2005), 181–193.

[9] H. B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience Publishers, John Wiley, 1965.

[10] M. B. Nathanson, *Additive number theory. Inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics 165, Springer Verlag, 1996.

[11] A. Plagne, Additive number theory sheds extra light on the Hopf-Stiefel $\circ$ function, Enseign. Math. (2) 49 (2003), 109–116.

[12] A. Plagne, 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), 27–44.

[13] A. Plagne, Optimally small sumsets in groups, II. The hypersmall sumsets property and restricted addition, Uniform Distribution Theory 1 (2006), 111–124.

[14] P. Samuel, *Théorie algébrique des nombres*, Hermann, Paris, 1967.
[15] P. Scherk, Distinct elements in a set of sums (solution to a problem of Leo Moser), Amer. Math. Monthly 62 (1955), 46–47.

Address: Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, École polytechnique, 91128 Palaiseau cedex, France
E-mail: plagne@math.polytechnique.fr
Received: 14 November 2006; **revised:** 30 July 2007