A POLYNOMIAL BOUND IN FREIMAN'S THEOREM

Mei-Chu Chang
Department of Mathematics
UCR
Riverside, CA 92521

Abstract. In this paper the following improvement on Freiman's theorem on set addition is obtained. (Theorem 1 and Theorem 2 in Section 1.)

Let $A \subset \mathbb{Z}$ be a finite set such that $|A+A| < \alpha|A|$. Then A is contained in a proper d-dimensional progression P, where $d \leq [\alpha - 1]$ and $\log \frac{|P|}{|A|} < C\alpha^2(\log \alpha)^3$.

Earlier bounds involved exponential dependence in α in the second estimate. Our argument combines Ruzsa's method, which we improve in several places, as well as Bilu's proof of Freiman's theorem.

A fundamental result in the theory of set addition is Freiman's theorem. Let $A \subset \mathbb{Z}$ be a finite set of integers with small sumset, thus assume

$$|A+A| < \alpha|A| \tag{0.1}$$

where

$$A+A = \{x+y|\ x, y \in A\} \tag{0.2}$$

and $|\cdot|$ denotes the cardinality. The factor α should be thought of as a (possibly large) constant. Then Freiman's theorem states that A is contained in a d-dimensional progression P, where

$$d \leq d(\alpha) \tag{0.3}$$

and

$$\frac{|P|}{|A|} \leq C(\alpha). \tag{0.4}$$

Typeset by $\mathcal{A}_{\mathcal{M}}\mathcal{S}$-TEX

(Precise definitions will be given in the next section.) Although this statement is very intuitive, there is no simple proof so far and it is one of the deep results in additive number theory.

Freiman's book [Fr] on the subject is not easy to read, which perhaps explains why in earlier years the result did not get its deserved publicity. More recently, two detailed proofs were given. One, due to Y. Bilu [Bi], is close to Freiman's and very geometric in spirit. The other, due to I. Ruzsa [Ru2], is less geometric and is based also on results in graph theory, such as Plünnecke's theorem. More details of Ruzsa's proof will be given later.

In (0.3), (0.4), we denoted by $d(\alpha)$ and $C(\alpha)$ constants that depend on α. In most applications of Freiman's theorem, it also matters to have some quantitative understanding of this dependence. An optimal result would be to show linear dependence of $d(\alpha)$ in α and exponential dependence of $C(\alpha)$ (trivial examples mentioned in [Ru2] show that this would be optimal). This paper addresses that issue and provides a substantial improvement of what was gotten so far from either Bilu's or Ruzsa's approach.

But before getting into details, we mention very briefly some results and problems, subject of current research, that are intimately related to quantitative versions of Freiman's theorem.

(i) *T. Gowers' work on arithmetic progressions.* [G1], [G2]

A celebrated theorem of Szemerédi [Sz], solving an old conjecture of Erdős and Turán, roughly asserts that if $S \subset \mathbb{Z}_+$ is a set of positive upper density, i.e.

$$\lim_{N\to\infty} \sup \frac{|S \cap [1,N]|}{N} > 0 \tag{0.5}$$

then S contains arbitrarily long arithmetic progressions

$$a, a+b, a+2b, \dots, a+jb. \tag{0.6}$$

More precisely, there is a function $\delta(N,j)$ such that if $T \subset [1,N]$ and

$$|T| > \delta(N,j)N \tag{0.7}$$

then T contains a progression (0.6) of size j. Moreover, for fixed j,

$$\delta(N, j) \to 0, \text{when } N \to \infty. \tag{0.8}$$

Szemerédi's proof was a tour de force in combinatorics, which only few people tried to read and, certainly, extracting any quantitative information about the function $\delta(N, j)$ from it looks hopeless.

Later a more conceptual approach based on ergodic theory was developed by H. Furstenberg and his collaborators (see [Fu], [F-K-O], ...). This method applies also in greater generality (see for instance [B-L] on polynomial versions of Szemerédi's theorem) but has the drawback of providing no quantitative information at all.

In recent work [G1], [G2], T. Gowers established a lower bound

$$\delta(N, j) < \frac{1}{(\log\log N)^{c(j)}}. \tag{0.9}$$

Notice that already for $j = 4$, absolutely no estimate was known (the case $j = 3$ goes back to K. Roth [Ro]). In fact, even for van der Waerden's theorem on progression [VdW], published in 1927, bounds expressed by primitively recursive functions were only given a few years ago (see [Sh]). Gowers' estimate (0.9) is therefore certainly most spectacular. The key ingredient in this approach is a quantitative version of Ruzsa's proof of Freiman's theorem. Further progress on this issue is therefore of primary importance to the problematic of progressions in 'thin' sets of integers (most notoriously, the set of prime numbers).

(ii) *The dimension of measurable rings of real numbers.*

Let $S \subset \mathbb{R}$ be a measurable set and a ring in the algebraic sense, i.e. $S + S \subset S$, $S.S \subset S$. An old conjecture of Erdős states that the Hausdorff-dimension of S is either 0 or 1. It is known that if $\frac{1}{2} < \dim S \leq 1$, then $\dim S = 1$ (see [Fal]). The problem for $0 \leq \dim S \leq \frac{1}{2}$ turns out to be much harder and is closely related to the following conjecture of Erdős and Szemerédi [E-S].

Conjecture. If A is a finite set of integers, then

$$|E_2(A)| \geqq |A|^{2-\varepsilon} \text{ for all } \varepsilon > 0 \tag{0.10}$$

where

$$E_2(A) = (A + A) \cup A.A. \tag{0.11}$$

In [N-T], it is shown that if $A_1, A_2 \subset \mathbb{Z}$ are finite sets and

$$|A_1| = |A_2| = k \geq 2, |A_1 + A_2| \leq 3k - 4 \tag{0.12}$$

then

$$|A_1.A_2| \geqq \left(\frac{k}{\log k}\right)^2. \tag{0.13}$$

Here one uses the fact that if (0.12) holds, then A_1 and A_2 are contained in a 1-dimensional arithmetic progression. This is a special case of Freiman's general theorem, where a strong conclusion holds.

Related to the general conjecture, the record at this point is (see [El])

$$|E_2(A)| > c|A|^{5/4} \tag{0.14}$$

obtained from the Szemerédi-Trotter theorem on line-incidences in the plane (see [S-T]).

(iii) *Relation of Freiman's theorem on set-addition to the problem of the dimension of Besicovitch sets in* $\mathbb{R}^d$.

Recall that a measurable subset $A \subset \mathbb{R}^d, d \geqq 2$ is a Besicovitch set if it contains a line segment in every direction. Such sets may be of zero-measure but it is likely that always $\dim A = d$ (the maximal dimension). For $d = 2$, this is a known result, but the question for $d > 2$ appears to be very hard (for $d = 3$, best result so far is Hausdorff-dim $A \geq \frac{5}{2}$, for Minkowski-dim $A \geq \frac{5}{2} + \epsilon$ [K-L-T]). This is a problem in geometric measure theory with major implications to Fourier Analysis in several variables. It has been subject to intensive research during the last decade, a survey

of which the reader may find in [W], [T] (relations of this problem and a number of other conjectures to the Erdős ring problem are discussed in [K-T], [T]).

For application in other subjects such as group theory, coding theory and integer programming, see [He], [Ru3], [C-Z], [Ch].

We now return to the content of the paper.

We will mostly follow Ruzsa's method (providing the best bounds so far) and improve several places in his argument. Basically there are two stages in Ruzsa's method. First, one generates a large progression $P_0 \subset 2A - 2A$ by embedding a subset of A in $\mathbb{Z}_N$, finding a large progression in this image, then pushing it back to $\mathbb{Z}$. Next, enlarges P_0 to get a progression $P_1 \supset A$. The progression P_0 is of dimension

$$d_0 \leq d_0(\alpha) \tag{0.15}$$

and

$$\frac{|A|}{|P_0|} < C_0(\alpha). \tag{0.16}$$

Rusza obtains $d_0(\alpha) < \alpha^4$ and $\log C_0(\alpha)$ bounded by some power of α. We improve this here to

$$d_0(\alpha) \lesssim \alpha \log \alpha \tag{0.17}$$

$$\log C_0(\alpha) \lesssim \alpha (\log \alpha)^2 \tag{0.17'}$$

by refining the harmonic analysis part related to the circle method. We do feel however that this statement is not optimal and it does not seem unreasonable to conjecture bounds α^{ε} or even $C \log \alpha$ in (0.17) (if true, this last statement would have substantial new applications). Notice that the construction of the progression P_0 inside A is the hard part of the argument. Once P_0 is obtained, one considers a maximal set of elements $a_1, \cdots, a_s \in A$ s.t. the sets $a_i + P_0$ are naturally disjoint. Then

$$A \subset \{a_1, \ldots, a_s\} + P_0 - P_0 \tag{0.18}$$

and we use $\{a_1, \dots, a_s\}$ as additional generators for a progression $P \supset A$, whose dimension may be bounded by

$$d(\alpha) \leq s + \dim P_0 \leq C_0(\alpha) + d_0(\alpha). \tag{0.19}$$

This procedure introduces thus an *exponential* dependence of $d(\alpha)$ on α in (0.3) because of the $C_0(\alpha)$-dependence. We present here a more economical procedure, replacing (0.19) by

$$d(\alpha) \lesssim \alpha \log C_0(\alpha) + d_0(\alpha) \lesssim \alpha^2 (\log \alpha)^2. \tag{0.20}$$

As mentioned earlier

$$d(\alpha) \lesssim \alpha \tag{0.21}$$

would be the optimal result here.

The progression P obtained is not necessarily proper (see next section for definition). In [Bi], it is shown how starting from Ruzsa's result one may replace P by a proper progression still satisfying (0.3), (0.4). Based on a variant of this argument, we obtain Theorem 2 below (cf. Section 1) , where $P \supset A$ is a *proper* progression of dimension $d \leq [\alpha - 1]$ and $\log \frac{|P|}{|A|} < C\alpha^2 (\log \alpha)^3$.

In this paper, $\mathbb{Z}_N$ always denote $\mathbb{Z}/N\mathbb{Z}$.

The paper is organized as following,

In Section 1, we give preliminaries, and the precise statement of our theorems. Also we summarize Ruzsa's method.

In Section 2, we improve step 4 in Ruzsa's method.

In Section 3, we prove a technical proposition which is used for the improvement of step 4 in Ruzsa's method.

In Section 4, we prove Theorem 2.

Acknowledgement The author would like to thank J. Bourgain for helpful discussions, particularly for explaining Ruzsa's method and various mathematics

(in fact, most of the introduction) related to Freiman's Theorem. The author would also like to thank T. Gowers for pointing out some errors in an earlier version of the paper.

SECTION 1. Preliminary and Ruzsa's method.

We begin this section with recalling some definitions. For the readers' convenience, we write here various theorems from [Na] in the form we need. For proofs, please see [Na].

A d-dimensional (generalized) arithmetic *progression* is a set of the form

$$\begin{aligned} P &= P(q_1, \dots, q_d; \ell_1, \dots, \ell_d; a) \\ &= \{a + x_1 q_1 + \cdots + x_d q_d \big| \ 0 \le x_i < \ell_i, i = 1, ..., d\} \end{aligned} \tag{1.1}$$

The *length* of P is

$$\ell(P) = \prod_{i=1}^{d} \ell_i. \tag{1.2}$$

Clearly $|P| \le \ell(P)$ (Here $|P|$ is the cardinality of P.)

If $|P| = \ell(P)$, the progression is called *proper*.

Denote

$$A + B = \{a + b| \ a \in A, b \in B\} \tag{1.3}$$

$$hA = A + \cdots + A \ (h \text{ fold}). \tag{1.4}$$

Observe that if P in (1.1) is proper, then

$$|2P| \le 2^d |P|. \tag{1.5}$$

The above makes sense in any Abelian group but we restrict ourselves to $\mathbb{Z}$ in this paper.

The following result is a structural theorem for subset of $\mathbb{Z}$ with "small" doubling set.

Freiman's theorem. *Let $A \subset \mathbb{Z}$ be a finite set and*

$$|2A| \leq \alpha |A|. \tag{1.6}$$

Then A is contained in a d-dimensional generalized arithmetic progression P, where

$$d \leq d(\alpha) \tag{1.7}$$

$$\ell(P) \leq C(\alpha)|A|. \tag{1.8}$$

Our interest here goes to the quantitative aspects. Known bounds (obtained in [Ru]) for $d(\alpha)$ in (1.7) (respectively, $C(\alpha)$ in (1.8)) are exponential (resp. double exponential) in α. The role of α here is a possibly large constant. In this paper, the following improvement will be obtained.

Theorem 1. *Freiman's theorem holds with $d(\alpha)$ and $\log C(\alpha)$ bounded by $C\alpha^2(\log \alpha)^2$ (the letter C will stand for various absolute constants).*

Theorem 2. *Assume $A \subset \mathbb{Z}$ a finite set satisfying (1.6). Then $A \subset P$, where P is a proper d-dimensional arithmetic progression, with*

$$d \leq [\alpha - 1] \tag{1.9}$$

$$\log \frac{|P|}{|A|} \leq C\alpha^2(\log \alpha)^3. \tag{1.10}$$

Remark 2.1. Compared with Theorem 1, (1,9) is an improvement of (1.7). Moreover, P is proper in Theorem 2.

Theorem 2 will be deduced from Theorem 1 using an additional argument from [Bi].

These statements answer to a satisfactory extent the question raised at the end of [Ru] (where it is conjectured that one may take $d(\alpha), \log C(\alpha) \lesssim \alpha$) and also in [Na].

To prove Theorem 1, we basically follow Ruzsa's proof in its consecutive steps and will bring an improvement in two of them. Notice that, although simpler than Freiman's, Ruzsa's argument remains fairly nontrivial and combines techniques and results from at least 3 different fields, graph theory (Plünnecke's inequalities), geometry of numbers (Minkowski's second theorem) and harmonic analysis (Bogolyubov's method).

Now, some preliminaries.

Recall that a "Freiman homomorphism of order h" ($h \geq 2$) is a map

$$\phi : A \to B \qquad (A, B \subset \mathbb{Z})$$

such that

$$\phi(a_1) + \cdots + \phi(a_h) = \phi(a'_1) + \cdots + \phi(a'_h) \tag{1.11}$$

if $a_1, \cdots, a_h, a'_1, \cdots, a'_h \in A$ and $a_1 + \cdots + a_h = a'_1 + \cdots a'_h$.

If $\phi : A \to B$ is a one-to-one correspondence and satisfies that

$$a_1 + \cdots + a_h = a'_1 + \cdots + a'_h$$

if and only if

$$\phi(a_1) + \cdots + \phi(a_n) = \phi(a'_1) + \cdots + \phi(a'_h) \tag{1.12}$$

then ϕ is called a Freiman isomorphism of order h.

We begin with two easy lemmas. Their proofs can be found in Nathanson's book. ([Na], Theorems 8.5 and 8.4)

Lemma 1.1. *If $h = h'(k + \ell)$ and A, B are Freiman isomorphic of order h, then $kA - \ell A$ and $kB - \ell B$ are Freiman isomorphic of order h'.*

Lemma 1.2. *Let P be a d-dimensional arithmetical progression and $\phi : P \to \mathbb{Z}$ a Freiman homomorphism of order $h \geq 2$. Then $\phi(P)$ is d-dimensional progression. If P is proper and ϕ a Freiman isomorphism, then $\phi(P)$ is also proper.*

The following is an important inequality due to Plünnecke.

Proposition 1.3. *([Na], Theorem 7.8) Let A be a finite subset of an Abelian group such that*

$$|2A| = |A + A| \leq \alpha |A|.$$

Then, for all $k, \ell > 1$

$$|kA - \ell A| \leq \alpha^{k+\ell} |A|.$$

Now, we summarize the main steps in Ruzsa's proof.

Step 1. ([Na], Theorem 8.9) Fix $h \geq 2$ and denote $D = hA - hA$. Let N be the smallest number such that

$$N > 4h|D|. \tag{1.13}$$

Then there is a subset $A_1 \subset A$,

$$|A_1| > \frac{|A|}{h} \tag{1.14}$$

which is Freiman isomorphic of order h to a subset of $\mathbb{Z}_N$.

Denote by

$$\phi : A_1 \to A_1' \subset \mathbb{Z}_N \tag{1.15}$$

this h-Freiman isomorphism.

From (1.13) and (1.14) and Proposition 1.3, we may thus ensure that

$$N < 8h|D| \leq 8h\alpha^{2h}|A| < 8h^2\alpha^{2h}|A_1'|. \tag{1.16}$$

Next, one invokes the following fact.

Step 2. (Bogolyubov, [Na], Theorem 8.6)

Let $\mathcal{R} \subset \mathbb{Z}_N$, with $|\mathcal{R}| = \lambda N$. Then for some integer $d \leq \lambda^{-2}$, there exist pairwise distinct elements $r_1, \ldots, r_d \in \mathbb{Z}_N$ s.t.

$$B\left(r_1, \cdots, r_d; \frac{1}{4}\right) \subset 2\mathcal{R} - 2\mathcal{R} \tag{1.17}$$

where

$$B(r_1,\dots,r_d,\varepsilon):=\{g\in\mathbb{Z}_N|\ \|\frac{gr_i}{N}\|<\varepsilon,\ \text{for } i=1,\dots,d\} \tag{1.18}$$

denotes the "Bohr neighborhood".

Also, for $x\in\mathbb{R}$, $\|x\|=\ \text{dist}\,(x,\mathbb{Z})$.

Remark. The proof of this is a discrete version of the usual circle method (cf. also [F-H-R], [R2]).

Step 3. ([Na], Theorem 8.7) The Bohr set $B(r_1,\dots,r_d;\varepsilon)$ defined in (1.18) contains a (proper) arithmetic progression $P\subset\mathbb{Z}_N$, $\dim P=d$ and

$$|P|>N(\frac{\varepsilon}{d})^d. \tag{1.19}$$

Remark. The main tool involved in the proof is Minkowski's second theorem on the consecutive minima.

Applying Step 2 with $\mathcal{R}=A_1',\lambda^{-1}\le 8h^2\alpha^{2h}$ (cf. (1.16)), yields thus a Bohr-set $B(r_1,\dots,r_d;\frac{1}{4})\subset 2A_1'-2A_1'$ with

$$d\le 64\,h^4\,\alpha^{4h}. \tag{1.20}$$

Application of Step 3 gives a d-dim progression $P'\subset 2A_1'-2A_1'$

$$|P'|>\frac{N}{(4d)^d}>\frac{|A|}{h(4d)^d}. \tag{1.21}$$

By Lemma 1.1, the map ϕ in (1.15) induces an $\frac{h}{4}$-Freiman isomorphism

$$\psi: 2A_1-2A_1\to 2A_1'-2A_1' \tag{1.22}$$

and, assuming $\frac{h}{4}\ge 2$, it follows from Lemma 1.2 that $P_0:=\psi^{-1}(P')$ is a (proper) d-dimensional progression in $2A_1-2A_1\subset 2A-2A$. Moreover, by (1.21)

$$|P_0|>\frac{|A|}{h(4d)^d}. \tag{1.23}$$

Step 4. This is the final step to conclude the proof. The argument is the same as that in [Chan]. Simply consider a maximal collection $\{a_1, \cdots, a_s\} \subset A$ for which the sets $a_i + P_0 \subset \mathbb{Z}$ are mutually disjoint. Hence, for each $a \in A$, we get

$$a + P_0 \cap a_i + P_0 \neq \phi, \text{ for some i.}$$

Therefore,

$$a \in a_i + P_0 - P_0, \text{ for some } i = 1, \ldots, s,$$

i.e.

$$a \in \{a_1, \ldots, a_s\} + P_0 - P_0. \tag{1.24}$$

The set in (1.24) is clearly contained in a progression P_1 of dimension

$$\dim P_1 = s + \dim P_0 = s + d \tag{1.25}$$

and

$$\ell(P_1) \leq 2^s 2^d \ell(P_0) = 2^{s+d}|P_0| \leq 2^{s+d}|2A - 2A| \leq 2^{s+d}\alpha^4|A|. \tag{1.26}$$

It remains to bound s. Clearly, from (1.23) and Proposition 1.3,

$$\frac{s}{h(4d)^d}|A| < s|P_0| = |P_0 + \{a_1, \ldots, a_s\}| \leq |2A - 2A + A| \leq \alpha^5|A|.$$

Hence,

$$s < h(4d)^d \alpha^5. \tag{1.27}$$

Observe that (1.20) and (1.27) lead to exponential dependence of s and $\dim P_1$ in α.

SECTION 2. Some improvement of Step 4.

In this section, we will improve Step 4 in Ruzsa's argument. The improvement is a rather trivial one, but permits already to replace the exponential α-dependence of $d(\alpha) = \dim P_1$ by a powerlike bound $d(\alpha) < \alpha^C$. This bound will mainly depend on $d = \dim P_0$ for the progression P_0, where P_0 is obtained above from Steps 2 and 3.

This section concerns what can be deduced from the following proposition, which will be prove in Section 3..

Proposition 2.1. *Let $A \subset \mathbb{Z}$ be a finite set such that $|2A| \leq \alpha|A|$. Then $2A - 2A$ contains a (proper) progression P with*

$$d = \dim P < C(\log \alpha)\alpha \tag{2.1}$$

and

$$|P| > \frac{|A|}{8(10d^2)^d}. \tag{2.2}$$

To improve step 4, we apply Proposition 2.1. This provides an arithmetic progression

$$P \subset 2A - 2A \tag{2.3}$$

such that, from (2.1) and (2.2), we have

$$d = \dim P \lesssim \alpha(\log \alpha) \tag{2.4}$$

$$|P| > \frac{|A|}{8(10d^2)^d} \tag{2.5}$$

Assuming that there exists a set $S_1 \subset A$

$$|S_1| = 10\alpha \tag{2.6}$$

such that

$$(P + x) \cap (P + y) = \emptyset \text{ for } x \neq y \text{ in } S_1, \tag{2.7}$$

we define

$$P^{(1)} = P + S_1 \subset 2A - 2A + A. \tag{2.8}$$

Then it follows from (2.6) and (2.7), we have

$$|P^{(1)}| = 10\alpha|P|. \tag{2.9}$$

Next, we assume again that there is a subset $S_2 \subset A$,

$$|S_2| = 10\alpha \tag{2.10}$$

such that

$$(P^{(1)} + x) \cap (P^{(1)} + y) = \emptyset, \text{ for } x \neq y \in S_2. \tag{2.11}$$

Thus

$$P^{(2)} = P^{(1)} + S_2 \subset 2A - 2A + A + A = 2A - 2A + 2A, \tag{2.12}$$

and

$$|P^{(2)}| = (10\alpha)^2 |P|. \tag{2.13}$$

If the process may be iterated t times, we obtain

$$P^{(t)} = P + S_1 + \cdots + S_t \subset 2A - 2A + tA, \tag{2.14}$$

and

$$|P^{(t)}| = (10\alpha)^t |P|. \tag{2.15}$$

It follows from (2.5), (2.15), (2.14) and Proposition 1.3, we have

$$(10\alpha)^t \frac{|A|}{8(10d^2)^d} \leq |(2+t)A - 2A| \leq \alpha^{4+t}|A|. \tag{2.16}$$

Hence,

$$10^t \leq 8\alpha^4 (10d^2)^d \tag{2.17}$$

Now, (2.4) gives

$$t \lesssim \log \alpha + d \log d \lesssim \alpha (\log \alpha)^2. \tag{2.18}$$

Therefore, after t steps (note that t is bounded in (2.18)), the set S_t can not be defined, i.e., there is a set $S_t' \subset A$, $|S_t'| < 10\alpha$, such that for each $x \in A$, there is $a \in S_t'$ with

$$(x + P^{(t-1)}) \cap (a + P^{(t-1)}) \neq \emptyset$$

hence

$$x \in a + P^{(t-1)} - P^{(t-1)} \subset S_t' + P^{(t-1)} - P^{(t-1)}. \tag{2.19}$$

It follows, recalling (2.14), that

$$A \subset (P - P) + (S_1 - S_1) + \cdots + (S_{t-1} - S_{t-1}) + S_t'. \tag{2.20}$$

If $P = P(q_1, \dots, q_d; \ell_1, \dots, \ell_d)$, (cf. (1.1)), then (2.20) is clearly contained in a translate of the progression

$$\bar{P} = P(q_1, \dots, q_d, \underset{r<t}{\cup} S_r \cup S'_t; 2\ell_1, \dots, 2\ell_d, 3, \dots, 3, 2) \tag{2.21}$$

of dimension

$$\bar{d} = \dim \bar{P} = d + \sum_{r<t} |S_r| + |S'_t| < d + 10\alpha t \tag{2.22}$$

and

$$\ell(\bar{P}) \leq 2^d \ell(P) \cdot 3^{10\alpha t} = 2^d 3^{10\alpha t} |P| \leq 2^d 3^{10\alpha t} \alpha^4 |A|. \tag{2.23}$$

(The last inequality is by (2.3) and Proposition 1.3.) Together with (2.4), (2.18), this yields Freiman's theorem with a $\bar{d}$-dimensional progression $\bar{P}$ satisfying

$$\bar{d} \lesssim \alpha^2 (\log \alpha)^2, \ell(\bar{P}) < C^{\bar{d}} |A|. \tag{2.24}$$

Remark. The progression $\bar{P}$ need not be proper.

SECTION 3. Proof of Proposition 2.1.

By theorem 8.9 in [Na] (in our Step 1, take $h = 8$), there is a subset $A_1 \subset A$,

$$|A_1| > \frac{|A|}{8} \tag{3.1}$$

which is 8-isomorphic to a subset $\mathcal{R}$ of $\mathbb{Z}_N$, with N prime and

$$N < 40|8A - 8A| < 40\alpha^{16}|A|. \tag{3.2}$$

Denote by $\phi : A_1 \to \mathcal{R}$ this 8-isomorphism. To prove the Proposition, it clearly suffices to produce a d-dimensional progression P in $2\mathcal{R} - 2\mathcal{R}$ satisfying (2.1), (2.2).

We will begin with some definitions and standard facts.

Let $f, g : \mathbb{Z}_N \to \mathbb{R}$ be functions. We define the following

1. $\hat{f}(m) \colon = \frac{1}{N} \sum_{0 \leq k < N} f(k) e^{-2\pi i \frac{km}{N}}$

2. $f * g(x) \colon = \frac{1}{N} \sum_{0 \le y < N} f(x-y) g(y)$

3. $f'(x) \colon = f(-x)$

Then the following facts are easy to verify.

a. $f(x) = \sum_{0 \le m < N} \hat{f}(m) e^{2\pi i \frac{mx}{N}}$

b. $\widehat{f * g}(m) = \hat{f}(m) \hat{g}(m)$

c. $f * f'(x) = \sum_{0 \le m < N} |\hat{f}(m)|^2 e^{2\pi i \frac{mx}{N}}$

d. $\sum_{0 \le m < N} |\hat{f}(m)|^2 = \frac{1}{N} \sum_{0 \le m < N} |f(m)|^2$

Let $f = \chi_{\mathcal{R}}$ be the indicator function of the set $\mathcal{R}$, i.e.

$\chi_{\mathcal{R}} = 1$, if $x \in \mathcal{R}$, 0 otherwise.

Then

e. $\mathrm{Supp}(f * f') \subset \mathcal{R} - \mathcal{R}$, and $\mathrm{Supp}(f * f) \subset 2\mathcal{R}$

f. $\mathrm{Supp}(f * f' * f * f') \subset 2\mathcal{R} - 2\mathcal{R}$

g. $f * f' * f * f'(x) = \sum_{0 \le m < N} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}}$

We also recall that the inner product of f and g is

4. $\langle f, g \rangle \colon = \frac{1}{N} \sum_{0 \le x < N} f(x) \bar{g}(x)$.

and we have the L^p-norm

5. $\|f\|_p \colon = (\frac{1}{N} \sum_{0 \le x < N} |f(x)|^p)^{\frac{1}{p}}$

We call a set $D = \{r_j\}_j \subset \mathbb{Z}_N$ *dissociated*, if

$$\sum \varepsilon_j r_j = 0 \text{ with } \varepsilon_j \in \{-1, 0, 1\}, \text{ then } \varepsilon_j = 0 \text{ for all } j. \tag{3.3}$$

h. (Rudin) If D is dissociated, then

$$\| \sum_{n \in D} a_n e^{2\pi i \frac{nx}{N}} \|_p \le C \sqrt{p} (\sum_{n \in D} |a_n|^2)^{\frac{1}{2}}.$$

Lemma 3.1. *Let $\mathcal{R} \subset \mathbb{Z}_N$ with $|\mathcal{R}| = \delta N$ and let $f = \chi_{\mathcal{R}}$ be the indicator function of $\mathcal{R}$. Let ρ be a constant. We define $\Gamma := \{0 \le m < N \big| |\hat{f}(m)| > \rho\delta\}$ and let Λ be a maximal dissociated subset of Γ. Then $|\Lambda| < \rho^{-2} \log \frac{1}{\delta}$.*

Proof. Let

$$g(x) = \sum_{n \in \Lambda} a_n e^{2\pi i \frac{nx}{N}}, \tag{3.4}$$

where

$$a_n = \frac{\hat{f}(n)}{\sqrt{\sum_{m \in \Lambda} |\hat{f}(m)|^2}}. \tag{3.5}$$

Let

$$p' = \frac{p}{p-1}. \tag{3.6}$$

Then Fact a, (3.4) and (3.5) give

$$\begin{aligned} \|f\|_{p'} \|g\|_p \ge |\langle f, g \rangle| = |\sum_{n \in \Lambda} \bar{a}_n \hat{f}(n)| &= \frac{\sum_{n \in \Lambda} |\hat{f}(n)|^2}{\sqrt{\sum_{m \in \Lambda} |\hat{f}(m)|^2}} \\ &= \sqrt{\sum_{n \in \Lambda} |\hat{f}(n)|^2} \ge \rho\delta\sqrt{|\Lambda|}. \end{aligned} \tag{3.7}$$

The last inequality is from the definition of Γ which contains Λ.

On the other hand,

$$\|f\|_{\frac{p}{p-1}} = (\frac{1}{N} \sum_{R} 1)^{\frac{p-1}{p}} = \delta^{\frac{p-1}{p}} \tag{3.8}$$

and

$$\|g\|_p \le C\sqrt{p}. \tag{3.9}$$

The last inequality follows from Fact h (Rudin).

Putting these together, we have

$$\rho\delta\sqrt{|\Lambda|} \le C\sqrt{p}\delta^{\frac{p-1}{p}}. \tag{3.10}$$

Now, choosing $p = \log \frac{1}{\delta}$, we have the bound claimed.

Lemma 3.2. *Let $\mathcal{R} \subset \mathbb{Z}_N$ with $|\mathcal{R}| = \delta N$ and $f = \chi_{\mathcal{R}}$, the indicator function of $\mathcal{R}$. Let ρ be a constant. We define $\Gamma := \{0 \le m < N \big| |\hat{f}(m)| > \rho\delta\}$. Denote $B = B(\Gamma, \varepsilon) = \{x \big| \|\frac{mx}{N}\| < \varepsilon, \text{for every } m \in \Gamma\}$, where $\varepsilon < \frac{1}{4}$.*

If $\rho^2\delta^3 < \frac{1-2\pi\varepsilon}{2-2\pi\varepsilon} \sum_{0\le m<N} |\hat{f}(m)|^4$, then $B \subset 2\mathcal{R} - 2\mathcal{R}$.

Proof. First, we note that from trignometry, for every $x \in B$, and for every $m \in \Gamma$

$$|1 - e^{2\pi i \frac{mx}{N}}| < 2\pi\varepsilon. \tag{3.11}$$

To show $B \subset 2\mathcal{R} - 2\mathcal{R}$, by Fact f, it suffices to show that

$$B \subset \text{Supp}(f * f' * f * f'). \tag{3.12}$$

According to Fact g, it suffices to show

$$\sum_{0\le m<N} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}} \neq 0, \text{for all } x \in B. \tag{3.13}$$

Write

$$\sum_m |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}} = \sum_{m\in\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}} + \sum_{m\notin\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}}, \tag{3.14}$$

The idea is to show $\big|\sum_{m\in\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}}\big|$ is big, while $\big|\sum_{m\notin\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}}\big|$ is small.

$$\begin{aligned}
\Big|\big|\sum_{m\in\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}}\big| - \sum_{m\in\Gamma} |\hat{f}(m)|^4\Big| &\le \big|\sum_{m\in\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}} - \sum_{m\in\Gamma} |\hat{f}(m)|^4\big| \\
&= \big|\sum_{m\in\Gamma} |\hat{f}(m)|^4 (e^{2\pi i \frac{mx}{N}} - 1)\big| \\
&\le \sum_{m\in\Gamma} |\hat{f}(m)|^4 |e^{2\pi i \frac{mx}{N}} - 1| \\
&< 2\pi\varepsilon \sum_{m\in\Gamma} |\hat{f}(m)|^4.
\end{aligned} \tag{3.15}$$

Therefore,

$$\begin{aligned}
\big|\sum_{m\in\Gamma} |\hat{f}(m)|^4 e^{2\pi i \frac{mx}{N}}\big| &> (1 - 2\pi\varepsilon) \sum_{m\in\Gamma} |\hat{f}(m)|^4 \\
&= (1 - 2\pi\varepsilon)(\sum_m |\hat{f}(m)|^4 - \sum_{m\notin\Gamma} |\hat{f}(m)|^4).
\end{aligned} \tag{3.16}$$

On the other hand,

$$\Big|\sum_{m\notin\Gamma}|\hat{f}(m)|^4 e^{2\pi i\frac{mx}{N}}\Big| \le \sum_{m\notin\Gamma}|\hat{f}(m)|^4. \tag{3.17}$$

The definition of Γ and Fact d give

$$\sum_{m\notin\Gamma}|\hat{f}(m)|^4 \le \rho^2\delta^2\sum_{m}|\hat{f}(m)|^2 = \rho^2\delta^3. \tag{3.18}$$

Putting (3.16), (3.17) and (3.18) together, we have

$$\begin{aligned}
\Big|\sum_{m}|\hat{f}(m)|^4 e^{2\pi i\frac{mx}{N}}\Big| &\ge \Big|\sum_{m\in\Gamma}|\hat{f}(m)|^4 e^{2\pi i\frac{mx}{N}}\Big| - \Big|\sum_{m\notin\Gamma}|\hat{f}(m)|^4 e^{2\pi i\frac{mx}{N}}\Big| \\
&> (1-2\pi\varepsilon)(\sum_{m}|\hat{f}(m)|^4 - \sum_{m\notin\Gamma}|\hat{f}(m)|^4) - \sum_{m\notin\Gamma}|\hat{f}(m)|^4 \\
&= (1-2\pi\varepsilon)\sum_{m}|\hat{f}(m)|^4 - (2-2\pi\varepsilon)\sum_{m\notin\Gamma}|\hat{f}(m)|^4 \\
&\ge (1-2\pi\varepsilon)\sum_{m}|\hat{f}(m)|^4 - (2-2\pi\varepsilon)\rho^2\delta^3.
\end{aligned} \tag{3.19}$$

which is positive by our assumption.

Lemma 3.3. *Let $\mathcal{R}\subset\mathbb{Z}_N$ with $|\mathcal{R}|=\delta N$ be as in inequalities (3.1) and (3.2), and let $f=\chi_{\mathcal{R}}$ be the indicator function of $\mathcal{R}$. Then*

$$\sum_{0\le m<N}|\hat{f}(m)|^4 > \frac{\delta^3}{8\alpha}. \tag{3.20}$$

Proof. We denote

$$f^{(2)} :\ = f * f, \tag{3.21}$$

and

$$S :\ = \mathrm{Supp} f^{(2)}. \tag{3.22}$$

First, we note that Fact e, Proposition 1.3, and (3.1) give

$$|S| \le |2\mathcal{R}| = |2A_1| \le |2A| \le \alpha|A| < 8\alpha|\mathcal{R}| = 8\alpha\delta N. \tag{3.23}$$

Next, Facts b and d give

$$\sum_{0\le m<N} |\hat{f}(m)|^4 = \sum_{0\le m<N} |\widehat{f^{(2)}}(m)|^2 = \frac{1}{N}\sum_{0\le m<N} |f^{(2)}(m)|^2 = \|f^{(2)}\|_2^2. \tag{3.24}$$

Now, Hölder's inequality and Definitions 2 and 4 give

$$\delta^2 = \|f^{(2)}\|_1 \le \|f^{(2)}\|_2 \|\chi_S\|_2 = \|f^{(2)}\|_2 \sqrt{\frac{|S|}{N}}. \tag{3.25}$$

Putting (3.23), (3.24), (3.25) together, we have (3.20).

In the following Lemma, we use the notation defined in either (1.18) or Lemma 3.2 for the Bohr neighborhood.

Lemma 3.4. *Let Γ be a subset of $\mathbb{Z}_N$, and let $\Lambda \subset \Gamma$ be a maximal dissociated subset with $|\Lambda| = d$. Then $B(\Lambda, \frac{\varepsilon}{d}) \subset B(\Gamma, \varepsilon)$.*

Proof. First, we notice that every $m \in \Gamma$ can be represented as

$$m = \sum_{m_j \in \Lambda} \gamma_j m_j, \text{ where } \gamma_j \in \{0, 1, -1\}. \tag{3.26}$$

Let $x \in B(\Lambda, \frac{\varepsilon}{d})$. Then

$$\left\| \frac{mx}{N} \right\| \le \sum_{m_j \in \Lambda} |\gamma_j| \left\| \frac{m_j x}{N} \right\| \le \sum_{m_j \in \Lambda} |\gamma_j| \frac{\varepsilon}{d} \le \varepsilon, \tag{3.27}$$

i.e. $x \in B(\Gamma, \varepsilon)$

Proof of Proposition 2.1. To apply Lemma 3.2, we choose ρ such that

$$10^2\alpha < \rho^{-2} < 10^3\alpha, \tag{3.28}$$

and we choose

$$\varepsilon = \frac{1}{10}. \tag{3.29}$$

Now, (3.28) and (3.29) imply

$$\rho^2 < \frac{1}{100\alpha} < (\frac{1-2\pi\varepsilon}{2-2\pi\varepsilon})\frac{1}{8\alpha}. \tag{3.30}$$

Lemma 3.3, and (3.30) imply that the hypothesis of Lemma 3.2 holds.

Inequalities (3.1) and (3.2) give

$$\delta > \frac{1}{320\alpha^{16}}. \tag{3.31}$$

Lemma 3.1, (3.28), and (3.31) give the bound (2.1) on d.

Now use Lemma 3.4 and Step 3. Substitute (3.29) in (1.19), we have (2.2), the bound on $|P|$.

Remark. Compared with the 'usual' argument presented in [Na] (Theorem 8.6), the method used above give a significant improvement of the dimension bound, i.e. $d \lesssim \alpha(\log \alpha)$. It is not unreasonable however to conjecture estimates in Proposition 2.1 of the form $d < (\log \alpha)^C$ (in this respect, compare with comments in [F-H-R]). If true, one would obtain estimates

$$d(\alpha), \log C(\alpha) < \alpha(\log \alpha)^{C'}$$

in Freiman's theorem (which would be essentially optimal).

SECTION 4. Proof of Theorem 2.

Starting from Ruzsa's result [Ru], it is indicated in [Bi] how to pass to a proper progression of dimension $\leq [\alpha - 1]$. Following this and the estimates in [Bi], the resulting estimate on $|P|$ becomes

$$\log \frac{|P|}{|A|} < \alpha^3(\log \alpha). \tag{4.1}$$

In order to preserve the bound (1.10), we will proceed a bit more carefully. Here, we adopt terminology and notations from [Bi] and highlight a number of key estimates. For further details, the reader will have to consult [Bi].

First, we redefine a 'triple' (m, B, φ). This means that

$$m \in \mathbb{Z}_+ \tag{4.2}$$

$$B \subset \mathbb{R}^m \text{ is a convex symmetric body such that } \dim(\mathrm{Span} B \cap \mathbb{Z}^m) = m \tag{4.3}$$

$$\varphi : \mathbb{Z}^m \to \mathbb{Z} \text{ is a group homomorphism.} \tag{4.4}$$

A m-dimensional progression P is the image of a parallelepiped in $\mathbb{Z}^m$ under the obvious φ. The property that φ being one- to-one implies that P is proper. To control the dimension of the progression, we use the argument in Section 9.3 of [Bi]. However, this argument only implies that A is in the image of a symmetric convex body. We use the proof of Theorem 1.2 (Section 3) in [Bi] for the construction of the parallelepiped.

We start with the progression

$$P_1 = P(q_1, \dots, q_d; \ell_1, \dots, \ell_d)$$

obtained in Theorem 1. We let $m_1 = d$ and let $\varphi_1 : \mathbb{Z}^{m_1} \to \mathbb{Z}$ be the homomorphism defined by $\varphi(e_i) = q_i$. Let B_1 be the box $\prod_{i=1}^{d}[-\ell_i + 1, \ell_i - 1]$. Thus

$$\varphi_1(B_1 \cap \mathbb{Z}^{m_1}) \supset A \tag{4.5}$$

$$\mathrm{Vol}_{m_1}(B_1) \leq 2^d \ell(P) \tag{4.6}$$

hence

$$m_1 \text{ and } \log \frac{\mathrm{Vol}\,(B_1)}{|A|} < C\alpha^2 (\log \alpha)^2. \tag{4.7}$$

First, we use the construction in the proof of Proposition 9.3 in Section 9.2 of [Bi] by letting $T = 2$ and we obtain a triple (m_2, B_2, φ_2) satisfying

$$m_2 \leq m_1 \tag{4.8}$$

$$\varphi_2(B_2 \cap \mathbb{Z}^{m_2}) \supset A. \tag{4.9}$$

The restriction

$$\varphi_2\big|_{TB_2 \cap \mathbb{Z}^{m_2}} \text{ is one-to-one ,} \tag{4.10}$$

and

$$\mathrm{Vol}_{m_2}(B_2) \leq (2m_1 T)^{m_1 - m_2} \mathrm{Vol}_{m_1}(B_1). \tag{4.11}$$

Hence, from (4.7),

$$\log \frac{\mathrm{Vol}\,(B_2)}{|A|} \leq Cd \log \alpha + \log \frac{\mathrm{Vol}\,(B_1)}{|A|} < C\alpha^2 (\log \alpha)^3. \tag{4.12}$$

Next, follow [Bi], Section 9.3 and replace (m_2, B_2, φ_2) by (m', B', φ') satisfying in particular

$$m' \leq [\alpha - 1] \tag{4.13}$$

$$\varphi'(B' \cap \mathbb{Z}^{m'}) \supset A \tag{4.14}$$

$$\mathrm{Vol}_{m'}(B') \leq m_2! \left(\frac{m_2}{2}\right)^{m_2} \mathrm{Vol}_{m_2}(B_2). \tag{4.15}$$

Hence, from (4.12),

$$\log \frac{\mathrm{Vol}\, B'}{|A|} \leq C\alpha^2 (\log \alpha)^3. \tag{4.16}$$

At this stage, what we gain is the estimate (4.13) on the dimension. Next, we need to replace B_2 by a parallelepiped. We first apply the proof of Proposition 9.3 in [Bi] again with (m_1, B_1, φ_1) replaced by (m', B', φ') and taking

$$T = 2\alpha([\alpha]!)^2. \tag{4.17}$$

We get a triple (m'', B'', φ'') such that

$$m'' \leq m' \leq [\alpha - 1] \tag{4.18}$$

$$\varphi''(B'' \cap \mathbb{Z}^{m''}) \supset A. \tag{4.19}$$

$$\text{The restriction } \varphi''\big|_{TB'' \cap \mathbb{Z}^{m''}} \text{ is one-to one} \tag{4.20}$$

$$\mathrm{Vol}_{m''}(B'') \leq (2m'T)^{m'-m''} \mathrm{Vol}_{m'}(B'). \tag{4.21}$$

Hence, from (4.16), (4.17)

$$\log \frac{\mathrm{Vol}\, B''}{|A|} \leq C\alpha^2 \log \alpha + C\alpha^2 (\log \alpha)^3 < C\alpha^2 (\log \alpha)^3. \tag{4.22}$$

To replace the body B by a parallelepiped, we use the argument in Section 3 of [Bi]. This finally yields a proper m''-dim progression $A \subset P$ satisfying

$$|P| \leq (m''!) \left(\frac{3}{2} 2^{1-m''} (m''!)^2\right)^{m''} \mathrm{Vol}\, B'' \tag{4.23}$$

thus

$$\log \frac{|P|}{|A|} \leq C\alpha^2 (\log \alpha)^3. \tag{4.24}$$

This proves Theorem 2.

References

[B-1]. V. Bergelson, A. Liebman, *Polynomial extensions of van der Waerden's and Szemerédi's theorem*, J. AMS, Vol 9, N3 (1996), 725-753.

[Bi]. Y. Bilu, *Structure of sets with small sumset*, in 'Structure Theory of Set Addition', Astérisque 258 (1999), 77-108.

[Ch]. M. Chaimovich, *New Structural approach to Integer Programming*, a Survey, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[Chan]. M.-C. Chang, *Inequidimensionality of Hilbert schemes*, Proceedings of AMS.

[C-Z]. G. Cohen, G. Zemor, *Subset sums and coding theory*, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[El]. G. Elekes, *On the number of sums and products*, Acta Arithmetica 81, Fase 4, 365-367 (1997).

[E-S]. P. Erdős, E. Szemerédi, *On sums and products of integers*, in 'Studies in Pure Mathematics', Birkhauser, Basel, 213-218 (1983).

[Fal]. K. Falconer, *The geometry of Fractal sets*, Cambridge UP (1986).

[Fr]. G. Freiman, *'Foundations of a structural theory of set addition'*, Translations of Math. Monographs, 37, AMS, 1973.

[F-H-R]. G. Freiman, H. Halberstam, I. Ruzsa, *Integer sumsets containing long arithmetic progressions*, JLMS (2), 46 (1992), no 2, 193-201.

[Fu]. H. Furstenberg, *Ergodic behaviours of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse math. 31 (1977), 204-256.

[F-K-O]. H. Furstenberg, Y. Katznelson, D. Ornstein, *The ergodic theoretical proof of Szemerédi's theorem*, Bulletin AMS, 7 (1982), no 3, 527-552.

[G1].

[G2]. W.T. Gowers, *A new proof of Szemerédi's theorem*, preprint.

[He]. M. Herzog, *New results on subset multiplication in groups*, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[K-L-T]. N. Katz, I. Laba, T. Tao, *An improved bound on the Minkowski dimension of Besicovitch sets in* R^3, Annals of Math..

[K-T]. N. Katz, T. Tao, *Some connections between the Falconer and Furstenburg conjectures*, New York J. Math..

[L-R]. J. Lopez, K. Ross, *Sidon sets*, Marcel Dekker ed, Lecture Notes in Pure and Applied Mathematics, Vol 13 (1975).

[Na]. M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer (1996)*..

[N-T]. M. Nathanson, G. Tenenbaum, *Inverse theorems and the number of sums and products*, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[Ro]. K. Roth, *On certain sets of integers*, J. London Math. Soc 28 (1953), 245-252.

[Ru1]. I. Ruzsa, *Arithmetic progressions in sumsets*, Acta Arithmetica 60 (1991), no 2, 191-202.

[Ru2]. I. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. 65 (1994), no 4, 379-388.

[Ru3]. I. Ruzsa, *An analog of Freiman's theorem in groups*, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[Sh]. S. Shelah, *Primitive recursive bounds for van der Waerden numbers*, J. AMS, Vol. 3 (1998), 683-697.

[Sz]. E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. 27 (1975), 199-245.

[S-T]. E. Szemerédi, W. Trotter, *Extremal problems in discrete geometry*, Combinatorica 3 (1983), 381-392.

[T]. T. Tao, *From rotating needles to stability of waves: emerging connections between combinatorics, analysis, and PDE*, Notices Amer. Math. Soc..

[VdW]. B.L. van der Waerden, *Beweis einer Baudetsche Vermutung*, Nieuw Arch. Wisk. 15 (1927), 212-216.

[W]. T. Wolff, *Recent work connected with the Kakeya problem*, in 'Prospects in mathematics', (Princeton, NJ, 1996), 129-162, AMS, Providence, RI (1999).