Astérisque

YURI BILU

Structure of sets with small sumset

Astérisque, tome 258 (1999), p. 77-108

<http://www.numdam.org/item?id=AST_1999__258__77_0>

Astérisque **258**, 1999, p. 77–108

STRUCTURE OF SETS WITH SMALL SUMSET

by

Yuri Bilu

Abstract. — Freiman proved that a finite set of integers K satisfying $|K+K| \leq \sigma|K|$ is a subset of a "small" m-dimensional arithmetical progression, where $m \leq \lfloor \sigma - 1 \rfloor$. We give a complete self-contained exposition of this result, together with some refinements, and explicitly compute the constants involved.

1. Introduction

This is an exposition of the fundamental theorem due to G. A. Freiman on the addition of finite sets. (It will be referred to as *Main theorem*). Let K be a finite set of integers (more generally, a finite subset of a torsion-free abelian group) of cardinality k. The Main Theorem states that if the sumset $K+K$ is "small", then K possesses a rigid structure. An example of a statement of this type is the following

Proposition 1.1

(i) *Any K satisfies $|K+K| \geq 2k-1$ and the equality $|K+K| = 2k-1$ implies that K is an arithmetical progression .*

(ii) *Assume that $|K+K| = 2k-1+t$, where $0 \leq t \leq k-3$. Then K is a subset of an arithmetical progression of length $k+t$.*

(iii) *Assume that $|K+K| = 3k-3$ and $k \geq 7$. Then either K is a subset of an arithmetical progression of length $2k-1$, or K is a union of two arithmetical progressions with the same difference.*

Here (i) is trivial, for (ii) and (iii) see [**12**, Theorems 1.9 and 1.11], where the result is obtained for subsets of integers. The case of subsets of an arbitrary torsion-free abelian group follows from [**12**, Lemma 1.14], which is Lemma 4.3 of the present paper.

Let us deviate for a while from our main subject, and make a short (and very incomplete) historical account. Item (i) easily generalizes to distinct summands: *if K*

1991 ***Mathematics Subject Classification.*** — 11B25, 11B05.

Key words and phrases. — Addition of finite sets; generalized arithmetical progressions; inverse additive theorems.

and L are finite subsets of a torsion-free abelian group, then $|K+L| \geq |K|+|L|-1$, and the equality $|K+L| = |K|+|L|-1$ implies that K and L are arithmetical progressions with the same difference. Freiman **[10]** extended item (ii) to two distinct summands; see also **[15, 23, 32, 35]**. An important generalization to several (equal or distinct) summands was obtained by Lev **[22]**. Concerning item (iii) see also Hamidoune **[17]**.

Item (i) extends to torsion-free non-abelian groups (Brailovski and Freiman **[4]**). It also has an analogue for cyclic groups of prime order (Cauchy **[6]**, Davenport **[7, 8]**, Vosper **[36]**). Hamidoune **[16]** gave short and conceptual proofs of the theorems of Brailovski-Freiman and Vosper. For general finite (abelian and/or non-abelian) groups see **[20, 18, 37, 38]**. However, we do not know non-commutative analogues of items (ii) and (iii), and we know only partial analogues of these items for cyclic groups of prime order **[11, 12, 2]**.

The first part of item (i) has various continuous analogues, for instance for connected unimodular locally compact groups **[19, 29]**. Item (ii) has a partial analogue for real tori **[1]**.

Many of the results mentioned above are proved in the books of Mann **[24]** and Nathanson **[26]**, where the reader can also find further references.

The Main Theorem, however, develops Proposition 1.1 in a completely different direction. Reformulate item (ii) as follows:

Let $\sigma < 3$ be a positive number. Assume that $|K+K| \leq \sigma k$ and $k > 3/(3-\sigma)$. Then K is a subset of an arithmetical progression of length $(\sigma-1)k+1$.

The Main Theorem extends this to arbitrary σ, without the restriction $\sigma < 3$. To formulate it, we need some definitions. Let A, B be abelian groups, $K \subset A$ and $L \subset B$. The map $\varphi : K \to L$ is *Freiman's homomorphism of order s* or, in the terminology of **[28]**, *F_s-homomorphism*, if for any $x_1, \ldots, x_s, y_1, \ldots, y_s \in K$ we have

$$x_1 + \cdots + x_s = y_1 + \cdots + y_s \Rightarrow \varphi(x_1) + \cdots + \varphi(x_s) = \varphi(y_1) + \cdots + \varphi(y_s)$$

In the other words, the map

$$\begin{array}{rccc} \psi: & \overbrace{K + \cdots + K}^{s} & \to & \overbrace{L + \cdots + L}^{s}, \\ & x_1 + \cdots + x_s & \mapsto & \varphi(x_1) + \cdots + \varphi(x_s) \end{array}$$

is well-defined. The F_s-homomorphism φ is an *F_s-isomorphism* if it is invertible and the inverse φ^{-1} is also an F_s-homomorphism; in other words, when both the maps φ and ψ are invertible. (In particular, *F_1-isomorphism* is a synonym to *bijection*.)

It is easy to find an F_s-isomorphism not induced by a group-theoretic homomorphism $A \to B$. A typical example is the map

$$\begin{array}{rcl} \{0, a, \ldots, (k-1)a\} & \to & \{0, \ldots, k-1\}, \\ xa & \mapsto & x, \end{array}$$

where a generates an additive cyclic group of order $p > (k-1)s$.

A *generalized arithmetical progression* (further *progression*) of rank m in an abelian group A is a set of the form

$$P = P(x_0; x_1, \ldots, x_m; b_1, \ldots, b_m) = \{x_0 + \beta_1 x_1 + \cdots + \beta_m x_m \ : \ \beta_i = 0, \ldots, b_i - 1\},$$

where $x_0, \dots, x_m$ are elements of the group and $b_1, \dots, b_m$ positive integers. We say that P is an *F_s-progression* if the map

$$\begin{array}{rcl} \{0, \dots, b_1 - 1\} \times \cdots \times \{0, \dots, b_m - 1\} & \to & P, \\ (\beta_1, \dots, \beta_m) & \mapsto & x_0 + \beta_1 x_1 + \cdots + \beta_m x_m, \end{array} \tag{1.1}$$

is an F_s-isomorphism. In particular, each F_s-progression is also an $F_{s'}$-progression for any $s' \le s$, and P is an F_1-progression if and only if $|P| = b_1 \cdots b_m$.

Now we are ready to formulate the Main Theorem[1].

***Theorem 1.2* (the Main Theorem).** — *Let σ be a positive real number, s a positive integer, and K a subset of a torsion-free abelian group such that*

$$k := |K| > k_0(\sigma) := \frac{\lfloor \sigma \rfloor \lfloor \sigma + 1 \rfloor}{2(\lfloor \sigma + 1 \rfloor - \sigma)}$$

and

$$|K + K| \le \sigma k.$$

Then K is a subset of an F_s-progression P of rank $m \le \lfloor \sigma - 1 \rfloor$ and cardinality

$$|P| \le c_{11}(\sigma, s) k. \tag{1.2}$$

It must be pointed out that, unlike Proposition 1.1, this theorem has only very few known analogues for other types of groups, all of them being more or less direct consequences of the Main Theorem; see Chapter 3 of Freiman's book **[12]**.

We also suggest the following more precise version of the Main Theorem, asserting that at most $\lfloor \log_2 \sigma \rfloor$ dimensions of the progression P can be "large"; the others are bounded by a constant, depending on σ.

Theorem 1.3. — *Assuming the hypothesis of Theorem 1.2, write the F_s-progression P as $P(x_0; x_1, \dots, x_m; b_1, \dots, b_m)$, where $b_1 \ge \cdots \ge b_m$. Then*

$$b_i \le c_{12}(\sigma, s) \quad (i > \lfloor \log_2 \sigma \rfloor). \tag{1.3}$$

(See Subsection 5.5, where Theorem 1.3 is derived from Theorem 1.2.)

The quantitative estimates for the constants involve the function $fr(n, \varepsilon)$, defined in Subsection 5.3. We obtain the estimates

$$c_{11}(\sigma, s) \le (2c_{13}(\sigma)s)^{\sigma^{30\sigma} c_{13}(\sigma)}, \quad c_{12}(\sigma, s) \le 2c_{11}(\sigma, s') fr\left(\lfloor \log_2 \sigma \rfloor + 1, \varepsilon_0\right),$$

where

$$c_{13}(\sigma) = fr\left(\lceil 8\sigma \log(2\sigma) \rceil, 1\right), \quad \varepsilon_0 = \lfloor \log_2 \sigma \rfloor + 1 - \log_2 \sigma, \quad s' = \min(s, 2).$$

At present, only a very poor estimate is known (see Subsection 5.3):

$$fr(n, \varepsilon) \le \left(2 + \varepsilon^{-1}\right)^{\exp \exp n}.$$

Therefore we have only

$$c_{11} \le (2s)^{\exp \exp \exp(9\sigma \log(2\sigma))}. \tag{1.4}$$

---

[1] With a few exceptions, we write explicit constants as c_{ij}, where i is the number of the section where the constant is defined, and j is the number of the constant in Section i.

Freiman published two expositions **[12, 13]** of his proof. Recently a new proof of Freiman's theorem, simpler and more transparent than the original, was found by Ruzsa **[30]**. Ruzsa's argument implies the estimate $c_{11} \leq (2s)^{\exp(\sigma^c)}$, which is better than (1.4) (here c is an absolute constant). In the final section we briefly review the main points of Ruzsa's proof. A detailed self-contained exposition of Ruzsa's proof is given in **[26**, Chapter 8]

Our exposition is based on the same principles as Freiman's original proof **[12, 13]**, though the technical details are different. The most substantial innovations are in Subsection 5.1, where we suggest a simpler proof of the Cube Lemma, and in Subsection 8.3, where we apply the Bombieri–Vaaler theorem instead of Freiman's sophisticated elementary argument. We believe that the original argument of Freiman is still of great interest, even after Ruzsa's work.

We tried to make the exposition self-contained. Only three standard results from the Geometry of Numbers, namely, the theorems of Minkowski, Mahler and Bombieri-Vaaler, are quoted without proofs (but with exact references). The other auxiliary facts are provided with complete proofs even if they are available in the literature.

In Section 2 we introduce the notation used throughout the paper. In Sections 3 and 4 we reduce the Main Theorem to certain more technical statements. At the end of Section 4 we give a plan of the remaining part of the article.

Acknowledgments. Gregory Freiman drew my attention to his theorem. Daniel Berend and Henrietta Dickinson read the drafts of the paper at different stages of its preparation and made a number of valuable remarks. Peter Pleasants sent me his unpublished notes on Freiman's theorem and Mel Nathanson put at my disposal a preliminary version of his book **[26]**. It is a pleasure to thank all of them.

My special gratitude is to Imre Ruzsa, who carefully studied the (pre)final version of this paper. I found his numerous comments and suggestions very useful. Many thanks for the hard job he has done.

The main part of this job was done in Bordeaux and was supported by the *Bourse Chateaubriand du gouvernement français.* I am grateful to Prof. J.-M. Deshouillers, Mrs D. Cooke and Mrs F. Duquesnoy for having done their best to make my work in Bordeaux pleasant and successful.

I must also acknowledge support of IMPA (Rio de Janeiro), Forschungsinstitut für Mathematik (ETH Zürich) and Lise Meitner Fellowship (Austria), during the final stage of my work on this paper.

2. Notation and conventions

For $B, C \subseteq \mathbb{R}^n$ and $\alpha \in \mathbb{R}$ put

$$B \pm C = \{b \pm c : b \in B, c \in C\}, \quad \alpha B = \{\alpha b : b \in B\},$$

etc.

A *plane* $\mathcal{L} \subseteq \mathbb{R}^n$ is a set of the form $v + \mathcal{L}'$, where $v \in \mathbb{R}^n$ and $\mathcal{L}'$ is a linear subspace of $\mathbb{R}^n$. By (x, y) we denote the standard inner product in $\mathbb{R}^n$. The Lebesgue measure in $\mathbb{R}^n$ is referred to as *volume* and is denoted by Vol or Vol_n. The standard

inner product on $\mathbb{R}^n$ induces an inner product on each subspace, and hence it induces a d-dimensional Lebesgue measure on each d-dimensional plane $\mathcal{L}$. This measure is referred to as *$\mathcal{L}$-volume*, and is denoted by $\mathrm{Vol}_{\mathcal{L}}$, or Vol_d, or simply Vol.

Given a set $S \subset \mathbb{R}^n$, we denote by $\mathcal{L}(S)$ the plain spanned by S. We put $\dim S = \dim \mathcal{L}(S)$, and call it *linear dimension* (or simply *dimension*) of S. The orthogonal complement to the set S is denoted by $S^{\perp}$:

$$S^{\perp} = \{x \in \mathbb{R}^n \,:\, (x,y) = 0 \text{ for all } y \in S\}.$$

Let $\mathcal{L}$ be a subspace of $\mathbb{R}^n$. A *lattice* in $\mathcal{L}$ is a maximal discrete subgroup of $\mathcal{L}$. The $\mathcal{L}$-volume of a fundamental domain of a lattice Γ is denoted by $\Delta(\Gamma)$.

A *convex body* in $\mathcal{L}$ is a bounded convex subset of $\mathcal{L}$ having inner points. A convex body is *symmetric* if it is symmetric with respect to the origin. Given a lattice Γ and a symmetric convex body B in $\mathcal{L}$, we say that B is *Γ-thick* if $\mathcal{L}(B \cap \Gamma) = \mathcal{L}$; in words, if the set $B \cap \Gamma$ generate $\mathcal{L}$ as a vector space.

When $\mathcal{L} = \mathbb{R}^n$ and $\Gamma = \mathbb{Z}^n$, we shall simply say *thick* instead of *$\mathbb{Z}^n$-thick*. Thus, a symmetric convex body $B \subseteq \mathbb{R}^n$ is *thick* if $\dim B \cap \mathbb{Z}^n = n$, where dim is the *linear dimension* defined above.

Let B be a symmetric convex body. The norm associated with B is $||x||_B := \inf\{\lambda^{-1} \,:\, \lambda x \in B\}$. Recall the following result of Mahler (see [**5**, Chapter VIII, Corollary of Theorem VII]).

***Lemma 2.1* (Mahler).** — *Let B be a symmetric convex body in $\mathbb{R}^n$. Then there exists a basis $e_1, \dots, e_n$ of $\mathbb{Z}^n$ such that*

$$\begin{aligned} ||e_1||_B &\leq \lambda_1, \\ ||e_i||_B &\leq i\lambda_i/2 \quad (2 \leq i \leq n), \end{aligned}$$

where $\lambda_1, \dots, \lambda_n$ are the successive minima of B with respect to the lattice $\mathbb{Z}^n$.

(Such a basis will be called a *Mahler basis* of the body B.)

We denote by $||x||$ the Euclidean norm of the vector $x = (x_1, \dots, x_r) \in \mathbb{R}^n$, and by $||x||_\infty$ its l_∞-norm, i.e.

$$||x|| = \sqrt{(x,x)} = \sqrt{x_1^2 + \dots + x_n^2}, \qquad ||x||_\infty = \max_{1 \leq i \leq n} |x_i|.$$

Finally, given $x \in \mathbb{R}$, we denote by $\lfloor x \rfloor$ (respectively, $\lceil x \rceil$) the maximal integer not exceeding x (respectively, the minimal integer not exceeded by x).

3. A geometric formulation of the Main Theorem

In this section we reformulate the Main Theorem and prove that the new formulation implies the one from the Introduction.

First of all, since K is a finite subset of of a torsion-free abelian group, we may assume that $K \subset \mathbb{Z}^n$ for some natural n.

Further, an F_s-progression may be defined as a set which is F_s-isomorphic to $B \cap \mathbb{Z}^m$, where $B = [0, b_1) \times \dots \times [0, b_m)$. However, it is more convenient to work with less particular convex bodies than rectangular parallelepipeds. Moreover, since we

apply the Geometry of Numbers, it will be preferable to deal with symmetric convex bodies. Therefore we shall assume that $0 \in K$, which does not effect the generality.

Finally, let $\varphi\colon \mathbb{Z}^m \to \mathbb{Z}^n$ be a (group-theoretic) homomorphism. Instead of the condition

(*) φ induces an F_s-isomorphism on the set $B \cap \mathbb{Z}^m$

we prefer a slightly stronger condition

(**) the restriction $\varphi|_{sB\cap\mathbb{Z}^m}$ is one-to-one.

(Actually, (*) and (**) are equivalent if B is the convex hull of its integer points.)

According to the previous paragraphs, we formulate the following theorem.

Theorem 3.1. — *Let K be a finite subset of $\mathbb{Z}^n$ of cardinality $k > k_0(\sigma)$, containing the origin, and satisfying $|K+K| \le \sigma k$. Then for any $T \ge 2$ there exist a positive integer m, a thick symmetric convex body $B \subset \mathbb{R}^m$ and a homomorphism $\varphi\colon \mathbb{Z}^m \to \mathbb{Z}^n$ with the following properties:*

(i) $m \le \lfloor \sigma - 1 \rfloor$;
(ii) $\varphi(B \cap \mathbb{Z}^m) \supseteq K$;
(iii) *the restriction $\varphi|_{TB\cap\mathbb{Z}^m}$ is one-to-one;*
(iv) $\operatorname{Vol} B \le c_{31}(\sigma,T)k$, *where* $c_{31}(\sigma,T) = (c_{13}T)^{\sigma^{25\sigma}c_{13}}$.

Proof of Theorem 1.2 (assuming Theorem 3.1). — If $m = 1$, then $\varphi(B \cap \mathbb{Z})$ is an arithmetical progression of length not exceeding $2c_{31}(\sigma,T)k + 1$, which is less than $c_{11}k$ if $T = 2$.

Now assume that $m \ge 2$. Let $e_1, \dots, e_m$ be a Mahler basis of the body B. Put $\rho_i = \|e_i\|_B$ and define a new norm on $\mathbb{R}^m$:

$$\|x\|_\rho = \max_{1\le i\le m} \rho_i |x_i|,$$

where $x = x_1e_1 + \cdots + x_me_m$. It is a general property of norms in finite dimensional spaces that

$$\|x\|_B \ll \|x\|_\rho \ll \|x\|_B, \tag{3.1}$$

where the implicit constants may *a priori* depend on B. We shall now prove the inequalities (3.1) with constants depending only on the dimension m.

The inequality on the left is easy:

$$\|x\|_B \le |x_1|\|e_1\|_B + \cdots + |x_m|\|e_m\|_B \le m\|x\|_\rho \tag{3.2}$$

The inequality on the right is less trivial. Denote by Δ_i the convex hull of the points $\pm x/\|x\|_B$ and $\pm\rho_j^{-1}e_j$, where $(j \ne i)$. Recall the second inequality of Minkowski [**5**, Chapter VIII, Theorem V]:

$$2^m/m! \le \lambda_1 \cdots \lambda_m \operatorname{Vol} B \le 2^m.$$

Then

$$\operatorname{Vol} B \ge \operatorname{Vol}\Delta_i = \frac{2^m|x_i|\rho_i}{m!\|x\|_B\rho_1\cdots\rho_m} \ge \frac{2^{2m-1}|x_i|\rho_i}{(m!)^2\|x\|_B\lambda_1\cdots\lambda_m} \ge \frac{2^{m-1}}{(m!)^2}\frac{|x_i|\rho_i}{\|x\|_B}\operatorname{Vol} B,$$

whence $|x_i|\rho_i \le c_{32}(m)\|x\|_B$, where $c_{32}(m) = 2^{1-m}(m!)^2$. This proves that

$$\|x\|_\rho \le c_{32}(m)\|x\|_B. \tag{3.3}$$

Now put $R = \{x \in \mathbb{R}^m : \|x\|_\rho \le c_{32}\}$. Then inequalities (3.2) and (3.3) may be rewritten as $B \subseteq R \subseteq mc_{32}B$. Therefore $\varphi(R) \supseteq \varphi(B) \supseteq K$. Further, put $T = smc_{32}$. Then the restriction $\varphi|_{sR\cap\mathbb{Z}^m}$ is one-to-one, whence $P = \varphi(R \cap \mathbb{Z}^m)$ is an F_s-progression.

It remains to estimate the cardinality $|P|$. Since B is thick, we have $\lambda_1 \le \cdots \le \lambda_m \le 1$. Therefore for $1 \le i \le m$ we have $\rho_i \le m/2$ (recall that $m \ge 2$), whence $c_{32}\rho_i^{-1} \ge 1$. Hence

$$|P| = |R \cap \mathbb{Z}^m| = \prod_{i=1}^{m}(2\lfloor c_{32}\rho_i^{-1}\rfloor + 1) \le \frac{(3c_{32})^m}{\rho_1 \cdots \rho_m}. \tag{3.4}$$

Now let $\rho_{i_1} \le \cdots \le \rho_{i_m}$ be the rearrangement of $\rho_1, \ldots, \rho_m$ in increasing order. Then, by the definition of successive minima,

$$\rho_{i_1} \ge \lambda_1, \ldots, \rho_{i_m} \ge \lambda_m,$$

whence

$$\rho_1 \cdots \rho_m \ge \lambda_1 \cdots \lambda_m \ge \frac{2^m}{m!}\frac{1}{\operatorname{Vol} B}.$$

Combining this with (3.4), we obtain finally

$$|P| \le m!\left(\tfrac{3}{2}c_{32}\right)^m \operatorname{Vol} B \le c_{33}k$$

with $c_{33} = m!\left(\frac{3}{2}c_{32}\right)^m c_{31}(\sigma, smc_{32}) \le c_{11}(\sigma, s)$. Thus, the Main Theorem follows from Theorem 3.1. □

4. Iteration step and partial covering

Let K, σ and T be as in Theorem 3.1. We shall deal with triples (m, B, φ), where m is a positive integer, $B \subset \mathbb{R}^m$ is a thick symmetric convex body, and $\varphi : \mathbb{Z}^m \to \mathbb{Z}^n$ is a group homomorphism. *Everywhere in this paper the word "triple" will refer to a triple defined as above, unless the contrary is stated explicitly.* We have to prove that there exists a triple (m, B, φ) satisfying the conditions (i)–(iv) of Theorem 3.1. We construct such a triple iteratively. Namely, we prove

***Proposition 4.1* (the base of iteration).** — *There exist triples (m, B, φ) satisfying the conditions (i)–(iii) of Theorem 3.1.*

(such triples will be called *T-admissible*) and

***Proposition 4.2* (the iteration step).** — *For any T-admissible triple (m, B, φ) there exists another T-admissible triple (m', B', φ') with*

$$\operatorname{Vol} B' \le c_{41}(\sigma, T)\operatorname{Vol} B\,(k/\operatorname{Vol} B)^{1/c_{42}(\sigma)}. \tag{4.1}$$

Here $c_{41} = (c_{13}T)^{\sigma^{20\sigma}c_{13}}$ and $c_{42} = 20\sigma\log(2\sigma)$.

Proof of Theorem 3.1 (assuming Propositions 4.1 and 4.2). — Put

$$V_0 = \inf\{\operatorname{Vol} B \,:\, (m, B, \varphi) \text{ is } T\text{-admissible}\}.$$

Then there exists a T-admissible triple with $\operatorname{Vol} B \leq 2V_0$. By Proposition 4.2

$$c_{41}(\sigma, T)\,(k/\operatorname{Vol} B)^{1/c_{42}(\sigma)} \geq 1/2,$$

whence $\operatorname{Vol} B \leq (2c_{41})^{c_{42}}\, k \leq c_{31} k$. □

Proposition 4.1 is a consequence of the following important lemma of Freiman [**12**, Lemma 1.14].

***Lemma 4.3* (Freiman).** — *Let $K \subset \mathbb{R}^n$ and $\dim K = m$. Then*

$$|K + K| \geq (m+1)k - m(m+1)/2. \tag{4.2}$$

Proof. — Clearly, $k \geq m+1$ and (4.2) is true when $m = 1$ or $k = m+1$. Now fix a pair (m, k) and suppose that (4.2) holds for all pairs (m', k') with $m' < m$ or $m' = m$, $k' < k$. We have to prove (4.2) for the pair (m, k).

Let x be a vertex of the convex polytope spanned by the set K and set $K' = K \setminus x$. There are two possibilities: $\dim K' = m-1$ and $\dim K' = m$.

In the first case

$$\begin{aligned} |K+K| &= |K'+K'| + |K'+x| + 1 \\ &\geq m(k-1) - m(m-1)/2 + k \\ &= (m+1)k - m(m+1)/2. \end{aligned}$$

In the second case let Π be the convex polytope spanned by K'. There is an $(m-1)$-dimensional face of Π with the following property: if $\mathcal{L}$ is the plain containing this face then x and Π lie in distinct half-spaces with the common boundary $\mathcal{L}$. Since $\dim K' \cap \mathcal{L} = m-1$, we have $|K' \cap \mathcal{L}| \geq m$. Then

$$\begin{aligned} |K+K| &\geq |K'+K'| + |K' \cap \mathcal{L} + x| + 1 \\ &\geq (m+1)(k-1) - m(m+1)/2 + m + 1 \\ &= (m+1)k - m(m+1)/2. \end{aligned}$$

□

Remark 4.4. — Ruzsa [**31**] obtained an analogue of this result for the sum of two distinct sets: *if* $\dim(K+L) = m$ *and* $|K| \geq |L|$ *then* $|K+L| \geq |K| + m|L| - m(m+1)/2$. The case $L = -K$ was treated earlier in [**14**]. See also [**34**].

Proof of Proposition 4.1. — Without loss of generality $\dim K = n$. Then, since $k > k_0(\sigma)$, Lemma 4.3 implies that $n \leq \lfloor \sigma - 1 \rfloor$. We conclude the proof, putting $m = n$, letting B be any thick symmetric convex body, containing K, and letting φ be the identical map. □

The proof of Proposition 4.2 is much more complicated. The main difficulties are concentrated in the following *Lemma on Partial Covering.*

***Lemma 4.5* (Partial Covering).** — *Let (m, B, φ) be a 2-admissible triple. Then there exist a subset $K_0 \subset K$ and a triple (m_0, B_0, φ_0) satisfying*

$$|K_0| \geq k/c_{44}(\sigma), \tag{4.3}$$

$$\operatorname{Vol} B_0 \leq c_{45}(\sigma) \operatorname{Vol} B \, (k/\operatorname{Vol} B)^{1/c_{42}(\sigma)}, \tag{4.4}$$

and having the following properties.

(i)' $m_0 \leq c_{46}(\sigma)$;

(ii)' $\varphi_0(B_0 \cap \mathbb{Z}^m) \supseteq K_0 - K_0$.

Here $c_{44} = 2^{9\sigma \log(2\sigma)} c_{13}$, $c_{45} = \exp(33\sigma \log^2(2\sigma))$, $c_{46} = 9\sigma \log(2\sigma)$.

(Intuitively, the triple (m_0, B_0, φ_0) is "not very far" from being admissible).

Note that the statement of the Lemma on Partial Covering does not depend on the parameter T. The dependence on T appears only in Section 9, where we deduce Proposition 4.2 from Lemma 4.5. The deduction involves some computations, but is in fact more or less straightforward. However, the Lemma on Partial Covering itself is a non-trivial combination of several very non-trivial facts. The most important and difficult of the latter is Freiman's 2^n-*theorem*, proved in Section 5. In Section 6 we establish several auxiliary facts, to be used in the proof of the Lemma on Partial Covering. The complete proof of Lemma 4.5 is given in Sections 7-8.

5. Freiman's 2^n-theorem

Lemma 4.3 yields that $|S+S| \geq (n+1-\varepsilon)|S|$ for a sufficiently large n-dimensional set S. However, for such "typical" n-dimensional sets as the set of integer points inside a large cube or ball, one has a stronger inequality $|S+S| \geq 2^n|S|$. In the general case Freiman [**12**, Lemma 2.12] obtained the following result.

***Theorem 5.1* (Freiman).** — *Let S be a finite subset of $\mathbb{R}^n$. Assume that $|S+S| \leq (2^n - \varepsilon)|S|$ for some $\varepsilon > 0$. Then there exists an $(n-1)$-dimensional plane $\mathcal{L}$ such that $|S \cap \mathcal{L}| \geq \delta|S|$, where the positive constant δ depends only on n and ε.*

We apply this remarkable theorem twice. First, in Subsection 5.5 we deduce Theorem 1.3 from Theorem 1.2. Second, the 2^n-theorem plays the key role in the proof of the Lemma on Partial Covering, see Subsection 7.2. (In both cases, instead of Theorem 5.1, we apply a slightly more general Theorem 5.6.)

The presented proof is divided into two steps. First we prove an auxiliary assertion, having some independent interest. We call it *Cube Lemma*. In the second step, which is much simpler, we deduce Theorem 5.1 from the Cube Lemma.

Both steps go back to Freiman's original proof, though they are not specified there explicitly. Our proofs are simpler than Freiman's original, but based on the same ideas.

For another (very long) proof of the 2^n-theorem see [**25**] and [**26**, Chapter 8]. Fishburn [**9**] and Stanchescu [**33**] found new proofs for the case $n = 2$, which give (in this case) better quantitative estimates for δ. Unfortunately, neither Fishburn's nor Stanchescu's argument extends to $n \geq 3$.

5.1. The Cube Lemma. — First we introduce some concepts. An *r-cube* in $\mathbb{R}^n$ is the set

$$\mathcal{C} = \mathcal{C}(b; a_1, \ldots, a_r) = \{b(t) := b + t_1 a_1 + \cdots t_r a_r \ : \ t = (t_1, \ldots, t_r) \in [-1; 1]^r\}.$$

Here $b, a_1, \ldots, a_r \in \mathbb{R}^n$ (we do not assume $a_1, \ldots, a_r$ linearly independent). The point b is the *center* of the r-cube $\mathcal{C}$, and the set $V(\mathcal{C}) := \{b(\alpha) \ : \ \alpha \in \{-1; 1\}^r\}$ is *the set of vertices* of $\mathcal{C}$.

***Lemma 5.2* (the Cube Lemma).** — *Let S be a finite subset of $\mathbb{R}^n$ and assume that*

$$|S + S| \leq \tau |S|. \tag{5.1}$$

Put $\delta_1 = \delta_1(n, \tau) = (3\tau)^{-2^n}$. Then there exists an n-cube $\mathcal{C}$ with $V(\mathcal{C}) \subset S$ such that $|\mathcal{C} \cap S| \geq \delta_1 |S|$.

It turns out to be more convenient to deal with sets symmetric with respect to a point $b \in \mathbb{R}^n$ (that is, for any $u \in S$ there exist $v \in S$ such that $u + v = 2b$).

Proposition 5.3. — *Let S be a finite subset of $\mathbb{R}^n$ satisfying (5.1). Then there is a subset $S_1 \subset S$ of cardinality $|S_1| \geq |S|/\tau$, symmetric with respect to some $b_1 \in \mathbb{R}^n$.*

Proof. — For any $b \in \mathbb{R}^n$ put $S_b = \{u \in S \ : \ 2b - u \in S\}$. By (5.1), there exist at most $\tau |S|$ non-empty sets S_b. Since any $u \in S$ belongs to exactly $|S|$ sets S_b, we have $\sum |S_b| = |S|^2$. Therefore there exists a set S_b of cardinality at least $|S|^2/\tau|S| = |S|/\tau$. □

The Cube Lemma is an easy consequence of Proposition 5.3 and the following assertion.

Proposition 5.4. — *Let S be a finite subset of $\mathbb{R}^n$, symmetric with respect to $b \in \mathbb{R}^n$. Let also $\mathcal{L}$ be a subspace of $\mathbb{R}^n$ of dimension $n - r$, where $1 \leq r \leq n$. Then there exists an r-cube $\mathcal{C}$ with $V(\mathcal{C}) \subset S$, with center in b and such that $|(\mathcal{C} + \mathcal{L}) \cap S| \geq \delta_2 |S|$, where $\delta_2 = \delta_2(r, \tau) = (9\tau)^{-2^{r-1}+1}$.*

Proof. — We use induction in r. Assume first that $r = 1$. For $x \in \mathbb{R}^n$ denote by $\rho(x)$ the (Euclidean) distance from the point $x \in \mathbb{R}^n$ to the plane $b + \mathcal{L}$. Let $b_1 \in S$ satisfy

$$\rho(b_1) = \max_{x \in S} \rho(x).$$

Put $a_1 = b_1 - b$. Then for the 1-cube $\mathcal{C} = \mathcal{C}(b; a_1)$ we have $|(\mathcal{C} + \mathcal{L}) \cap S| = |S| = \delta_2(1, \tau)|S|$.

Now assume that $2 \leq r \leq n$. The argument splits into two cases, depending on how many points from S belong to the plane $b + \mathcal{L}$.

Case 1: $|(b + \mathcal{L}) \cap S| \geq \frac{1}{3}|S|$. — Let a be any element of the set $(b + \mathcal{L}) \cap S$. Then the r-cube $\mathcal{C}(b, a, \ldots, a)$ is as desired, because $1/3 \geq \delta_2(r, \tau)$.

Case 2: $|(b+\mathcal{L})\cap S| \le \frac{1}{3}|S|$. — There exists a subspace $\mathcal{L}'$ of dimension $n-1$ such that $\mathcal{L}\subset\mathcal{L}'$ and

$$(b+\mathcal{L}')\cap S = (b+\mathcal{L})\cap S.$$

At least one of the two open half-spaces with boundary $b+\mathcal{L}'$ contains a subset $S'\subset S$ of cardinality $|S'|\ge\frac{1}{3}|S|$. The set S' need not be symmetric. But since

$$|S'+S'| \le |S+S| \le \tau|S| \le 3\tau|S'|, \tag{5.2}$$

the set S' contains a symmetric subset S_1 of cardinality $|S_1|\ge|S'|/3\tau\ge|S|/9\tau$. As in (5.2), we obtain

$$|S_1+S_1| \le 9\tau^2|S_1|. \tag{5.3}$$

Let b_1 be the center of symmetry of the set S_1. By our construction, $a_1 := b_1 - b \notin \mathcal{L}'$, in particular $a_1\notin\mathcal{L}$. Therefore the subspace $\mathcal{L}_1$, generated by $\mathcal{L}$ and a_1, is of dimension $n-r+1$. By induction, there is an $(r-1)$-cube $\mathcal{C}_1$ with center b_1 such that $V(\mathcal{C}_1)\subset S_1$ and

$$|(\mathcal{C}_1+\mathcal{L}_1)\cap S_1| \ge \delta_2(r-1,9\tau^2)|S_1| \ge \delta_2(r,\tau)|S|. \tag{5.4}$$

Write $\mathcal{C}_1 = \mathcal{C}(b_1,a_2,\dots,a_r)$ and put $\mathcal{C}=\mathcal{C}(b,a_1,\dots,a_r)$. Each vertex of the cube $\mathcal{C}$ is either a vertex of $\mathcal{C}_1$ or is symmetric to a vertex of $\mathcal{C}_1$ with respect to b. Therefore $V(\mathcal{C})\subset S$. We shall prove that

$$|(\mathcal{C}+\mathcal{L})\cap S| \ge |(\mathcal{C}_1+\mathcal{L}_1)\cap S_1|. \tag{5.5}$$

Together with (5.4) this will complete the proof.

Let u belong to the set $\widehat{S}_1 := (\mathcal{C}_1+\mathcal{L}_1)\cap S_1$. Then the point $v=2b_1-u$ also belongs to $\widehat{S}_1$. We shall see that

(∗) *at least one of the points u, v belongs to the set $\widehat{S} := (\mathcal{C}+\mathcal{L})\cap S$.*

Assume (∗) to be true and consider the map

$$\begin{array}{ccc} \widehat{S}_1 & \to & \widehat{S}, \\ u & \mapsto & \begin{cases} u, & \text{if } u\in\widehat{S}, \\ 2b-v, & \text{if } v=2b_1-u\in\widehat{S} \text{ and } u\notin\widehat{S}. \end{cases} \end{array}$$

This map is one-to-one[(2)], whence $|\widehat{S}|\ge|\widehat{S}_1|$, as desired. Thus, it remains to prove the assertion (∗).

So, let u belong to $\widehat{S}_1$ and put $v=2b_1-u$. Then $u=u_1+ta_1+y$ and $v=v_1-ta_1-y$, where $u_1,v_1\in\mathcal{C}_1$ are such that $u_1+v_1=2b_1$, and $y\in\mathcal{L}$. Recall (this is crucial) that, by our construction, the $(r-1)$-cube $\mathcal{C}_1$ and the set $\widehat{S}_1$ belong to the same open half-space with the boundary $b+\mathcal{L}'$. In particular, the points u, v, u_1, v_1 belong to this half-space.

[(2)]Indeed, let u and u' be two distinct elements of $\widehat{S}_1$. If both are in $\widehat{S}$ or both are not in $\widehat{S}$ then their images are obviously distinct. If one of them belongs to $\widehat{S}$ but the other not, then the images lie in the distinct half-spaces with boundary $b+\mathcal{L}'$.

Since $a_1 \notin \mathcal{L}'$, there exists a linear functional $f\colon \mathbb{R}^n \to \mathbb{R}$ vanishing on $\mathcal{L}'$ and positive at a_1. Then the open half-space mentioned above is defined by the inequality $f(x) > f(b)$. Hence

$$f(u) = f(u_1) + tf(a_1) > f(b), \tag{5.6}$$

$$f(v) = f(v_1) - tf(a_1) > f(b), \tag{5.7}$$

$$f(u_1) > f(b), \tag{5.8}$$

$$f(v_1) > f(b). \tag{5.9}$$

Since $u_1 + v_1 = 2b + 2a_1$, the latter two inequalities imply that

$$f(u_1), f(v_1) < f(b) + 2f(a_1).$$

Then (5.6) and (5.7) yield that $-2 < t < 2$.

Obviously, $\mathcal{C} = \{x - \theta a_1 \,:\, x \in \mathcal{C}_1, 0 \le \theta \le 2\}$. Therefore $u \in \mathcal{C} + \mathcal{L}$ if $-2 < t \le 0$ and $v \in \mathcal{C} + \mathcal{L}$ if $0 \le t < 2$. The assertion $(*)$ is proved, which completes the proof of Proposition 5.4. □

Proof of Lemma 5.2. — The case $r = n$ of Proposition 5.4 is exactly the assertion of the Cube Lemma for symmetric sets, $\delta_1(n, \tau)$ being replaced by $\delta_2(n, \tau)$. To establish the Cube Lemma for arbitrary sets, apply Proposition 5.4 to the symmetric set S_1 from Proposition 5.3. As in (5.2), we obtain $|S_1 + S_1| \le \tau^2 |S_1|$. Since $\delta_2(n, \tau^2)/\tau \ge \delta_1(n, \tau)$, Lemma 5.2 follows. □

5.2. Proof of the 2^n-theorem. — Now we are ready to prove Theorem 5.1. For a positive real number δ put $\varepsilon(\delta, n) = 2^n(4n\delta/\delta_1)^\nu$, where $\nu = \delta_1/10n$ and $\delta_1 = \delta_1(n, 2^n)$ is defined in Lemma 5.2.

Let S be a finite subset of $\mathbb{R}^n$ with at most $\delta|S|$ points on every hyperplane. We shall prove that $|S + S| \ge (2^n - \varepsilon)|S|$, where $\varepsilon = \varepsilon(\delta, n)$. Since this is trivial when $\delta \ge \delta_1/4n$, we shall assume that $\delta \le \delta_1/4n$.

Let $\mathcal{C}$ be the n-cube constructed in Lemma 5.2 (where we put $\tau = 2^n$). Since $|\mathcal{C} \cap S| \ge \delta_1|S| > \delta|S|$, we have $\dim \mathcal{C} = n$; in particular, the interior $\mathcal{C}^\circ$ is non-empty. Moreover, since the boundary of $\mathcal{C}$ is contained in a union of $2n$ hyperplanes, we have for the set $S_0 := S \cap \mathcal{C}^\circ$ the estimate

$$|S_0| \ge |S \cap \mathcal{C}| - 2n\delta|S| \ge (\delta_1 - 2n\delta)|S| \ge (\delta_1/2)|S|. \tag{5.10}$$

The $2n$ hyperplanes defined by the faces of the cube $\mathcal{C}$ divide $\mathbb{R}^n \setminus \mathcal{C}^\circ$ into $p := 3^n - 1$ disjoint convex sets. This divides the set $S \setminus S_0$ into p subsets $S_1, \dots, S_p$. We have

$$(S_i + S_i) \cap (S_j + S_j) = \varnothing \quad (0 \le i < j \le p), \tag{5.11}$$

because S_i and S_j are subsets of disjoint convex sets, and by the same reason

$$(S_0 + V) \cap (S_i + S_i) = \varnothing \quad (1 \le i \le p), \tag{5.12}$$

where $V = V(\mathcal{C})$ is the set of the vertices of the cube $\mathcal{C}$. (Recall that $V \subseteq S$ by the definition of the cube $\mathcal{C}$.) Further,

$$|S_0 + V| = |V||S_0| = 2^n|S_0|, \tag{5.13}$$

because all the sums $x+v$, where $x \in \mathcal{C}^\circ$ and $v \in V$, are distinct. Also, since $|S_i| < |S|$ for $i = 1, \dots, p$, we have by induction

$$|S_i + S_i| \geq (2^n - \varepsilon_i)|S_j| \quad (1 \leq i \leq p), \tag{5.14}$$

where $\varepsilon_i = \varepsilon(\delta/\eta_i, n)$ and $\eta_i = |S_i|/|S|$. Now

$$|S+S| \geq |S_0 + V| + \sum_{i=1}^{p} |S_i + S_i| \geq 2^n |S_0| + \sum_{i=1}^{p} (2^n - \varepsilon_i)|S_i| = \left(2^n - \sum_{i=1}^{p} \varepsilon_i \eta_i\right) |S|,$$

and it remains to observe that

$$\sum_{i=1}^{p} \varepsilon_i \eta_i = \varepsilon \sum_{i=1}^{p} \eta_i^{1-\nu} \leq \varepsilon p \left(\frac{1}{p} \sum_{i=1}^{p} \eta_i\right)^{1-\nu} = \varepsilon p^\nu \left(1 - \frac{|S_0|}{|S|}\right)^{1-\nu} \leq \varepsilon e^{\frac{\delta_1}{4}} \left(1 - \frac{\delta_1}{2}\right)^{\frac{1}{2}} \leq \varepsilon.$$

(It is a trivial exercise in calculus to show that the function $e^{x/4}(1-x/2)^{1/2}$ decreases on the interval $[0,1]$.) Theorem 5.1 is proved. □

Remark 5.5. — The argument of this section is a version of Freiman's original, with some modifications due to Ruzsa. Ruzsa also noticed that $\mathbb{R}^n \setminus \mathcal{C}^\circ$ can be divided into $2n$ rather than $3^n - 1$ parts, but this does not affect much the final result.

5.3. The function $fr(n, \varepsilon)$. — Put

$$fr(n,\varepsilon) = \sup_S \min_{\mathcal{L}} \frac{|S|}{|S \cap \mathcal{L}|},$$

where S runs over the finite subsets of $\mathbb{R}^n$ satisfying (5.1) and $\mathcal{L}$ runs over the hyperplanes of $\mathbb{R}^n$. Then $fr(n,\varepsilon) \leq \delta^{-1}$, where δ is from Theorem 5.1. A calculation shows that

$$fr(n,\varepsilon) \leq \left(2 + \varepsilon^{-1}\right)^{\exp\exp n}. \tag{5.15}$$

It would be nice to improve against this extremely weak estimate. Such an improvement would have been possible if Proposition 5.3 were replaced by the following assertion:

Given a finite set $S \subset \mathbb{R}^n$, there exists a symmetric subset $S_1 \subseteq S$ satisfying $|S_1| \geq \tau^{-\alpha}|S|$ and $|S_1 + S_1| \ll \tau |S_1|$. Here α is an absolute constant, and the implied constant is also absolute.

However, Don Coppersmith (private communication) and Imre Ruzsa (private communication) had independently disproved this assertion by similar probabilistic arguments. Moreover, the τ^2-term in (5.3) cannot be replaced even by $\tau^{2-\varepsilon}$, let alone $O(\tau)$. Therefore the estimate (5.15) is probably best possible for the method.

Note in conclusion that Freiman's original argument yields only exponential dependence of $fr(n,\varepsilon)$ in ε^{-1} (when n is fixed). Polynomial dependence in ε^{-1} was achieved due to a suggestion of Ruzsa concerning the argument of Subsection 5.2.

5.4. A generalized 2^n-theorem. — Actually, we need the following simple generalization of Theorem 5.1.

Theorem 5.6. — *Let $1 \leq r \leq n$. Assume that S satisfies (5.1) with $\tau \leq 2^r - \varepsilon$. Put $\delta = (fr(r,\varepsilon))^{-1}$. Then there exists a plane $\mathcal{L} \subset \mathbb{R}^n$ of dimension $\dim \mathcal{L} \leq r-1$ such that $|S \cap \mathcal{L}| \geq \delta |S|$.*

Proof. — For any set $T \subseteq \mathbb{R}^n$ denote by $\mathcal{L}_0(T)$ the subspace of the same dimension, parallel to the plane $\mathcal{L}(T)$. We say that the subspace $\Lambda \subseteq \mathbb{R}^n$ of dimension $n-r$ is *generic* if

$$\dim (\Lambda \cap \mathcal{L}_0(S_1)) = \max(0, \dim \mathcal{L}_0(S_1) - r)$$

for any $S_1 \subseteq (S-S)$. Clearly, generic subspaces exist.

Let Λ be a generic subspace and let $\mathbb{R}^n = \Lambda \oplus \mathrm{M}$. Denote by $\pi \colon \mathbb{R}^n \to \mathrm{M}$ the projection along Λ. For any distinct $u, v \in S$ we have $\pi(u) \neq \pi(v)$, because Λ is generic. Hence the finite set $\pi(S) \subset \mathrm{M}$ satisfies

$$|\pi(S) + \pi(S)| = |\pi(S+S)| \leq |S+S| \leq \tau |S| = \tau |\pi(S)|.$$

Since $\dim \mathrm{M} = r$, we may use Theorem 5.1. Hence for some plane $\mathcal{L}' \subset \mathrm{M}$ of dimension $r-1$ we have $|\mathcal{L}' \cap \pi(S)| \geq \delta |\pi(S)| = \delta |S|$. Put $S_1 = (\mathcal{L}' + \Lambda) \cap S$ and $\mathcal{L} = \mathcal{L}(S_1)$. Then $|S \cap \mathcal{L}| \geq |S_1| \geq \delta |S|$. Since both the subspaces Λ and $\mathcal{L}_0(S_1)$ are parallel to the plane $\mathcal{L}' + \Lambda$ of dimension $n-1$, we have

$$\dim (\Lambda \cap \mathcal{L}_0(S_1)) \geq \dim \mathcal{L}_0(S_1) - r + 1.$$

This is possible only when $\dim \mathcal{L} = \dim \mathcal{L}_0(S_1) \leq r-1$. □

5.5. Proof of Theorem 1.3 (assuming Theorem 1.2). — As the first application of the 2^n-theorem, we show that Theorem 1.3 follows from Theorem 1.2. This is an immediate consequence of the following assertion.

Proposition 5.7. — *Let $P = P(x_0; x_1, \dots, x_m; b_1, \dots, b_m)$ be an F_2-progression with $b_1 \geq \dots \geq b_m$ and let K be a subset of P. Assume that $|P| \leq \alpha k$ and*

$$|K+K| \leq (2^r - \varepsilon) k, \tag{5.16}$$

where $k = |K|$. Then

$$b_i \leq 2\alpha fr(r,\varepsilon) \quad (i \geq r). \tag{5.17}$$

Proof. — Denote by φ the map (1.1). Since φ is an F_2-isomorphism, the set $K' = \varphi^{-1}(K)$ also satisfies (5.16). Put $\delta = (fr(r,\varepsilon))^{-1}$. By Theorem 5.6, there exists a plane $\mathcal{L} \subset \mathbb{R}^m$ of dimension at most $r-1$ such that $|K' \cap \mathcal{L}| \geq \delta k$.

Let now $e_1 = (1,0,\dots,0), \dots, e_m = (0,\dots,0,1)$ be the standard basis of $\mathbb{Z}^m$. Since $\dim \mathcal{L} \leq r-1$, there is an index $j \leq r$ such that the vector e_j is not parallel to the plane $\mathcal{L}$. Then the sets

$$\mu e_j + (K' \cap \mathcal{L}) \quad (0 \leq \mu \leq b_i - 1) \tag{5.18}$$

are pairwise disjoint. On the other hand, all the sets (5.18) are contained in the progression $P' = P(0; e_1, \dots, e_m; b_1, \dots, b_{j-1}, 2b_j, b_{j+1}, b_m)$. Therefore

$$2\alpha k \geq 2|P| = |P'| \geq \sum_{\mu=0}^{b_j-1} |\mu e_j + (K' \cap \mathcal{L})| \geq b_j \delta k,$$

whence $b_j \leq 2\alpha\delta^{-1}$. Since $j \leq r$ and $b_1 \geq \cdots \geq b_m$, we obtain (5.17). □

6. Some lemmas

In this section we prove some auxiliary facts, which, together with Theorem 5.6, will be used the proof of the Lemma on Partial Covering.

Lemma 6.1. — *Let $\gamma_1, \dots, \gamma_k$ be real numbers, and for any $\beta \in \mathbb{R}$ let $k(\beta) = k(\beta; \gamma_1, \dots, \gamma_k)$ be the number of indices j satisfying $0 \leq \gamma_j - \beta < 1/2 \pmod 1$. Assume that*

$$\left| \sum_{j=1}^{k} e^{2\pi i \gamma_j} \right| \geq \delta k$$

Then $k(\beta) \geq (1+\delta)k/2$ for some $\beta \in [0, 1)$.

Remark 6.2. — This result is due to Freiman [**11**]. A simpler proof was suggested by Postnikova [**27**] and reproduced in [**12**, Lemma 2.2]. We follow this argument with slight modifications.

Proof. — Since $k(\beta)$ is periodic with period 1, it is sufficient to find $\beta \in \mathbb{R}$ with the required property. Also, $k(\beta; \gamma_1, \dots, \gamma_k) = k(\beta + \gamma; \gamma_1 + \gamma, \dots, \gamma_k + \gamma)$ for any real γ. Therefore, replacing each γ_i by $\gamma_i + \gamma$, with a suitable $\gamma \in \mathbb{R}$, we may assume that

$$\left| \sum_{j=1}^{k} e^{2\pi i \gamma_j} \right| = \sum_{j=1}^{k} e^{2\pi i \gamma_j} = \sum_{j=1}^{k} \cos 2\pi\gamma_j. \tag{6.1}$$

For $0 \leq x \leq 1$ let $F(x)$ be the number of indices j such that $0 \leq \gamma_j < x \pmod 1$. Then for $0 \leq \beta \leq 1/2$ we have $k(\beta) = F(\beta + 1/2) - F(\beta)$.

Assume that $k(\beta) < (1+\delta)k/2$ for all $\beta \in [0, 1)$. Then $k(\beta) > \frac{1}{2}(1-\delta)k$ for all $\beta \in [0, 1)$. Estimate now the last sum in (6.1):

$$\begin{aligned} \sum_{j=1}^{k} \cos 2\pi\gamma_j = \int_0^1 \cos 2\pi x \, dF(x) &= F(x) \cos 2\pi x \Big|_0^1 + 2\pi \int_0^1 F(x) \sin 2\pi x \, dx \\ &= k + 2\pi \int_0^1 F(x) \sin 2\pi x \, dx. \end{aligned} \tag{6.2}$$

For the last integral we have

$$\begin{aligned}\int_0^1 F(x)\sin 2\pi x dx &= -\int_0^{1/2}(F(x+1/2)-F(x))\sin 2\pi x dx \\ &= -\int_0^{1/2} k(x)\sin 2\pi x dx \\ &< -\frac{1}{2}(1-\delta)k\int_0^{1/2}\sin 2\pi x dx \\ &= -(2\pi)^{-1}(1-\delta)k.\end{aligned}$$

Substituting this into (6.2), we obtain $\sum_{j=1}^{k}\cos 2\pi\gamma_j < \delta k$, a contradiction. □

Lemma 6.3. — *Let K be a finite set of k elements with $K_1,\dots,K_r \subset K$ satisfying*

$$|K_i| \geq (1+\delta)k/2 \quad (1 \leq i \leq r),$$

where $0 < \delta < 1/2$. For $\alpha = (\alpha_1,\dots,\alpha_r) \in \{0,1\}^r$ put $S_\alpha = \bigcap_{i=1}^r K_i^{\alpha_i}$, where $K_i^1 = K_i$ and $K_i^0 = K\backslash K_i$. Then there exists $\alpha \in \{0,1\}^r$ such that

$$|S_\alpha| \geq (\gamma/2)^r k, \tag{6.3}$$

where $\gamma = (1+\delta)^{(1+\delta)/2}(1-\delta)^{(1-\delta)/2}$.

Remark 6.4. — Note that $\gamma > 1$, and, moreover,

$$\gamma = \exp\left(\sum_{i=1}^{\infty}\frac{\delta^{2i}}{2i(2i-1)}\right) \geq e^{\delta^2/2}.$$

This lemma is also due to Freiman [F1, Lemma 2.11]. He used a probabilistic method, and his result was slightly weaker, with an additional factor $c(\delta)r^{-1/2}$ in the right-hand side of (6.3). The following elegant argument was suggested by Ruzsa (private communication).

Proof. — For $\alpha \in \{0,1\}^r$ write $|\alpha| = \alpha_1 + \cdots + \alpha_r$. Notice that

$$\sum |S_\alpha| = k, \quad \sum |\alpha||S_\alpha| = |K_i| + \cdots + |K_r| \geq (1+\delta)kr/2, \tag{6.4}$$

where here and below the summation extends to $\alpha \in \{0,1\}^r$.

Let z be a positive real number, to be specified later. Using (6.4) and the weighted arithmetic and geometric mean inequality[(3)], we obtain:

$$\sum z^{|\alpha|}|S_\alpha| \geq kz^{(1/k)\sum|\alpha||S_\alpha|} \geq kz^{(1+\delta)r/2}.$$

On the other hand, $\sum z^{|\alpha|} = (1+z)^r$, whence

$$\max|S_\alpha| \geq k\left(z^{(1+\delta)/2}/(1+z)\right)^r.$$

[(3)]That is, the inequality $a_1b_1 + \cdots + a_nb_n \geq a_1^{b_1}\cdots a_n^{b_n}$, where $a_n,\dots,a_n$ are positive real numbers and $b_1,\dots,b_n$ non-negative real numbers satisfying $b_1 + \cdots + b_n = 1$. It is an immediate consequence of the Jensen inequality for the logarithm.

The optimal choice $z = (1+\delta)/(1-\delta)$ leads to $\max |S_\alpha| \geq k(\gamma/2)^r$. □

In the next two lemmas we state elementary geometric properties of convex bodies.

Lemma 6.5. — *Let $B \subset R^n$ be a convex body. Suppose that its closure $\bar{B}$ contains an n-dimensional ball of radius ρ. Then for any measurable $B_1 \subseteq B$*

$$\mathrm{Vol}_d(B_1) \leq \frac{n!}{d!\rho^{n-d}} \mathrm{Vol}_n(B), \tag{6.5}$$

where $d = \dim(B_1)$.

Proof. — We use induction in $n-d$. When $n-d=0$, the assertion is trivial. Now suppose that $d \leq n-1$. Let Ω be an n-dimensional ball of radius ρ, contained in $\bar{B}$. Then there exists a point $x \in \Omega$ such that the distance between x and $\mathcal{L}(B_1)$ is $\delta \geq \rho$. Put

$$B_2 = \{xt + b(1-t) \,:\, b \in B_1, t \in [0;1]\}.$$

Then $\dim B_2 = d+1$ and by induction

$$\mathrm{Vol}_{d+1}(B_2) \leq \frac{n!}{(d+1)!\rho^{n-d-1}} \mathrm{Vol}_n(B).$$

On the other hand,

$$\mathrm{Vol}_{d+1}(B_2) = \frac{\delta}{d+1} \mathrm{Vol}_d(B_1),$$

which proves (6.5). □

Lemma 6.6. — *Let $w \in \mathbb{R}^n$ be a non-zero vector, $\mathcal{W} = w^\perp$ and $\pi\colon \mathbb{R}^n \to \mathcal{W}$ the orthogonal projection. Then for any symmetric convex body B we have*

$$\mathrm{Vol}_{n-1}(\pi(B)) \leq \frac{n}{2} \frac{\|w\|_B}{\|w\|} \mathrm{Vol}_n(B). \tag{6.6}$$

Proof. — We shall prove the following more general statement.

Let $\mathcal{L}$ be a subspace of $\mathbb{R}^n$ and $\mathcal{W} = \mathcal{L}^\perp$. Denote by $\pi\colon \mathbb{R}^n \to \mathcal{W}$ the orthogonal projection. Then for any symmetric convex body B we have

$$\mathrm{Vol}_m(\pi(B)) \cdot \mathrm{Vol}_l(B \cap \mathcal{L}) \leq \binom{n}{l} \mathrm{Vol}_n(B), \tag{6.7}$$

where $l = \dim \mathcal{L}$, $m = n - l = \dim \mathcal{W}$.

Let $\mathcal{L}$ be the one-dimensional subspace generated by the vector w. Then $\mathrm{Vol}_1(\mathcal{L} \cap B) = 2\|w\|/\|w\|_B$. Therefore inequality (6.6) is the case $l = 1$ of inequality (6.7).

Proof of (6.7). — Let S_{m-1} be the unit sphere in $\mathcal{W}$. For any $x \in S_{m-1}$ let $L(x)$ be the $(l+1)$-dimensional half-plane containing x and having $\mathcal{L}$ as the boundary. Put

$$\begin{aligned} r(x) &= \sup\{r > 0 : rx \in \pi(B)\}, \\ B(x) &= L(x) \cap B, \\ h(x,r) &= \mathrm{Vol}_l(\pi^{-1}(rx) \cap B). \end{aligned}$$

Then

$$\mathrm{Vol}_m(\pi(B)) = \frac{1}{m} \int_{S_{m-1}} r^m(x) dx, \tag{6.8}$$

$$\mathrm{Vol}_n(B) = \int_{S_{m-1}} dx \int_0^{r(x)} r^{m-1} h(x,r) dr. \tag{6.9}$$

Note that $B(x) \supset (B \cap \mathcal{L})$ and $B(x) \cap \pi^{-1}(xr(x)) \neq \varnothing$. Hence

$$h(x,r) \geq \left(\frac{r(x) - r}{r(x)} \right)^l \mathrm{Vol}_l(\mathcal{L} \cap B). \tag{6.10}$$

Combining (6.8)–(6.10) with the well-known equality

$$\int_0^1 t^{m-1}(1-t)^l dt = \frac{(m-1)!l!}{(m+l)!},$$

we obtain (6.7). The lemma is proved. □

Now let B be a symmetric convex body, $X \geq 1$ and $C > 0$.

Definition 6.7. — *The system of vectors $a_1, \dots, a_r \in \mathbb{R}^n$ is (B, X, C)-*badly approximable *if for any $x \in \mathbb{Z}^n$ and $y = (y_1, \dots, y_r) \in \mathbb{Z}^r$ satisfying*

$$\|x\|_\infty \leq X, \quad 0 < \|y\|_\infty \leq X, \tag{6.11}$$

we have

$$\|y_1 a_1 + \dots + y_r a_r - x\|_B \geq C.$$

Lemma 6.8. — *Let $M_1, \dots, M_r \subseteq \mathbb{R}^n$ be measurable sets, and assume that*

$$\mathrm{Vol}\, M_i > 6^n 3^i X^{n+i} C^n \,\mathrm{Vol}\, B.$$

Then there exists a (B, X, C)-badly approximable system $a_1, \dots, a_r$ such that $a_1 \in M_1, \dots, a_r \in M_r$.

Proof. — Use induction in r. Let $r \geq 1$, and suppose that $a_1, \dots, a_{r-1}$ form a badly approximable system. Estimate the volume of the set

$$M = \{a_r \in \mathbb{R}^n : a_1, \dots, a_{r-1}, a_r \text{ is not a badly approximable system}\}.$$

By definition, $a_r \in M$ if and only if there exists x, y satisfying (6.11) and

$$\|y_1 a_1 + \dots + y_{r-1} a_{r-1} + y_r a_r - x\|_B < C. \tag{6.12}$$

Since $a_1, \dots, a_{r-1}$ is a badly approximable system, we have $y_r \neq 0$. Therefore

$$M = \bigcup_{\substack{\|x\|_\infty, \|y\|_\infty \leq X \\ y_r \neq 0}} M(x,y)$$

where $M(x,y) = \{a_r \in \mathbb{R}^n : \text{(6.12) is true}\}$. We have trivially

$$\operatorname{Vol} M(x,y) = \frac{(2C)^n \operatorname{Vol} B}{|y_r|} \leq (2C)^n \operatorname{Vol} B.$$

whence

$$\begin{aligned} \operatorname{Vol} M &\leq \sum_{\substack{\|x\|_\infty, \|y\|_\infty \leq X \\ y_r \neq 0}} \operatorname{Vol} M(x,y) \\ &\leq (2X+1)^{n+r-1} \cdot 2X \cdot (2C)^n \operatorname{Vol} B \\ &\leq 6^n 3^r X^{n+r} C^n \operatorname{Vol} B \\ &< \operatorname{Vol} M_r. \end{aligned}$$

Therefore we can choose $a_r \in M_r \backslash M$, which proves the lemma. □

For the next lemma we have to define the determinant of the linear map $\varphi\colon \mathcal{L} \to \mathbb{R}^n$, where $\mathcal{L}$ is a subspace of $\mathbb{R}^n$. We put $\det \varphi = 0$ if $\dim \varphi(\mathcal{L}) < \dim \mathcal{L}$. If $\dim \varphi(\mathcal{L}) = \dim \mathcal{L}$, choose orthogonal bases in both $\mathcal{L}$ and $\varphi(\mathcal{L})$ (with respect to the standard inner product in $\mathbb{R}^n$), and let $\det \varphi$ be the determinant of the matrix of φ with respect to these bases (clearly, $\det \varphi$ is independent of the choice of bases).

Lemma 6.9. — *Let $\mathcal{W}$ and $\mathcal{L}$ be proper subspaces of $\mathbb{R}^n$, the subspace $\mathcal{W}$ being of dimension $n-1$. Let w be a non-zero vector orthogonal to $\mathcal{W}$ and l a non-zero vector, orthogonal to $\mathcal{L}$. Denote by $\pi\colon \mathbb{R}^n \to \mathcal{W}$ the orthogonal projection. Then*

$$|\det \pi|_{\mathcal{L}}| \geq \frac{|(w,l)|}{\|w\| \cdot \|l\|}. \tag{6.13}$$

(Here $\pi|_{\mathcal{L}}$ is the restriction of π on $\mathcal{L}$.)

Proof. — Without loss of generality, $\|l\| = \|w\| = 1$. We may also assume that $\mathcal{L} \not\subset \mathcal{W}$, since otherwise $\pi|_{\mathcal{L}}$ is the identity map, and (6.13) follows from the Cauchy-Schwarz inequality.

Let $e_1, \dots, e_{d-1}$ be an orthonormal basis of the subspace $\mathcal{L} \cap \mathcal{W}$. Complete it to orthonormal bases $e_1, \dots, e_{d-1}, e_d$ and $e_1, \dots, e_{d-1}, e'_d$ of the subspaces $\mathcal{L}$ and $\pi(\mathcal{L})$, respectively. The matrix of the linear map $\pi|_{\mathcal{L}}$ in these bases is

$$\operatorname{diag}\left(1, \dots, 1, \pm\sqrt{1-(e_d,w)^2}\right)$$

(here the sign of the square root depends on the directions of the vectors e_d and e'_d). Therefore $|\det \pi|_{\mathcal{L}}| = \sqrt{1-(e_d,w)^2}$. But $(e_d,w)^2 + (l,w)^2 \leq \|w\|^2 = 1$ by Bessel's inequality, whence $|\det \pi|_{\mathcal{L}}| \geq |(w,l)|$, as wanted. □

Our final lemma is a well-known result of Bombieri and Vaaler [**3**, Theorem 1].

Lemma 6.10. — *Let $\mathcal{L}$ be a proper subspace of $\mathbb{R}^n$ such that $\Gamma = \mathcal{L} \cap \mathbb{Z}^n$ is a lattice in $\mathcal{L}$. Then there exists a non-zero vector $l \in \mathcal{L}^\perp \cap \mathbb{Z}^n$ such that $\|l\|_\infty \leq \Delta(\Gamma)$.*

□

7. Proof of the Lemma on Partial Covering: constructing the triple (m_0, B_0, φ_0)

In this and the next section we prove the Lemma on Partial Covering. Thus, until the end of Section 9 we fix a 2-admissible triple (m, B, φ). If $\operatorname{Vol} B \leq c_{45}(\sigma)^{c_{42}(\sigma)}k$, then (4.4) holds with $B_0 = B$, and the assertion of Lemma 4.5 becomes trivial. Therefore we may assume that

$$\operatorname{Vol} B \geq c_{45}(\sigma)^{c_{42}(\sigma)}k \geq \exp(600\sigma^2)k. \tag{7.1}$$

Fix a Mahler basis $e_1, \dots, e_m$ of the body B (see Lemma 2.1). Since B is thick, we have

$$\|e_i\|_B \leq \max(1, i/2) \quad (1 \leq i \leq m). \tag{7.2}$$

We shall assume that this basis is orthonormal, redefining the inner product if necessary.

Put $K' = \varphi^{-1}(K)$. Since our triple is 2-admissible, the restriction $\varphi|_{K'} : K' \to K$ is an F_2-isomorphism. Therefore

$$|K'| = k, \quad |K' + K'| = |K + K| \leq \sigma k.$$

7.1. Freiman's map. — Let r be a positive integer, $a_1, \dots, a_r \in [0,1)^m$ and $b_1, \dots, b_r \in [0,1)$. Define *Freiman's map*

$$\begin{array}{rcl} \Phi\colon \mathbb{Z}^m & \to & \mathbb{Z}^{m+r} \\ x = (x_1, \dots, x_m) & \mapsto & (x_1, \dots, x_m, \lfloor (a_1, x) - b_1 \rfloor, \dots, \lfloor (a_r, x) - b_r \rfloor). \end{array}$$

The map Φ is one-to-one, but it does not induce an F_2-isomorphism $\mathbb{Z}^m \to \Phi(\mathbb{Z}^m)$. However, if for any $\alpha = (\alpha_1, \dots, \alpha_r) \in \{0;1\}^r$ we put

$$\begin{array}{rcl} Z_\alpha & = & \{x \in \mathbb{Z}^m : \ \alpha_i/2 \leq (x, a_i) - b_i < (\alpha_i + 1)/2 \ (\mathrm{mod}1) \quad \text{for} \ \ 1 \leq i \leq m\}, \\ S_\alpha & = & K' \cap Z_\alpha, \end{array} \tag{7.3}$$

then we obtain the following statement.

Proposition 7.1. — *For any $\alpha \in \{0,1\}^r$ the map $\Phi\colon Z_\alpha \to \Phi(Z_\alpha)$ is an F_2-isomorphism. In particular,*

$$|\Phi(S_\alpha)| = |S_\alpha|, \quad |\Phi(S_\alpha) + \Phi(S_\alpha)| = |S_\alpha + S_\alpha|. \tag{7.4}$$

Proof. — Trivial. □

We put $K'' = \Phi(K')$.

7.2. Distorting vectors. — Fix $\delta > 0$, to be specified later. We say that vector $a \in [0,1)^m$ is *δ-distorting* (or shortly, *distorting*) if

$$\left| \sum_{x \in K'} e^{2\pi i (a,x)} \right| > \delta k.$$

This definition is motivated by Lemma 6.1. Applying this lemma in our situation, we obtain the following assertion.

Proposition 7.2. — *For any δ-distorting vector $a \in [0,1)^m$ there exist $b \in [0,1)$ such that*

$$|\{x \in K' : 0 \le (a,x) - b < 1/2 \pmod 1\}| \ge (1+\delta)k/2. \tag{7.5}$$

Return to the construction of Subsection 7.1. We did not yet impose any restrictions on a_i and b_i. Let now all the vectors $a_1, \dots, a_r$ be δ-distorting, and for each a_i let b_i be the b from Proposition 7.2.

Now Lemma 6.3 shows how "small" distortions in (7.5) (where we have $(1+\delta)k/2$ instead of the expected $k/2$) can be combined to obtain "substantial" distortion for one of the sets S_α in (7.3). Applying it, we obtain the following:

Proposition 7.3. — *For any positive integer r there exists $\alpha \in \{0,1\}^r$ such that $|S_\alpha| \ge (\gamma/2)^r k$, where $\gamma = (1+\delta)^{(1+\delta)/2}(1-\delta)^{(1-\delta)/2} \ge e^{\delta^2/2}$.*

Now specify

$$\delta = 1/2\sqrt{\sigma}, \quad r = \lceil 2\delta^{-2} \log(2\sigma) \rceil = \lceil 8\sigma \log(2\sigma) \rceil.$$

(Our choice of δ will be motivated in Subsection 8.1.) Then $|S_\alpha| \ge 2^{1-r}\sigma k$, whence

$$|S_\alpha + S_\alpha| \le |K' + K'| \le \sigma k \le 2^{r-1}|S_\alpha|,$$

and by (7.4)

$$|\Phi(S_\alpha) + \Phi(S_\alpha)| \le 2^{r-1}|\Phi(S_\alpha)| \le (2^r - 1)|\Phi(S_\alpha)|.$$

Now it is the time to apply the 2^n-theorem. By Theorem 5.6, there exists a plane $\mathcal{L} \subset \mathbb{R}^{m+r}$ of dimension $\dim \mathcal{L} \le r-1$ such that

$$|\mathcal{L} \cap \Phi(S_\alpha)| \ge |\Phi(S_\alpha)|/c_{71} \ge k/c_{72}$$

with $c_{71} = fr(r,1) = c_{13}$ and $c_{72} = 2^r fr(r,1) = 2^r c_{13}$. In particular, putting[4] $K_0'' = K'' \cap \mathcal{L}$ we obtain

$$|K_0''| \ge k/c_{72} \ge k/c_{44}.$$

Without loss of generality

$$\mathcal{L} = \mathcal{L}(K_0''), \tag{7.6}$$

otherwise we can replace $\mathcal{L}$ by the plane $\mathcal{L}(K_0'')$.

[4] Recall that $K'' = \Phi(K')$.

7.3. Constructing the triple (m_0, B_0, φ_0). — Now we are ready to construct the triple (m_0, B_0, φ_0). It will sometimes be notationally convenient to write $\mathbb{R}^m \oplus \mathbb{R}^r$ instead of $\mathbb{R}^{m+r}$ (and $\mathbb{Z}^m \oplus \mathbb{Z}^r$ instead of $\mathbb{Z}^{m+r}$). In these cases, we shall write the elements of $\mathbb{R}^m \oplus \mathbb{R}^r$ as $x \oplus y$, where $x = (x_1, \dots, x_m) \in \mathbb{R}^m$ and $y = (y_1, \dots, y_r) \in \mathbb{R}^r$.

By the definition of the map Φ, the set K'' is contained in the convex body

$$\{x \oplus y \in \mathbb{R}^m \oplus \mathbb{R}^r \ : \ x \in B, \ \ 0 \le (x, a_i) - b_i - y_i < 1 \ \ (1 \le i \le r)\}.$$

Therefore the set $K'' - K''$ is contained in the symmetric convex body

$$\Omega := \{x \oplus y \in \mathbb{R}^m \oplus \mathbb{R}^r \ : \ x \in 2B, \ \ -1 < (x, a_i) - y_i < 1 \ \ (1 \le i \le r)\}. \tag{7.7}$$

Proposition 7.4. — *There exist a proper subspace $\mathcal{L}_0$ of $\mathbb{R}^{m+r}$ with the following properties.*

1. *Let K_0'' be the subset of K'' defined at the end of the previous subsection. Then the set $B_0 := \mathcal{L}_0 \cap \Omega$ contains $K_0'' - K_0''$.*
2. *Put $\Gamma_0 = \mathcal{L}_0 \cap \mathbb{Z}^{m+r}$. Then $B_0 \cap \Gamma_0$ generates $\mathcal{L}_0$ as a vector space. In particular, Γ_0 is a lattice in $\mathcal{L}_0$, and B_0 is Γ_0-thick.*
3. *Let $x \oplus y \in \mathbb{R}^m \oplus \mathbb{R}^r$ be a non-zero vector orthogonal to $\mathcal{L}_0$. Then $y \ne 0$.*

Proof. — For every $x \in B$ there exists $y \in \mathbb{Z}^r$ such that $x \oplus y \in \Omega$. (Indeed, we can always find $y_i \in \mathbb{Z}$ satisfying $-1 < (x, a_i) - y_i < 1$.) Since B is thick (by assumption), there exists an m-element subset $M \subset B \cap \mathbb{Z}^m$ of linear dimension m. For any $x \in M$ fix $y \in \mathbb{Z}^r$ such that $x \oplus y \in \Omega$. We obtain an m-element subset $M' \subset \Omega \cap \mathbb{Z}^{m+r}$ of linear dimension m.

Let $\mathcal{L}_1$ be the subspace of $\mathbb{R}^{m+r}$ parallel to the plane $\mathcal{L}$ and of the same dimension[(5)]. Then $\mathcal{L}_0 := \mathcal{L}_1 + \mathcal{L}(M')$ is a proper subspace of $\mathbb{R}^{m+r}$, because $\dim \mathcal{L}_0 \le \dim \mathcal{L}_1 + m \le m + r - 1$.

Proof of item 1. — Since the plane $\mathcal{L}$ contains K_0'', the subspace $\mathcal{L}_1$ contains $K_0'' - K_0''$. Since Ω contains $K'' - K''$, even the set $\mathcal{L}_1 \cap \Omega$ contains $K_0'' - K_0''$. □

Proof of item 2. — Since $B_0 \cap \Gamma_0$ contains both the sets $K_0'' - K_0''$ and M', and since $K_0'' - K_0''$ generates $\mathcal{L}_1$ by (7.6), the set $B_0 \cap \Gamma_0$ generates $\mathcal{L}_0$. □

Proof of item 3. — Let $x \oplus 0 \in \mathbb{R}^m \oplus \mathbb{R}^r$ be orthogonal to $\mathcal{L}_0$. Then it is orthogonal to the set M', whence $x \in \mathbb{R}^m$ is orthogonal to M. Since M generates the whole space $\mathbb{R}^m$, we have $x = 0$. □

Now the Lemma on Partial Covering becomes an easy consequence of the following assertion.

Proposition 7.5. — *We can choose the δ-distorting vectors $a_1, \dots, a_r$ in our construction to have*

$$(\operatorname{Vol} B_0)/\Delta(\Gamma_0) \le c_{45}(\sigma) \operatorname{Vol} B_0 \, (k/\operatorname{Vol} B_0)^{1/2(2m+r)}. \tag{7.8}$$

(Recall that $\delta = 1/2\sqrt{\sigma}$ and $r = \lceil 8\sigma \log(2\sigma) \rceil$.)

(5) Recall that plane $\mathcal{L}$ was defined at the end of the previous subsection.

Proof of Lemma 4.5 (assuming Proposition 7.5). — Let $\pi\colon \mathbb{Z}^m \oplus \mathbb{Z}^r \to \mathbb{Z}^m$ be the projection on the first summand. By the very definition of Freiman's map Φ, we have $\pi \circ \Phi = \mathrm{id}_{\mathbb{Z}^m}$. Therefore π induces a one-to-one map $K'' \to K'$. Hence $\varphi \circ \pi$ induces a one-to-one map $K'' \to K$. It follows that the set $K_0 := \varphi \circ \pi(K_0'')$ satisfies $|K_0| = |K_0''| \geq k/c_{44}$, which is (4.3).

Let $\mathcal{L}_0$, B_0 and Γ_0 be defined from Proposition 7.4, and let φ_0 be the restriction of $\varphi \circ \pi$ to Γ_0. If we change coordinates, identifying Γ_0 with $\mathbb{Z}^{m_0}$ and $\mathcal{L}_0$ with $\mathbb{R}^{m_0}$, then we obtain a triple (m_0, B_0, φ_0), satisfying the requirements of Lemma 4.5. Indeed,

$$m_0 = \dim \mathcal{L}_0 \leq m + r - 1 \leq c_{46}(\sigma),$$

which is the condition (i)$'$ of Lemma 4.5. Further, $K_0'' - K_0'' \subset B_0 \cap \Gamma_0$, whence $\varphi_0(B_0 \cap \Gamma_0) \supset K_0 - K_0$, which is the condition (ii)$'$ of Lemma 4.5. Finally, the left-hand side of (7.8) is independent on the choice of coordinates. Since in the new coordinates we have $\Delta(\Gamma_0) = 1$, we obtain

$$\mathrm{Vol}\, B_0 \leq c_{45}(\sigma)\, \mathrm{Vol}\, B_0\, (k/\,\mathrm{Vol}\, B_0)^{1/2(2m+r)}\,.$$

Since $2(2m + r) \leq c_{42}$, this proves (4.4). □

It remains to prove Proposition 7.5, which will be done in the next section.

8. Proof of the Lemma on Partial Covering: estimating $(\mathrm{Vol}\, B_0)/\Delta(\Gamma_0)$

8.1. A badly approximable system of distorting vectors. — Let B^* be the convex body *dual to* B, that is

$$B^* = \{x^* \in \mathbb{R}^m \ :\ (x, x^*) \leq 1 \text{ for any } x \in B\}.$$

As proved in [**5**, Chapter IV, Theorem VI],

$$\mathrm{Vol}\, B^* \leq 4^m V^{-1} \ = 4^m (\Sigma k)^{-1}, \tag{8.1}$$

where we put $V = \mathrm{Vol}\, B$ and $\Sigma = V/k$.

We want $a_1, \ldots, a_r$ to be a (B^*, X, C)-badly approximable system of δ-distorting vectors (see Definition 6.7), X and C to be specialized later. First we need to estimate the measure of δ-distorting vectors in the unit cube. We follow the argument of [**12**, Section 2.16].

Proposition 8.1. — *Let δ be a positive real number*[(6)] *satisfying $\delta < 1/\sqrt{\sigma}$. Then the set $M(\delta)$ of $\delta-$ distorting vectors $a \in [0,1)^m$ satisfies*

$$\mathrm{Vol}\, M(\delta) \geq \frac{1 - \delta\sqrt{\sigma}}{\sigma} \frac{1}{k}. \tag{8.2}$$

(6) We forget for a while that we have already specified δ.

Proof. — We use the circle method. For $a \in [0,1)^m$ put

$$S(a) = \sum_{x \in K'} e^{2\pi i(a,x)}, \quad S_1(a) = \sum_{x \in K'+K'} e^{-2\pi i(a,x)}.$$

Then

$$k^2 = \int_{[0,1)^m} \sum_{\substack{x,y \in K' \\ z \in K'+K'}} e^{2\pi i(a,x+y-z)} da = \int_{[0,1)^m} S^2(a) S_1(a) da.$$

We have trivially

$$\int_{M(\delta)} S^2(a) S_1(a) da \leq k^2 \, |K' + K'| \, \mathrm{Vol} M(\delta) \leq \sigma k^3 \, \mathrm{Vol}\, M(\delta),$$

and by the Cauchy-Schwarz inequality

$$\begin{aligned} \int_{[0,1)^m \setminus M(\delta)} S^2(a) S_1(a) da &\leq \delta k \int_{[0,1)^m} |S(a)||S_1(a)| da \\ &\leq \delta k \sqrt{\int_{[0,1)^m} |S(a)|^2 da} \sqrt{\int_{[0,1)^m} |S_1(a)|^2 da} \\ &\leq \delta k \sqrt{k} \sqrt{\sigma k} = \delta \sqrt{\sigma} k^2. \end{aligned}$$

Hence $k^2 \leq \sigma k^3 \mathrm{Vol} M(\delta) + \delta \sqrt{\sigma} k^2$, which implies (8.2). □

The next proposition is a direct consequence of Proposition 8.1, Lemma 6.8 and inequality (8.1).

Proposition 8.2. — *Assume that $0 < \delta < 1/\sqrt{\sigma}$ and let $\kappa, \nu > 0$ satisfy the condition*

$$(m+r)\kappa + m\nu < 1.$$

Also, assume that

$$\Sigma > \left(\frac{\sigma \cdot 24^m \cdot 3^r}{1 - \delta\sqrt{\sigma}} \right)^{\frac{1}{1-(m+r)\kappa+m\nu}}.$$

Then for $X = \Sigma^\kappa$ and $C = \Sigma^\nu$ there exists a (B^*, X, C)-badly approximable system of δ-distorting vectors $a_1, \ldots, a_r \in [0,1)^m$.

In particular, specifying $\kappa = \mu = 1/2(2m+r)$, we obtain the following.

Proposition 8.3. — *Assume that $\Sigma \geq e^{26\sigma \log(2\sigma)}$. Then for $\delta = 1/2\sqrt{\sigma}$ and $X = C = \Sigma^{1/2(2m+r)}$ there exists a (B^*, X, C)-badly approximable system of δ-distorting vectors $a_1, \ldots, a_r \in [0,1)^m$.*

8.2. Estimating $\operatorname{Vol} B_0$. — Since we are going to apply Lemma 6.5, we start with the following assertion.

Proposition 8.4. — *The convex body* Ω *defined in (7.7) contains an* $(m+r)$*-dimensional ball of radius* $(m+1)^{-1}$.

Proof. — Since the Mahler's basis of the body B is orthonormal (see the beginning of Section 7), we obtain

$$\|x\|_B \le \max(1, m/2)\|x\| \quad (x \in \mathbb{R}^m). \tag{8.3}$$

Define a linear map $A\colon \mathbb{R}^m \to \mathbb{R}^r$ by $Ax = ((x,a_1),\dots,(x,a_r))$. Since $a_1,\dots,a_r \in [0,1)^m$, we have $\|Ax\|_\infty \le m\|x\|_\infty$. Now fix $x \oplus y \in \mathbb{R}^m \oplus \mathbb{R}^r (\cong \mathbb{R}^{m+r})$. Then

$$\begin{aligned} \|x \oplus y\|_\Omega &= \max\left(\|x\|_{2B}, \|Ax - y\|_\infty\right) \\ &\le \max\left(\tfrac{1}{2}\|x\|_B, m\|x\|_\infty + \|y\|_\infty\right) \\ &\le (m+1)\|x \oplus y\|_\infty \\ &\le (m+1)\|x \oplus y\|. \end{aligned}$$

Therefore Ω contains the $(m+r)$-dimensional ball of radius $(m+1)^{-1}$ with center in the origin. □

Now we are able to estimate $\operatorname{Vol} B_0$.

Proposition 8.5. — *We have*

$$\operatorname{Vol} B_0 \le c_{81} V, \tag{8.4}$$

where $c_{81} = 2^{m+r}(m+r)!(m+1)^{m+r}$.

Proof. — We have

$$\operatorname{Vol} \Omega = 2^{m+r} V. \tag{8.5}$$

Combining this with Proposition 8.4 and Lemma 6.5, we obtain (8.4). □

8.3. Proof of Proposition 7.5. — Now we are in a position to complete the proof of Proposition 7.5. Let X and C be defined as in Proposition 8.3. By (7.1), the assumption of Proposition 8.3 is satisfied. Therefore we may assume that vectors $a_1,\dots,a_r$ form a (B^*, X, C)-badly approximable system. We shall see that this yields (7.8).

Put $\Delta_0 = \Delta(\Gamma_0)$. The argument splits into two cases (recall that $\Sigma = V/k$).

Case 1: $\Delta_0 \ge \Sigma^{1/2(2m+r)}$. — Since $c_{81} \le c_{45}$, in this case the inequality (7.8) follows immediately from (8.4). (Note that in this case we did not need the fact that $a_1,\dots,a_r$ form a badly approximable system.)

Case 2: $\Delta_0 \leq \Sigma^{1/2(2m+r)}$. — By Lemma 6.10 there exists a vector $l = \lambda \oplus \mu \in \mathbb{Z}^m \oplus \mathbb{Z}^r$ orthogonal to the subspace $\mathcal{L}_0$ and satisfying $0 < \|l\|_\infty \leq \Delta_0$. By Proposition 7.4 (3), $\mu = (\mu_1, \dots, \mu_r) \neq 0$. Now, since $\|\mu\| \leq \|l\| \leq \Delta_0 \leq X$ and since $a_1, \dots, a_r$ form a (B^*, X, C)-badly approximable system, we have $\|\mu_1 a_1 + \dots + \mu_r a_r + \lambda\|_{B^*} \geq C$. This means that for some $x \in \mathbb{R}^m$ we have

$$|(\mu_1 a_1 + \dots + \mu_r a_r + \lambda, x)| \geq C\|x\|_B. \tag{8.6}$$

Put $w = x \oplus Ax \in \mathbb{R}^m \oplus \mathbb{R}^r$ (where A is the linear map defined in the proof of Proposition 8.4). Clearly, $\|w\|_\Omega = \frac{1}{2}\|x\|_B$. Since the left-hand side of (8.6) is equal to $|(w, l)|$, we have

$$|(w, l)| \geq C\|x\|_B = 2C\|w\|_\Omega \tag{8.7}$$

Let $W = w^\perp$ be the orthogonal complement to w and $\pi\colon \mathbb{R}^{m+r} \to W$ the orthogonal projection. We have the following three inequalities:

$$\mathrm{Vol}_{m+r-1}(\pi(\Omega)) \leq c_{82}\frac{\|w\|_\Omega}{\|w\|}V; \tag{8.8}$$

$$\mathrm{Vol}_{m_0}(\pi(B_0)) \leq c_{83}\,\mathrm{Vol}_{m+r-1}(\pi(\Omega)); \tag{8.9}$$

$$\mathrm{Vol}_{m_0}(B_0) \leq \frac{\|w\|\|l\|}{|(w,l)|}\,\mathrm{Vol}_{m_0}(\pi(B_0)). \tag{8.10}$$

Here $c_{82} = (m+r)2^{m+r}$ and $c_{83} = (m+r-1)!(m+1)^{m+r-1}$.

Indeed, (8.8) follows at once from (8.5) and Lemma 6.6. To prove (8.10) note that by Lemma 6.9

$$\mathrm{Vol}_{m_0}(B_0) = \frac{\mathrm{Vol}_{m_0}(\pi(B_0))}{\det \pi\,|_{\mathcal{L}_0}} \leq \frac{\|w\|\|l\|}{|(w,l)|}\,\mathrm{Vol}_{m_0}(\pi(B_0)).$$

Finally, as we have seen in Proposition 8.4, the body Ω contains an $(m+r)$-dimensional ball of radius $(m+1)^{-1}$. The projection π maps it onto an $(m+r-1)$-dimensional ball of the same radius. Now we obtain (8.9) applying Lemma 6.5.

Combining the inequalities (8.7)–(8.10), we obtain $\mathrm{Vol}_{m_0}(B_0) \leq c_{84}\|l\|VC^{-1}$ with $c_{84} = \frac{1}{2}c_{82}c_{83}$. Since $\|l\| \leq \sqrt{m+r}\|l\|_\infty \leq \sqrt{m+r}\Delta_0$, we obtain finally

$$\mathrm{Vol}_{m_0}(B_0) \leq c_{85}\Delta_0 V \Sigma^{-1/2(2m+r)}$$

with $c_{85} = \sqrt{m+r}c_{84} \leq c_{45}$, which proves (7.8). This completes the proof of Proposition 7.5 and the Lemma on Partial Covering. □

9. Proof of Proposition 4.2 (the iteration step)

In this section we prove Proposition 4.2. We fix a real number $T \geq 2$, and write "admissible" instead of "T-admissible" in the sequel. Given an admissible triple (m, B, φ), we have to construct another admissible triple (m', B', φ') satisfying (4.1). Note that (4.1) holds (with another constant) for the triple (m_0, B_0, φ_0) constructed in Lemma 4.5. However, instead of conditions (i)–(iii) of Theorem 3.1, we have only (i)′ and (ii)′, which can be regarded as weaker analogues of (i) and (ii). Our strategy

will be to "correct" the triple (m_0, B_0, φ_0) step-by-step, obtaining at the final step the desired (m', B', φ').

Thus, fix an admissible triple (m, B, φ), and again put $V = \operatorname{Vol} B$ and $\Sigma = V/k$.

9.1. The condition (ii)

Proposition 9.1. — *There exists a triple (m_1, B_1, φ_1) satisfying*

$$\operatorname{Vol} B_1 \le c_{91}(\sigma) V \Sigma^{-1/c_{42}(\sigma)} \tag{9.1}$$

and the conditions

(i)$''$ $m_1 \le c_{92}(\sigma)$;

(ii) $\varphi_1(B_1 \cap \mathbb{Z}^{m_1}) \supset K$.

Here $c_{91} = 2^{\sigma c_{44}} c_{45}$ and $c_{92} = c_{46} + \sigma c_{44}$.

Proof. — What follows is a combination of arguments due to Freiman [**12**, Section 2.24] and Ruzsa [**30**, Section 5]. Let (m_0, B_0, φ_0) and K_0 be constructed in Lemma 4.5. Let $A = \{a_1, \dots, a_s\}$ be a maximal subset of K with the following property:

$$(a_i + K_0) \cap (a_j + K_0) = \varnothing \quad (i \ne j). \tag{9.2}$$

Then

$$s = |A| \le \sigma c_{44}. \tag{9.3}$$

(Indeed, (9.2) yields that $|A + K_0| \ge s|K_0|$, whence

$$\sigma k \ge |K + K| \ge |A + K_0| \ge s|K_0| \ge sk/c_{44},$$

which proves (9.3).) By the maximal choice of the set A, for any $b \in K$ there exist $a_i \in A$ such that $(b + K_0) \cap (a_i + K_0) \ne \varnothing$. In other words,

$$K \subset A + (K_0 - K_0). \tag{9.4}$$

Now put $\Xi = \{x \in \mathbb{R}^s : \|x\|_\infty \le 1\}$, and define a homomorphism $\psi\colon \mathbb{Z}^s \to \mathbb{Z}^n$ by $e_i \mapsto a_i$, where $e_1 = (1, 0, \dots, 0), \dots, e_s = (0, \dots, 0, 1)$ is the standard basis of $\mathbb{R}^s$. Further, put

$$m_1 = m_0 + s, \quad B_1 = B_0 \oplus \Xi,$$

(where we identify $\mathbb{R}^{m_1} \cong \mathbb{R}^{m_0} \oplus \mathbb{R}^s$ and $\mathbb{Z}^{m_1} \cong \mathbb{Z}^{m_0} \oplus \mathbb{Z}^s$) and define $\varphi_1\colon \mathbb{Z}^{m_1} \to \mathbb{Z}^n$ by

$$\varphi_1 |_{\mathbb{Z}^{m_0}} = \varphi_0, \quad \varphi_1 |_{\mathbb{Z}^s} = \psi.$$

Since $\varphi_0(B_0) \supset K_0 - K_0$ and $\psi(\Xi) \supset A$, we have (ii). Estimates (i)$''$ and (9.1) are obvious. □

Remark 9.2. — We could replace the cube Ξ by the "octahedron"

$$\Xi' = \{x = (x_1, \dots, x_s) \in \mathbb{R}^s : |x_1| + \dots + |x_s| \le 1\}.$$

This would imply a better value for the constant c_{91}. However, this would not have much influence on the final value of the constant c_{11} in the Main Theorem.

9.2. Condition (iii)

Proposition 9.3. — *There exists a triple (m_2, B_2, φ_2) satisfying*

$$\operatorname{Vol} B_2 \le c_{93}(\sigma, T) V \Sigma^{-1/c_{42}(\sigma)} \tag{9.5}$$

and the conditions

(i)$''$ $m_2 \le c_{92}$;
(ii) $\varphi_2(B_2 \cap \mathbb{Z}^{m_2}) \supset K$.
(iii) *the restriction $\varphi_2 |_{TB_2 \cap \mathbb{Z}^{m_2}}$ is one-to-one;*

Here $c_{93} = (2c_{92}T)^{c_{92}} c_{91}$.

Proof. — We follow the argument of [**12**, Lemma 2.26] with some changes. Let (m_1, B_1, φ_1) be the triple constructed in Proposition 9.1. We say that the triple (m_2, B_2, φ_2) is *appropriate* if it satisfies the conditions

$$m_2 \le m_1, \quad \varphi_2(B_2 \cap \mathbb{Z}^{m_2}) \supset K, \quad \operatorname{Vol} B_2 \le (2m_1 T)^{m_1 - m_2} \operatorname{Vol} B_1.$$

Appropriate triples exist — for example, the triple (m_1, B_1, φ_1) is such. Fix an appropriate triple (m_2, B_2, φ_2) with the *minimal* value of m_2. To prove the proposition we have to show that this triple satisfies (iii).

Assuming the contrary, we find a non-zero $e \in 2TB_2 \cap \mathbb{Z}^{m_2}$ such that $\varphi_2(e) = 0$. We may assume that the greatest common divisor of the coordinates of vector e is 1. Then there exists a basis $e_1, \dots, e_{m_2}$ of $\mathbb{Z}^{m_2}$ such that $e_{m_2} = e$. We assume this basis to be orthonormal, redefining the inner product.

Let $\pi \colon \mathbb{R}^{m_2} \to \mathbb{R}^{m_2 - 1}$ be the projection on the first $m_2 - 1$ coordinates. Put $B_2' = \pi(B_2)$. Since $e = e_{m_2} \in \operatorname{Ker} \varphi_2$, there is a uniquely defined map $\varphi_2' \colon \mathbb{Z}^{m_2 - 1} \to \mathbb{Z}^n$ such that $\varphi_2 = \varphi_2' \circ \pi$. We have

$$\varphi_2'(B_2' \cap \mathbb{Z}^{m_2 - 1}) = \varphi_2'(\pi(B_2) \cap \pi(\mathbb{Z}^{m_2})) \supset \varphi_2' \circ \pi(B_2 \cap \mathbb{Z}^{m_2}) = \varphi_2(B_2 \cap \mathbb{Z}^{m_2}) \supset K.$$

Also, since $e \in 2TB_2$, we have $\|e\|_{B_2} \le 2T$, and by Lemma 6.6

$$\operatorname{Vol}_{m_2 - 1} B_2' \le 2Tm_2 \operatorname{Vol}_{m_2} B_2 \le (2m_1 T)^{m_1 - (m_2 - 1)} \operatorname{Vol} B_1.$$

Thus, the triple $(m_2 - 1, B_2', \varphi_2')$ is appropriate, which contradicts the minimal choice of m_2. □

9.3. The condition (i). — Now it is easy to complete the proof of Proposition 4.2. Let (m_2, B_2, φ_2) be the triple constructed in Proposition 9.3. Put $K' = \varphi_2^{-1}(K)$. Since $T \ge 2$, it follows from (ii) and (iii) that the map $\varphi_2 \colon K' \to K$ is F_2-isomorphic. Therefore $|K' + K'| \le \sigma |K'|$, whence by Lemma 4.3 we have $m' := \dim K' \le \lfloor \sigma - 1 \rfloor$. Put $\mathcal{L}' = \mathcal{L}(K')$.

We may assume that the Mahler's basis of the body B_2 is orthonormal. Then B_2 contains an m_2-dimensional ball of radius $2/m_2$. Putting $B' = \mathcal{L}' \cap B_2$, we have by Lemma 6.5

$$\operatorname{Vol}_{m'}(B') \le m_2! (m_2/2)^{m_2} \operatorname{Vol}_{m_2}(B_2) \le c_{94}(\sigma, T) V \Sigma^{-1/c_{42}(\sigma)} \tag{9.6}$$

with $c_{94}(\sigma, T) = c_{92}(\sigma)^{2c_{92}(\sigma)} c_{93}(\sigma, T) \le c_{41}$.

Finally, put $\Gamma' = \mathcal{L}' \cap \mathbb{Z}^{m_2}$ and $\varphi' = \varphi_2 \,|_{\Gamma'}$. When we identify $\mathcal{L}'$ with $\mathbb{R}^{m'}$ and Γ' with $\mathbb{Z}^{m'}$, the volume of B' should be multiplied by $\Delta(\Gamma)^{-1}$. Since $\Delta(\Gamma) \geq 1$, we will still have (9.6).

Thus, the triple (m', B', φ') is admissible and satisfies (4.1). Proposition 4.2 is proved. □

10. Final remarks

10.1. Various formulations of Freiman's theorem. — Both Theorems 1.2 and 1.3 are new, though not very much is added to Freiman's proof. Freiman's original formulation of his theorem is similar to our Theorem 3.1, but with $|B \cap \mathbb{Z}^m|$ instead of $\operatorname{Vol} B$. Ruzsa's result is as follows.

***Theorem 10.1* (Ruzsa [30]).** — *Let K and L be finite subsets of a torsion-free abelian group. Suppose that $|K| = |L| = k$ and $|K + L| \leq \sigma k$. Then K is a subset of a generalized arithmetical progression P of rank $m \leq c_{101}(\sigma)$ and cardinality $|P| \leq c_{102}(\sigma)k$.*

The main advantage of Ruzsa's theorem is that it deals with distinct sets. Ruzsa's proof implies an estimate $c_{102}(\sigma) \leq \exp\exp(\sigma^c)$ with an absolute constant c, which is better than (1.4). However, Ruzsa does not prove that P is an F_s-progression (even for $s = 1$), nor does he obtain the inequality $m \leq \lfloor \sigma - 1 \rfloor$, having only the weaker bound $m \leq \exp(\sigma^c)$.

Both these difficulties can be overcome in the case $K = \pm L$: one should combine Ruzsa's result with the arguments from Sections 9 and 3 of the present paper. (In the case $L = -K$ Lemma 4.3 should be replaced by its analogue for $K - K$ proved in [14].) This would give us a new proof of Theorem 1.2, the estimate (1.4) being replaced by $c_{11}(\sigma) \leq (2s)^{\exp(\sigma^c)}$, and an analogue of the Main Theorem with $K - K$ instead of $K + K$.

It is very likely that a similar approach (with some additional ideas) would lead to a complete analogue of Theorem 1.2 for the addition of two distinct sets of the same cardinality.

***Remark 10.2* (added in revision).** — Nathanson [26, Section 9.6] posed the following *proper conjecture*:

Let $\alpha \leq 1$ and σ be positive real numbers, let k be a positive integer, and let K and L be finite subsets of a torsion-free abelian group such that

$$\alpha k \leq |K|, |L| \leq k \quad \text{and} \quad |K + L| \leq \sigma k.$$

Then K is a subset of an F_1-progression P of rank $c(\alpha, \sigma)$ and cardinality $|P| \leq c'(\alpha, \sigma)k$.

It is easy to see that this conjecture is a consequence of Theorem 1.2. Indeed, it follows from [**28**, Lemma 3.3] (reproduced in [**26**] as Theorem 7.8) that

$$|K+K| \le |K+K-K| \le \left(\frac{\sigma k}{|L|}\right)^3 |L| \le (\sigma/\alpha)^3 |K|.$$

Applying Theorem 1.2, we prove the conjecture with $c = \lfloor (\sigma/\alpha)^3 - 1 \rfloor$ and $c' = c_{11}((\sigma/\alpha)^3, 1)$. (A slightly more accurate argument gives $(\sigma/\alpha)^2$ instead of $(\sigma/\alpha)^3$.)

10.2. Freiman's proof and Ruzsa's proof. — Put $Ks = \overbrace{K+\cdots+K}^{s}$. Ruzsa starts with proving that

$$|K+L| \le \sigma k \Rightarrow |Ks_1 - Ks_2| \le \sigma^{s_1+s_2} k, \tag{10.1}$$

(where s_1 and s_2 are arbitrary positive integers) and then works with the set K only. He shows also that it is sufficient to consider the case $K \subset \mathbb{Z}$.

The first crucial step of his proof is the following nice theorem.

Theorem 10.3 **([28])**. — *Let K be a finite set of integers, and s a positive integer. Then for any $N \ge 2s|Ks-Ks|$ there is a a subset $K' \subset K$ of cardinality $|K'| \ge k/s$, which is F_s-isomorphic to a subset of the cyclic group of order N.*

Due to this result one may work in a "close environment", which essentially simplifies the reasoning and allows one to avoid iterations.

The second crucial step is the following result:

Theorem 10.4 **([30])**. — *If A is a subset of a cyclic group of order $N \le \alpha|A|$, then the second difference set $A2-A2$ contains a progression of rank at most $c_{103}(\alpha)$ and cardinality at least $N/c_{104}(\alpha)$.*

A simple combination of these two theorems shows that there is a progression $P \subset K2-K2$ of bounded rank, satisfying $|P| \ge k/c_{105}(\sigma)$. Now it is easy to complete the proof proceeding in the same manner as in Subsection 9.1 of this paper.

Thus, in both Freiman's and Ruzsa's proofs one first takes care of an "substantial part" of the set in question (or a relative set), and then covers by a progression the whole set. In Freiman's argument the main tools for finding a "partial covering" are the 2^n-theorem and the circle method. In Ruzsa's argument the same role belongs to Theorem 10.4, in the proof of the latter the circle method being crucial too.

Evidently, there are deep interconnections between the two proofs. Revealing them will lead to a much better understanding of the problems connected with Freiman's theorem.

References

[1] Bilu Y., *The $(\alpha+2\beta)$-inequality on the torus*, J. London Math. Soc., to appear.

[2] Bilu Y., Lev V. F., Ruzsa I. Z., *Rectification principles in additive number theory*, Discr. Comput. Geom., **19**, 1998, 343–353.

[3] Bombieri E., Vaaler J., *On Siegel's Lemma*, Inv. Math., **73**, 1983, 11–31.

[4] Brailovski L.V, Freiman G.A., *On a Product of Finite Subsets in a Torsion-Free Group*, J. Algebra, **130**, 1990, 462–476.

[5] Cassels J.W.S., *An Introduction to the Geometry of Numbers*, Springer, 1959.

[6] Cauchy A.L., *Recherches sur les nombres*, J. Ècole Polytech., **9**, 1813, 99–116.

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

[8] Davenport H., *A historical note*, J. London Math. Soc., **22**, 1947, 100–101.

[9] Fishburn P.C., *On a contribution of Freiman to additive number theory*, J. Number Theory, **35**, 1990, 325–334.

[10] Freiman G.A., *Inverse problems in additive number theory VI., On the addition of finite sets III* (Russian), Izv. Vysš. Učebn. Zaved. Matem., no. **3 (28)**, 1962, 151–157.

[11] Freiman G.A., *Inverse problems of additive number theory, VII. On addition of finite sets, IV. The method of trigonometric sums* (Russian), Izv. Vysš. Učebn. Zaved. Matem., No **3(28)**, 1962, 131–144.

[12] Freiman G.A., *Foundations of a Structural Theory of Set Addition* (Russian), Kazan', 1959; English Translation: Translation of Mathematical Monographs **37**, Amer. Math. Soc., Providence, 1973.

[13] Freiman G.A., *What is the structure of K if $K + K$ is small?*, Number Theory, New York 1984–1985, Lecture Notes in Math., **1240**, Springer, 1987, 109–134,

[14] Freiman G.A., Heppes A., Uhrin B., *A lower estimation for the cardinality of finite difference sets in $\mathbb{R}^n$*, Proc. Conf. Number Theory, Budapest 1987, Coll. Math. Soc. J. Bolyai, Budapest, **51**, 1989, 125–139.

[15] Hamidoune Y.O., *On inverse additive problems*, Preprint EC95/01, Inst. Blaise Pascal, Paris, January 1995.

[16] Hamidoune Y.O., *An Isoperimetric Method in Additive Theory*, J. Algebra, **179**, 1996, 622–630.

[17] Hamidoune Y.O., *Some Results in Additive Number Theory*, Rapport ECH197, Univ. Paris VI, 1997.

[18] Kemperman I.H.B., *On small sumsets in an abelian group*, Acta Math., **103**, 1960, 63–88.

[19] Kemperman I.H.B., *On products of sets in a locally compact group*, Fund. Math., **56**, 1964, 51–68.

[20] Kneser M., *Ein Satz über abelschen Gruppen mit Anwendungen auf die Geometrie der Zahlen*, Math. Z., **61**, 1955, 429–434.

[21] Kneser M., *Summenmengen in lokalkompakten abelschen Gruppen*, Math. Z., **66**, 1956, 88–110.

[22] Lev V.F., *Structure Theorem for Multiple Addition and Frobenius Problem*, J. Number Th., **58**, 1996, 79–88; addendum: **65**, 1997, 96–100.

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

[24] Mann H., *Addition Theorems: the Addition Theorems of Group Theory and Number Theory*, Wiley, New York, 1965.

[25] Nathanson M.B., *An inverse theorem for sums of sets of lattice points*, J. Number Theory, **46**, 1994, 29–59.

[26] Nathanson M.B., *Additive Number Theory: 2. Inverse Theorems and the Geometry of Sumsets*, Graduate Text in Math. **165**, Springer, New York, 1996.

[27] Postnikova L.P., *Fluctuations in the distribution of fractional parts* (Russian), Dokl. Akad. Nauk SSSR, **161**, 1965, 1282–1284; English Translation: Soviet Math. Dokl., **6**, 1965, 597–600.

[28] Ruzsa I.Z., *Arithmetical progressions and the number of sums*, Per. Math. Hung., **25**, 1992, 105–111.

[29] Ruzsa I.Z., *A concavity property of for the measure of product sets in groups*, Fund. Math., **140**, 1992, 247–254.

[30] Ruzsa I.Z., *Generalized arithmetical progressions and sumsets*, Acta Math. Hungar., **65** (1994), 379–388.

[31] Ruzsa I.Z., *Sums of sets in several dimensions*, Combinatorica, **14**, 1994, 485–490.

[32] Stanchescu Y., *On addition of two distinct sets of integers*, Acta Arith., **75**, 1996, 191–194.

[33] Stanchescu Y., *On the structure of sets with small doubling property on the plane (i)*, Acta Arith., **83**, 1998, 127–141.

[34] Stanchescu Y., *On finite difference sets*, Acta Math. Hungar., **79**, 1998, 123–138.

[35] Steinig J., *On Freiman's theorems concerning the sum of two finite sets of integers*, this volume.

[36] Vosper A.G., *The critical pairs of subsets of a group of prime order*, J. London Math. Soc., **31**, 1956, 200–205, 280–282.

[37] Zemor G., *Subset sums for binary spaces*, Europ. J. Combin., **13**, 1992, 221–230.

[38] Zemor G., *A generalization to noncommutative groups of a theorem of Mann*, Discr. Math., **126**, 1994, 365–372.

Y. BILU, Mathematisches Institut, Universitaet Basel, Rheinsprung 21, CH-4051 Basel, Switzerland
E-mail : yuri@math.unibas.ch