Annals of Mathematics, **157** (2003), 939–957

The Erdős-Szemerédi problem on sum set and product set

By Mei-Chu Chang*

Summary

The basic theme of this paper is the fact that if A is a finite set of integers, then the sum and product sets cannot both be small. A precise formulation of this fact is Conjecture 1 below due to Erdős-Szemerédi [E-S]. (see also [El], [T], and [K-T] for related aspects.) Only much weaker results or very special cases of this conjecture are presently known. One approach consists of assuming the sum set $A+A$ small and then deriving that the product set AA is large (using Freiman's structure theorem) (cf. [N-T], [Na3]). We follow the reverse route and prove that if $|AA| < c|A|$, then $|A+A| > c'|A|^2$ (see Theorem 1). A quantitative version of this phenomenon combined with the Plünnecke type of inequality (due to Ruzsa) permit us to settle completely a related conjecture in [E-S] on the growth in k. If

$$g(k) \equiv \min\{|A[1]| + |A\{1\}|\}$$

over all sets $A \subset \mathbb{Z}$ of cardinality $|A| = k$ and where $A[1]$ (respectively, $A\{1\}$) refers to the simple sum (resp., product) of elements of A. (See (0.6), (0.7).) It was conjectured in [E-S] that $g(k)$ grows faster than any power of k for $k \to \infty$. We will prove here that $\ln g(k) \sim \frac{(\ln k)^2}{\ln \ln k}$ (see Theorem 2) which is the main result of this paper.

Introduction

Let A, B be finite sets of an abelian group. The *sum set* of A, B is

$$A + B \equiv \{a + b \mid a \in A, b \in B\}. \tag{0.1}$$

We denote by

$$hA \equiv A + \cdots + A \ \ (h \text{ fold}) \tag{0.2}$$

the h-fold sum of A.

*Partially supported by NSA.

Similarly we can define the *product set* of A, B and h-fold product of A.

$$AB \equiv \{ab \mid a \in A, b \in B\}, \tag{0.3}$$

$$A^h \equiv A \cdots A \ \ (h \text{ fold}). \tag{0.4}$$

If $B = \{b\}$, a singleton, we denote AB by $b \cdot A$.

In 1983, Erdős and Szemerédi [E-S] conjectured that for subsets of integers, the sum set and the product set cannot both be small. Precisely, they made the following conjecture.

Conjecture 1 (Erdős-Szemerédi). *For any $\varepsilon > 0$ and any $h \in \mathbb{N}$ there is $k_0 = k_0(\varepsilon)$ such that for any $A \subset \mathbb{N}$ with $|A| \geq k_0$,*

$$|hA \cup A^h| \gg |A|^{h-\varepsilon}. \tag{0.5}$$

We note that there is an obvious upper bound $|hA \cup A^h| \leq 2\binom{|A|+h-1}{h}$.

Another related conjecture requires the following notation of *simple sum* and *simple product.*

$$A[1] \equiv \left\{ \sum_{i=1}^{k} \varepsilon_i a_i \mid a_i \in A, \varepsilon_i = 0 \ \text{ or } \ 1 \right\}, \tag{0.6}$$

$$A\{1\} \equiv \left\{ \prod_{i=1}^{k} a_i^{\varepsilon_i} \mid a_i \in A, \varepsilon_i = 0 \ \text{ or } \ 1 \right\}. \tag{0.7}$$

For the rest of the introduction, we only consider $A \subset \mathbb{N}$.

Conjecture 2 (Erdős-Szemerédi). *Let $g(k) \equiv \min_{|A|=k}\{|A[1]|+|A\{1\}|\}$. Then for any t, there is $k_0 = k_0(t)$ such that for any $k \geq k_0, g(k) > k^t$.*

Toward Conjecture 1, all work has been done so far, are for the case $h = 2$.

Erdős and Szemerédi [E-S] got the first bound:

Theorem (Erdős-Szemerédi). *Let $f(k) \equiv \min_{|A|=k} |2A \cup A^2|$. Then there are constants c_1, c_2, such that*

$$k^{1+c_1} < f(k) < k^2 e^{-c_2 \frac{\ln k}{\ln \ln k}}. \tag{0.8}$$

Nathanson showed that $f(k) > ck^{\frac{32}{31}}$, with $c = 0.00028\dots$.
At this point, the best bound is

$$|2A \cup A^2| > c|A|^{5/4} \tag{0.9}$$

obtained by Elekes [El] using the Szemerédi-Trotter theorem on line-incidences in the plane (see [S-T]).

On the other hand, Nathanson and Tenenbaum [N-T] concluded something stronger by assuming the sum set is small. They showed

Theorem (Nathanson-Tenenbaum). *If*

$$|2A| \leq 3|A| - 4, \tag{0.10}$$

then

$$|A^2| \geqq \left(\frac{|A|}{\ln |A|}\right)^2. \tag{0.11}$$

Very recently, Elekes and Ruzsa [El-R] again using the Szemerédi-Trotter theorem, established the following general inequality.

Theorem (Elekes-Ruzsa). *If $A \subset \mathbb{R}$ is a finite set, then*

$$|A + A|^4 \, |AA| \ln |A| > |A|^6. \tag{0.12}$$

In particular, their result implies that if

$$|2A| < c|A|, \tag{0.13}$$

then

$$|A^2| \geqq \frac{|A|^2}{c' \ln |A|}. \tag{0.14}$$

For further result in this direction, see [C2].

Related to Conjecture 2, Erdős and Szemerédi [E-S] have an upper bound:

Theorem (Erdős-Szemerédi). *Let $g(k) \equiv \min_{|A|=k}\{|A[1]|+|A\{1\}|\}$. There is a constant c such that*

$$g(k) < e^{c\frac{(\ln k)^2}{\ln \ln k}}. \tag{0.15}$$

Our first theorem is to show that the h-fold sum is big, if the product is small.

Theorem 1. *Let $A \subset \mathbb{N}$ be a finite set. If $|A^2| < \alpha|A|$, then*

$$|2A| > 36^{-\alpha}|A|^2, \tag{0.16}$$

and

$$|hA| > c_h(\alpha)|A|^h. \tag{0.17}$$

Here

$$c_h(\alpha) = (2h^2 - h)^{-h\alpha}. \tag{0.18}$$

Our approach is to show that there is a constant c such that

$$\int \left|\sum\nolimits_{m\in A} e^{2\pi i m x}\right|^{2h} dx < c|A|^h \tag{0.19}$$

by applying an easy result of Freiman's theorem (see the paragraph after Proposition 10) to obtain

$$A \subset P \equiv \left\{ \frac{a}{b}\left(\frac{a_1}{b_1}\right)^{j_1}\cdots\left(\frac{a_s}{b_s}\right)^{j_s} \mid 0 \le j_i < \ell_i \right\} \tag{0.20}$$

and carefully analyzing the corresponding trigonometric polynomials (see Proposition 8). These are estimates in the spirit of Rudin [R]. The constant c here depends, of course, on s and h.

In order to have a good universal bound c, we introduce the concept of multiplicative dimension of a finite set of integers, and derive some basic properties of it (see Propositions 10 and 11). We expect more applications coming out of it.

Another application of our method together with a Plünnecke type of inequality (due to Ruzsa) gives a complete answer to Conjecture 2.

Theorem 2. *Let $g(k) \equiv \min_{|A|=k}\{|A[1]| + |A\{1\}|\}$. Then there is $\varepsilon > 0$ such that*

$$k^{(1+\varepsilon)\frac{\ln k}{\ln\ln k}} > g(k) > k^{(\frac{1}{8}-\varepsilon)\frac{\ln k}{\ln\ln k}}. \tag{0.21}$$

Remark 2.1 (Ruzsa). The lower bound can be improved to $k^{(\frac{1}{2}-\varepsilon)\frac{\ln k}{\ln\ln k}}$. We will give more detail after the proof of Theorem 2.

Using a result of Laczkovich and Rusza, we obtain the following result related to a conjecture in [E-S] on undirected graphs.

Theorem 3. *Let $G \subset A\times A$ satisfy $|G| > \delta|A|^2$. Denote the restricted sum and product sets by*

$$A \overset{G}{+} A = \{a + a' | (a, a') \in G\} \tag{0.22}$$

$$A \overset{G}{\times} A = \{aa' | (a, a') \in G\}. \tag{0.23}$$

If

$$|A \overset{G}{\times} A| < c|A|, \tag{0.24}$$

then

$$|A \overset{G}{+} A| > C(\delta, c)|A|^2. \tag{0.25}$$

The paper is organized as follows:

In Section 1, we prove Theorem 1 and introduce the concept of multiplicative dimension. In Section 2, we show the lower bound of Theorem 2 and Theorem 3. In Section 3, we repeat Erdős-Szemerédi's upper bound of Theorem 2.

Notation. We denote by $\lfloor a \rfloor$ the greatest integer $\leq a$, and by $|A|$ the cardinality of a set A.

Acknowledgement. The author would like to thank J. Bourgain for various advice, and I. Ruzsa and the referee for many helpful comments.

1. Proof of Theorem 1

Let $A \subset \mathbb{N}$ be a finite set of positive integers, and let $\Gamma_{h,A}(n)$ be the number of representatives of n by the sum of h (ordered) elements in A, i.e.,

$$\Gamma_{h,A}(n) \equiv \left| \{(a_1, \ldots, a_h) \mid \sum a_i = n, a_i \in A\} \right| . \tag{1.1}$$

The two standard lemmas below provide our starting point.

Lemma 3. *Let $A \subset \mathbb{N}$ be finite and let $h \in \mathbb{N}$. If there is a constant c such that*

$$\sum_{n \in hA} \Gamma^2_{h,A}(n) < c|A|^h, \tag{1.2}$$

then

$$|hA| > \frac{1}{c}|A|^h. \tag{1.3}$$

Proof. Cauchy-Schwartz inequality and the hypothesis give

$$\begin{aligned} |A|^h = \sum_{n \in hA} \Gamma_{h,A}(n) &\leq |hA|^{1/2} \left(\sum_{n \in hA} \Gamma^2_{h,A}(n) \right)^{1/2} \\ &< |hA|^{1/2} c^{1/2} |A|^{h/2}. \end{aligned}$$ □

Lemma 4. *The following equality holds*:

$$\sum_{n \in hA} \Gamma^2_{h,A}(n) = \left(\| \sum_{m \in A} e^{2\pi i m x} \|_{2h} \right)^{2h} .$$

Proof.

$$\begin{aligned}\left(\left\|\sum_{m\in A} e^{2\pi imx}\right\|_{2h}\right)^{2h} &= \int\left|\sum_{m\in A} e^{2\pi imx}\right|^{2h} dx\\ &= \int\left|\left(\sum_{m\in A} e^{2\pi imx}\right)^{h}\right|^{2} dx\\ &= \int\left|\left(\sum_{n\in hA} \Gamma_{h,A}(n) e^{2\pi inx}\right)\right|^{2} dx\\ &= \sum_{n\in hA} \Gamma^2_{h,A}(n).\end{aligned}$$

The last equality is Parseval equality. □

From Lemmas 3 and 4, it is clear that to prove Theorem 1, we want to find a constant c such that

$$\left(\left\|\sum_{m\in A} e^{2\pi imx}\right\|_{2h}\right)^{2} < c|A|. \tag{1.4}$$

In fact, we will prove something more general to be used in the inductive argument.

Proposition 5. *Let $A \subset \mathbb{N}$ be a finite set with $|A^2| < \alpha|A|$. Then for any $\{d_a\}_{a\in A} \subset \mathbb{R}_+$,*

$$\left(\left\|\sum_{a\in A} d_a e^{2\pi iax}\right\|_{2h}\right)^{2} < c\sum d_a^2 \tag{1.5}$$

for some constant c depending on h and α only.

For a precise constant c, see Proposition 9.

The following proposition takes care of the special case of (1.5) when there exists a prime p such that for every nonnegative integer j, p^j appears in the prime factorization of at most one element in A. It is also the initial step of our iteration.

First, for convenience, we use the following:

Notation. We denote by $\langle G\rangle^+$, the set of linear combinations of elements in G with coefficients in $\mathbb{R}^+$.

Proposition 6. *Let p be a fixed prime, and let*

$$F_j(x) \in \left\langle \left\{ e^{2\pi i p^j n x} \mid n \in \mathbb{N}, (n,p) = 1 \right\} \right\rangle^+ . \tag{1.6}$$

Then

$$\left(\left\| \sum_j F_j \right\|_{2h} \right)^2 \leq c_h \sum_j \|F_j\|_{2h}^2 , \quad \textit{where } c_h = 2h^2 - h. \tag{1.7}$$

Proof. To bound $\int |\sum_j F_j|^{2h} dx$, we expand $|\sum_j F_j|^{2h}$ as

$$\left(\sum F_j\right)^h \left(\sum \overline{F}_j\right)^h . \tag{1.8}$$

Let

$$F_{j_1} \cdots F_{j_h} \, \overline{F}_{j_{h+1}} \cdots \overline{F}_{j_{2h}} \tag{1.9}$$

be a term in the expansion of (1.8). After rearrangement, we may assume $j_1 \leq \cdots \leq j_h$, and $j_{h+1} \leq \cdots \leq j_{2h}$.

When (1.9) is expressed as a linear combination of trignometric functions, a typical term is of the form

$$n e^{2\pi i x (p^{j_1} n_1 + \cdots + p^{j_h} n_h - p^{j_{h+1}} n_{h+1} - \cdots - p^{j_{2h}} n_{2h})}. \tag{1.10}$$

We note that the integral of (1.10) is 0, if the expression in the parenthesis in (1.10) is nonzero. In particular, independent of the n_i's, the integral of (1.10) is 0, if

$$j_1 \neq j_2 \leq j_{h+1}, \quad \text{or} \quad j_1 \neq j_{h+1} \leq \min\{j_2, j_{h+2}\}, \quad \text{or} \quad j_{h+1} \neq j_{h+2} \leq j_1. \tag{1.11}$$

Therefore, if any of the statements in (1.11) is true, then the integral of (1.9) is 0.

We now consider the integral of (1.9) where the index set $\{j_1, \ldots, j_{2h}\}$ does not satisfy any of the conditions in (1.11). For the case $j_1 = j_2 \leq j_{h+1}$, we see that in an ordered set of h elements coming from the expansion of (1.8) (before the rearrangement), there are exactly $\binom{h}{2}$ choices for the positions of j_1, j_2. On the other hand, if $F_{j_1} F_{j_2}$ is factored out, the rest is symmetric with respect to $j_3, \ldots, j_h$, and $j_{h+1}, \ldots, j_{2h}$, i.e., all the terms involving $j \equiv j_1 = j_2 \leq j_{h+1}$ are simplified to

$$\binom{h}{2} (F_j)^2 \left(\sum_{k \geq j} F_k \right)^{h-2} . \tag{1.12}$$

With the same reasoning for the other two cases, we conclude that

$$\begin{aligned}\left(\Big\|\sum_j F_j\Big\|_{2h}\right)^{2h} =&\binom{h}{2}\sum_j\int F_j^2\left(\sum_{k\geq j}F_k\right)^{h-2}\left(\sum_{k\geq j}\overline{F}_k\right)^{h} dx\\ &+h^2\sum_j\int |F_j|^2\left(\sum_{k\geq j}F_k\sum_{k\geq j}\overline{F}_k\right)^{h-1} dx\\ &+\binom{h}{2}\sum_j\int \overline{F}_j^2\left(\sum_{k\geq j}F_k\right)^{h}\left(\sum_{k\geq j}\overline{F}_k\right)^{h-2} dx.\end{aligned}$$

The right-hand side is

$$\begin{aligned}&\leq\left[h^2+2\binom{h}{2}\right]\sum_j\int |F_j|^2\left|\sum_{k\geq j}F_k\right|^{2h-2} dx\\ &\leq(2h^2-h)\sum_j\|F_j^2\|_h\|\left(\sum_{k\geq j}F_k\right)^{2h-2}\|_{\frac{h}{h-1}}\\ &=(2h^2-h)\sum_j\|F_j\|_{2h}^2\left(\Big\|\sum_{k\geq j}F_k\Big\|_{2h}\right)^{2h-2}.\end{aligned}$$

The last inequality is Hölder inequality.

Now, the next lemma concludes the proof of Proposition 6. □

LEMMA 7. *Let $F_k\in\langle\{e^{2\pi i m_k x}\mid m_k\in\mathbb{Z}\}\rangle^+$. Then*

$$\left\|\sum_k F_k\right\|_{2h}\geq\left\|\sum_{k\geq j}F_k\right\|_{2h},\quad \textit{for any}\quad j. \tag{1.13}$$

Proof.

$$\begin{aligned}&\int\left|\sum_k F_k\right|^{2h} dx\\ &\quad=\int\left(\sum_{k\geq j}F_k+\sum_{k<j}F_k\right)\\ &\qquad\cdots\left(\sum_{k\geq j}F_k+\sum_{k<j}F_k\right)\left(\sum_{k\geq j}\overline{F}_k+\sum_{k<j}\overline{F}_k\right)\cdots\left(\sum_{k\geq j}\overline{F}_k+\sum_{k<j}\overline{F}_k\right)dx\\ &\quad\geq\int\left(\sum_{k\geq j}F_k\sum_{k\geq j}\overline{F}_k\right)^h dx=\left(\|\sum_{k\geq j}F_k\|_{2h}\right)^{2h}.\end{aligned}$$

The inequality holds because the coefficients of the trignometric functions (as in (1.10)) in the expansion are all positive. □

Remark 7.1. This is a special case of a general theorem in martingale theory.

PROPOSITION 8. *Let* $p_1, \cdots, p_t$ *be distinct primes, and let*

$$F_{j_1,\dots,j_t}(x) \in \left\langle \left\{ e^{2\pi i p_1^{j_1}\cdots p_t^{j_t} n x} \mid n \in \mathbb{N}, (n, p_1 \cdots p_t) = 1 \right\} \right\rangle^{+}. \tag{1.14}$$

Then

$$\left\| \sum_{j_1,\cdots,j_t} F_{j_1,\dots,j_t} \right\|_{2h}^{2} \leq c_h^t \sum_{j_1,\cdots,j_t} \|F_{j_1,\dots,j_t}\|_{2h}^2, \quad \textit{where } c_h = 2h^2 - h. \tag{1.15}$$

Proof. We do induction on t. The left-hand side of (1.15) becomes

$$\left\| \sum_{j_1} \sum_{j_2,\cdots,j_t} F_{j_1,\dots,j_t} \right\|^2 \leq c_h \sum_{j_1} \left\| \sum_{j_2,\cdots,j_t} F_{j_1,\dots,j_t} \right\|^2 \leq c_h \sum_{j_1} c_h^{t-1} \sum_{j_2,\cdots,j_t} \|F_{j_1,\dots,j_t}\|^2,$$

which is the right-hand side. □

Proposition 5 is proved, if we can find a *small* t such that the Fourier transform of $F_{j_1,\dots,j_t}$ is supported at one point and such t is bounded by α. So we introduce the following notion.

Definition. Let A be a finite set of positive rational numbers in lowest terms (cf. (0.20)). Let $q_1, \dots, q_\ell$ be all the prime factors in the obvious prime factorization of elements in A. For $a \in A$, let $a = q_j^{j_1} \cdots q_\ell^{j_\ell}$ be the prime factorization of a. Then the map $\nu : A \to \mathbb{R}^\ell$ by sending a to $(j_1, \dots, j_\ell)$ is one-to-one. The *multiplicative dimension* of A is the dimension of the smallest (affine) linear space in $\mathbb{R}^\ell$ containing $\nu(A)$.

We note that for any nonzero rational number q, $q \cdot A$ and A have the same multiplicative dimension, since $\nu(q \cdot A)$ is a translation of $\nu(A)$.

The following proposition is a more precise version of Lemma 5.

PROPOSITION 9. *Let* $A \subset \mathbb{N}$ *be finite with* mult.dim$(A) = m$. *Then*

$$\left(\left\| \sum_{a \in A} d_a e^{2\pi i a x} \right\|_{2h} \right)^2 < c_h^m \sum d_a^2, \qquad \textit{where} \qquad c_h = 2h^2 - h. \tag{1.16}$$

Proof. To use (1.15) in Proposition 8, we want to show that there are primes $q_1, \dots, q_m$ such that a term of the trigonometric polynomial in the left-hand side of (1.15), when expressed in terms of the notation in (1.14), is $F_{j_1,\cdots,j_m} = d_a e^{2\pi i q_1^{j_1}\cdots q_m^{j_m} nx}$. In other words, we want to show that among the prime factors $q_1, \dots, q_\ell$ of elements in A, there are m of them, say $q_1, \dots, q_m$ such that

$(*)$ for all $(j_1, \dots, j_m) \in \mathbb{Z}^m$, there is at most one $a \in A$ such that $q_1^{j_1} \cdots q_m^{j_m}$ is part of the prime factorization of a. This is equivalent to

$(**)$ $\pi \circ \nu$ is injective, where ν is as in the definition of multiplicative dimension and $\pi : \mathbb{R}^\ell \to \mathbb{R}^m$ is the projection to the first m coordinates.

Since $\dim \nu(A) = m$, $(**)$ is clear after some permutation of the q_i's. □

Proposition 10. *Let $A \subset \mathbb{N}$ be finite with* mult.dim $A = m$. *Then*

$$\sum_{n \in hA} \Gamma^2_{h,A}(n) < c_h^{mh} |A|^h, \quad \textit{where} \quad c_h = 2h^2 - h. \tag{1.17}$$

Proof. This is a consequence of Lemma 4 and Proposition 9 (with $d_a = 1$). □

The hypothesis of Theorem 1 gives a universal bound on the multiplicative dimension of A by applying Freiman's theorem (cf. [Fr1], [Fr2], [Fr3], [Bi], [C1], [Na1]). In fact, we do not need the full content of *the* Freiman's theorem, but a much easier result by Freiman. A small modification (over $\mathbb{Q}$ instead of over $\mathbb{R}$) of Lemma 4.3 in [Bi] is sufficient. (As Ruzsa pointed out it is also Lemma 1.14 in [Fr1].)

Theorem (Freiman). *Let $G \subset \mathbb{R}$ be a subgroup and $A_1 \subset G$ be finite. If there is a constant α, $\alpha < \sqrt{|A_1|}$, such that $|2A_1| < \alpha |A_1|$, then there is an integer*

$$s \le \alpha$$

such that A_1 is contained in an s-dimensional proper progression P_1; i.e., there exist $\beta, \alpha_1, \dots, \alpha_s \in G$ and $J_1, \cdots, J_s \in \mathbb{N}$ such that

$$A_1 \subset P_1 = \{\beta + j_1\alpha_1 + \cdots + j_s\alpha_s \mid 0 \le j_i < J_i\},$$

and $|P_1| = J_1 \cdots J_s$.

Note that if $|A_1| > \frac{\lfloor \alpha \rfloor \lfloor \alpha+1 \rfloor}{2(\lfloor \alpha+1 \rfloor - \alpha)}$, then $s \le \lfloor \alpha - 1 \rfloor$.

Recall that the full Freiman theorem also permits one to state a bound $J_1 \cdots J_s < c(\alpha)|A_1|$. However this additional information will not be used in what follows.

We would like to work on a sum set instead of a product set. So we define

$$A_1 \equiv \ln A = \{\ln a \mid a \in A\}. \tag{1.18}$$

Note that ln is an isomorphism between the two groups $(\mathbb{Q}^+, \cdot\,)$ and $(\ln \mathbb{Q}^+, +)$.

Applying the theorem to $A_1 \subset \ln \mathbb{Q}^+$, then pushing back by $(\ln)^{-1}$, we have

$$A \subset P \equiv \left\{ \frac{a}{b} (\frac{a_1}{b_1})^{j_1} \cdots (\frac{a_s}{b_s})^{j_s} \mid 0 \leq j_i < J_i \right\} \subset \mathbb{Q}^+, \tag{1.19}$$

where $a, b, a_i, b_i, J_i \in \mathbb{N}$, and $(a, b) = 1, (a_i, b_i) = 1$. Moreover, $s \leq \lfloor \alpha - 1 \rfloor$ and different ordered sets $(j_1, \cdots, j_s)$ represent different rational numbers. Clearly,

$$\text{mult.} \dim A \leq \text{mult.dim } P = \dim E \leq s \leq \lfloor \alpha - 1 \rfloor, \tag{1.20}$$

where E is the vector space generated by $\nu(\frac{a_1}{b_1}), \cdots, \nu(\frac{a_s}{b_s})$.

Therefore, we have

Proposition 11. *Let $A \subset \mathbb{N}$ be a finite set. If $|A|^2 < \alpha|A|$ for some constant α, $\alpha < |A|^{1/2}$, then* mult.dim $A \leq \alpha$. *Furthermore, if $|A| > \frac{\lfloor \alpha \rfloor \lfloor \alpha+1 \rfloor}{2(\lfloor \alpha+1 \rfloor - \alpha)}$, then* mult.dim $A \leq \lfloor \alpha - 1 \rfloor$.

Putting Propositions 10 and 11 together, we have

Proposition 12. *Let $A \subset \mathbb{N}$ be finite. If $|A^2| < \alpha|A|$ for some constant α, $\alpha < |A|^{1/2}$, then*

$$\sum_{n \in hA} \Gamma^2_{h,A}(n) < c_h^{\alpha h} |A|^h, \quad \textit{where} \quad c_h = 2h^2 - h.$$

Now, Theorem 1 follows from Proposition 12 and Lemma 3. □

2. Simple sums and products

In this section we will prove the lower bound in Theorem 2.

Let $A \subset \mathbb{N}$ be finite. We define

$$g(A) \equiv |A[1]| + |A\{1\}|, \tag{2.1}$$

where $A[1]$ and $A\{1\}$ are the simple sum and simple product of A. (See (0.6), (0.7) for precise definitions.)

We will show that for any ε and any $A \subset \mathbb{N}$ with $|A| = k \gg 0$,

$$g(A) > k^{(\frac{1}{8} - \varepsilon) \frac{\ln k}{\ln \ln k}}. \tag{2.2}$$

For those who like precise bounds, we show:

For $0 < \varepsilon_1, \varepsilon_2 < \frac{1}{2}$,

$$g(A) > e^{-3} \lfloor k^{\frac{1}{2} - \varepsilon_2} \rfloor^{\lfloor (\frac{1}{4} - \frac{\varepsilon_1}{2}) \frac{\ln k}{\ln \ln k} \rfloor}, \tag{2.3}$$

if $|A| = k$ is large enough such that

$$\ln \ln k > \frac{\sqrt{2}}{8\varepsilon_1}, \tag{2.4}$$

and

$$\frac{\ln k}{\ln \ln k} > \frac{2}{\varepsilon_2}. \tag{2.5}$$

Proposition 13. *Let $B \subset \mathbb{N}$ be finite with* mult.dim $B = m$. *Then for any $h_1 \in \mathbb{N}$,*

$$|h_1 B \cap B[1]| > \left[\frac{|B|}{(2h_1^2 - h_1)^{m+1}}\right]^{h_1}. \tag{2.6}$$

Proof. Since $h_1 B \cap B[1]$ is the set of simple sums with exactly h_1 summands, we have

$$\binom{|B|}{h_1} \le \sum_{n \in h_1 B \cap B[1]} \Gamma_{h_1,B}(n). \tag{2.7}$$

Therefore,

$$\begin{aligned}\left(\frac{|B|}{h_1}\right)^{h_1} &< (h_1 B \cap B[1])^{1/2} \left(\sum_{n \in h_1 B} \Gamma^2_{h_1,B}(n)\right)^{1/2} \\ &\le (h_1 B \cap B[1])^{1/2} \left[(2h_1^2 - h_1)^{m h_1} |B|^{h_1}\right]^{1/2}.\end{aligned}$$

The first inequality is because of the Cauchy-Schwartz inequality and the fact that $h_1 B \cap B[1] \subset h_1 B$. The second inequality is Proposition 10. □

Remark 13.1. Clearly, from our proof, the denominator in (2.6) can be replaced by $(2h_1^2 - h_1)^m h_1^2$.

Proposition 14. *Let $B \subset \mathbb{N}$ with $|B| \ge \sqrt{k}$ and* mult.dim $B = m$. *For any $0 < \varepsilon_1 < \frac{1}{2}$, if*

$$m + 1 \le \left(\frac{1}{4} - \frac{\varepsilon_1}{2}\right) \frac{\ln k}{\ln \ln k}, \tag{2.8}$$

then

$$g(B) > k^{\varepsilon_1 \lfloor \frac{\ln k}{\sqrt{2}} \rfloor}. \tag{2.9}$$

Proof. Inequality (2.8) is equivalent to

$$(\ln k)^{2m+2} \le k^{1/2 - \varepsilon_1}. \tag{2.10}$$

In Proposition 13, we take $h_1 = \lfloor \frac{\ln k}{\sqrt{2}} \rfloor$. This gives

$$2h_1^2 \leq (\ln k)^2. \tag{2.11}$$

Combining (2.11), (2.10) and (2.6), we have

$$g(B) > |h_1 B \cap B[1]| > \left(\frac{k^{1/2}}{k^{1/2-\varepsilon_1}}\right)^{\lfloor \frac{\ln k}{\sqrt{2}} \rfloor} = k^{\varepsilon_1 \lfloor \frac{\ln k}{\sqrt{2}} \rfloor}. \qquad \square$$

Remark 14.1. Let $A \subset \mathbb{N}$ with $|A| = k, k \gg 0$ (see (2.4)). The set B in Proposition 14 will be taken as a subset of A. Then the bound in (2.9) is bigger than that in (2.2), and our proof is done. Therefore for the rest of the section, we assume

$$\text{mult.dim} B \geq \lfloor (\frac{1}{4} - \frac{\varepsilon_2}{2}) \frac{\ln k}{\ln \ln k} \rfloor, \text{ for any } B \subset A \text{ with } |B| > \sqrt{k}. \tag{2.12}$$

We need the following:

Notation. We denote $B' \equiv \nu(B)$ for any $B \subset A$, where $\nu = A \to \mathbb{Z}^\ell$ is as in the definition of multiplicative dimension.

Note that

$$|B'[1]| = |B\{1\}|. \tag{2.13}$$

We will use the following Plünnecke type of inequality due to Ruzsa.

Ruzsa's Inequality [Ru2]. *For any $h, \ell \in \mathbb{N}$:*

$$\textit{If } |M + N| \leq \rho |M|, \textit{ then } |hN - \ell N| \leq \rho^{h+\ell} |M|.$$

Proof of (2.2). We divide A into $\lfloor \sqrt{k} \rfloor$ pieces $B_1, B_2, \cdots$, each of cardinality at least $\sqrt{k}$. For $0 < \varepsilon_2 < \frac{1}{2}$, let

$$\rho = 1 + k^{-1/2+\varepsilon_2}, \tag{2.14}$$

and let

$$A_s \equiv \bigcup_{i=1}^{s} B_i. \tag{2.15}$$

There are two cases:

(i) For all $s, |(A_s \bigcup B_{s+1})'[1]| > \rho |A_s'[1]|$. Iterating gives

$$|A'[1]| = |(B_1 \cup B_2 \cup \cdots)'[1]| > \rho^{\sqrt{k}-2} \sqrt{k}. \tag{2.16}$$

Therefore

$$g(A) > |A\{1\}| = |A'[1]| > e^{(\sqrt{k}-2)\ln\rho+\frac{1}{2}\ln k} \tag{2.17}$$
$$> e^{(\sqrt{k}-2)\frac{4}{5}k^{-1/2+\varepsilon_2}+\frac{1}{2}\ln k}$$
$$> e^{\frac{4}{5}k^{\varepsilon_2}}.$$

Inequality (2.5) is equivalent to

$$k^{\varepsilon_2} > (\ln k)^2.$$

which is certainly stronger than what we need to show (2.2).

(ii) There exists s such that $|(A_s \cup B_{s+1})'[1]| \leq \rho|A'_s[1]|$. We use the fact that $(A_s \cup B_{s+1})'[1] = A'_s[1] + B'_{s+1}[1]$, and Ruzsa's inequality (with $h = h_2 + 1, \ell = 1$) to obtain

$$|(h_2+1)B'_{s+1}[1] - B'_{s+1}[1]| \leq \rho^{h_2+2}|A'_s[1]|. \tag{2.18}$$

Let $m = \text{mult.dim}B_{s+1}$. For a set B, for $h \in \mathbb{N}$, denote

$$B[h] \equiv \left\{\sum \varepsilon_i x_i \mid \varepsilon_i = 0, \dots, h, x_i \in B\right\}. \tag{2.19}$$

The left-hand side of (2.18) is

$$\geq |h_2 B'_{s+1}[1]| \tag{2.20}$$
$$\geq |B'_{s+1}[h_2]|$$
$$\geq h_2^m.$$

We take $h_2 = \lfloor k^{1/2-\varepsilon_2}\rfloor$. Then in the right-hand side of (2.18),

$$\rho^{h_2+2} \leq (1+k^{-1/2+\varepsilon_2})^{k^{1/2-\varepsilon_2}+2} \tag{2.21}$$
$$< (e^{k^{-1/2+\varepsilon_2}})^{k^{1/2-\varepsilon_2}+2}$$
$$< e^3.$$

Therefore, (2.18), (2.20) and (2.21) imply

$$g(A) > g(A_s)$$
$$> |A'_s[1]|$$
$$> e^{-3}h_2^m$$
$$> e^{-3}\lfloor k^{1/2-\varepsilon_2}\rfloor^{\lfloor(\frac{1}{4}-\frac{\varepsilon_1}{2})\frac{\ln k}{\ln\ln k}\rfloor}.$$

The last inequality follows from our choice of h_2 and Remark 14.1. □

Proof of Remark 2.1. In Proposition 14, if we take B with $|B| \geq \frac{k}{2}$, then we will replace (2.8), and (2.9) by

$$m+1 \leq \frac{1}{2}(1-\varepsilon_1)\frac{\ln k}{\ln\ln k}, \tag{2.8$'$}$$

and

$$g(B) > \left(\frac{k^{\varepsilon_1}}{2}\right)^{\lfloor\frac{\ln k}{\sqrt{2}}\rfloor}. \tag{2.9$'$}$$

Let

$$m_0 = \lfloor\frac{1}{2}\,(1-\varepsilon_1)\,\frac{\ln k}{\ln\ln k}\rfloor.$$

Then (2.12) will be replaced by

$$\text{mult.dim}B \geq m_0, \text{ for any } B \subset A \text{ with } |B| > \frac{k}{2}. \tag{2.12$'$}$$

Now we modify the proof of (2.2).

Since $|A| = k > \frac{k}{2}$, we have mult.dimA $\geq m_0$. So there is $B_1 \subset A$ with mult.dimB$_1 = m_0$ and $|B_1| = m_0 + 1$. Similarly, we have $B_2 \subset A - B_1$ with mult.dimB$_2 = m_0$ and $|B_2| = m_0 + 1$. We continue this process until $r > \frac{k}{2(m_0+1)}$. We have

$$A \supset B_1 \cup \cdots \cup B_r$$

with

$$\text{mult.dim}B_i = m_0,$$

and

$$|B_i| = m_0 + 1.$$

With more replacements,

$$\frac{\ln k}{\ln\ln k} > \frac{3}{\varepsilon_2}. \tag{2.5$'$}$$

and

$$\rho = 1 + k^{-1+\varepsilon_2}, \tag{2.14$'$}$$

Identical arguments give

$$g(A) > e^{-3}\lfloor k^{1-\varepsilon_2}\rfloor^{\lfloor(\frac{1}{2}-\frac{\varepsilon_1}{2})\frac{\ln k}{\ln\ln k}\rfloor}. \qquad \square$$

Sketch of Proof of Theorem 3. Let $|A| = N$. Then the Laczkovich-Ruzsa theorem [L-R] and (0.24) give $A_1 \subset A$ with

$$|A_1A_1| < c'N, \tag{2.22}$$

and

$$|G \cap (A_1 \times A_1)| > \delta' N^2. \tag{2.23}$$

The weak Freiman theorem and (2.22) imply

$$\text{mult.dim}A_1 < c'. \tag{2.24}$$

It follows from Proposition 10 (with $h = 2$) and the proof of Lemma 4 that

$$\beta \equiv |\{(n_1, n_2, n_3, n_4) \in A_1^4 | n_1 - n_2 + n_3 - n_4 = 0\}| < 36^{c'} N^2. \tag{2.25}$$

Hence

$$\delta' N^2 < \sum_{n \in A_1 \overset{G}{+} A_1} |\{(n_1, n_2) \in A_1^2 | n = n_1 + n_2\}| < |A_1 \overset{G}{+} A_1|^{\frac{1}{2}} \beta^{\frac{1}{2}}. \tag{2.26}$$

The first inequality is (2.23), while the second one is the Cauchy-Schwartz inequality.

Therefore, (2.25) and (2.26) give

$$|A \overset{G}{+} A| \geq |A_1 \overset{G}{+} A_1| \geq \frac{(\delta')^2 N^4}{\beta} > CN^2. \qquad \square$$

3. The example

In this section for completeness we repeat a family of examples by Erdős-Szemerédi which provide the upper bound in Theorem 2. Precisely, we will show

Proposition 15. *Given $\varepsilon_3 > 0$, for J so large that*

$$\frac{\ln J}{\ln \ln J} > \frac{1}{\varepsilon_3}, \tag{3.1}$$

there is a set A of cardinality $|A| = k \equiv J^J$, such that

$$g(A) < 2k^{(1+\varepsilon)\frac{\ln k}{\ln \ln k}}, \tag{3.2}$$

where

$$\varepsilon = 3\varepsilon_3 + \varepsilon_3^2. \tag{3.3}$$

The example really comes from the proof of the lower bound of Theorem 2.

Let $p_1, \cdots, p_J$ be the first J primes, and let

$$A \equiv \left\{ p_1^{j_1} \cdots p_J^{j_J} \mid 0 \leq j_i < J \right\}. \tag{3.4}$$

Then

$$k \equiv |A| = J^J. \tag{3.5}$$

We will use the following relations between k and J.

Lemma 16. *Let k, J be as in* (3.5). *Then*

(i) $\ln k = J \ln J$.

(ii) $\ln\ln k = \ln J + \ln\ln J$.

If J and ε_3 satisfy (3.1), *then*

(iii) $\ln\ln k < (1+\varepsilon_3)\ln J$.

(iv) $J < (1+\varepsilon_3)\frac{\ln k}{\ln\ln k}$.

(v) $J^2 < (1+\varepsilon')(\frac{\ln k}{\ln\ln k})^2$, *where* $\varepsilon' = 2\varepsilon_3 + \varepsilon_3^2$.

Proof. Each one follows immediately from the preceding one. For (iii) implying (iv), we use $J = \frac{\ln k}{\ln J}$. □

Remark 16.1. The inequality $\frac{\ln J}{\ln\ln J} > \frac{1}{\varepsilon_3}$ clearly implies

$$\frac{\ln k}{\ln\ln k} > \frac{1}{\varepsilon_3}. \tag{3.6}$$

Lemma 17. (i) *For all $a \in A$, $a < (\ln k)^{J^2}$,*

(ii) $|A[1]| < k(\ln k)^{J^2}$,

(iii) $|A\{1\}| < (kJ)^J$.

Proof. (i) For $a \in A$, (3.4) gives

$$\begin{aligned} a < \left(\prod_{i<J} p_i\right)^J &< \left(\prod_{i<J} i\ln i\right)^J \\ &< \left(J^J (\ln J)^J\right)^J \\ &= (J\ln J)^{J^2} \\ &= (\ln k)^{J^2}. \end{aligned}$$

The second inequality is by the Prime Number Theorem. The last equality is Lemma 16 (i).

(ii) follows from (i).

(iii) We see that

$$A\{1\} = \left\{ p_1^{\sum_{s=1}^k j_1^{(s)}} \cdots p_J^{\sum_{s=1}^k j_J^{(s)}} \mid 0 \le j_i^{(s)} < J \right\}. \tag{3.7}$$

Since $\sum_{s=1}^k j_i^{(s)} < kJ$, (iii) holds. □

Proof of Proposition 15. Lemma 17 (ii) and Lemma 16 (v) give

$$
\begin{aligned}
|A[1]| &< k(\ln k)^{(1+\varepsilon')(\frac{\ln k}{\ln\ln k})^2} \\
&= e^{\ln k + (1+\varepsilon')\frac{(\ln k)^2}{\ln\ln k}} \\
&= e^{\ln k(1+(1+\varepsilon')\frac{\ln k}{\ln\ln k})} \\
&< e^{\ln k(1+\varepsilon)\frac{\ln k}{\ln\ln k}} \\
&= k^{(1+\varepsilon)\frac{\ln k}{\ln\ln k}}.
\end{aligned}
\tag{3.8}
$$

Here $\varepsilon = \varepsilon' + \varepsilon_3 = 3\varepsilon_3 + \varepsilon_3^2$. We use (3.6) for the last inequality.

Lemmas 17 (iii), 16 (iv), and (3.5) give

$$
\begin{aligned}
|A\{1\}| < k^J k = k^{J+1} &< k^{(1+\varepsilon_3)\frac{\ln k}{\ln\ln k}+1} \\
&< k^{(1+2\varepsilon_3)\frac{\ln k}{\ln\ln k}}.
\end{aligned}
\tag{3.9}
$$

The last inequality is again by (3.6).

Putting (3.8) and (3.9) together, we have $g(A) < 2k^{(1+\varepsilon)\frac{\ln k}{\ln\ln k}}$. □

University of California, Riverside, CA
E-mail address: mcc@math.ucr.edu

References

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

[C1] M.-C. Chang, A polynomial bound in Freiman's theorem, *Duke Math. J.* **113** (2002), 399–419.

[C2] ______, Factorization in generalized arithmetic progressions and applications to the Erdös-Szemerédi sum-product problems, *GAFA*, to appear.

[El] G. Elekes, On the number of sums and products, *Acta Arith.* **81** (1997), 365–367.

[El-R] G. Elekes and I. Ruzsa, Product sets are very large if sumsets are very small, preprint.

[E] P. Erdős, Problems and results on combinatorial number theory. III, in *Number Theory Day*, 43–72 (*Proc. Conf. Rockefeller Univ., New York*, 1976), *Lecture Notes in Math.* **626**, Springer-Verlag, New York, 1977.

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

[Fr1] G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, *Transl. of Math. Monographs* **37**, A. M. S., Providence, RI, 1973.

[Fr2] ______, On the addition of finite sets. I, *Izv. Vysh. Ucheb. Zaved. Matematika* **13** (1959), 202–213.

[Fr3] ______, Inverse problems of additive number theory. VI. On the addition of finite sets. III, *Izv. Vysh. Ucheb. Zaved. Matematika* **28** (1962), 151–187.

[H-T] R. R. Hall and G. Tenenbaum, *Divisors*, *Cambridge Tracts in Math.* **90**, Cambridge Univ. Press, Cambridge, 1988.

[K-T] N. Katz and T. Tao, Some connections between Falconer's distance set conjecture and sets of Furstenberg type, *New York J. Math.* **7** (2001), 149–157.

[L-R] M. Laczkovich and I. Z. Ruzsa, The number of homothetic subsets, in *The Mathematics of P. Erdős*, *II* (R. L. Graham and J. Nesetril, eds.), Springer-Verlag, New York, 1977, 294–302.

[Na1] M. B. Nathanson, *Additive Number Theory*. *Inverse Problems and the Geometry of Sumsets*, *Grad. Texts in Math.* **165**, Springer-Verlag, New York, 1996.

[Na2] ———, The simplest inverse problems in additive number theory, in *Number Theory with an Emphasis on the Markloff Spectrum* (Provo, UT, 1991), 191–206, Marcel Dekker, New York, 1993.

[Na3] ———, On sums and products of integers, *Proc. Amer. Math. Soc.* **125** (1997), 9–16.

[N-T] M. Nathanson and G. Tenenbaum, Inverse theorems and the number of sums and products, in *Structure Theory of Set Addition*, *Astérisque* **258** (1999), 195–204.

[P] H. Plünnecke, Eine zahlentheoretische Anwendung der Graphtheorie, *J. Reine Angew. Math.* **243** (1970), 171–183.

[R] W. Rudin, Trigonometric series with gaps, *J. Math. Mech.* **9** (1960), 203–227.

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

[Ru2] ———, Sums of finite sets, in *Number Theory* (New York, 1991–1995), Springer-Verlag, New York, 1996.

[S-T] E. Szemerédi and 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.* **48** (2001), 294–303.

(Received November 27, 2001)