Uniform Distribution Theory **1** (2006), no.1, 27–44

uniform distribution theory

OPTIMALLY SMALL SUMSETS IN GROUPS, I. THE SUPERSMALL SUMSETS PROPERTY, THE $\mu_G^{(k)}$ AND THE $\nu_G^{(k)}$ FUNCTIONS

Alain Plagne

ABSTRACT. We introduce the generalized supersmall sumsets property and prove that it holds for all solvable groups. As applications, using this tool together with a generalized version of Kneser's theorem, we establish, for G Abelian, an explicit formula for the generalized $\mu_G^{(k)}$ functions in terms of the cardinalities of the finite subgroups of G and we study the $\nu_G^{(k)}$ functions, which count the minimal cardinality of a sumset containing an element with a single representation.

Communicated by Georges Grekos

1. Introduction

Let G be a group, k be a positive integer and $r_1, \dots, r_k$ be k positive integers $\leq |G|$. Here $|G|$ denotes the cardinality of the group G if it is finite or $+\infty$ if G is infinite (in this case, a constraint like $r_1 \leq |G|$ is clearly empty). The groups we shall deal with in this paper will always (even the non-commutative ones) be written additively and their neutral element will be always denoted by 0.

The function $\mu_G^{(k)}(r_1, \dots, r_k)$ is defined as the minimal cardinality of a (Minkowski) sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k = \{a_1 + \cdots + a_k,\ a_1 \in \mathcal{A}_1, \dots, a_k \in \mathcal{A}_k\}$ with $\mathcal{A}_1, \dots, \mathcal{A}_k \subset G$ and $|\mathcal{A}_1| = r_1, \dots, |\mathcal{A}_k| = r_k$, namely

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

2000 Mathematics Subject Classification: 11B75, 20F16, 20D60, 11P99, 20Kxx.
Keywords: group, Abelian, cyclic, solvable, sumset.

The function $\mu_G = \mu_G^{(2)}$ is already classical in additive number theory (see [14] or [15] for a general introduction to this field) and the functions $\mu_G^{(k)}$ are a natural generalization of it.

It is known that if G is a finite Abelian group, then

$$\mu_G(r,s) = \mu_G^{(2)}(r,s) = \min_{d\,|\,|G|} \left(\left\lceil \frac{r}{d} \right\rceil + \left\lceil \frac{s}{d} \right\rceil - 1 \right) d. \tag{1}$$

This type of formula was introduced by the author in [16]. It is not very astonishing to those who know Kneser's theorem, a central tool for obtaining such a formula: the term $\lceil r/d \rceil + \lceil s/d \rceil - 1$ being clearly reminiscent of the condition under which Kneser's theorem ensures that a sumset $\mathcal{A}+\mathcal{B}$ is periodic. Recall first that the *period* of a subset $\mathcal{A}$ in a group G is the largest subset (and in fact, subgroup) H such that $\mathcal{A}+H=\mathcal{A}$; if $H \neq \{0\}$ then $\mathcal{A}$ is said to be *periodic*. For the sake of completeness, we restate the fundamental Kneser's theorem [12, 13] now.

Theorem 1 (Kneser's Theorem)**.** *Let $\mathcal{A}$ and $\mathcal{B}$ be two non-empty finite subsets of an Abelian group G, satisfying $|\mathcal{A}+\mathcal{B}| \leq |\mathcal{A}| + |\mathcal{B}| - 1$. If H is the period of $\mathcal{A}+\mathcal{B}$, then*

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

In particular, if $|\mathcal{A}+\mathcal{B}| \leq |\mathcal{A}| + |\mathcal{B}| - 2$, then $\mathcal{A}+\mathcal{B}$ is periodic.

In the above-quoted paper [16], formula (1) is proved to hold in the case of cyclic groups and – via Theorem 10 in [1] – finite Abelian p-groups (the case of $\mathbb{Z}/p\,\mathbb{Z}$ reduces to the Cauchy-Davenport theorem [2, 3]) with an eye to applying it to the explicit computation of the ubiquitous, and therefore important, Hopf-Stiefel $\circ$ function (see for instance [20]). By developping the techniques used in [4] and [16], formula (1) was then generalized to all finite Abelian groups in [7]. Ref. [5] contains the generalization to general Abelian groups.

A central tool, introduced by the authors of [7], in the proof of formula (1) for Abelian groups, is the so-called small sumsets property. We say that a group has the *small sumsets property* if for any $1 \leq r,s \leq |G|$, there exist $\mathcal{A},\mathcal{B} \subset G$, with $|\mathcal{A}| = r, |\mathcal{B}| = s$ and $|\mathcal{A}+\mathcal{B}| \leq r+s-1$.

In the present paper, we first generalize this definition into two directions: we allow more summands and ask for a slightly (but very useful, see the end of this section and [18, 19]) more powerful upper bound. While the small sumsets property has a "Kneser's flavour", our new definition will have a Kemperman's flavour. We do not recall here the powerful Kemperman's theorem since it is a slightly technical statement that we will not need here (the interested reader may consult Kemperman's original papers [10, 11]).

Before giving the definition of what we call the generalized supersmall sumsets property, we introduce a terminology: 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

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

We shall say that a group G has the *generalized supersmall sumsets property* if for any positive integer k, any $1 \leq r_1, \ldots, r_k \leq |G|$, there exist subsets $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset G$ containing 0, with $|\mathcal{A}_1| = r_1, \ldots, |\mathcal{A}_k| = r_k$ and either

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

In this definition (and in the following), the word *generalized* refers evidently to the number of summands.

Our first result will be the following.

Theorem 2. *Every solvable group has the generalized supersmall sumsets property.*

Since the generalized supersmall sumsets property implies trivially the small sumsets property (and even a generalized small sumsets property), a subproduct of this theorem implies immediately the result mentionned at the end of [7] (section 5, point (2.3)) that every finite solvable group has the small sumsets property (for a proof in this special case only, see Proposition 6 of [5] and [6]).

As a first application of the generalized supersmall sumsets property, we prove the following result (for which we shall also need a generalized form of Kneser's theorem, see Theorem 6) which generalizes (1).

Theorem 3. *Let k be a positive integer and G be a finite Abelian group. Then for any integers $r_1, \ldots, r_k$ satisfying $1 \leq r_1, \ldots, r_k \leq |G|$, we have*

$$\mu_G^{(k)}(r_1, \ldots, r_k) = \min_{d \,|\, |G|} \left(\left\lceil \frac{r_1}{d} \right\rceil + \cdots + \left\lceil \frac{r_k}{d} \right\rceil - k + 1 \right) d.$$

Having this result at hand, it is almost immediate to generalize it to the case of general Abelian groups.

Theorem 4. *Let k be a positive integer and G be an arbitrary Abelian group. Then for any integers $r_1, \ldots, r_k$ satisfying $1 \leq r_1, \ldots, r_k \leq |G|$, we have*

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

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

We give two proofs of Theorem 4. In the first one, we use the same approach as in [5] (where a proof in the special case $k = 2$ is presented), namely the methods and proofs used in the case of a finite group (elaborated in [16] and [7]) are – in a quite immediate way – adapted. The second proof is also short and elementary (having the preceding Theorem 3 at hand) and we find it particularly instructive since we deduce Theorem 4 from Theorem 3, using a "cyclification" principle which allows us to use the whole strength of the result for the case of finite groups. This second approach, which is independent of that of [5], was introduced some years ago by the author (in an early version of this paper, *Optimally small sumsets in general Abelian groups*, an unpublished manuscript where the case $k = 2$ was already treated) in order to extend the main result of [7] to the case of infinite Abelian groups.

As a second application of the problematic of the generalized supersmall sumsets property, we show that it can be useful in the study of the following quite natural function (at least in the context of additive number theory, having Kemperman's theorem in mind). Let

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

There are good reasons why this function is mysterious and therefore interesting. Indeed it has a typical "extremal combinatorics" behaviour since two opposite forces have to collaborate in it: a small sumset $|\mathcal{A}_1+\cdots+\mathcal{A}_k|$ implies some kind of structure – this is the general philosophy of the so-called structural theory of set addition (see [8] or [9]) – while structure implies, in general, many representations of the elements in the sumset.

In the final section, we will give already several results on these $\nu_G^{(k)}$ functions. In particular, we shall prove the following general theorem.

Theorem 5. *Let G be an Abelian group. As soon as $r_1+\cdots+r_k \geq |G|+k$, we have*

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

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

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

Some other results on $\nu_G^{(k)}$ will be stated and proved in Section 5, to which the reader is referred.

This paper is the first one in a series in which we intend to derive some other new results related to the present problematic (the reader is referred to [18, 19] which will be put soon on the `arXiv.org`). We hope this series will convince the reader that the extension of the small sumsets property to the generalized supersmall sumsets property is far from being anecdotic. In [18, 19], this new tool (and more elaborate versions of it) will be applied – among others – in order to obtain new bounds on functions related to the problem of optimally small sumsets in groups.

2. Proof of Theorem 2

Let us first mention as a lemma a simple but useful remark.

Lemma 1. *Let G be a group and H be an infinite subgroup of G. If H has the generalized supersmall sumsets property then so does G itself.*

P r o o f. It is enough to take the required sets in H where they have to exist since H is infinite and has itself the generalized supersmall sumsets property. □

Now, in order to prove Theorem 2, we start with a very important lemma.

Lemma 2. *Let G be a group and H be a normal subgroup of G. If both G/H and H have the generalized supersmall sumsets property then so does G itself.*

P r o o f. If H is infinite, since by assumption it has the generalized supersmall sumsets property, then so does G itself by Lemma 1. From now on, we assume that H is finite.

Let k be an arbitrary positive integer. Write, for $1 \le i \le k$, $\rho_i = \lceil r_i/|H| \rceil$ (the ceiling of $r_i/|H|$). Note that, since each r_i is an integer, we have

$$\rho_i = \left\lceil \frac{r_i}{|H|} \right\rceil \le \frac{r_i + |H| - 1}{|H|}. \tag{2}$$

We write $\pi : G \to G/H$ the canonical homomorphism.

Since G/H has the generalized supersmall sumsets property, there are subsets $\mathcal{A}'_1, \dots, \mathcal{A}'_k$ containing 0 in G/H verifying $|\mathcal{A}'_i| = \rho_i$ $(1 \le i \le k)$ such that either

(i) $|\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| \le \rho_1 + \cdots + \rho_k - k$ or

(ii) $|\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| = \rho_1 + \cdots + \rho_k - k + 1$ and 0 has the unique representation $0 + \cdots + 0$ in $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k$.

If we are in case (i), we may select for each index i, a set $\mathcal{A}_i$ in G such that $0 \in \mathcal{A}_i$, $|\mathcal{A}_i| = r_i$ and $\mathcal{A}_i \subset \pi^{-1}(\mathcal{A}'_i)$. Therefore

$$\begin{aligned} |\mathcal{A}_1 + \cdots + \mathcal{A}_k| &\leq |\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| \times |H| \\ &\leq (\rho_1 + \cdots + \rho_k - k)\,|H| \\ &\leq \left(\frac{r_1 + |H| - 1}{|H|} + \cdots + \frac{r_k + |H| - 1}{|H|} - k\right)|H| \\ &= r_1 + \cdots + r_k - k, \end{aligned}$$

thanks to (2).

In case (ii), since H satisfies the generalized supersmall sumsets property, we may select some subsets $\mathcal{X}_i \subset H$ $(1 \leq i \leq k)$ containing 0 and of respective (positive and $\leq |H|$) cardinalities $r_i - (\rho_i - 1)|H|$ such that they satisfy themselves the property required by the generalized supersmall sumsets property in H.

Now, we define $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset G$ as follows

$$\mathcal{A}_i = \pi^{-1}(\mathcal{A}'_i \setminus \{0\}) \cup \mathcal{X}_i \quad (1 \leq i \leq k).$$

We check that

$$|\mathcal{A}_i| = (|\mathcal{A}'_i| - 1)|H| + |\mathcal{X}_i| = (\rho_i - 1)|H| + |\mathcal{X}_i| = r_i.$$

Since $(\mathcal{A}_1 + \cdots + \mathcal{A}_k) \cap H$ reduces to $\mathcal{X}_1 + \cdots + \mathcal{X}_k$ (by the unicity of the representation of 0 in $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k$), we finally have

$$\begin{aligned} |\mathcal{A}_1 + \cdots + \mathcal{A}_k| &= (|\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| - 1) \times |H| + |\mathcal{X}_1 + \cdots + \mathcal{X}_k| \\ &\leq \big((\rho_1 + \cdots + \rho_k - k + 1) - 1\big)|H| + |\mathcal{X}_1| + \cdots + |\mathcal{X}_k| - k + 1 \\ &= \big((\rho_1 - 1)|H| + |\mathcal{X}_1|\big) + \cdots + \big((\rho_k - 1)|H| + |\mathcal{X}_k|\big) - k + 1 \\ &= r_1 + \cdots + r_k - k + 1. \end{aligned}$$

What remains to be proved is that if equality holds in this inequality, that is if $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = r_1 + \cdots + r_k - k + 1$, then 0 can be written in a unique way in $\mathcal{A}_1 + \cdots + \mathcal{A}_k$. But if equality holds, we must have $|\mathcal{X}_1 + \cdots + \mathcal{X}_k| = |\mathcal{X}_1| + \cdots + |\mathcal{X}_k| - k + 1$ and by the definition of the generalized supersmall sumsets property in H, this implies that 0 (viewed in the sumset $\mathcal{X}_1 + \cdots + \mathcal{X}_k \subset H$) can be written in a unique way. It follows from the fact that the elements in $\mathcal{X}_1 + \cdots + \mathcal{X}_k$ are exactly those of $(\mathcal{A}_1 + \cdots + \mathcal{A}_k) \cap H$ that 0 has a single representation in $\mathcal{A}_1 + \cdots + \mathcal{A}_k$.

From the two cases considered above, the result follows. □

Before starting the proof of Theorem 2, we need yet another preliminary lemma.

Lemma 3. *Let G be a group isomorphic to $\mathbb{Z}$ or a cyclic group. Let k be a positive integer. If $r_1, \ldots, r_k$ are positive integers, such that $r_1+\cdots+r_k \leq |G|+k-1$, then there are subsets $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset G$ containing 0 such that $|\mathcal{A}_i| = r_i$ $(1 \leq i \leq k)$,*

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = r_1 + \cdots + r_k - k + 1$$

and 0 has a unique representation in the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$.

P r o o f. In both cases, for any positive integer k and any $r_1, \ldots, r_k \geq 1$, we consider $\mathcal{A}_1 = \{0, \ldots, r_1 - 1\}, \ldots, \mathcal{A}_k = \{0, \ldots, r_k - 1\}$ which implies

$$\mathcal{A}_1 + \cdots + \mathcal{A}_k = \{0, \ldots, r_1 + \cdots + r_k - k\}.$$

If $G = \mathbb{Z}$ or G is a cyclic group (and $r_1 + \cdots + r_k - k \leq |G| - 1$), then $|\mathcal{A}_1| = r_1, \ldots, |\mathcal{A}_k| = r_k$ and $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = r_1 + \cdots + r_k - k + 1$. The result follows since, in both cases, the element 0 in the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ can be written in the unique way $0 + \cdots + 0$. □

We are now ready to prove Theorem 2.

P r o o f o f T h e o r e m 2.

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

This follows directly from Lemma 3 (and we are always in case (ii) of the definition of the property).

Step 2: Every cyclic group has the generalized supersmall sumsets property.

Indeed, if $r_1+\cdots+r_k-k < |G|$ then the result (case (ii)) follows by Lemma 3. Otherwise, $r_1 + \cdots + r_k - k \geq |G|$ and we have $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \leq |G| \leq r_1 + \cdots + r_k - k$ (and this is case (i)).

We shall now apply several times Lemma 2.

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

By the general structure theorem of finite Abelian groups (see for instance Chapter I.5 in [21]), in order to prove this assertion, it is enough to show – by induction (on the number m of factors) – that a product of a finite number of cyclic groups has the generalized supersmall sumsets property. If $m = 1$, Step 2 gives the result. If the result holds for a product of m cyclic groups, then considering a product $G = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_{m+1}\mathbb{Z}$ of $m+1$ ones, we get the result by Lemma 2 (taking $H = \{0\} \times \cdots \times \{0\} \times \mathbb{Z}/n_{m+1}\mathbb{Z} \sim \mathbb{Z}/n_{m+1}\mathbb{Z}$, a group having the desired property by Step 2), since the factor group

$$\begin{aligned} G/H &= (\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z} \times \mathbb{Z}/n_{m+1}\mathbb{Z})/(\{0\} \times \cdots \times \{0\} \times \mathbb{Z}/n_{m+1}\mathbb{Z}) \\ &\sim \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_m\mathbb{Z}, \end{aligned}$$

is a product of m cyclic groups.

Step 4: Any Abelian group has the generalized supersmall sumsets property.

If this group, say G, is finite, the result follows from Step 3. Otherwise, for any positive integer k and integers $r_1, \dots, r_k \geq 1$, we choose $\max(r_1, \dots, r_k)$ arbitrary elements in G. Let H be the subgroup of G generated by these elements. It is by definition finitely generated. But, by the general structure theorem on finitely generated Abelian groups (see Chapter I.5 of [21] again), either H is finite in which case the result follows by Step 3, or H contains a subgroup isomorphic to $\mathbb{Z}$ in which case the result follows by Lemma 1 and the result of Step 1.

Step 5: Any solvable group has the generalized supersmall sumsets property.

Let G be a solvable group. There exists a finite normal series of subgroups

$$\{0\} = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_k = G,$$

with Abelian factors H_{i+1}/H_i $(0 \leq i \leq k-1)$.

Now, the result follows by induction: we show below that each H_i $(0 \leq i \leq k)$ has the generalized supersmall sumsets property; in particular $G = H_k$, which gives the result of Step 5.

Indeed, this is clear for H_0 (and H_1 as well) and if we suppose the result to be true for the subgroup H_i (for some $0 \leq i \leq k-1$), then the result follows for H_{i+1}, by Lemma 2, since the factor group H_{i+1}/H_i, being Abelian, has the generalized supersmall sumsets property (by Step 4) as well as H_i (by the induction hypothesis).

The proof is complete. □

From Theorem 2, we deduce the following corollary.

Corollary 1. *Let G be an arbitrary solvable group, k be a positive integer and $r_1, \dots, r_k$ be any integers satisfying $1 \leq r_1, \dots, r_k \leq |G|$. Then, for any finite normal subgroup H of G, we have*

$$\mu_G^{(k)}(r_1, \dots, r_k) \leq \left(\left\lceil \frac{r_1}{|H|} \right\rceil + \cdots + \left\lceil \frac{r_k}{|H|} \right\rceil - k + 1 \right) |H|.$$

Proof. Since G is solvable and $H \lhd G$, the factor group G/H itself is solvable. By Theorem 2, it follows that G/H has the generalized supersmall sumsets property. In particular, if we put $\rho_i = \lceil r_i/|H| \rceil$ $(1 \leq i \leq k)$, we obtain that there exist subsets $\mathcal{A}'_1, \dots, \mathcal{A}'_k$ containing 0 in G/H, with respective cardinalities $|\mathcal{A}'_i| = \rho_i$ $(1 \leq i \leq k)$, satisfying $|\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| \leq \rho_1 + \cdots + \rho_k - k + 1$. Since

$\rho_i = \lceil r_i/|H| \rceil$, if we put $\pi : G \to G/H$ the canonical homomorphism, we may find subsets $\mathcal{A}_i \subset G$, with $|\mathcal{A}_i| = r_i$ such that $\mathcal{A}_i \subset \pi^{-1}(\mathcal{A}'_i)$. We obtain

$$\begin{aligned} \mu_G^{(k)}(r_1, \ldots, r_k) &\leq |\mathcal{A}_1 + \cdots + \mathcal{A}_k| \\ &\leq |\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| \times |H| \\ &\leq (\rho_1 + \cdots + \rho_k - k + 1)\,|H| \\ &= \left(\left\lceil \frac{r_1}{|H|} \right\rceil + \cdots + \left\lceil \frac{r_k}{|H|} \right\rceil - k + 1 \right) |H|, \end{aligned}$$

as announced. □

3. Proof of Theorem 3

We shall use a generalized version of Kneser's theorem, namely the following.

Theorem 6 (Generalized Kneser's Theorem)**.** *Let G be an Abelian group and $\mathcal{A}_1, \ldots, \mathcal{A}_k$ be k non-empty finite subsets of G such that $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \leq |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k$. Then the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ is periodic and if H denotes its period one has*

$$|\mathcal{A}_1/H + \cdots + \mathcal{A}_k/H| \geq |\mathcal{A}_1/H| + \cdots + |\mathcal{A}_k/H| - k + 1$$

where for each $\mathcal{A}_i$ we denote $\mathcal{A}_i/H$ the projection of $\mathcal{A}_i$ by the canonical map $G \to G/H$.

For the reader's convenience, we include a proof of this folkloric easy result.

Proof of the generalized Kneser's Theorem. Assume that $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ is aperiodic. Then none of the sums $\mathcal{A}_1 + \cdots + \mathcal{A}_j$ for $j = 2, \ldots, k$ can be periodic. By Kneser's theorem, the fact that $\mathcal{A}_1 + \cdots + \mathcal{A}_j$ is aperiodic implies $|\mathcal{A}_1 + \cdots + \mathcal{A}_j| \geq |\mathcal{A}_1 + \cdots + \mathcal{A}_{j-1}| + |\mathcal{A}_j| - 1$. Summing all these inequalities for $j = 2$ to k, we obtain

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \geq |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k + 1,$$

a contradiction.

We denote by H the period of $\mathcal{A}_1 + \cdots + \mathcal{A}_k$. Assume that the second part of the Theorem is false, namely

$$|\mathcal{A}_1/H + \cdots + \mathcal{A}_k/H| \leq |\mathcal{A}_1/H| + \cdots + |\mathcal{A}_k/H| - k.$$

By what we have just proved applied to the sets $\mathcal{A}_1/H, \ldots, \mathcal{A}_k/H$ in G/H, the sumset $\mathcal{A}_1/H + \cdots + \mathcal{A}_k/H$ is periodic (in G/H). But this contradicts the fact that H, being the period of $\mathcal{A}_1 + \cdots + \mathcal{A}_k$, is maximal. □

We are now ready to embark for the proof of Theorem 3.

P r o o f o f T h e o r e m 3. Let $1 \leq r_1, \ldots, r_k \leq |G|$ be integers.

Let d be any divisor of $|G|$ and H be a subgroup of order d of G (recall that G is assumed to be Abelian). By Corollary 1, we get

$$\mu_G^{(k)}(r_1, \ldots, r_k) \leq \left(\left\lceil \frac{r_1}{d} \right\rceil + \cdots + \left\lceil \frac{r_k}{d} \right\rceil - k + 1 \right) \, d.$$

Since this is true for any divisor d of $|G|$, we obtain

$$\mu_G^{(k)}(r_1, \ldots, r_k) \leq \min_{d \,|\, |G|} \left(\left\lceil \frac{r_1}{d} \right\rceil + \cdots + \left\lceil \frac{r_k}{d} \right\rceil - k + 1 \right) d, \tag{3}$$

which gives the upper bound.

To prove the lower bound, we choose subsets $\mathcal{A}_i \subset G$ with $|\mathcal{A}_i| = r_i$ (for $1 \leq i \leq k$) such that

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = \mu_G^{(k)}(r_1, \ldots, r_k).$$

In particular, we have (taking $d = 1$ in (3))

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \leq |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k + 1.$$

If this inequality is an equality then we are done. Otherwise

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \leq |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k$$

and the generalized Kneser's theorem (Theorem 6) implies that the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ is periodic and, if we denote by H its period, that

$$|\mathcal{A}_1/H + \cdots + \mathcal{A}_k/H| \geq |\mathcal{A}_1/H| + \cdots + |\mathcal{A}_k/H| - k + 1. \tag{4}$$

Finally, we obtain (in view of the H-periodicity of the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$ and of (4))

$$\begin{aligned} |\mathcal{A}_1 + \cdots + \mathcal{A}_k| &= |\mathcal{A}_1/H + \cdots + \mathcal{A}_k/H| \times |H| \\ &\geq (|\mathcal{A}_1/H| + \cdots + |\mathcal{A}_k/H| - k + 1)|H| \\ &\geq \left(\left\lceil \frac{r_1}{|H|} \right\rceil + \cdots + \left\lceil \frac{r_k}{|H|} \right\rceil - k + 1 \right) |H|, \end{aligned}$$

since a subset of G with r_i elements meets at least $\lceil r_i/|H| \rceil$ H-cosets. Since $|H|$ is a divisor of $|G|$, the lower bound follows.

The theorem is proved. □

4. Two proofs of Theorem 4

F i r s t p r o o f. The argument given for the proof of the upper bound in Theorem 3 (preceding section) is still valid if we replace the set of divisors of $|G|$ by the set of cardinalities of the finite subgroups H of G (see Corollary 1).

The argument given in the proof of the lower bound in Theorem 3 (preceding section) is also still valid since Kneser's theorem (and its generalized version, Theorem 6, as well) does not require G to be finite. □

S e c o n d p r o o f. Let us fix positive integers $1 \leq r_1, \ldots, r_k \leq |G|$. We choose sets $\mathcal{A}_1, \ldots, \mathcal{A}_k \subset G$ with $|\mathcal{A}_i| = r_i$, in which the quantity $\mu_G^{(k)}(r_1, \ldots, r_k)$ is attained. We consider the subgroup of G generated by $\mathcal{A}_1, \ldots, \mathcal{A}_k$, say $H = \langle \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_k \rangle$. We clearly have $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = \mu_G^{(k)}(r_1, \ldots, r_k) = \mu_H^{(k)}(r_1, \ldots, r_k)$ since $H \leq G$ and the definitions of the $\mu^{(k)}$ functions imply $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = \mu_G^{(k)}(r_1, \ldots, r_k) \leq \mu_H^{(k)}(r_1, \ldots, r_k) \leq |\mathcal{A}_1 + \cdots + \mathcal{A}_k|$. Since H is a finitely generated Abelian group, by the general structure theorem, it is isomorphic to $\mathbb{Z}^r \times T$ where r is some nonnegative integer and T is a finite product of cyclic groups. Without loss of generality, we shall assume that $H = \mathbb{Z}^r \times T$.

For any positive integer p, denote by π_p the canonical projection from $H = \mathbb{Z}^r \times T$ onto $(\mathbb{Z}/p\mathbb{Z})^r \times T$. Clearly, if p is large enough, we have $|\pi_p(\mathcal{A}_i)| = |\mathcal{A}_i|$ for all $1 \leq i \leq k$ and $|\pi_p(\mathcal{A}_1) + \cdots + \pi_p(\mathcal{A}_k)| = |\pi_p(\mathcal{A}_1 + \cdots + \mathcal{A}_k)| = |\mathcal{A}_1 + \cdots + \mathcal{A}_k|$ (this is in some sense a "cyclification principle" in contrast to the so-called rectification principle). It follows that for p large enough,

$$\mu_H^{(k)}(r_1, \ldots, r_k) = |\pi_p(\mathcal{A}_1) + \cdots + \pi_p(\mathcal{A}_k)| \geq \mu_{(\mathbb{Z}/p\mathbb{Z})^r \times T}^{(k)}(r_1, \ldots, r_k).$$

We apply this formula with p a prime larger than $\mu_H^{(k)}(r_1, \ldots, r_k) + 1$. By the result in the finite case (Theorem 3), we obtain

$$\mu_H^{(k)}(r_1, \ldots, r_k) \geq \min_{d \,|\, p^r|T|} \left(\left\lceil \frac{r_1}{d} \right\rceil + \cdots + \left\lceil \frac{r_k}{d} \right\rceil - k + 1 \right) d.$$

If d_0 is a divisor of $p^r|T|$ in which the minimum in the right-hand side of this inequality is attained, then p cannot divide d_0 otherwise

$$p - 1 \geq \mu_H^{(k)}(r_1, \ldots, r_k) \geq \left(\left\lceil \frac{r_1}{d_0} \right\rceil + \cdots + \left\lceil \frac{r_k}{d_0} \right\rceil - k + 1 \right) d_0 \geq d_0 \geq p,$$

a contradiction. Therefore, we finally get

$$\begin{aligned}\mu_G^{(k)}(r_1,\dots,r_k) &= \mu_H^{(k)}(r_1,\dots,r_k) \\ &\geq \min_{d\,|\,|T|}\Big(\Big\lceil\frac{r_1}{d}\Big\rceil+\cdots+\Big\lceil\frac{r_k}{d}\Big\rceil-k+1\Big)\,d \\ &\geq \min_{d\in\mathcal{D}}\Big(\Big\lceil\frac{r_1}{d}\Big\rceil+\cdots+\Big\lceil\frac{r_k}{d}\Big\rceil-k+1\Big)\,d,\end{aligned} \tag{5}$$

because any divisor of $|T|$ is the cardinality of a finite subgroup of T and thus of G.

To finish the proof, we shall show that for an arbitrary $d\in\mathcal{D}$, we have

$$\mu_G^{(k)}(r_1,\dots,r_k)\leq\Big(\Big\lceil\frac{r_1}{d}\Big\rceil+\cdots+\Big\lceil\frac{r_k}{d}\Big\rceil-k+1\Big)\,d. \tag{6}$$

This yields

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

which, with (5), implies the Theorem.

Let us thus consider any $d\in\mathcal{D}$. By definition, there is a subgroup W of G such that $|W|=d$. We now select an arbitrary subset $\mathcal{S}$ of G, having $\max(r_1,\dots,r_k,d)$ elements and containing W and we define V to be the subgroup of G generated by $\mathcal{S}$.

If the subgroup V of G is finite, then d clearly divides $|V|$ and $r_1,\dots,r_k\leq|V|$. Therefore $\mu_G^{(k)}(r_1,\dots,r_k)\leq\mu_V^{(k)}(r_1,\dots,r_k)$ and using Theorem 3 for V, we obtain

$$\begin{aligned}\mu_G^{(k)}(r_1,\dots,r_k) &\leq \min_{t\,|\,|V|}\Big(\Big\lceil\frac{r_1}{t}\Big\rceil+\cdots+\Big\lceil\frac{r_k}{t}\Big\rceil-k+1\Big)\,t \\ &\leq \Big(\Big\lceil\frac{r_1}{d}\Big\rceil+\cdots+\Big\lceil\frac{r_k}{d}\Big\rceil-k+1\Big)\,d,\end{aligned}$$

which proves (6).

If the subgroup V of G is infinite, since it is finitely generated, it contains a subgroup isomorphic to $\mathbb{Z}\times W$ (again, this follows from the general structure theorem on finitely generated Abelian groups). Taking any $\mathcal{A}_i\subset\{0,\dots,\lceil r_i/d\rceil-1\}\times W$ (which is always possible), implies

$$\mathcal{A}_1+\cdots+\mathcal{A}_k\subset\Big\{0,\dots,\Big\lceil\frac{r_1}{d}\Big\rceil+\cdots+\Big\lceil\frac{r_k}{d}\Big\rceil-k\Big\}\times W.$$

It follows that

$$\begin{aligned}\mu_G^{(k)}(r_1,\dots,r_k) &\le |\mathcal{A}_1+\cdots+\mathcal{A}_k| \\ &\le \left(\left\lceil\frac{r_1}{d}\right\rceil+\cdots+\left\lceil\frac{r_k}{d}\right\rceil-k+1\right)|W| \\ &= \left(\left\lceil\frac{r_1}{d}\right\rceil+\cdots+\left\lceil\frac{r_k}{d}\right\rceil-k+1\right)d,\end{aligned}$$

which implies (6) and finishes the proof. □

5. On the $\nu_G^{(k)}$ functions

We start with a useful result in our context, known as the Scherk or the Kemperman-Scherk theorem (see [10, 22]). Since this result is now well known and several proofs widely spread (see for instance Théorème 10 in [17]), we state it without proof.

Theorem 7. *Let $\mathcal{A}$ and $\mathcal{B}$ be two finite non-empty subsets of an Abelian group G. Then, any element of $\mathcal{A}+\mathcal{B}$ has at least $|\mathcal{A}|+|\mathcal{B}|-|\mathcal{A}+\mathcal{B}|$ representations.*

An immediate corollary is the following.

Corollary 2. *Let $\mathcal{A}$ and $\mathcal{B}$ be two finite non-empty subsets of an Abelian group G such that $\mathcal{A}+\mathcal{B}$ contains an element with a unique representation, then $|\mathcal{A}+\mathcal{B}|\ge|\mathcal{A}|+|\mathcal{B}|-1$.*

We therefore obtain

Corollary 3. *Let $\mathcal{A}_1,\dots,\mathcal{A}_k$ be finite non-empty subsets of an Abelian group G such that $\mathcal{A}_1+\cdots+\mathcal{A}_k$ contains an element with a unique representation, then*

$$|\mathcal{A}_1+\cdots+\mathcal{A}_k|\ge|\mathcal{A}_1|+\cdots+|\mathcal{A}_k|-k+1.$$

Proof. Indeed, if $\mathcal{A}_1+\cdots+\mathcal{A}_k$ contains an element with a unique representation, then so do $\mathcal{A}_1+\mathcal{A}_2,\dots,\mathcal{A}_1+\cdots+\mathcal{A}_{k-1}$. Therefore Corollary 2 yields consecutively

$$\begin{aligned}|\mathcal{A}_1+\mathcal{A}_2| &\ge |\mathcal{A}_1|+|\mathcal{A}_2|-1 \\ |\mathcal{A}_1+\cdots+\mathcal{A}_3| &\ge |\mathcal{A}_1+\mathcal{A}_2|+|\mathcal{A}_3|-1 \\ &\vdots \\ |\mathcal{A}_1+\cdots+\mathcal{A}_k| &\ge |\mathcal{A}_1+\cdots+\mathcal{A}_{k-1}|+|\mathcal{A}_k|-1,\end{aligned}$$

and, summing these inequalities, we obtain

$$|\mathcal{A}_1 + \cdots + \mathcal{A}_k| \geq |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k + 1.$$

□

These preliminaries are enough to prove Theorem 5.

Proof of Theorem 5. It follows from Corollary 3 that

$$\nu_G^{(k)}(r_1, \ldots, r_k) \geq r_1 + \cdots + r_k - k + 1$$

and in particular since this has to be always $\leq |G|$ we deduce immediately the result that as soon as $r_1 + \cdots + r_k \geq |G| + k$, we have

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

□

The behaviour of the function $\nu_G^{(k)}(r_1, \ldots, r_k)$ for some types of Abelian groups follows.

Theorem 8. *Let G be either a cyclic group or an Abelian group containing a subgroup isomorphic to $\mathbb{Z}$. Then*

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

as long as $r_1 + \cdots + r_k \leq |G| + k - 1$ and ∞ otherwise.

Proof. The upper bound follows from Lemma 3 and the lower bound from Theorem 5. □

In general, $\nu_G^{(k)}(r_1, \ldots, r_k) \neq r_1 + \cdots + r_k - k + 1$ as follows from the following ultra-basic example: take $G = (\mathbb{Z}/2\mathbb{Z})^2$, $k = 2$ and $r_1 = r_2 = 2$. Since any subset of G with two elements is either a subgroup or a coset modulo a subgroup, it follows that $|\mathcal{A}_1 + \mathcal{A}_2|$ can only be equal to 2 or 4. Henceforth

$$\nu_{(\mathbb{Z}/2\mathbb{Z})^2}^{(2)}(2, 2) = 4.$$

A slightly less trivial example is $G = (\mathbb{Z}/3\mathbb{Z})^2$, $k = 2$ and $r_1 = 2$, $r_2 = 3$. In this case, we may compute

$$\nu_{(\mathbb{Z}/3\mathbb{Z})^2}^{(2)}(2, 3) = 5,$$

a value different from $r_1 + r_2 - 1$ but also from a multiple of the cardinality of any non-trivial subgroup.

The following lemma is of interest in the present context. It is clearly reminiscent of Lemma 2 and the proof of it follows indeed the same lines.

Lemma 4. *Let G be a group and H be a finite normal subgroup of G. Let k be a positive integer. We assume that there are finite subsets $\mathcal{A}'_1,\dots,\mathcal{A}'_k \subset G/H$, containing 0 (in G/H) such that $|\mathcal{A}'_1+\cdots+\mathcal{A}'_k| = |\mathcal{A}'_1|+\cdots+|\mathcal{A}'_k|-k+1$ and 0 has a unique representation in $\mathcal{A}'_1+\cdots+\mathcal{A}'_k$. We also assume that there are finite subsets $\mathcal{X}_1,\dots,\mathcal{X}_k \subset H$, containing 0, such that $|\mathcal{X}_1+\cdots+\mathcal{X}_k| = |\mathcal{X}_1|+\cdots+|\mathcal{X}_k|-k+1$ and 0 has a unique representation in $\mathcal{X}_1+\cdots+\mathcal{X}_k$.*

Then there are (finite) subsets $\mathcal{A}_1,\dots,\mathcal{A}_k \subset G$ containing 0 with $|\mathcal{A}_i| = (|\mathcal{A}'_i|-1)|H|+|\mathcal{X}_i|$ such that $|\mathcal{A}_1+\cdots+\mathcal{A}_k| = |\mathcal{A}_1|+\cdots+|\mathcal{A}_k|-k+1$ and 0 has a unique representation in the sumset $\mathcal{A}_1+\cdots+\mathcal{A}_k$.

P r o o f. We define $\mathcal{A}_1,\dots,\mathcal{A}_k \subset G$ as follows

$$\mathcal{A}_i = \pi^{-1}(\mathcal{A}'_i \setminus \{0\}) \cup \mathcal{X}_i \quad (1 \le i \le k)$$

and we check that $|\mathcal{A}_i| = (|\mathcal{A}'_i|-1)|H|+|\mathcal{X}_i|$.

Since $(\mathcal{A}_1+\cdots+\mathcal{A}_k)\cap H$ reduces to $\mathcal{X}_1+\cdots+\mathcal{X}_k$ (by the unicity of the representation of 0 in $\mathcal{A}'_1+\cdots+\mathcal{A}'_k$), we have

$$\begin{aligned}
|\mathcal{A}_1+\cdots+\mathcal{A}_k| &= (|\mathcal{A}'_1+\cdots+\mathcal{A}'_k|-1)\times|H| + |\mathcal{X}_1+\cdots+\mathcal{X}_k| \\
&= \big((|\mathcal{A}'_1|+\cdots+|\mathcal{A}'_k|-k+1)-1\big)\times|H| \\
&\quad +|\mathcal{X}_1|+\cdots+|\mathcal{X}_k|-k+1 \\
&= \big((|\mathcal{A}'_1|-1)|H|+|\mathcal{X}_1|\big)+\cdots \\
&\quad +\big((|\mathcal{A}'_k|-1)|H|+|\mathcal{X}_k|\big)-k+1 \\
&= |\mathcal{A}_1|+\cdots+|\mathcal{A}_k|-k+1.
\end{aligned}$$

Since 0 (viewed as an element of the sumset $\mathcal{X}_1+\cdots+\mathcal{X}_k \subset H$) can be written in a unique way, it follows from the fact that the elements in $\mathcal{X}_1+\cdots+\mathcal{X}_k$ are exactly those of $(\mathcal{A}_1+\cdots+\mathcal{A}_k)\cap H$ that 0 has a single representation in $\mathcal{A}_1+\cdots+\mathcal{A}_k$. □

From this lemma, we shall deduce a theorem leading to other situations where Theorem 8 gives in fact the true value of the $\nu_G^{(k)}$ functions.

First, recall that if $n_1,\dots,n_r$ are r positive integers, any integer $n \le n_1\cdots n_r - 1$ can be written in a unique way as a sum

$$n = \alpha_1 n_2\cdots n_r + \alpha_2 n_3\cdots n_r + \cdots + \alpha_{r-1}n_r + \alpha_r,$$

where each α_i is an integer verifying $0 \le \alpha_i \le n_i - 1$ (for $1 \le i \le r$).

Theorem 9. *Let G be an Abelian group. Let k be a positive integer and $r_1,\dots,r_k$ be positive integers. Assume that G contains a subgroup isomorphic to the product $\mathbb{Z}/n_1\mathbb{Z}\times\cdots\times\mathbb{Z}/n_r\mathbb{Z}$ and that we may write for each $1 \le i \le k$*

$$r_i = \alpha_1^{(i)} n_2\cdots n_r + \alpha_2^{(i)} n_3\cdots n_r + \cdots + \alpha_{r-1}^{(i)} n_r + \alpha_r^{(i)}$$

with integers $0 \leq \alpha_j^{(i)} \leq n_j - 1$ $(1 \leq j \leq r)$.

If we have

- *for each* $1 \leq j \leq r-1$, $\alpha_j^{(1)} + \cdots + \alpha_j^{(k)} \leq n_j - 1$,
- *for each* $1 \leq i \leq k$, $\alpha_r^{(i)} > 0$, *and*
- $\alpha_r^{(1)} + \cdots + \alpha_r^{(k)} \leq n_r + k - 1$,

then

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

P r o o f. Write $H = \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \subset G$. We shall show that

$$\nu_H^{(k)}(r_1, \ldots, r_k) \leq r_1 + \cdots + r_k - k + 1.$$

This yields $\nu_G^{(k)}(r_1, \ldots, r_k) \leq r_1 + \cdots + r_k - k + 1$ and the result follows by Theorem 5.

The proof is mainly by induction. We show that for any $1 \leq j \leq r-1$, there are subsets $\mathcal{A}_1, \ldots, \mathcal{A}_k$ containing 0 in $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_j\mathbb{Z}$, with

$$|\mathcal{A}_i| = \alpha_1^{(i)} n_2 \cdots n_j + \alpha_2^{(i)} n_3 \cdots n_j + \cdots + \alpha_j^{(i)} + 1 \quad (1 \leq i \leq k)$$

such that $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k + 1$ and 0 has a unique representation in $\mathcal{A}_1 + \cdots + \mathcal{A}_k \subset \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_j\mathbb{Z}$.

For $j = 1$, the result follows from the assumption that

$$(\alpha_1^{(1)} + 1) + \cdots + (\alpha_1^{(k)} + 1) \leq n_1 + k - 1$$

and Lemma 3 applied to the cyclic group $\mathbb{Z}/n_1\mathbb{Z}$.

Assume now the result to be proved for some integer $j-1$, with $1 \leq j-1 \leq r-2$.

First, as above, by Lemma 3 applied to the cyclic group $\mathbb{Z}/n_j\mathbb{Z}$ and since

$$(\alpha_j^{(1)} + 1) + \cdots + (\alpha_j^{(k)} + 1) \leq n_j + k - 1,$$

there are subsets $\mathcal{A}'_1, \ldots, \mathcal{A}'_k$ containing 0 in $\mathbb{Z}/n_j\mathbb{Z}$, with $|\mathcal{A}'_i| = \alpha_j^{(i)} + 1$ such that $|\mathcal{A}'_1 + \cdots + \mathcal{A}'_k| = |\mathcal{A}'_1| + \cdots + |\mathcal{A}'_k| - k + 1$ and 0 has a unique representation in $\mathcal{A}'_1 + \cdots + \mathcal{A}'_k \subset \mathbb{Z}/n_j\mathbb{Z}$.

Second, the induction hypothesis implies the existence of such a k-tuple of subsets $\mathcal{A}''_1, \ldots, \mathcal{A}''_k$ containing 0 in $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_{j-1}\mathbb{Z}$, with

$$|\mathcal{A}''_i| = \alpha_1^{(i)} n_2 \cdots n_{j-1} + \alpha_2^{(i)} n_3 \cdots n_{j-1} + \cdots + \alpha_{j-1}^{(i)} + 1$$

such that $|\mathcal{A}''_1 + \cdots + \mathcal{A}''_k| = |\mathcal{A}''_1| + \cdots + |\mathcal{A}''_k| - k + 1$ and 0 has a unique representation in $\mathcal{A}''_1 + \cdots + \mathcal{A}''_k \subset \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_{j-1}\mathbb{Z}$.

With these two points, we are in a position to apply Lemma 4. We deduce that there are subsets $\mathcal{A}_1, \dots, \mathcal{A}_k$ containing 0 in $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_j\mathbb{Z}$ with

$$\begin{aligned} |\mathcal{A}_i| &= (|\mathcal{A}_i''| - 1)n_j + |\mathcal{A}_i'| \\ &= (\alpha_1^{(i)} n_2 \cdots n_{j-1} + \alpha_2^{(i)} n_3 \cdots n_{j-1} + \cdots + \alpha_{j-1}^{(i)})n_j + \alpha_j^{(i)} + 1 \end{aligned}$$

such that $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k + 1$ and 0 has a unique representation in the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$. This gives the induction step for j.

Now, making the same reasoning at the r-th step and using the assumptions $\alpha_r^{(i)} > 0$ $(1 \le i \le k)$ and

$$\alpha_r^{(1)} + \cdots + \alpha_r^{(k)} \le n_r + k - 1,$$

we obtain that there are subsets $\mathcal{A}_1, \dots, \mathcal{A}_k$ containing 0 in $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$ with

$$|\mathcal{A}_i| = (\alpha_1^{(i)} n_2 \cdots n_{r-1} + \alpha_2^{(i)} n_3 \cdots n_{r-1} + \cdots + \alpha_{r-1}^{(i)})n_r + \alpha_r^{(i)}$$

such that $|\mathcal{A}_1 + \cdots + \mathcal{A}_k| = |\mathcal{A}_1| + \cdots + |\mathcal{A}_k| - k + 1$ and 0 has a unique representation in the sumset $\mathcal{A}_1 + \cdots + \mathcal{A}_k$. This gives the result. □

Notice that a less conceptual proof of this result could be obtained by giving explicit subsets $\mathcal{A}_i$ having the required properties.

We also underline the fact that this result is clearly reminiscent of Kemperman's Theorem [11]. It is certainly no chance.

Acknowledgements. The author thanks Olivier Ramaré for pointing out an inaccuracy in a preliminary version of this paper, *Optimally small sumsets in general Abelian groups*. He is also grateful to an anonymous referee, whose precise comments allowed to improve on the readability of the paper. Finally, he thanks Georges Grekos for his careful reading and his remarks on this article.

REFERENCES

[1] BOLLOBÁS, B. – LEADER, I.: *Sums in the grid,* Discrete Mathematics **162** (1996), 31-48.

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

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

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

[5] ELIAHOU, S.—KERVAIRE, M.: *Minimal sumsets in infinite abelian groups*, J. Algebra **287** (2005), 449–457.

[6] ELIAHOU, S. – KERVAIRE, M.: *The small sumsets property for solvable finite groups,* European Journal of Combinatorics **27** (2006), 1102-1110.

[7] ELIAHOU, S.—KERVAIRE, M.—PLAGNE, A.: *Optimally small sumsets in finite abelian groups*, J. Number Theory **101** (2003), 338–348.
[8] FREIMAN,G. A.: *Foundations of a Structural Theory of Set Addition*, Trans. AMS Monographs Vol. 37, A. M. S., 1973.
[9] FREIMAN, G. A.: *Structure theory of set addition*, Astérisque **258** (1999), 1–33.
[10] KEMPERMAN, J. H. B.: *On complexes in a semi-group*, Indag. Math. **18** (1956), 247–254.
[11] KEMPERMAN, J. H. B.: *On small sumsets in an abelian group*, Acta Math. **103** (1960), 63–88.
[12] KNESER, M.: *Abschätzung der asymptotischen Dichte von Summenmengen*, Math. Z. **58** (1953), 459–484.
[13] KNESER, M.: *Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z. **61** (1955), 429–434.
[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.: *À propos de la fonction X d'Erdős et Graham*, Ann. Inst. Fourier (Grenoble) **54** (2004), 1717–1767.
[18] PLAGNE, A.: *Optimally small sumsets in groups, II. The hypersmall sumsets property and restricted addition*, Uniform Distribution Theory **1** (2006), 111–124.
[19] PLAGNE, A.: *Optimally small sumsets in groups, III. The generalized increasingly small sumsets property and the $\nu_G^{(k)}$ functions*, preprint (2006).
[20] SHAPIRO, D.: *Products of sums of squares*, Exposition. Math. **2** (1984), 235–261.
[21] SAMUEL, P.: *Théorie Algébrique des Nombres*, Hermann, Paris, 1967.
[22] SCHERK, P.: *Distinct elements in a set of sums (solution to a problem of Leo Moser)*, Amer. Math. Monthly **62** (1955), 46–47.

Received June 5, 2006
Revised August 25, 2006

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