COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **24** (1) (2004) 53–68

ON SMALL SUMSETS IN $(\mathbb{Z}/2\mathbb{Z})^n$

JEAN-MARC DESHOUILLERS, FRANÇOIS HENNECART, ALAIN PLAGNE

Received February 28, 2001

It is proved that any subset $\mathcal{A}$ of $(\mathbb{Z}/2\mathbb{Z})^n$, having k elements, such that $|\mathcal{A}+\mathcal{A}|=c|\mathcal{A}|$ (with $c<4$), is contained in a subgroup of order at most $u^{-1}k$ where $u=u(c)>0$ is an explicit function of c which does not depend on k nor on n. This improves by a radically different method the corresponding bounds deduced from a more general result of I. Z. Ruzsa.

1. Introduction

About half a century ago, some authors, among others M. Kneser and G. A. Freiman, began a systematic study of what is now called "inverse additive number theory" (see [7] for a review of this theory and [12] for an extensive presentation). Roughly speaking, the general problematic is the following: extracting information on the structure of sets whose sumset has some special property. A special case consists in identifying the sets having the so-called "small doubling" property. Given an abelian group $(G,+)$, define for subsets $\mathcal{A},\mathcal{B}$ of G their sum

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

In the sequel we shall denote $\mathcal{A}+\mathcal{A}$ by $2\mathcal{A}$. A general question is to describe the structure of the finite subsets $\mathcal{A}$ of G satisfying

$$|2\mathcal{A}|\le C|\mathcal{A}|, \tag{1}$$

where C is some positive constant.

Mathematics Subject Classification (2000): 11P70; 11B75

In 1953, Kneser [10] obtained (as a special case of his investigations) his famous result on the structure of sets $\mathcal{A}$ such that $|2\mathcal{A}| < 2|\mathcal{A}| - 1$. Then Kemperman [9] gave an exhaustive, but of recursive nature, description of sets $\mathcal{A}$ such that $|2\mathcal{A}| \leq 2|\mathcal{A}| - 1$, and finally Lev [11] expressed it in a less precise but more intuitive form. These results which apply to arbitrary abelian groups G, need in return C to be less than 2 in (1).

However, in a large variety of special cases, more is known.

For $G = \mathbb{Z}$, it is readily seen that $|2\mathcal{A}| \geq 2|\mathcal{A}| - 1$ and that equality occurs if and only if $\mathcal{A}$ is an arithmetic progression. Freiman obtained a description of this kind for subsets $\mathcal{A} \subset \mathbb{Z}$ such that $|2\mathcal{A}| \leq 3|\mathcal{A}| - 4$. For larger C in (1), Freiman's main structure Theorem [6] gives a description of $\mathcal{A}$ in terms of generalized arithmetic progressions (see also [2,15]). Note that Bilu's proof [2] is valid even when C is growing as $\log\log\log\log|\mathcal{A}|$.

The Cauchy-Davenport Theorem states that for any subset $\mathcal{A}$ of $\mathbb{Z}/p\mathbb{Z}$ (p prime) one has $|2\mathcal{A}| \geq \min(p, 2|\mathcal{A}| - 1)$ and can be considered as the first result of inverse additive number theory in finite abelian group. The study of inverse problems in $\mathbb{Z}/p\mathbb{Z}$ led Freiman [6] to an almost complete characterisation of those $\mathcal{A}$ satisfying the small doubling property (1) for $C \leq 12/5$. This has been recently extended [3] to any C, but unfortunately under some heavy restrictions on the density of $\mathcal{A}$. The main feature of the method used by Freiman in [6] consists in a lifting process, which transfers the problem into $\mathbb{Z}$.

Ruzsa [16] adapted his own proof [15] of Freiman's Theorem for $\mathbb{Z}$ in the case of commutative groups whose elements have a bounded order, say r. We emphasize the importance of this result of fundamental theoretical interest, since it is valid for any constant C. Practically, this leads to an intuitive description of the structure: if $\mathcal{A}$ has the small doubling property (1) then $\mathcal{A}$ is included in a subgroup H such that $|\mathcal{A}|/|H| \geq 1/C^2 r^{C^4}$. Unfortunately, this lower bound is very small, even for $r = C = 2$. When $G = (\mathbb{Z}/2\mathbb{Z})^n$, any subset $\mathcal{A}$ of $(\mathbb{Z}/2\mathbb{Z})^n$ of cardinality k is obviously contained in a subgroup of order 2^k, thus Ruzsa's result is meaningful up to C about $|\mathcal{A}|^{1/4}$.

Recently, Deshouillers and Freiman [5] obtained the first results in $\mathbb{Z}/n\mathbb{Z}$ (and n sufficiently large) for values of C larger than 2, namely when $C \leq 2.04$. Once again they used a lifting process which is similar in nature to that introduced by Freiman. Having in mind to study every commutative group, the opposite side of the spectrum is concerned with the group $(\mathbb{Z}/2\mathbb{Z})^n$.

This is not the only reason why $(\mathbb{Z}/2\mathbb{Z})^n$ is specially interesting. Indeed, additive properties in $(\mathbb{Z}/2\mathbb{Z})^n$ are related to coding theory (see [19,4,7]). It can be easily seen that a t-error-correcting linear code $\mathcal{C} \subset (\mathbb{Z}/2\mathbb{Z})^n$ is precisely such that $d(2\mathcal{C} \setminus \{0\}, 0) > 2t$, where d is the Hamming distance.

Zémor [19], motivated by this application to coding theory, investigated this problem from a viewpoint similar to that of Mann and Kneser. Zémor's Theorem shows in particular that for a subset $\mathcal{A}$ of $(\mathbb{Z}/2\mathbb{Z})^n$, which contains 0 and generates $(\mathbb{Z}/2\mathbb{Z})^n$, satisfying the small doubling condition $|2\mathcal{A}| = 2|\mathcal{A}| + k - 1$ $(k \geq 0)$, there exists a proper subgroup H of $(\mathbb{Z}/2\mathbb{Z})^n$ such that $|\mathcal{A} + H| - |\mathcal{A}| < |H| + k$. This means that $\mathcal{A}$ is filling, with at most $|H| + k$ exceptions, a collection of H-cosets. This result is meaningful only for $k \leq |\mathcal{A}| - 1$, since otherwise any subgroup H of order 2 is convenient for any $\mathcal{A}$. It thus leads to a structural result only for the range $C < 3$. For $C < 2$, it can be made precise but when $C \geq 2$, we seemingly cannot derive satisfactory bounds for the cardinality of the subgroup generated by $\mathcal{A}$.

In this paper, we study the case of $(\mathbb{Z}/2\mathbb{Z})^n$ by analytical methods. Our result (cf. Theorem 2) looks like Ruzsa's Theorem in this particular case. It applies only for $\mathcal{A}$ such that (1) holds with $C < 4$, but gives in this range much more accurate bounds than those given by Ruzsa's result in its general form [16]. However, as noticed by Ruzsa himself, his proof was not optimized for $G = (\mathbb{Z}/2\mathbb{Z})^n$ and can be somewhat improved: Theorem 1 in Section 2 states this improvement while Section 3 is devoted to Ruzsa's proof of it. Still, our structural result (Theorem 2) is more precise than Ruzsa's result, even in the strongest form of Theorem 1.

2. Statement of the results

We first state the following theorem which improves the main result of [16] for $G = (\mathbb{Z}/2\mathbb{Z})^n$. For the sake of completeness, we will give in Section 3, with the kind permission of I. Z. Ruzsa, his unpublished proof (cf. [18]).

Theorem 1 (Ruzsa). *Let $\mathcal{A}$ be a subset of $(\mathbb{Z}/2\mathbb{Z})^n$ such that $|2\mathcal{A}| = c|\mathcal{A}|$. Then there exist a subgroup H of $(\mathbb{Z}/2\mathbb{Z})^n$ and an element a in $(\mathbb{Z}/2\mathbb{Z})^n$ such that*

(i) $\mathcal{A} \subset a + H$,
(ii) $|H| \leq c2^{[c^3]-1}|\mathcal{A}|$.

Before stating our main result, we introduce some notation.

For any real number c such that $1 \leq c \leq 12/5$, we put

$$u(c) = \frac{-c^2 + 3c - 1}{2c - 1}. \tag{2}$$

Let φ be the piecewise linear mapping from $[11/5,4)$ onto $[12/5,4)$ defined by

$$\varphi(t)=\begin{cases}2(t-1) & \text{if } 11/5\le t\le 12/5,\\ 3t/4+1 & \text{if } 12/5\le t<4.\end{cases}$$

Since $\varphi(t)>t$ for any $11/5\le t<4$, we may define the sequence of intervals

$$I_0=(11/5,12/5],\quad I_1=\varphi(I_0)=(12/5,14/5],$$
$$I_k=\varphi(I_{k-1})=\varphi^{k-1}(I_1)=(\varphi^k(11/5),\varphi^{k+1}(11/5)],\quad k\ge 1,$$

where φ^k denotes the k-th iterate of φ. We have $\lim_{k\to+\infty}\varphi^k(11/5)=4$, hence the (disjoint) union of the I_k's covers the whole interval $(11/5,4)$.

We are now ready to extend the domain of definition of u up to $c<4$. Let c be such that $12/5<c<4$. There exists a unique integer $k=k(c)\ge 1$ such that $c\in I_k$. In fact, since for any $t\ge 11/5$ and any positive integer i we have

$$\varphi^i(t)=4-\left(\frac{3}{4}\right)^{i-1}(4-\varphi(t)),\tag{3}$$

the integer $k(c)$ is the smallest one which satisfies

$$\left(\frac{3}{4}\right)^{k-1}(4-14/5)\le 4-c,$$

that is

$$k=\left\lceil\frac{\log(4-14/5)-\log(4-c)}{\log 4-\log 3}\right\rceil+1.$$

For $j=1,2,\dots,k+1$, we define the real number c_j (depending on c) by

$$c_j=\varphi^{-(k+1-j)}(c),\tag{4}$$

so that $c_j\in I_{j-1}$ and $c_{k+1}=c$. We put

$$u(c)=\frac{u(c_1)}{2^k}.\tag{5}$$

Observe that this definition implies more generally (for $1\le j\le k+1$)

$$u(c)=\frac{u(\varphi^{-1}(c))}{2}=\frac{u(c_k)}{2}=\cdots=\frac{u(c_j)}{2^{k-j+1}}=\cdots=\frac{u(c_2)}{2^{k-1}}=\frac{u(c_1)}{2^k}.\tag{6}$$

We shall give in Section 6 some properties of u.

Our result is the following

Theorem 2. *Let $\mathcal{A}$ be a subset of $(\mathbb{Z}/2\mathbb{Z})^n$ such that $|2\mathcal{A}| = c|\mathcal{A}|$ with $1 \le c < 4$. Then there exist a subgroup H of $(\mathbb{Z}/2\mathbb{Z})^n$ and an element a in $(\mathbb{Z}/2\mathbb{Z})^n$ such that*

(i) $\mathcal{A} \subset a + H$,
(ii) $|H| \le |\mathcal{A}|/u(c)$.

We first prove the result for $c \le 12/5$ (Section 5). Then we use it in order to fill, via an induction argument, the remaining gap $12/5 < c < 4$ (Section 7). In Section 8, we plot our function $1/u$ and compare it to the corresponding one deduced from Ruzsa's result (Theorem 1).

Our proof is inspired by Freiman's [6] and Deshouillers–Freiman's [5]. The main tool is the introduction of exponential sums, which has been very efficient in a number of contexts, as well for direct problems (for instance, the Hardy–Littlewood method) as for inverse problems (Erdős–Fuchs Theorem, Roth's Theorem on sets of integers with no three terms in arithmetic progression, results on sum-free sets, Freiman's result on $\mathbb{Z}/p\mathbb{Z}$, ...). For any abelian group G, any finite $\mathcal{B} \subset G$ and any character χ of G, we put

$$S_{\mathcal{B}}(\chi) = \sum_{b \in \mathcal{B}} \chi(b). \tag{7}$$

In Freiman's proof for $\mathbb{Z}/p\mathbb{Z}$ for example, the fundamental step is to get from the small doubling property, the existence of some non principal character (i.e., different from the unit character that we shall denote systematically by χ_0 in the sequel) such that the sum $S_{\mathcal{A}}(\chi)$ is large; this means that the set $\mathcal{A}$ is unbalanced and thus a large part of $\mathcal{A}$ is lying in half a circle; this is the key argument (the so-called "rectification" principle) which permits to apply classical inverse results on $\mathbb{Z}$. Here, we take advantage of special properties of $(\mathbb{Z}/2\mathbb{Z})^n$. This allows us to choose optimally the character χ so that not only some $S_{\mathcal{A}}(\chi)$ is large but also a certain weighted product of $S_{\mathcal{A}}(\chi)$ and $S_{2\mathcal{A}}(\chi)$ is large as well. By the arithmetic mean-geometric mean inequality, it will be deduced that $\max_{\chi \neq \chi_0}(|S_{\mathcal{A}}(\chi)| + |S_{2\mathcal{A}}(\chi)|)$ is large, then showing that $|\mathcal{A}|/|\langle \mathcal{A} \rangle|$ cannot be too small, where $\langle \mathcal{A} \rangle$ denotes the subgroup generated by $\mathcal{A}$. Those crucial results on characters sum will be presented in Section 4 and in Section 5.

3. Proof of Theorem 1

The following result can be deduced from Plünnecke's inequality [13] (see also [12, Theorem 7.6] and [14, Lemma 3.1]):

Lemma 1 (cf. [17, Theorem 5.1]). *Let j and k be integers such that $1\le j\le k$. Let $\mathcal{B}$ and $\mathcal{C}$ be finite subsets of an arbitrary abelian group. Define c by $|\mathcal{B}+j\mathcal{C}|=c|\mathcal{B}|$. Then there is a non empty $\mathcal{B}'\subset\mathcal{B}$ such that*

$$|\mathcal{B}'+k\mathcal{C}|\le c^{k/j}|\mathcal{B}'|.$$

This lemma is now used to prove Theorem 1.

Proof of Theorem 1. Assume first that $0\in\mathcal{A}$. Since $|2\mathcal{A}|=c|\mathcal{A}|$, Lemma 1 (with $k=3$) shows that there is a non empty set $\mathcal{A}'\subset\mathcal{A}$ such that

$$|\mathcal{A}'+3\mathcal{A}|\le c^3|\mathcal{A}'|. \tag{8}$$

Now let $\mathcal{B}=\{0,b_1,b_2,\dots,b_m\}$ be a maximal collection of elements of $3\mathcal{A}$ (which does contain 0) such that the sets $\mathcal{A}'+b_i$ are pairwise disjoint. From (8) we get $m\le[c^3]-1$. Furthermore by the maximality of $\mathcal{B}$, any set $\mathcal{A}'+x$ where $x\in3\mathcal{A}$ intersects some $\mathcal{A}'+b_i$, that is, $x\in\mathcal{A}'-\mathcal{A}'+b_i$. Since $-\mathcal{A}'=\mathcal{A}'$ (remind that $\mathcal{A}'$ is a binary set), we get $x\in2\mathcal{A}'+\mathcal{B}\subset2\mathcal{A}+\mathcal{B}$. This shows

$$3\mathcal{A}\subset2\mathcal{A}+\mathcal{B}.$$

By induction we obtain $k\mathcal{A}\subset2\mathcal{A}+(k-2)\mathcal{B}$ for any integer $k\ge2$. Thus

$$\langle\mathcal{A}\rangle\subset2\mathcal{A}+\langle\mathcal{B}\rangle.$$

We deduce

$$|\langle\mathcal{A}\rangle|\le|2\mathcal{A}|2^{|\mathcal{B}|}\le c2^{[c^3]-1}|\mathcal{A}|,$$

and Theorem 1 follows with $H=\langle\mathcal{A}\rangle$ and $a=0$.

Now if $0\notin\mathcal{A}$ then we define $\widetilde{\mathcal{A}}=a+\mathcal{A}$ for some $a\in\mathcal{A}$, and by the above argument Theorem 1 holds with $H=\langle\widetilde{\mathcal{A}}\rangle$. ∎

4. Preliminary results

Let G be a finite abelian group and $\mathcal{A}$ be a non empty finite subset of G. We start from the sum

$$S=\sum_{\chi\ne\chi_0}S_{\mathcal{A}}(\chi)^2\overline{S_{2\mathcal{A}}(\chi)},$$

which can be easily calculated: by the orthogonality of the characters, we classically have $S=(|G|-|2\mathcal{A}|)|\mathcal{A}|^2$ and therefore

$$\sum_{\chi\ne\chi_0}|S_{\mathcal{A}}(\chi)|^2|S_{2\mathcal{A}}(\chi)|\ge|S|=(|G|-|2\mathcal{A}|)|\mathcal{A}|^2. \tag{9}$$

Now we put

$$\alpha = |\mathcal{A}|/|G|, \quad c = |2\mathcal{A}|/|\mathcal{A}|, \tag{10}$$

and

$$u_\chi = |S_{\mathcal{A}}(\chi)|/|G|, \quad v_\chi = |S_{2\mathcal{A}}(\chi)|/|G|, \tag{11}$$

and we write

$$U^2 = \textstyle\sum_{\chi\neq\chi_0} u_\chi^2 = \alpha(1-\alpha), \qquad V^2 = \sum_{\chi\neq\chi_0} v_\chi^2 = c\alpha(1-c\alpha), \tag{12}$$
$$W = \max_{\chi\neq\chi_0}(u_\chi + v_\chi).$$

Then for any β such that $0\leq\beta\leq 1$, we have

$$\sum_{\chi\neq\chi_0} u_\chi^2 v_\chi \leq \Big(\sum_{\chi\neq\chi_0} u_\chi^{1+\beta} v_\chi^{1-\beta}\Big) \max_{\chi\neq\chi_0}(u_\chi^{1-\beta} v_\chi^{\beta}). \tag{13}$$

We estimate the sum on the right-hand side by Hölder's inequality,

$$\sum_{\chi\neq\chi_0} u_\chi^{1+\beta} v_\chi^{1-\beta} \leq U^{1+\beta} V^{1-\beta}. \tag{14}$$

From (13) and (14), we are able to obtain an upper bound for $\sum_{\chi\neq\chi_0} u_\chi^2 v_\chi$ that we may compare with the estimate from below given by (9). This gives

$$\alpha^2(1-c\alpha) \leq U^{1+\beta} V^{1-\beta} \max_{\chi\neq\chi_0}(u_\chi^{1-\beta} v_\chi^{\beta}). \tag{15}$$

We then deduce the following result, which generalizes the key lemma introduced by Freiman [6] for studying small doubling sets in $\mathbb{Z}/p\mathbb{Z}$.

Proposition 1. *Let $\mathcal{A}$, α and c be as above. For any $\beta\in[0,1]$, there exists a non principal character $\chi=\chi_\beta$ such that*

$$|S_{\mathcal{A}}(\chi)|^{1-\beta} |S_{2\mathcal{A}}(\chi)|^{\beta} \geq \lambda(c,\alpha,\beta)|\mathcal{A}|,$$

where

$$\lambda(c,\alpha,\beta) = c^\beta \left(\frac{1-c\alpha}{c(1-\alpha)}\right)^{(\beta+1)/2}.$$

Now, we can bound the maximum in (13) using the weighted arithmetic mean-geometric mean inequality: for $\chi\neq\chi_0$, we have

$$u_\chi^{1-\beta} v_\chi^{\beta} \leq \beta^\beta (1-\beta)^{1-\beta}(u_\chi + v_\chi) \leq \beta^\beta (1-\beta)^{1-\beta} W.$$

This, with the optimal choice $\beta = V/(U+V)$ and (15) leads to the inequality

$$\alpha^2(1-c\alpha) \leq \sum_{\chi\neq\chi_0} u_\chi^2 v_\chi \leq \frac{U^2 V W}{U+V}, \tag{16}$$

which shall be needed in the next section.

5. Proof of Theorem 2, first step

In this section, we prove Theorem 2 up to 12/5. We start as follows.

Since shifting the set $\mathcal{A}$ does not affect the cardinality of both $\mathcal{A}$ and $2\mathcal{A}$, we can assume that 0 is in $\mathcal{A}$. Moreover any subgroup of $(\mathbb{Z}/2\mathbb{Z})^n$ is isomorphic to some $(\mathbb{Z}/2\mathbb{Z})^\ell$, thus we also assume that $\mathcal{A}$ generates $G = (\mathbb{Z}/2\mathbb{Z})^n$. We have

Lemma 2. *Let χ be any character which is not constant on $\mathcal{A}$. Then*

$$|S_{\mathcal{A}}(\chi)| + |S_{2\mathcal{A}}(\chi)| \le |2\mathcal{A}| - |\mathcal{A}|. \tag{17}$$

Proof. For $j=0,1$, we denote

$$\mathcal{A}_j = \{a \in \mathcal{A} \,:\, \chi(a) = (-1)^j\} \quad \text{and} \quad \mathcal{B}_j = \{b \in 2\mathcal{A} \,:\, \chi(b) = (-1)^j\}.$$

We have

$$|\mathcal{A}_0| + |\mathcal{A}_1| = |\mathcal{A}|, \quad |\mathcal{B}_0| + |\mathcal{B}_1| = |2\mathcal{A}|.$$

Since χ is not constant on $\mathcal{A}$, both sets $\mathcal{A}_0$ and $\mathcal{A}_1$ are non empty. Thus, writing

$$\mathcal{B}_0 = 2\mathcal{A}_0 \cup 2\mathcal{A}_1, \quad \mathcal{B}_1 = \mathcal{A}_0 + \mathcal{A}_1,$$

we deduce $\min(|\mathcal{B}_0|, |\mathcal{B}_1|) \ge \max(|\mathcal{A}_0|, |\mathcal{A}_1|)$. Hence we have

$$\begin{aligned} |S_{\mathcal{A}}(\chi)| + |S_{2\mathcal{A}}(\chi)| &= \big||\mathcal{A}_0| - |\mathcal{A}_1|\big| + \big||\mathcal{B}_0| - |\mathcal{B}_1|\big| \\ &= 2\max\left(|\mathcal{A}_0|, |\mathcal{A}_1|\right) - |\mathcal{A}| + |2\mathcal{A}| - 2\min\left(|\mathcal{B}_0|, |\mathcal{B}_1|\right), \end{aligned}$$

yielding (17). ∎

Defining u_χ and v_χ as in (11) we obtain

$$W = \max_{\chi \ne \chi_0} (u_\chi + v_\chi) \le (c-1)\alpha.$$

This gives by (12) and (16)

$$\alpha^2(1-c\alpha) \le \frac{\alpha(1-\alpha)\sqrt{c\alpha(1-c\alpha)}(c-1)\alpha}{\sqrt{\alpha(1-\alpha)} + \sqrt{c\alpha(1-c\alpha)}},$$

whence after some easy calculation

$$\alpha \ge \frac{-c^2+3c-1}{2c-1}.$$

Theorem 2 follows with $H=G$ and $a=0$, when $c \le 12/5$.

Remark. This method provides actually a non trivial bound in Theorem 2 also for $12/5 \le c < (3+\sqrt{5})/2$. However we shall see in Section 7 that, in this range, this bound can be largely improved.

6. Some basic properties of u

1) We first show that u is decreasing.

We easily check from (2) that it is true on $[1,12/5]$.

Let c and c' such that $11/5 < c < c' < 4$. There are two non negative integers $k \le k'$ such that $c \in I_k$ and $c' \in I_{k'}$. We denote $c_1 = \varphi^{-k}(c)$ and $c_1' = \varphi^{-k'}(c')$. If $k = k'$, then $c_1 < c_1'$ since φ is increasing. Thus by (5) we get $u(c) > u(c')$ since u is decreasing on $[1,12/5]$. Assume that $k < k'$. We have $c_1, c_1' \in I_0$, thus $c_1' > 11/5$ and $c_1 \le 12/5$. We check that $u(11/5) < 2u(12/5)$ (note that the choice of I_0 has been performed to have this condition). Since u is decreasing on $[1,12/5]$ we get

$$u(c_1') < u(11/5) < 2u(12/5) \le 2u(c_1).$$

We finally deduce from (5) that $u(c) > 2^{k'-k-1}u(c') \ge u(c')$.

The remaining case $1 \le c \le 11/5 < c_1' \le 12/5 < c'$ is easily seen.

2) Now we show that

$$\begin{cases} u(c-2/3) \ge 2u(c), & \text{for} \quad 2 \le c < 4, \\ u(c-5/3) \ge 4u(c), & \text{for} \quad 8/3 \le c < 4, \\ u(c-8/3) \ge 8u(c), & \text{for} \quad 11/3 \le c < 4. \end{cases} \tag{18}$$

Using (2), we check, by a tedious but straightforward calculation, that the first inequality is true for $2 \le c \le 12/5$. If $c > 12/5$, there is a $k \ge 1$ such that $c \in I_k$. We have $c - 2/3 < \varphi^{-1}(c)$, thus since u is decreasing, we obtain $u(c-2/3) > u(\varphi^{-1}(c)) = 2u(c)$, by (6). This proves the first inequality. Now, we write $u(c-5/3) > u(c-4/3)$ and $u(c-8/3) > u(c-6/3)$ and apply respectively twice and three times the inequality we have just proved in order to obtain the two other relations.

3) We end this section by showing

$$4 - c > 12u(c), \quad \text{for} \quad 12/5 < c < 4. \tag{19}$$

Indeed, let $k \ge 1$ such that $c \in I_k$. Let $c_1 < c_2 < \cdots < c_k < c_{k+1} = c$ be the sequence defined by (4). We check using (2) that $3u(c_1) < 3 - c_1$ holds (again by a simple computation).

If $k = 1$, using $c_1 = c/2 + 1$ (which follows from (4)), the definition of φ and (5), we directly obtain that (19) holds true on I_1.

Let now $k \ge 2$. By (3) and the result on I_1, we get

$$4 - c = (3/4)^{k-1}(4 - c_2) > 12(3/4)^{k-1}u(c_2).$$

Using now (6) with $j=2$ yields

$$4-c>12(3/4)^{k-1}2^{k-1}u(c)>12u(c),$$

that is (19).

7. Proof of Theorem 2, concluded

We now extend, by induction, the range of validity of Theorem 2 up to $c<4$.

Let us formulate our induction hypothesis for $k\geq 0$: for any given $c\in I_k$, any subset $\mathcal{B}$ of a binary space such that $|2\mathcal{B}|=c|\mathcal{B}|$ is included in a coset of some subgroup whose cardinality is less than $|\mathcal{B}|/u(c)$.

In Section 5, we proved Theorem 2 up to $12/5$. In particular, this shows the validity of our hypothesis for $k=0$.

We now assume that our induction hypothesis is true for some $k-1$ ($k\geq 1$). Our aim is to show that the result holds true for $c\in I_k$. We consider a subset $\mathcal{A}$ of a binary space G satisfying $|2\mathcal{A}|=c|\mathcal{A}|$. As above we may assume that $0\in\mathcal{A}$, and that G is the subgroup generated by $\mathcal{A}$. Let $c_1<c_2<\cdots<c_k<c_{k+1}=c$ be the sequence defined by (4). We have in particular

$$c_k=\begin{cases} c/2+1 & \text{if } k=1,\\ 4(c-1)/3 & \text{if } k\geq 2,\end{cases} \tag{20}$$

and, by (6) with $j=k$,

$$u(c)=\frac{u(c_k)}{2}. \tag{21}$$

From Proposition 1, with $\beta=0$, we deduce that there exists a non principal character χ of G such that

$$\Big|\sum_{a\in\mathcal{A}}\chi(a)\Big|\geq\sqrt{\frac{1-c\alpha}{c(1-\alpha)}}|\mathcal{A}|,$$

where $\alpha=|\mathcal{A}|/|G|$. We are going to show that $\alpha\geq u(c)$.

We define $\mathcal{A}_0=\mathcal{A}\cap\operatorname{Ker}\chi$ and $\mathcal{A}_1=\mathcal{A}\setminus\mathcal{A}_0$ which are both not empty since χ is not constant on $\mathcal{A}$ (otherwise $\langle\mathcal{A}\rangle\neq G$). We further suppose that $|\mathcal{A}_0|\geq|\mathcal{A}_1|$ (it can be plainly done without loss of generality) and we write $x_0=|\mathcal{A}_0|/|\mathcal{A}|$. We thus have

$$x_0\geq\frac{1}{2}\left(1+\sqrt{\frac{1-c\alpha}{c(1-\alpha)}}\right). \tag{22}$$

If $x_0 < 3/4$, we get $\alpha > (4-c)/3c$. Thus, in view of (19), we obtain $\alpha > u(c)$ and we are done. From now on, we assume that

$$x_0 \geq \frac{3}{4}. \tag{23}$$

If H_0 denotes the group generated by $\mathcal{A}_0$, it is always possible to write $\mathcal{A}_1 \subset S_1 + H_0$, where S_1 is some subset of $\mathcal{A}_1$. We choose S_1 with the minimal possible cardinality, say s_1 (this is exactly the number of H_0-cosets met by $\mathcal{A}_1$). We obtain the lower bound

$$|\mathcal{A}_0 + \mathcal{A}_1| \geq s_1 |\mathcal{A}_0|. \tag{24}$$

Finally, by letting $c' = |2\mathcal{A}_0|/|\mathcal{A}_0|$, we get

$$c|\mathcal{A}| = |2\mathcal{A}| \geq c'|\mathcal{A}_0| + |\mathcal{A}_0 + \mathcal{A}_1|. \tag{25}$$

We consider three cases.

1) We first assume that at least one of the following three conditions holds:

(i) $s_1 \geq 5$,
(ii) $4 \geq s_1 \geq 2$ and $c' > c_k + 4/3 - s_1$,
(iii) $s_1 = 1$, $c' > c_k$ and $|\mathcal{A}_0 + \mathcal{A}_1| \geq |\mathcal{A}|$.

We deduce from (23), (24) and (25) that in any of the three possible subcases (i), (ii) or (iii), we have $c \geq c_k x_0 + 1$. Then, in view of (22), we get

$$c \geq c_k x_0 + 1 \geq \frac{c_k}{2}\left(1 + \sqrt{\frac{1-c\alpha}{c(1-\alpha)}}\right) + 1.$$

This gives

$$\alpha \geq h(c_k, c) := \frac{c_k^2 - c(2c - c_k - 2)^2}{4c(c-1)(1-c+c_k)}. \tag{26}$$

Replacing c_k with its value as given in formula (20), it follows that if $k = 1$ (thus $12/5 < c \leq 14/5$), then

$$\alpha \geq \frac{-9c^2 + 28c - 4}{8c(4-c)} > \frac{1}{8} > u\Big(\frac{12}{5}\Big) > u(c),$$

and if $k \geq 2$

$$\alpha \geq \frac{4-c}{3c},$$

whence, by (19), in any case

$$\alpha \geq u(c). \tag{27}$$

2) Now assume that either $2 \leq s_1 \leq 4$ and $1 \leq c' \leq c_k + 4/3 - s_1$, or $s_1 = 1$ and $c' \leq c_k$. Since in both cases $|2\mathcal{A}_0|/|\mathcal{A}_0| = c' \leq c_k$, we can apply the induction hypothesis to $\mathcal{A}_0$, and we obtain the following structure result for $\mathcal{A}_0$: the subgroup H_0 generated by $\mathcal{A}_0$ satisfies

$$\frac{|\mathcal{A}_0|}{|H_0|} \geq u(c').$$

Now, $\mathcal{A}_0 \cup \mathcal{A}_1$ generates G, therefore the subgroup generated by H_0 and S_1 is G. We obtain that $|G| \leq 2^{s_1}|H_0|$, on recalling that any non zero element in G has order 2. Since u is decreasing, we get

$$\alpha = \frac{|\mathcal{A}|}{|G|} \geq \frac{|\mathcal{A}_0|}{2|H_0|} \geq \frac{u(c')}{2} \geq \frac{u(c_k)}{2}, \quad \text{for} \quad s_1 = 1,$$

and, using (18),

$$\alpha = \frac{|\mathcal{A}|}{|G|} \geq \frac{|\mathcal{A}_0|}{2^{s_1}|H_0|} \geq \frac{u(c')}{2^{s_1}} \geq \frac{u(c_k + 4/3 - s_1)}{2^{s_1}} \geq \frac{u(c_k)}{2}, \quad \text{for} \quad 2 \leq s_1 \leq 4.$$

In any case, we conclude by (21) that

$$\alpha \geq u(c). \tag{28}$$

3) We finally assume that $s_1 = 1$, $c' > c_k$ and $|\mathcal{A}_0 + \mathcal{A}_1| < |\mathcal{A}|$. From (25), (24) and (20), we obtain

$$x_0 \leq \frac{c}{c_k + 1} = \begin{cases} 2c/(c+4) & \text{if } k = 1, \\ 3c/(4c-1) & \text{if } k \geq 2, \end{cases}$$

thus (since $c \leq 14/5$ if $k = 1$ and $c > 14/5$ if $k \geq 2$)

$$x_0 \leq 14/17 < 0.83. \tag{29}$$

Hence

$$|\mathcal{A}_1| > 0.17|\mathcal{A}|. \tag{30}$$

We have $|\mathcal{A}_0 + \mathcal{A}_1| < |\mathcal{A}| = |\mathcal{A}_0| + |\mathcal{A}_1|$, thus we can apply the following special case of a result due to Lev [11]:

Lemma 3 (Lev). *Let $\mathcal{A}_0$ and $\mathcal{A}_1$ be two non empty subsets of $(\mathbb{Z}/2\mathbb{Z})^n$ such that $|\mathcal{A}_0+\mathcal{A}_1| \le |\mathcal{A}_0|+|\mathcal{A}_1|-1$. Then there exist a subgroup K of $(\mathbb{Z}/2\mathbb{Z})^n$ and two subsets R_0 and R_1 such that $\mathcal{A}_0 \subset R_0+K$, $\mathcal{A}_1 \subset R_1+K$ and one of the following holds:*

(i) $|R_0|=|R_1|=1$ *and* $|K|<2|\mathcal{A}_0+\mathcal{A}_1|$,

(ii) $\min(|R_0|,|R_1|)=1$, $r=\max(|R_0|,|R_1|)>1$ *and*

$$(r-1)|K| < |\mathcal{A}_0+\mathcal{A}_1|. \tag{31}$$

It is interesting to notice that in the general case of arbitrary abelian groups, there is a third possible conclusion, which states that each of the subsets R_0 and R_1 could be an arithmetic progression with a same difference which is an element of order at least $|R_0|+|R_1|+1$. In binary spaces $(\mathbb{Z}/2\mathbb{Z})^n$, this conclusion cannot hold since any element is of order at most 2.

When (i) holds, we can assume $R_0=\{0\}$ since $0\in\mathcal{A}_0$. Hence G is generated by K and R_1. Moreover we have $|K|<2|\mathcal{A}_0+\mathcal{A}_1|<2|\mathcal{A}|$, thus $|G|=2|K|<4|\mathcal{A}|$, yielding

$$\alpha > 1/4. \tag{32}$$

Assume now that we are in case (ii). The case $|R_0|=1$ and $r=|R_1|\ge 2$ leads to $|\mathcal{A}|>|\mathcal{A}_0+\mathcal{A}_1|\ge r|\mathcal{A}_0|$, a contradiction, since $|\mathcal{A}_0|>|\mathcal{A}|/2$. Therefore we may assume that $|R_1|=1$ and $r=|R_0|\ge 2$ with $0\in R_0$. Then

$$|\mathcal{A}| > |\mathcal{A}_0+\mathcal{A}_1| \ge r|\mathcal{A}_1|. \tag{33}$$

Using (30) we immediately get $r\le 5$. The subgroup generated by $R_0\cup R_1$ and K contains $\mathcal{A}$, and thus coincides with G. It follows by (31) that $|G|\le 2^r|K|<2^r|\mathcal{A}|/(r-1)\le 8|\mathcal{A}|$. Hence

$$\alpha > 1/8. \tag{34}$$

By (27), (28), (32) and (34), we conclude in view of $u(c)<u(12/5)=0.115\ldots<1/8$ that

$$\alpha \ge u(c).$$

This ends the proof that the result holds true for $c\in I_k$ and the induction step.

Theorem 2 follows.

8. Conclusions and remarks

Using (2), (4) and (5), we can compute $u(c)$ for any $c<4$. We give in the following table some special (rounded by excess) values taken by u, and in Figure 1 below the full graph of u.

c	1	3/2	7/4	2	11/5	12/5	8/3	3	22/7	29/8	19/5
$1/u(c)$	1	1.6	2.2	3	4.5	8.7	13.2	26.4	39.5	294	1307

Table 1.

Comparing the bounds for $|\langle\mathcal{A}\rangle|/|\mathcal{A}|$ given respectively by Theorem 1 and by Theorem 2, we observe that the latter becomes weaker than the former only from $c=3.999999960\ldots$

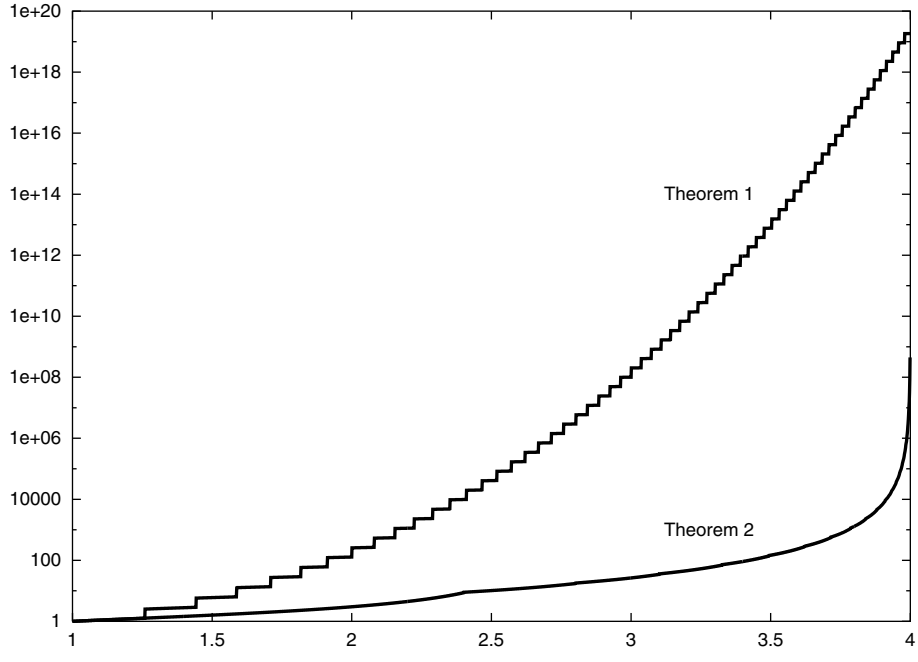

Figure 1. Comparison (on logarithmic scale) of the bounds given respectively by Theorem 1 and Theorem 2

Though our proof is rather accurate (specially in the induction step), it can be further, but slightly, improved leading to sharper bounds, for instance

by optimizing for a given c the choice of the sequence $c_1<c_2<\cdots<c=c_{k+1}$ with $c_j\in I_{j-1}$ where the sequence of intervals $(I_j)_{j\geq 0}$ is also optimized. We proceed as follows.

Let $v_0=2.1513\ldots$ (resp. $w_0=2.3827\ldots$) be the solution of $u(x)=1/4$ (resp. $u(x)=1/8$). For $j\geq 1$, we let v_j (resp. w_j) be the solution of

$$h(v_{j-1},x)=2^{-j-2}\quad(\text{resp. } h(w_{j-1},x)=2^{-j-2}),$$

where h is the function defined in (26). We finally define the intervals $I_j=(v_j,v_{j+1}]$, $j\geq 0$. We know that $u(c)=(-c^2+3c-1)/(2c-1)$ is an admissible value for any c in $[v_0,w_0]$ and we check that $u(c)=1/8$ is an admissible value for any c in $[w_0,v_1]$. For a given $c\in I_k$, we compute the sequence $c_1<c_2<\cdots<c_k<c_{k+1}$ where $c_j\in I_{j-1}$ by solving the system

$$h(c_j,c_{j+1})=\frac{u(c_1)}{2^j},\quad j=1,\ldots,k,$$

and we obtain that $u(c)=u(c_1)/2^k$ is an admissible bound. This gives

c	12/5	8/3	3	22/7	29/8	19/5
$1/u(c)$	8	8.3	16	24.3	128	347

Table 2.

Consider now the following example: for $m\geq 1$, let $a_1,a_2,\ldots,a_m\in G=(\mathbb{Z}/2\mathbb{Z})^n$ be m linearly independent (over $\mathbb{Z}/2\mathbb{Z}$) elements. For $\mathcal{A}=\{0,a_1,a_2,\ldots,a_m\}$ we get

$$|2\mathcal{A}|=\frac{2+m(m+1)}{2(m+1)}|\mathcal{A}|,\quad |\langle\mathcal{A}\rangle|=\frac{2^m}{m+1}|\mathcal{A}|.$$

By putting $m=5,6,7$, this shows that the best possible lower bounds for $c=8/3,22/7,29/8$ are at least respectively $16/3,64/7,16$. Let us finally remark that, for $m=3$, we obtain a set $\mathcal{A}$ containing 0 for which $|\langle\mathcal{A}\rangle|/|2\mathcal{A}|=8/7$. Conversely, it can be shown that for any $\mathcal{A}\subset G$ such that $0\in\mathcal{A}$ and $|2\mathcal{A}|<2|\mathcal{A}|$, we have $|\langle\mathcal{A}\rangle|/|2\mathcal{A}|\leq 8/7$ (cf. [8] and [19]).

Acknowledgements

We are indebted to Professor Imre Ruzsa for his valuable comments, and in particular for pointing out to us his result (Theorem 1). We would like also to thank the referees for many useful remarks and important improvements over the first submitted version of this paper.

A. P. is supported by the DGA-Recherche, France.

References

[1] *Structure theory of set addition*, J.-M. Deshouillers, B. Landreau and A. A. Yudin eds, Astérisque **258** (1999).
[2] Yu. Bilu: Structure of sets with small sumset, in [1], 77–108.
[3] Yu. Bilu, V. F. Lev and I. Z. Ruzsa: Rectification principles in additive number theory, Disc. Comput. Geom. **19** (1998), 343–353.
[4] G. Cohen and G. Zémor: Subset sums and coding theory, in [1], 327–339.
[5] J.-M. Deshouillers and G. A. Freiman: A step beyond Kneser's theorem for finite abelian groups, *Proc. London Math. Soc.* (3) **86** (2003), 1–28.
[6] G. A. Freiman: *Foundations of a structural theory of set addition*, Translation of Mathematical Monographs 37, AMS: Rhode Island, 1973.
[7] G. A. Freiman: Structure theory of set addition, in [1], 1–33.
[8] F. Hennecart and A. Plagne: On the subgroup generated by a small doubling binary set, *European J. Combin.* **24** (2003), 5–14.
[9] J. H. B. Kemperman: On small sumsets in an abelian group, *Acta Math.* **103** (1960), 63–88.
[10] M. Kneser: Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 549–584.
[11] V. F. Lev: On small sumsets in abelian groups, in [1], 317–321.
[12] M. B. Nathanson: *Additive number theory: Inverse problems and the geometry of sumsets*, Springer-Verlag, 1996.
[13] H. Plünnecke: Eine zahlentheoretische Anwendung der Graphtheorie, *J. Reine Angew. Math.* **243** (1970), 171–183.
[14] I. Z. Ruzsa: Arithmetical progressions and the number of sums, *Period. Math. Hungar.* **25** (1992), 105–111.
[15] I. Z. Ruzsa: Generalized arithmetic progressions and sumsets, *Acta Math. Hungar.* **65** (1994), 379–388.
[16] I. Z. Ruzsa: An analog of Freiman's theorem in groups, in [1], 323–326.
[17] I. Z. Ruzsa: An application of graph theory to additive number theory, *Scientia Ser. A* **3** (1989), 97–109.
[18] I. Z. Ruzsa: Personal communication, (2001).
[19] G. Zémor: Subset sums in binary spaces, *European J. Combin.* **13** (1992), 221–230.

Jean-Marc Deshouillers

A2X, UMR 5465
Université Bordeaux 1 et CNRS
351, cours de la Libération
33405 Talence Cedex, France
dezou@math.u-bordeaux.fr

François Hennecart

Laral, EA 769
Université Jean-Monnet
23, rue du Docteur Paul Michelon
42023 Saint-Étienne Cedex 2, France
francois.hennecart@univ-st-etienne.fr

Alain Plagne

Centre de Mathématiques Laurent Schwartz
UMR 7640 du CNRS
École polytechnique
91128 Palaiseau Cedex, France
plagne@math.polytechnique.fr