NOTES ON PROGRESSIONS AND CONVEX GEOMETRY

BEN GREEN

Abstract. Our purpose is to informally explain some parts of Chang's paper on Freiman's theorem, [2], which depend on results in Bilu's exposition of Freiman's original proof [1]. Specifically we prove that if P is a d-dimensional progression then P is contained in a proper progression $\widetilde{P}$ of dimension at most d and size no more than $d^{Cd^2}|P|$. We also prove Chang's bounds for Freiman's theorem in the following form. Suppose that $A \subseteq \mathbb{Z}^m$ is a set with $|A+A| \leqslant K|A|$, and that $\varepsilon > 0$. Suppose that $|A| \geqslant CK^6/\varepsilon$. Then there is a proper progression P of dimension $d \leqslant \lfloor K - 1 + \varepsilon \rfloor$ and size at most $\exp(CK^2 \log^3 K)|A|$ such that $A \subseteq P$.

These notes may be regarded as a Chapter 4 to add to my earlier notes [3]. I intend to integrate them properly at some point soon, and also to add a Chapter 5, in which I will discuss my recent work with Tao [4] on the Freiman-Bilu theorem, and probably also a Chapter 6, in which I will describe Tao's "universal ambient group" proof of Freiman's theorem. The resultant notes will then give a more-or-less complete discussion of our current knowledge on Freiman's theorem for sets of integers.

These notes were inspired by the original papers of Bilu and Chang (especially the paper of Bilu, which we have followed very closely), and also by the forthcoming book of Tao and Vu [5]. There is no original material here.

1. Some geometry of numbers

A *centred progression* of dimension d inside a lattice Λ in some Euclidean space is any set having the form

$$P := \{\mu_1 v_1 + \cdots + \mu_d v_d : |\mu_i| \leqslant L_i\},$$

where $v_1, \ldots, v_d \in \Lambda$ and the integer parameters $L_1, \ldots, L_d$ are referred to as the *side-lengths* of P. The *size* of P, $\mathrm{size}(P)$, is defined to be $\prod_{i=1}^d (2L_i + 1)$. Note that the size of P need not equal its cardinality (though it does if P is *proper*: see below).

We will be concerned with various properties of progressions. It turns out to be natural to view them in the somewhat more general context of *convex progressions*.

Definition 1.1 (Convex progressions)**.** Suppose that $B \subseteq \mathbb{R}^d$ is a closed, centrally symmetric, convex body. If $B \cap \mathbb{Z}^d$ spans $\mathbb{R}^d$ as a vector space then we say that B is *full*. Suppose that B is full, and that $\phi : \mathbb{Z}^d \to \mathbb{Z}^m$ is a homomorphism. Then we refer to the image

$$X := \phi(B \cap \mathbb{Z}^d)$$

as a *convex progression*. If $s \geqslant 1$ is some integer and if the restriction $\phi|_{sB \cap \mathbb{Z}^d}$ is one-to-one, then we say that X is s-proper. The *size* of X is simply $\mathrm{size}(X) := |B \cap \mathbb{Z}^d|$, and the *volume* is $\mathrm{vol}(X) := \mathrm{vol}_d(B)$. ◊

The author is a Clay Research Fellow, and is pleased to acknowledge the support of the Clay Mathematics Institute. Some of this work was carried out while he was on a long-term visit to MIT.

Remark. The size and volume of a convex progression are somewhat related; see Lemma 2.4 below. Note that the volume $\mathrm{vol}(P)$ of a centred progression is $2^d L_1 \dots L_d$. One should really regard a convex progression as the *pair* (B, ϕ) rather than as the *set* X; in this way the notions of size and of volume are well-defined.

It is clear that every centred progression is a convex progression: simply take B to be the box

$$Q = Q(L_1, \dots, L_d) := \prod_{i=1}^{d} [-L_i, L_i] \subseteq \mathbb{R}^d.$$

As we will see in this section, every convex progression both contains and is contained within a centred progression reasonably economically. However, certain arguments and results are more naturally formulated in the more general context of convex progressions.

Let us start by recalling some nomenclature concerning convex bodies and their behaviour as regards lattices. Let B be a closed, centrally symmetric convex body in $\mathbb{R}^d$, and let Λ be a lattice which spans $\mathbb{R}^d$. We define the *successive minima*,

$$0 < \lambda_1 \leqslant \lambda_2 \leqslant \dots \leqslant \lambda_d,$$

of B with respect to Λ by

$$\lambda_k := \inf\{\lambda : \lambda B \text{ contains } k \text{ linearly independent elements of } \Lambda\}.$$

One imagines starting with a very small dilate ϵB, and "expanding" this slowly outwards. Every time we reach a value of λ for which $\dim_{\mathbb{R}}(\lambda B \cap \Lambda)$ increases, we make a note of that value, and this gives the list of successive minima.

We may also, during this process, write down successive vectors $b_1, \dots, b_d \in \Lambda$ in such a way that $\dim_{\mathbb{R}} \mathrm{Span}(b_1, \dots, b_i) = i$. Such a collection of vectors b_i forms a basis for $\mathbb{R}^d$, and this basis is rather natural if one is interested in studying the body B. We call it a *directional basis*.

We write $\| \cdot \|_B$ for the natural norm associated to B, that is to say

$$\|v\|_B := \inf\{\lambda : v \in \lambda B\}.$$

Note, then, that with this notation we have

$$\|b_i\|_B = \lambda_i.$$

Example (brought to my attention by Joseph Myers in 1999). Let $d = 5$, and suppose that B is the open unit ball $\{x \in \mathbb{R}^5 : \|x\|_2 < 1$. Let Λ be the lattice spanned by $\mathbb{Z}^5$ and $v := (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$. Then it is easy to check that $\lambda_1 = \dots = \lambda_5 = 1$. An example of a direction basis is given by $b_i = e_i$, that is to say the standard basis vectors. Note, however, that the b_i do not form an integral basis for Λ, since $v \notin \bigoplus_{i=1}^{5} \mathbb{Z} b_i$.

It is very useful to have an integral basis for Λ which is natural for studying B. We prove that there is such a basis in Lemma 1.3 below. The argument is due to Mahler.

Lemma 1.2 (Extending an integral basis)**.** *Suppose that V is a d-dimensional vector space, and that $\Lambda \subseteq V$ is a lattice. Suppose that $V' \leqslant V$ is a codimension 1 subspace, and that $\Lambda' := \Lambda \cap V'$ has an integral basis $\{f_1, \dots, f_{d-1}\}$. Then there is a vector $v \in \Lambda$ such that $\{f_1, \dots, f_{d-1}, v\}$ is an integral basis for Λ.*

Proof. Applying a suitable isomorphism $\tau : V \to \mathbb{R}^d$, we may assume that $f_i = e_i$, where the e_i are the standard basis vectors (so that $\Lambda' = \mathbb{Z}^{d-1} \times \{0\}$). Let $\pi_d : \mathbb{R}^d \to \mathbb{R}$ be projection onto the coordinate vector e_d. Pick a vector $v \in \Lambda$ such that $l := \pi_d(v)$ is positive, yet as small as possible. Suppose that $v' \in \Lambda$. Then we may find an integer m such that $0 \leqslant \pi_d(v' - mv) < l$. Since l was assumed to be minimal we must have $\pi_d(v' - mv) = 0$, which means that $v' \in mv + (\mathbb{Z}^{d-1} \times \{0\})$. The result follows. □

Remark. An inductive application of this lemma proves the well-known result that every lattice has an integral basis.

Lemma 1.3 (Mahler)**.** *There is an integral basis $w_1, \dots, w_d$ for Λ such that $\|w_i\|_B \leqslant i\lambda_i$ for $i = 1, \dots, d$.*

Proof. Pick a directional basis $b_1, \dots, b_d$. This, recall, is a particular collection of elements of Λ which span $\mathbb{R}^d$. Set

$$V_i := \mathrm{Span}(b_1, \dots, b_i),$$

and define $\Lambda_i := \Lambda \cap V_i$. Suppose that the vectors $w_1, \dots, w_{j-1}$ have been selected so that they form an integral basis for Λ_{j-1}, and so that the requisite inequalities $\|w_i\|_B \leqslant i\lambda_i$ are satisfied. Now apply Lemma 1.2 with $V = V_j$, $V' = V_{j-1}$ and the integral basis $\{w_1, \dots, w_{j-1}\}$ for $\Lambda' = \Lambda_{j-1}$. By that lemma we may find w^* such that $\{w_1, \dots, w_{j-1}, w^*\}$ is an integral basis for Λ_j.

Now we may write

$$w^* = t_1 b_1 + \cdots + t_j b_j \tag{1.1}$$

for some real numbers $t_1, \dots, t_j$. In particular

$$w^* - t_j b_j \in V_{j-1}. \tag{1.2}$$

Since $b_j \in \Lambda_j$, we also have

$$b_j = \lambda_1 w_1 + \cdots + \lambda_{j-1} w_{j-1} + \lambda^* w^*,$$

for some *integers* $\lambda_1, \dots, \lambda_{j-1}, \lambda^*$. Thus

$$\lambda^* w^* - b_j \in V_{j-1}.$$

Comparing this with (1.2) we see that $\lambda^* \neq 0$ and that $t_j = 1/\lambda^*$. In particular,

$$|t_j| \leqslant 1. \tag{1.3}$$

Note that w^* may be replaced by $w^{**} := w^* - \mu_1 w_1 - \cdots - \mu_{d-1} w_{d-1}$, for arbitrary integers $\mu_1, \dots, \mu_{d-1}$. Recalling (1.1), we may choose the μ_i so that

$$w^{**} = u_1 b_1 + \cdots + u_{j-1} b_{j-1} + t_j b_j,$$

where $|u_i| \leqslant 1$ for $i = 1, \dots, j-1$. Recalling (1.3), we have the bound

$$\|w^*\|_B \leqslant \sum_{i=1}^{j-1} |u_j| \|b_i\|_B + |t_j| \|b_j\|_B \leqslant \lambda_1 + \cdots + \lambda_j \leqslant j\lambda_j.$$

Setting $w_j := w^{**}$, we see that $\{w_1, \dots, w_j\}$ is an integral basis for Λ_j in which each w_i satisfies the bound $\|w_i\|_B \leqslant i\lambda_i$. We may conclude by induction. □

Remark. Actually, it is easy to see that we may insist on slightly more, namely that $\|w_i\|_B \leqslant i\lambda_i/2$ for $i \geqslant 2$. This improvement will be of little consequence to us here, however.

Let $\{w_i\}$ be a Mahler basis for Λ with respect to B. We are going to establish (somewhat loose) necessary and sufficient conditions on the size of coefficients $\mu_1, \dots, \mu_d \in \mathbb{Z}$ in order that the vector $x = \mu_1 w_1 + \cdots + \mu_d w_d$ lies in $B \cap \Lambda$.

Lemma 1.4 (Containment in $B \cap \Lambda$)**.** *Let $x = \mu_1 w_1 + \cdots + \mu_d w_d$ be an element of Λ, where $\mu_i \in \mathbb{Z}$. Then*

(i) *If $|\mu_i| \leqslant 1/di\lambda_i$ for all i, then $x \in B \cap \Lambda$.*
(ii) *If $x \in B \cap \Lambda$ then $|\mu_i| \leqslant (d!)^2/i\lambda_i$ for all i.*

Proof. The proof of (i) involves nothing more than the triangle inequality. Indeed if $\mu_i \leqslant 1/di\lambda_i$ for all i then

$$\|x\|_B \leqslant \sum_{i=1}^{d} |\mu_i| \|w_i\|_B \leqslant \sum_{i=1}^{d} |\mu_i| i\lambda_i \leqslant 1.$$

The proof of (ii) is rather more subtle, and involves Minkowski's second theorem. This was proved in [3, Ch. 3]; it is the bound

$$\lambda_1 \dots \lambda_d \mathrm{vol}(B) \leqslant 2^d \det(\Lambda).$$

Now note that the octahedron O spanned by $\pm x$ and the vectors $\pm w_j/j\lambda_j$, $j \neq i$, lies in B. Since the w_i are an integral basis for Λ, we have

$$\mathrm{vol}(B) \geqslant \mathrm{vol}(O) = \frac{2^d \mu_i}{d! \prod_{j \neq i} j\lambda_j} \det(\Lambda).$$

The result follows immediately from Minkowski's second theorem. □

Finally, we may conclude the main result of this section, which provides a link between progressions and convex bodies.

Lemma 1.5. *Let B be a symmetric convex body in $\mathbb{R}^d$, and let Λ be a lattice of dimension d. Then there is a progression $P \subseteq B \cap \Lambda$ such that $B \cap \Lambda \subseteq d(d!)^2 P$.*

Proof. Define P to be the progression

$$P := \{\mu_1 w_1 + \cdots + \mu_d w_d : |\mu_i| \leqslant 1/di\lambda_i \text{ for } i = 1, \dots, d\}.$$

The result follows immediately from the previous lemma. □

2. Progressions inside proper progressions

Our aim in this section is to prove the following result, which may be found in [1] and which is used in [2].

Theorem 2.1 (Progressions inside proper progressions)**.** *Suppose that $P \subseteq \mathbb{Z}^m$ is a centred progression of dimension d. Let $t \geqslant 1$ be an integer. Then there is a t-proper progression $\widetilde{P}$ of dimension $\widetilde{d} \leqslant d$ such that $P \subseteq \widetilde{P}$, and such that*

$$\mathrm{size}(\widetilde{P}) \leqslant (2t)^d d^{6d^2} \mathrm{size}(P).$$

Roughly speaking, we proceed by *dimension reduction*, which could work as follows. If $P = P_0$ is not proper then there is some non-trivial relation

$$\sum_{i=1}^{d} \mu_i v_i = \sum_{i=1}^{d} \mu_i' v_i$$

involving the elements of P_0, and we may use this to place it inside a progression P_1 of dimension $d-1$ and having size not much bigger than $|P_0|$. If P_1 is not proper, we repeat the process, and so on until we reach a progression which is proper (note that any 1-dimensional progression is proper). It turns out that this procedure is a little inefficient, though it does work (cf. [5, Ch. 5]). It is rather better to replace the chain

$$P = P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots \subseteq P_k,$$

$\dim(P_i) = d - i$, of progressions by a chain

$$P = X_0 \subseteq X_1 \subseteq X_2 \subseteq \cdots \subseteq X_k, \tag{2.1}$$

$\dim(X_i) = d - i$ of convex progressions[1]. Only when this process has terminated do we place the final convex progression inside a true progression P'. To ensure that P' is proper we require each X_i to be s-proper for rather large s, and this is a somewhat inefficient feature of the argument.

Lemma 2.2 (Dimension reduction for convex progressions)**.** *Suppose that $X \subseteq \mathbb{Z}^m$ is a convex progression of dimension d which is not s proper. Then there is a convex progression X' of dimension $d-1$ such that $X \subseteq X'$, and for which*

$$\mathrm{vol}(X') \leqslant sd\,\mathrm{vol}(X).$$

Proof. Suppose that $X = \phi(B \cap \mathbb{Z}^d)$. We will construct $B \subseteq \mathbb{R}^{d-1}$ and a homomorphism $\phi : \mathbb{Z}^{d-1} \to \mathbb{Z}^m$, and then define $X' := \phi'(B \cap \mathbb{Z}^{d-1})$.

Now our assumption that X is not s-proper implies that there is a vector $x \in 2sB \cap \mathbb{Z}^d$, $e \neq 0$, such that $\phi(x) \neq 0$. Write $x = (x_1, \ldots, x_d)$ in coordinates relative to the standard basis vectors $e_1, \ldots, e_d$. We may assume (since ϕ is linear) that $\mathrm{hcf}(x_1, \ldots, x_d) = 1$. This means that we may complete $\{x\}$ to an integral basis $\{f_1, \ldots, f_{d-1}, x\}$ for $\mathbb{Z}^d$.

Let $\tau : \mathbb{R}^d \to \mathbb{R}^d$ be the linear endomorphism for which $\tau(f_i) = e_i$ and $\tau(x) = e_d$. Note that τ preserves $\mathbb{Z}^d$, and hence is unimodular (has determinant ± 1). Let $\pi : \mathbb{R}^d \to \mathbb{R}^{d-1}$ be the projection onto the first $d-1$ coordinates. Define

$$B' := \pi(\tau(B))$$

and define $\phi' : \mathbb{Z}^{d-1} \to \mathbb{Z}$ by

$$\phi'(\pi(\tau(v)) = \phi(v).$$

Define

$$X' := \phi'(B' \cap \mathbb{Z}^{d-1}).$$

Note that ϕ', though defined implicitly, is well-defined since if $\pi(\tau(v_1)) = \pi(\tau(v_1'))$ then $v_1 - v_1' \in \mathbb{Z}e$, which means that $\phi(v_1) = \phi(v_1')$.

[1]Actually here, as in other parts of these notes, there are other "categories" that one might consider using. Tao (personal communication) mentioned ellipsoids; one might also look at "round" convex bodies which contain an inscribed unit sphere, and so on. Each seems to have its own advantages.

B' is manifestly a full, centrally symmetric, convex body in $\mathbb{R}^{d-1}$. We must show that $\phi(B \cap \mathbb{Z}^d) \subseteq \phi(B' \cap \mathbb{Z}^{d-1})$. This is trivial; we have the inclusion $\pi\tau(B \cap \mathbb{Z}^d) \subseteq \pi\tau(B)) \cap \mathbb{Z}^{d-1}$, whence

$$\phi(B \cap \mathbb{Z}^d) = \phi'((\pi\tau(B \cap \mathbb{Z}^d)) \subseteq \phi'(\pi\tau(B) \cap \mathbb{Z}^{d-1}) = \phi'(B' \cap \mathbb{Z}^{d-1}).$$

It remains to establish an upper bound for the volume of B'. To do this, let us first note that $e \in 2sB$, and so $\tau(B)$ contains the vectors $\pm\frac{1}{2s}e_d$. Since $\tau(B)$ is convex, it contains the *suspension* S, defined to be the convex hull of $B' = \pi\tau(B)$ and the vectors $\pm\frac{1}{2s}e_d$. A well-known geometrical lemma (following from the fact that the volume of a the simplex $\mathrm{conv}(0, e_1, \dots, e_d)$ is $1/d$) implies that

$$\mathrm{vol}_d(S) = \frac{1}{sd}\mathrm{vol}_{d-1}(B').$$

Now (as we remarked), $S \subseteq \tau(B)$. Since τ is unimodular, we have

$$\mathrm{vol}(X') = \mathrm{vol}_{d-1}(B') = sd\ \mathrm{vol}_d(S) \leqslant sd\ \mathrm{vol}_d(B) = sd\ \mathrm{vol}(X),$$

which is what we wanted to prove. □

Iterating this lemma, we come up with the following result, stating that convex progressions are contained in (very) proper convex progressions.

Lemma 2.3. *Suppose that $X \subseteq \mathbb{Z}^m$ is a convex progression of dimension d. Then there is an s-proper convex progression X' of dimension $d' \leqslant d$ such that $X \subseteq X'$, and for which*

$$\mathrm{vol}(X') \leqslant s^d d!\ \mathrm{vol}(X).$$ □

We are almost ready to prove Theorem 2.1. Before we can do that, however, we must relate the size and the volume of a convex progression. In fact, we only require a bound in one direction. The following is [5, Lemma 3.26].

Lemma 2.4. *Suppose that X is a convex progression. Then*

$$\frac{\mathrm{size}(X)}{\mathrm{vol}(X)} \leqslant \frac{3^d d!}{2^d}.$$

Proof. Write $X = \phi(B \cap \mathbb{Z}^d)$. Then (by definition) $\mathrm{size}(X) = |B \cap \mathbb{Z}^d|$ and $\mathrm{vol}(X) = \mathrm{vol}_d(B)$. Now B is full, and so there exist d linearly independent vectors $v_1, \dots, v_d \in B \cap \mathbb{Z}^d$. We may choose these so that the interior O° of the octahedron O spanned by $\pm v_1, \dots, \pm v_d$ contains no point of $\mathbb{Z}^d \setminus \{0\}$, for example by selecting O to be the octahedron of minimal volume with vertices in $B \cap \mathbb{Z}^d$. By convexity we have $O \subseteq B$. Now the fact that $O^\circ \cap \mathbb{Z}^d = \{0\}$ implies that the translates $x + \frac{1}{2}O^\circ$, $x \in B \cap \mathbb{Z}^d$, are all disjoint. Since they are all contained in $\frac{3}{2}B$, this leads to the inequality

$$|B \cap \mathbb{Z}^d| \leqslant \frac{\mathrm{vol}_d(\frac{3}{2}B)}{\mathrm{vol}_d(\frac{1}{2}O)} = \frac{3^d \mathrm{vol}_d(B)}{\mathrm{vol}_d(O)}.$$

The result now follows from the observation that any nondegenerate octahedron with vertices in $\mathbb{Z}^d$ has volume at least $2^d/d!$. □

Remark. In fact one can also prove the lower bound

$$\frac{1}{2^d} \leqslant \frac{\mathrm{size}(X)}{\mathrm{vol}(X)}$$

by another elementary covering argument; see [5, Ch. 3] for details.

We move on now to the proof of Theorem 2.1. In view of later applications, it makes sense to prove the following more general result which has Theorem 2.1 as a trivial corollary.

Theorem 2.5 (Convex inside proper)**.** *Suppose that $X = \phi(B \cap \mathbb{R}^d)$ is a convex progression. Let $t \geqslant 1$ be an integer. Then there is some $\widetilde{d} \leqslant d$ and a t-proper centred progression $\widetilde{P}$ of dimension $\widetilde{d}$ such that $X \subseteq \widetilde{P}$, and which satisfies the estimate*

$$\mathrm{size}(\widetilde{P}) \leqslant (2t)^d d^{6d^2} \mathrm{vol}(X).$$

Proof. Apply Lemma 2.3 with $s := d(d!)^2 t$. This gives us an s-proper convex progression X' of dimension $d' \leqslant d$, such that $X \subseteq X'$ and

$$\mathrm{vol}(X') \leqslant s^d d! \, \mathrm{vol}(X). \tag{2.2}$$

Write $X' = \phi'(B' \cap \mathbb{Z}^{d'})$. Now Lemma 1.5 implies that there is a progression $P' \subseteq B' \cap \mathbb{Z}^{d'}$ such that $B' \cap \mathbb{Z}^{d'} \subseteq d(d!)^2 P'$. Write $P'' := d(d!)^2 P'$. The fact that $\phi'|_{sB' \cap \mathbb{Z}^{d'}}$ is one-to-one implies that $\phi'|_{tP'' \cap \mathbb{Z}^{d'}}$ is one-to-one, and therefore the progression $\widetilde{P} := \phi'(P'')$ is t-proper and contains X.

It remains to bound the size of $\widetilde{P}$. Since $P' \subseteq B' \cap \mathbb{Z}^{d'}$, it follows from Lemma 2.4 and (2.2) that

$$\mathrm{size}(P') \leqslant \mathrm{size}(X') \leqslant \frac{3^d d!}{2^d} \mathrm{vol}(X') \leqslant \big(\frac{3s}{2}\big)^d (d!)^2 \mathrm{vol}(X).$$

But since P' is proper we clearly have

$$\mathrm{size}(\widetilde{P}) \leqslant \big(d(d!)^2\big)^d \mathrm{size}(P').$$

Putting these bounds together, recalling that $s = d(d!)^2 t$ and making some crude simplifications, the result follows. □

3. Chang's version of Freiman's theorem

In this section we use Theorem 2.5 to make a deduction concerning Freiman's theorem. The following is shown in Chang's paper [2]; see also [3].

Proposition 3.1 (Chang)**.** *Suppose that $A \subseteq \mathbb{Z}$ is a set with $|A + A| \leqslant K|A|$. Then there is a progression P of dimension $d \leqslant CK^2 \log^3 K$ and size at most*[2]

$$|P| \leqslant \exp(CK^2 \log^2 K)|A| \tag{3.1}$$

such that $A \subseteq P$.

In the last few pages of [2] it is shown how one can bootstrap this to a theorem in which the bound on the dimension is $d \leqslant \lfloor K - 1 \rfloor$, the progression P is proper, and the containment bound (3.1) is not substantially worse. It is this refined result we discuss here.

[2]In fact in the notes [3] the explicit value $C = 2^{20}$ is obtained; as a rule, I am too old and lazy nowadays to worry overly much about explcit constants.

Theorem 3.2 (Chang)**.** *Suppose that $A \subseteq \mathbb{Z}$ is a set with $|A+A| \leqslant K|A|$. Let $\epsilon > 0$, and suppose that $|A| \geqslant N_0(K,\varepsilon)$, where we can take $N_0(K) := CK^6/\varepsilon$. Then there is a t-proper progression $\widetilde{P}$ of dimension $\widetilde{d} \leqslant \lfloor K - 1 + \varepsilon \rfloor$ and size at most*

$$|\widetilde{P}| \leqslant t^K \exp(CK^2 \log^3 K)|A|. \tag{3.2}$$

such that $A \subseteq P'$.

Remarks. In any application that I can imagine, t would be taken to be some absolute constant, in which case the t^K term here may be absorbed into the $\exp(CK^2 \log^3 K)$ term.

The dependence on ε, which does not feature in Chang's formulation of this result, has been introduced so that the function $N_0(K,\varepsilon)$ behaves reasonably. The result still holds with $\varepsilon = 0$, but the function $N_0(K,0)$ necessarily behaves very erratically. Consider, for example, the set

$$A = \{1, \dots, m\} \cup \{M\},$$

where $M \gg m$. It is easy to check that $|A+A| = 3m$, and so A has doubling $3m/(m+1)$. It is clear, however, that A is not economically contained in an arithmetic progression. This example implies that $N_0(3-\eta, 0) \geqslant 3/\eta$, and so $N_0(K,0)$ is not bounded as $K \to 3^-$; a similar phenomenon may be observed just to the left of any positive integer $K \geqslant 4$.

Let us start working with the conclusions of Proposition 3.1. We have a set A with $|A| \geqslant N_0(K,\varepsilon)$ and $|A+A| \leqslant K|A|$, and it is known to be contained in P, a (not necessarily proper) progression of dimension $d \ll K^2 \log^2 K$ and size bounded by $\exp(CK^2 \log^2 K)|A|$. Pick an arbitrary $a \in A$, and consider the set $\widetilde{A} = A - a$. It is clear that this set is contained in a *centred* progression $\widetilde{P}$ with the same dimension as P and size no more than 2^d size(P).

Dropping the tildes, we assume from now on that $0 \in A$ and that P is centred. P may therefore be represented as a convex progression, thus $P = \phi(B \cap \mathbb{Z}^d)$, where B is a box and $\mathrm{vol}(P) \leqslant \mathrm{size}(P)$. Applying Lemma 2.3 with $s = 2$, we may find some $d_1 \leqslant d$ and a 2-proper convex progression X_1 such that $P \subseteq X_1$ and

$$\mathrm{vol}(X_1) \leqslant 2^d d! \mathrm{vol}(P) \leqslant \exp(CK^2 \log^3 K)|A|. \tag{3.3}$$

Write $X_1 = \phi_1(B_1 \cap \mathbb{Z}^{d_1})$, where $\phi_1|_{2B_1 \cap \mathbb{Z}^{d_1}}$ is one-to-one. Then we see that the map $\phi_1|_{B_1 \cap \mathbb{Z}^{d_1}}$ is a *Freiman isomorphism,* and so the inverse image $Y := \phi^{-1}(A)$ has $|Y| = |A|$ and $|Y+Y| = |A+A| \leqslant K|Y|$. Our next task is to prove the rather remarkable result that Y is contained in an affine subspace of dimension at most $\lfloor K - 1 + \varepsilon \rfloor$.

It is rather convenient to drop the subscript 1 henceforth. Thus we write $X := X_1$, $d_1 := d$, $B_1 := B$. All we need recall is the bound (3.3).

Proposition 3.3 (Freiman's Lemma)**.** *Suppose that $A \subseteq \mathbb{R}^r$ is not contained in an affine subspace. Then we have the lower bound*

$$|A+A| \geqslant (r+1)|A| - \tfrac{1}{2}r(r+1). \tag{3.4}$$

In particular if $r \leqslant CK^3$ and if $|A| \geqslant N_0(K,\varepsilon) = CK^6/\varepsilon$, then in fact

$$r \leqslant \lfloor K - 1 + \varepsilon \rfloor. \tag{3.5}$$

Proof. The set $A+A$ obviously has the same size as the set $m(A) := \frac{1}{2}(A+A)$ of midpoints of line segments of A (note that $A \subseteq m(A)$). Let $F(r,n)$ denote the minimum value of $|m(A)|$ amongst all sets $A \subseteq \mathbb{R}^r$ which are not contained in an affine subspace and for which $|A| = n$. Consider an extreme point a on the convex hull of A. The set $A' := A \setminus \{a\}$ is either contained in an $(r-1)$-dimensional affine subspace, or it is not. In the former case we clearly have $m(A) \geqslant m(A') + n$, since none of the midpoints of the line segments $[ax]$, $x \in A$, lies in $m(A')$. In the latter case we have $m(A) \geqslant m(A') + r + 1$. Indeed if S is the r-face nearest to a then none of the midpoints of the segments $[ax]$, $x \in S$, lie in $m(A')$, and nor does a.

Both of the cases here are compatible with the inequality

$$F(r,n) \geqslant \min(F(r-1,n-1)+n, F(r,n-1)+r+1).$$

It follows by induction on $r+n$ that

$$F(r,n) \geqslant (r+1)n - \tfrac{1}{2}r(r+1),$$

which immediately implies (3.4). The bound (3.5) follows after a short computation. □

Recall now the paragraph before the statement of Proposition 3.3, where we had a full, centrally symmetric convex body $B \subseteq \mathbb{R}^d$ and a set $Y \subseteq B \cap \mathbb{Z}^d$ such that $|Y+Y| \leqslant K|Y|$ and $|Y| \geqslant N_0(K,\varepsilon)$. Since d is known to be $O(K^2 \log^2 K)$, and hence certainly at most CK^3, Proposition 3.3 applies and we may conclude that Y is contained in B', the intersection of B with some subspace $H \leqslant \mathbb{R}^d$ of dimension $d' = \lfloor K - 1 + \varepsilon \rfloor$. Note that $0 \in A$, and so H really can be taken to be a linear subspace, rather than just an affine subspace. It certainly follows that A is contained in a convex progression of dimension at most d'; our task now is to show that the volume of this convex progression can be taken to be reasonably small.

In order to do this, we first make sure that B is appropriately "round[3]". To do this, we simply apply an endomorphism $\tau : \mathbb{R}^d \to \mathbb{R}^d$ with $|\det \tau| = 1$ such that the Mahler basis $\{w_1, \dots, w_d\}$ of $\mathbb{Z}^d$ with respect to B is mapped to the standard orthonormal basis $\{e_1, \dots, e_d\}$. Write $\widetilde{B} := \tau(B)$, and set $\widetilde{\phi} := \phi \circ \tau^{-1}$. Note that the convex progression $\widetilde{X} := \widetilde{\phi}(\widetilde{B} \cap \mathbb{Z}^d)$ is, as a set of points[4], precisely the same as X.

Recall that $w_i \in i\lambda_i B$ for all $i = 1, \dots, d$, where $\lambda_1 \leqslant \dots \leqslant \lambda_d$ are the successive minima of B with respect to $\mathbb{Z}^d$. Since B is full, we have $\lambda_i \leqslant 1$ for all i. It follows that $\widetilde{B}$ contains the points $\pm e_i/i$, $i = 1, \dots, d$, and hence the octahedron O spanned by these points.

Now the Cauchy-Schwarz inequality implies that if $x_1^2 + \dots + x_d^2 \leqslant d^3$ then $x_1 + 2x_2 + \dots + dx_d \leqslant 1$. It follows that O, and hence $\widetilde{B}$, contains the Euclidean ball $\mathcal{B}(0, d^{-3/2})$.

Once more we drop tildes for notational convenience, redefining $B := \widetilde{B}$, $X := \widetilde{X}$ and $\phi := \widetilde{\phi}$. The gain from our previous situation is that we have replaced the knowledge

[3]This is all rather close to John's theorem, but we persist in using just the tools we have already created, viz. Minkowski's second theorem and the Mahler basis.

[4]As we remarked earlier, X and $\widetilde{X}$ should not, technically, be regarded as the same convex progression.

that B is full with the fact that $\mathcal{B}(0, d^{-3/2}) \subseteq B$. The convex body B might now reasonably be described as "round". The next lemma is [1, Lemma 6.5].

Lemma 3.4 (Sections of round convex bodies)**.** *Suppose that $B \subseteq \mathbb{R}^m$ is a centrally symmetric convex body and that $\mathcal{B}(0,\rho) \subseteq B$. Suppose that $H \leqslant \mathbb{R}^m$ is a subspace of dimension $m - r$. Write $B' = B \cap H$. Then we have*

$$\mathrm{vol}_{m-r}(B') \leqslant \frac{m!}{(m-r)!\rho^r}\mathrm{vol}_m(B).$$

Proof. Set $H_0 := H$, $B_0 := B'$ and $m_0 := m - r$. Now there must be some point $x_1 \in \mathcal{B}(0,\rho)$ whose distance from H_0 is at least ρ. Set $H_1 := \mathrm{Span}_{\mathbb{R}}(H, x_1)$ and $m_1 := m - r + 1$. Then $B_1 := B \cap H_1$ contains the section B_0 and the points $\pm x$, and hence the convex hull of these points, which is a double-sided cone. The volume of this cone is $2\rho\mathrm{vol}_{m_0}(B_0)/m_1$, and thus

$$\mathrm{vol}_{m_1}(B_1) \geqslant \frac{\rho}{m-r+1}\mathrm{vol}_{m_0}(B_0).$$

Continuing inductively, we obtain

$$\mathrm{vol}_{m_j}(B_j) \geqslant \frac{\rho^j}{(m-r+1)\dots(m-r+j)}\mathrm{vol}_{m_0}(B_0).$$

Taking $j = r$ gives the result. □

Let us return now to the paragraph immediately following Proposition 3.3. We had $A \subseteq \phi(B \cap \mathbb{Z}^d)$, and we are now in a position to assume that B is *round* in the sense that $\mathcal{B}(0, d^{-3/2}) \subseteq B$. Recall that d is subject to the bound

$$d \leqslant CK^2 \log^2 K. \tag{3.6}$$

We observed that $Y := \phi^{-1}(A)$ was, being Freiman isomorphic to A, subject to the doubling estimate $|Y+Y| \leqslant K|Y|$. We concluded that $Y \subseteq B' := B \cap H$, where $H \leqslant \mathbb{R}^d$ is subspace of dimension $d' = \lfloor K - 1 + \varepsilon \rfloor$. By relaxing this condition to $d' \leqslant \lfloor K - 1 + \varepsilon \rfloor$ if necessary, we may assume that the lattice $\Lambda' := H \cap \mathbb{Z}^d$ is d'-dimensional, and that B' is full with respect to Λ'. Write $\phi' := \phi|_H$, and let $\psi : H \to \mathbb{R}^{d'}$ be any endomorphism such that $\psi(\Lambda') = \mathbb{Z}^{d'}$. It is clear that $|\det(\psi)| \leqslant 1$. Define

$$B'' := \psi(B')$$

and

$$\phi'' := \phi' \circ \psi^{-1}.$$

Then A is contained in the coset progression $X'' := \phi''(B'' \cap \mathbb{Z}^{d'})$. We estimate the volume of X''. Note first of all that, since $|\det(\psi)| \leqslant 1$, we have

$$\mathrm{vol}(X'') := \mathrm{vol}_{d'}(B'') \leqslant \mathrm{vol}_{d'}(B').$$

However Lemma 3.4 and the fact that $\mathcal{B}(0, d^{-3/2}) \subseteq B$ tell us that

$$\mathrm{vol}_{d'}(B) \leqslant d! d^{3d/2}\mathrm{vol}_d(B) = d! d^{3d/2}\mathrm{vol}(X).$$

Combining these estimates with (3.3) leads to

$$\mathrm{vol}(X'') \leqslant \exp(CK^2 \log^3 K)|A|. \tag{3.7}$$

Now simply apply Theorem 2.5, and we are done. □

References

[1] Y. Bilu, *Structure of sets with small sumset,* Structure theory of set addition. Astérisque **258** (1999), xi, 77–108.
[2] M. C. Chang, *Generalized arithmetical progressions and sumsets,* Acta Math. Hungar. **65** (1994), no. 4, 379–388.
[3] B. J. Green, *Edinburgh lecture notes on Freiman's theorem,* unpublished.
[4] B. J. Green and T. C. Tao, *Convex geometry and the Freiman-Bilu theorem,* in preparation.
[5] T. C. Tao and V. H. Vu, *Additive combinatorics,* book in preparation.

Department of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, England
E-mail address: b.j.green@bristol.ac.uk