#A49 INTEGERS 10 (2010), 639-667

SUMS AND PRODUCTS OF DISTINCT SETS AND DISTINCT ELEMENTS IN $\mathbb{C}$

Karsten Chipeniuk[1]
Department of Mathematics, University of British Columbia, Vancouver, British Columbia V6T 1Z2, Canada

Received: 3/11/09, Revised: 1/5/10, Accepted: 7/1/10, Published: 11/11/10

Abstract

Let A and B be finite subsets of $\mathbb{C}$ such that $|B| = C|A|$. We show the following variant of the sum product phenomenon: If $|AB| < \alpha|A|$ and $\alpha \ll \log|A|$, then $|kA+lB| \gg |A|^k|B|^l$. This is an application of a result of Evertse, Schlickewei, and Schmidt on linear equations with variables taking values in multiplicative groups of finite rank, in combination with an earlier theorem of Ruzsa about sumsets in $\mathbb{R}^d$. As an application of the case $A = B$ we give a lower bound on $|A^+| + |A^\times|$, where A^+ is the set of sums of distinct elements of A and $A^\times$ is the set of products of distinct elements of A.

1. Introduction

Let A and B be finite subsets of a commutative ring R. Then we can form the sumset $A + B = \{a + b : a \in A,\ b \in B\}$ and the productset $AB = \{a \cdot b : a \in A,\ b \in B\}$. In the case $A = B$, we denote the sumset by $2A$ and the productset by $A^{(2)}$, and we may also consider the variants $kA = \{a_1 + ... + a_k : a_1, ..., a_k \in A\}$ and $A^{(k)} = \{a_1 \cdot ... \cdot a_k : a_1, ..., a_k \in A\}$, for $k \in \mathbb{Z}^+$, $k \geq 2$.

The sum product phenomenon, roughly, is the observation that $|kA|$ and $|A^{(k)}|$ cannot both be small (except in degenerate cases; for example, when A is a subring of R). The most general result, which holds in arbitrary rings, is due to Tao [14]. On the other hand, the classical conjecture, due to Erdős and Szemerédi, relates to the specific case when $R = \mathbb{Z}$:

Conjecture 1. (Erdős-Szemerédi) *Let $A \subset \mathbb{Z}$ be finite with $|A| = N$. Let $\epsilon > 0$. Then if $N \geq N_0 = N_0(\epsilon)$ we have*

$$\max(|A + A|, |A \cdot A|) \geq N^{2-\epsilon}.$$

[1]The author was partially supported by an NSERC Postgraduate Scholarship.

While this remains open, Erdős and Szemerédi did prove that on the right-hand side we must have at least $N^{1+\delta}$ for some $\delta > 0$. We then have the following numerical lower bounds for δ: 1/31 [9], 1/15 [8], 1/4 [5], 3/14 [13],and $1/3 - \epsilon$ for any $\epsilon > 0$ [12]. The latter three in fact hold for subsets of $\mathbb{R}$. There is also an extension of Conjecture 1 to k-fold sums and products: if A is a finite set of integers then it is conjectured that for any $\epsilon > 0$

$$|kA| + |A^{(k)}| \gg_\epsilon |A|^{k-\epsilon}.$$

There are also analogues of the sum-product phenomena which apply to sums and products of distinct elements from a finite set $A \subset R$. In particular, letting $A = \{a_1, \ldots, a_n\}$, one can construct the set of simple sums of A and the set of simple products of A, respectively

$$A^+ = \left\{ \sum_{i=1}^{n} \epsilon_i a_i : \epsilon_i \in \{0,1\} \text{ for each } i = 1, \ldots, n \right\} \tag{1}$$

and

$$A^\times = \left\{ \prod_{i=1}^{n} a_i^{\epsilon_i} : \epsilon_i \in \{0,1\} \text{ for each } i = 1, \ldots, n \right\}. \tag{2}$$

It is then possible to consider

$$g_R(n) = \min_{A \subset R,\ |A|=n} \{|A^+| + |A^\times|\}. \tag{3}$$

Such expressions were investigated by Erdős and Szemerédi in [6] in the integer setting. They showed that

$$g_{\mathbb{Z}}(n) < n^{c\frac{\log n}{\log\log n}} \tag{4}$$

for some absolute constant $c > 0$. Later, in addition to providing an upper bound on c, Chang proved ([2]) their conjecture that this provides the lower bound as well; more precisely, she showed that for large enough values of n

$$g_{\mathbb{Z}}(n) > n^{(1/8-\epsilon)\frac{\log n}{\log\log n}}. \tag{5}$$

More recently, in [3], Chang addressed a question of Ruzsa, proving that $g_{\mathbb{C}}(n)$ grows faster than any power of n,

$$\lim_{n\to\infty} \frac{\log(g_{\mathbb{C}}(n))}{\log n} = \infty. \tag{6}$$

In this article we will obtain an explicit lower bound for $g_{\mathbb{C}}(n)$. In particular, since $g_{R_2}(n) \le g_{R_1}(n)$ whenever R_1 is a subring of R_2, this bound will hold for any subring of $\mathbb{C}$. Our result in this direction is the following.

Theorem 2. *Let $\epsilon > 0$ and let $n_0 = n_0(\epsilon)$ be sufficiently large in terms of ϵ. Then for any $n \geq n_0$ we have*

$$g_{\mathbb{C}}(n) \geq n^{(1/200-\epsilon)\frac{\log\log(n)}{\log\log\log(n)}}. \tag{7}$$

The proof largely follows that of [2]. This approach uses yet another manifestation of the sum-product phenomenon, the statement that a small productset requires a large iterated sumset. Chang proved that if $A \subset \mathbb{Z}$ is finite, and $|A \cdot A| \leq \alpha|A|$ for some α, then for every $h \geq 2$ we have

$$|hA| \geq \frac{|A|^h}{(2h^2-h)^{h\alpha}}.$$

In [4], Chang also proved an analogous result in $\mathbb{R}$, provided the multiplicative doubling constant α satisfies $\alpha \ll \log|A|$. We will use a version which holds in $\mathbb{C}$:

Theorem 3. *Let $A \subset \mathbb{C}$ be finite, and suppose that $|A^{(2)}| \leq \alpha|A|$. Then there is an absolute constant c_1 such that for any integer $h \geq 2$ we have*

$$|hA| \geq c_1 e^{-h^{49h}\alpha}|A|^h.$$

We will prove this result by following Chang's argument for the real case, making necessary alterations to deal with the possibility of torsion elements in $\mathbb{C}$. Note the explicit dependence on h, which will be essential in our proof of Theorem 2. Using a result of Ruzsa ([10], Theorem 17 below), we have also extended Theorem 3 to distinct sets A and B.

Theorem 4. *Let $A, B \subset \mathbb{C}$ with $|B| = C|A|$ for some $C \geq 1$, and suppose that $|AB| < \alpha|A|$. If $\alpha \ll \log|A|$ then there is an absolute constant c_1 such that*

$$|kA + lB| \geq c_1 \frac{|A|^k|B|^l}{(k+l)^{4(k+l)}} - O_{k,l,\alpha}(|B|^{k+l-1})$$

where the implicit constant in the O term can be taken as $c_2 e^{4(k+l)^{15(k+l)}\alpha}$ for an absolute constant c_2.

This builds on the theme of sum product phenomena for distinct sets; other results in a similar vein may also be found in [4].

The proofs of Theorems 3 and 4 rely on bounding the number of additive $2h$-tuples in A^{2h} (respectively, additive $(2k+2l)$-tuples in $A^k \times B^l$); this is accomplished by using a result of Evertse, Schlickewei, and Schmidt [7] which we next describe.

Let K be an algebraically closed field of characteristic 0. Let $K^* = K \setminus \{0\}$ be the multiplicative subgroup of nonzero elements in K. For a positive integer d let Γ be a subgroup of $(K^*)^d$ with rank r (so the minimum number of elements from which we can generate Γ is r). For coefficients $a_1, \ldots, a_d \in K$, let $A(d,r)$ denote the number of solutions $(x_1, \ldots, x_d) \in \Gamma$ to

$$a_1x_1 + a_2x_2 + \cdots + a_dx_d = 1$$

which are nondegenerate (namely, no proper subsum of the left side vanishes).

It is crucial that in the following result, which we will refer to as the Subspace Theorem, the bound is finite and depends only on r and d, and not on the particular group Γ nor the particular coefficients of the objective equation.

Theorem 5. (Evertse, Schlickewei, and Schmidt [7]) *Let d, r, and $A(d,r)$ be as defined above. Then*

$$A(d,r) \leq \exp\left((6d)^{3d}(r+1)\right).$$

We will also use two other standard tools of additive combinatorics (see, for example, [15]). The first is Freiman's theorem in torsion-free groups [1] (given for general torsion free groups in, for example, [15]).

Theorem 6. (Freiman's Theorem) *Let Z be a torsion-free abelian group, and let $A \subset Z$ with $|A+A| \leq K|A|$ for some $K \in \mathbb{R}$. Then there exists a proper generalized arithmetic progression P of dimension at most $K-1$ and size $|P| \leq C(K)|A|$ which contains A. Here $C(K)$ depends only on K.*

The second is the Plünnecke-Ruzsa Inequality, in a version due to Ruzsa [11].

Theorem 7. (Plünnecke-Ruzsa Inequality [11]) *Let Z be an abelian group and let A and B be subsets of Z with $|A+B| \leq K|A|$. Then for every $n, m \in \mathbb{N}$ we have $|nB - mB| \leq K^{n+m}|A|$.*

In Section 2 we begin by extending Chang's notion of multiplicative dimension of a set of integers to sets of complex numbers, and prove three key properties of it. The third of these is an application of Freiman's Theorem, and allows us to bound the multiplicative dimension of a set from above by its multiplicative doubling constant $|A^{(2)}|/|A|$. This allows us to work with sets of low multiplicative dimension without loss of generality in order to use Theorem 5 to prove Theorem 3.

In Section 3 we carry out the argument which proves Theorem 2 on simple sums and products, using Theorem 3.

In Section 4, we use a Theorem of Ruzsa in place of Freiman's Theorem to show that if distinct sets A and B have a small productset, then we may once again bound the multiplicative dimension of both of them by $|AB|/|A|$. We are then once again able to proceed using Theorem 5 to prove Theorem 4.

Notation. We will use the notation $f(x) \ll g(x)$ or $f(x) = O(g(x))$ to denote that there is a constant C such that for every x, $f(x) \leq Cg(x)$. Similarly, $f(x) \gg g(x)$ is the same as $g(x) \ll f(x)$, and $f(x) \approx g(x)$ means that there are constants C_1, C_2 such that $C_1 g(x) \leq f(x) \leq C_2 g(x)$ for every x. We will use $\mathbb{N}$ to denote the positive integers, $\mathbb{N}_0$ to denote the nonnegative integers, and $\mathbb{Z}$ to denote the set of all integers. For an integer L, $\mathbb{Z}_L$ will denote the integers modulo L.

2. Sums and Products of a Single Set

2.1. Multiplicative Dimension and Bounding the Doubling Constant

Throughout this section A will denote a finite subset of $\mathbb{C}$ and n will denote the cardinality of A. Let $h \geq 2$ be an integer. Also, let

$$A^* := A \setminus \{0\}.$$

Then A^* consists of those elements of A contained in the multiplicative subgroup $\mathbb{C}^*$ of complex numbers. Lastly, the multiplicative subgroup of $\mathbb{C}^*$ generated by the elements $z_1, \ldots, z_m \in \mathbb{C}^*$ will be denoted by $\langle z_1, \ldots, z_m \rangle$.

We begin by extending the definition of multiplicative dimension from [2].

Definition 8. Let $A \subset \mathbb{C}$ be finite. Then we define the multiplicative dimension of A, denoted $\dim_\times(A)$, by

$$\dim_\times(A) = \min\Big\{M : \exists\, z, z_1, \ldots, z_M \in \mathbb{C}^* \text{ such that } A^* \subset z \cdot \langle z_1, \ldots, z_M \rangle\Big\}. \quad (8)$$

In other words, the multiplicative dimension of A is the minimal number M such that A^* is contained in a coset of subgroup of $\mathbb{C}^*$ of rank M.

For $d \in \mathbb{Z}^+$ and $X \subset \mathbb{R}^d$ we will say that X is r-dimensional if the affine subspace of $\mathbb{R}^d$ of smallest dimension in which X may be contained has dimension r. Note that if a set is r-dimensional it must contain at least $r+1$ elements, and must also contain r linearly independent differences. From this fact, observe that for $X, Y \subset \mathbb{R}^d$,

$$\dim(X+Y) \leq \dim(X) + \dim(Y) \quad (9)$$

and also that

$$\dim(X \cup Y) \geq \dim(X + Y). \tag{10}$$

We wish to relate the above two concepts of dimension to each other. To do so, we will need to transition between groups of the form $\langle z_1, ..., z_m \rangle$ and the group $\mathbb{Z}^m$. The Fundamental Theorem of Finitely Generated Abelian Groups provides the necessary maps to do so, in the proof of Lemma 9 below. However, some preliminary examples will help to clarify the argument.

Example. Let $A = \{2, \frac{1}{3}e^{i\pi/4}, \frac{1}{9}e^{i\pi/2}, e^{i\pi\sqrt{2}}\}$. Then A has multiplicative dimension equal to 3, since it is contained in $\langle 2, \frac{1}{3}e^{i\pi/4}, e^{i\pi\sqrt{2}} \rangle$ which is torsion-free. But this is just isomorphic to $\mathbb{Z}^3$, and furthermore if the isomorphism is denoted ν then we can take $\nu(2) = (1, 0, 0)$, $\nu(\frac{1}{3}e^{i\pi/4}) = (0, 1, 0)$, and $\nu(e^{i\pi\sqrt{2}}) = (0, 0, 1)$. Then we will have

$$\nu(A) = \{(1, 0, 0), (0, 1, 0), (0, 2, 0), (0, 0, 1)\}.$$

Note that $\dim(\nu(A)) = 3$.

Example. The situation is slightly more complicated if A contains torsion elements. Let $A = \{2, \frac{1}{3}e^{i\pi/4}, e^{i\pi/2}, e^{i\pi/3}\}$. Then A once again has multiplicative dimension equal to 3, since it is contained in $\langle 2, \frac{1}{3}e^{i\pi/4}, e^{i\pi/6} \rangle := G$. This group is isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}_6$. Denoting this isomorphism by η and proceeding as in the previous example, we have

$$\eta(A) = \{(1, 0, 0), (0, 1, 0), (0, 0, 2), (0, 0, 3)\}.$$

However, we can consider this to be a subset of $\mathbb{Z}^3$ of dimension 3 by considering the last component of each point to be in $[0, 5] \subset \mathbb{Z}$. This provides a one-to-one mapping η'' between $\eta(G)$ and $\mathbb{Z}^3$, and so we have a one-to-one mapping $\nu = \eta'' \circ \eta$ between G and $\mathbb{Z}^3$.

By extending the above calculations to the general case, one obtains the following key properties of multiplicative dimension, which we will use extensively.

Lemma 9. *Let $A \subset \mathbb{C}^*$ be finite with $\dim_\times(A) = m$. Let $G = \langle z_1, ..., z_m \rangle$ for some $z_1, ..., z_m \in \mathbb{C}^*$, and suppose that $A \subset z \cdot G$ for some $z \in \mathbb{C}^*$. Let $h \in \mathbb{N}$, $h \geq 2$. Then*

(a) *There is an injection $\nu : zG \to \mathbb{Z}^m$ mapping zG into the additive group of m-tuples of integers such that for every $B \subset A$ we have $\dim(\nu(B)) \geq \dim_\times(B)$ where $\nu(B)$ is viewed as a subset of $\mathbb{R}^m$.*

(b) *If ν is the map from (a), then for sets $B, B_1, ..., B_h \subset zG$ we have*

$$|B_1 \cdot ... \cdot B_h| \geq \frac{1}{h}|\nu(B_1) + ... + \nu(B_h)|. \tag{11}$$

and

$$|B^{\times}| \geq \frac{1}{|B|}|\nu(B)^{+}| \tag{12}$$

(c) $m \leq (2|(A)^{(2)}|/|A|) - 1$

Proof. **(a)** The map which takes $za \in G$ to a is an isomorphism, so we may assume without loss of generality that $A \subset \langle z_1, ..., z_m \rangle = G$.

By the fundamental theorem of finitely generated abelian groups applied to $\langle z_1, \ldots, z_m \rangle$, there is such a mapping if G is torsion-free.

Suppose that G is not torsion-free. We claim that, in this case, the fundamental theorem of finitely generated abelian groups guarantees an isomorphism $\eta : G \to \mathbb{Z}^{m-1} \times \mathbb{Z}_L$ for some integer L.

It certainly guarantees an isomorphism $\eta' : G \to \mathbb{Z}^{m-t} \times \mathbb{Z}_{L_1} \times ... \times \mathbb{Z}_{L_t}$ for some integer t, $1 \leq t \leq m$ and some $L_1, ..., L_t \in \mathbb{N}$. Then for $1 \leq j \leq m$ we let

$$\xi_j = \eta^{-1}((0, ...0, 1, 0, ..., 0))$$

where the nonzero entry is in the jth component.

For $m - t + 1 \leq j \leq m$, ξ_j has finite order, so it must be a root of unity. Hence there are positive integers r_j, s_j such that

$$\xi_j = e^{2\pi i r_j / s_j}.$$

Then, letting $s = s_{m-t+1} \cdot ... \cdot s_m$ and $\xi = e^{2\pi i/s}$ we see that $\xi_j = \xi^{r_j(s/s_j)}$, where $r_j(s/s_j) \in \mathbb{Z}$. In other words,

$$\xi_j \in \langle \xi \rangle$$

for each j, $m - t + 1 \leq j \leq m$. Therefore,

$$A \subset \langle \xi_1, ..., \xi_{m-t}, \xi \rangle$$

implying that $\dim_{\times} A \leq m - t + 1$. This is only possible if $t = 1$, and the claim follows.

Now, the map $\eta'' : \mathbb{Z}^{m-1} \times \mathbb{Z}_L \to \mathbb{Z}^m$ which takes $(x_1, ..., \overline{x}_m) \in \mathbb{Z}^{m-1} \times \mathbb{Z}_L$ to $(x_1, ..., x_m)$, where x_m is the residue in $[0, L-1]$ of the class $\overline{x}_m \in \mathbb{Z}_L$, is an injection. We take $\nu = \eta'' \circ \eta$. Note that ν maps G injectively onto $\mathbb{Z}^{m-1} \times [0, L-1]$, but that η^{-1} may be extended to a surjection defined on all of $\mathbb{Z}^m$ by setting $\eta^{-1}((x_1, ..., x_m)) = (x_1, ..., \overline{x}_m)$.

It remains to prove the claim that $\nu(B)$ has dimension $\dim_\times(B)$ for each $B \subset A$. This will follow from the definition of multiplicative dimension.

If $\nu(B)$ is contained in an affine subspace S of $\mathbb{R}^m$ of dimension d, we let $x^{(0)} \in S$. It follows that there are vectors $x^{(1)}, ..., x^{(d)} \in S - \{x^{(0)}\}$ such that $\nu(B) \subset \text{span}(x^{(1)}, ..., x^{(d)}) + \{x^{(0)}\}$. In other words, if $b \in B$, we can represent $\nu(b)$ as

$$\nu(b) = x^{(0)} + \sum_{i=1}^{d} k_i x^{(i)}$$

for some integers k_i, $i = 1, ..., d$.

Next, suppose that $x^{(i)} = (x_1^{(i)}, ..., x_m^{(i)})$ for $i = 0, ..., d$, and denote by $\overline{x^{(i)}}$ the element of $\mathbb{Z}^{m-1} \times \mathbb{Z}_L$ given by

$$\overline{x^{(i)}} = \left(x_1^{(i)}, ..., x_{m-1}^{(i)}, \overline{x_m^{(i)}}\right),$$

where once again $\overline{x_m^{(i)}} \in \mathbb{Z}_L$ is the residue class of $x_m^{(i)} \in [0, L-1]$. It follows that

$$\eta(b) = \overline{x^{(0)}} + \sum_{i=1}^{d} k_i \overline{x^{(i)}}.$$

Then

$$\begin{aligned} b = \eta^{-1}(\eta(b)) &= \eta^{-1}\left(\overline{x^{(0)}} + \sum_{i=1}^{d} k_i \overline{x^{(i)}}\right) \\ &= \eta^{-1}\left(\overline{x^{(0)}}\right) \prod_{i=1}^{d} \left(\eta^{-1}\left(\overline{x^{(i)}}\right)\right)^{k_i} \\ &\in \eta^{-1}\left(\overline{x^{(0)}}\right) \left\langle \eta^{-1}\left(\overline{x^{(1)}}\right), ..., \eta^{-1}\left(\overline{x^{(d)}}\right) \right\rangle. \end{aligned}$$

By definition of multiplicative dimension, it follows that $d \geq \dim_\times(B)$.

(b) Equations (11) and (12) follow immediately in the case where G is torsion-free (and hence ν is an isomorphism). We may therefore assume that G contains roots of unity.

Let $\eta : G \to \mathbb{Z}^{m-1} \times \mathbb{Z}_L$ be the isomorphism from (a). Then to prove (11), it is sufficient to show $|\eta(B_1) + ... + \eta(B_h)| \geq \frac{1}{h}|\nu(B_1) + ... + \nu(B_h)|$. Let

$$x = (x_1, ..., x_m) \in \nu(B_1) + ... + \nu(B_h).$$

Then there are elements $x^{(i)} = (x_1^{(i)}, ..., x_m^{(i)}) \in \nu(B_i)$ for each i, $1 \leq i \leq h$ such that

$$x = \sum_{i=1}^{h} x^{(i)},$$

so

$$(x_1, ..., \overline{x_m}) \in \eta(B_1) + ... + \eta(B_h).$$

But

$$\nu(B_1) + ... + \nu(B_h) \subset \mathbb{Z}^{m-1} \times [0, hL]$$

and so there are at most h elements $(x_1, ..., x_{m-1}, y)$ of the left side such that $(x_1, ..., x_{m-1}, \overline{y})$ evaluates to $(x_1, ..., \overline{x_m})$. Hence there are at least

$$|\nu(B_1) + ... + \nu(B_h)|/h$$

elements in $\eta(B_1) + ... + \eta(B_h)$ as required.

The proof of (12) is nearly identical to that of (11). It is sufficient to show $|\eta(B)^+| \geq \frac{1}{|B|}|\nu(B)^+|$. Denote $\nu(B) = \{x^{(1)}, ..., x^{(|B|)}\}$, and let

$$x = (x_1, ..., x_m) \in \nu(B)^+.$$

Then there are values $\epsilon_i \in \{0, 1\}$ for each i, $1 \leq i \leq |B|$ such that

$$x = \sum_{i=1}^{|B|} \epsilon_i x^{(i)},$$

so

$$(x_1, ..., \overline{x_m}) \in \eta(B)^+.$$

But

$$\nu(B)^+ \subset \mathbb{Z}^{m-1} \times [0, |B|L]$$

and so there are at most $|B|$ elements $(x_1, ..., x_{m-1}, y)$ of the left side such that $(x_1, ..., x_{m-1}, \overline{y})$ evaluates to $(x_1, ..., \overline{x_m})$. Hence there are at least

$$|\nu(B)^+|/|B|$$

elements in $\eta(B)^+$ as required.

(c) Let $\beta = |(A)^{(2)}|/|A|$. Then by the first claim in part (b), $|\nu(A) + \nu(A)| \leq 2|(A)^{(2)}| \leq 2\beta|\nu(A)|$. Now, Theorem 6 applies, and we may contain $\nu(A)$ in a progression in $\mathbb{Z}^m$ of dimension $\lfloor 2\beta - 1 \rfloor$, say

$$\nu(A) \subset \left\{ x^{(0)} + \sum_{i=1}^{\lfloor 2\beta - 1 \rfloor} j_i x^{(i)} : 0 \leq j_i \leq k_i - 1 \right\}.$$

But then

$$A \subset \eta^{-1}(\overline{x^{(0)}}) \left\langle \eta^{-1}(\overline{x^{(1)}}), ..., \eta^{-1}(\overline{x^{\lfloor 2\beta - 1 \rfloor}}) \right\rangle,$$

which demonstrates the desired bound. □

Note that if $0 \in A$ and $\alpha = |A^{(2)}|/|A|$, then we may apply Lemma 9 to A^*, noting that

$$\begin{aligned} |(A^*)^{(2)}| &= |A^{(2)} \setminus \{0\}| \\ &= |A^{(2)}| - 1 \\ &\leq \alpha|A| - 1 \\ &= \alpha(|A^*| + 1) - 1 \\ &\leq 2\alpha|A^*|, \end{aligned}$$

so that we obtain the inequality

$$m \leq 4\alpha - 1. \tag{13}$$

2.2. Bounding Additive $2h$-tuples

In light of (13), we are free to work with sets of low multiplicative dimension. Theorem 3 will follow as a corollary of the following.

Proposition 10. *Let $A \subset \mathbb{C}$ be finite, and suppose that $\dim_\times(A) = m$. Then for any $h \in \mathbb{N}$, $h \geq 2$ there is n sufficiently large such that if $|A| \geq n$ we have*

$$|hA| \geq e^{-h^{49h}m}|A|^h$$

We will say that a $2h$-tuple $(a_1, ..., a_{2h}) \in A^{2h}$ is an additive $2h$-tuple if $a_1 + ... + a_h = a_{h+1} + ... + a_{2h}$. The above proposition is a consequence of the following lemma from [2].

Lemma 11. *Let $A \subset \mathbb{C}$ be finite. Let M denote the number of additive $2h$-tuples in A^{2h}. Then*

$$|hA| \geq \frac{|A|^{2h}}{M}.$$

To prove Proposition 10 we therefore seek to bound the number of solutions $(a_1, ..., a_{2h})$ in A^{2h} to the equation

$$x_1 + \cdots + x_h = x_{h+1} + \cdots + x_{2h}. \tag{14}$$

To do so, one finds a likely tool in Theorem 5. However, Theorem 5 gives a bound on the number of nondegenerate solutions, whereas we must also account for the possibility of degenerate solutions. The result is the following statement, similar to a lemma of Chang in [4]:

Lemma 12. *Suppose that $A \subset \mathbb{C}$ satisfies $0 \notin A$, and let $\dim_\times(A) = m$. For every $k \geq 1$ there is n sufficiently large such that if $|A| \geq n$ and $c_1, ..., c_k \in \mathbb{C}^*$ then*

(a) *The number of elements $(y_1, \ldots, y_k) \in A^k$ satisfying $c_1y_1 + \cdots + c_ky_k = 1$ is at most $e^{k^{12k}m}n^{\lfloor k/2 \rfloor}$ if k is odd and $e^{k^{12k}m}n^{k/2-1}$ if k is even.*

(b) *The number of elements $(y_1, \ldots, y_k) \in A^k$ satisfying $c_1y_1 + \cdots + c_ky_k = 0$ is at most $e^{k^{12k}m}n^{\lfloor k/2 \rfloor}$.*

Proof. For $r, s \in \mathbb{N}$, let

$$D_{s,r} = \exp(s^{12s}r),$$

and let

$$\gamma_1(s) = \begin{cases} \lfloor s/2 \rfloor, & \text{if } s \text{ is odd} \\ s/2 - 1, & \text{if } s \text{ is even} \end{cases}, \tag{15}$$

$$\gamma_0(s) = \lfloor s/2 \rfloor. \tag{16}$$

Then the statement we need to prove is that the number of solutions $(y_1, ..., y_k)$ in A^k to $c_1y_1 + \cdots + c_ky_k = 1$ is at most $D_{k,m}n^{\gamma_1(k)}$ and that the number of solutions to $c_1y_1 + \cdots + c_ky_k = 0$ is at most $D_{k,m}n^{\gamma_0(k)}$.

Since A has multiplicative dimension m, $A \subset zH$ for some subgroup H of $\mathbb{C}^*$ of rank m; hence $G = \langle zH \rangle$ is a group of rank at most $m + 1$ which contains A.

The proof proceeds by induction on the number of variables k.

`Base Cases:` The case $k = 1$ is immediate.

When $k = 2$ we see directly that the number of solutions $(y_1, y_2) \in A \times A$ to $c_1y_1 + c_2y_2 = 0$ is at most n (Each of $|A| = n$ choices for y_1 determines a value $-c_1y_1/c_2$ for y_2). Meanwhile the number of nondegenerate solutions $(y_1, y_2) \in A \times A$ to $c_1y_1 + c_2y_2 = 1$ is at most $\exp((12)^6(2(m + 1) + 1))$ by Theorem 5, and the only two possible degenerate solutions are $(0, 1)$ and $(1, 0)$. We have

$$\exp((12)^6(2m + 3)) + 2 \leq \exp(2^{24}m).$$

Hence the bound holds for $k = 2$ and all pairs (c_1, c_2) of coefficients.

`Induction:` Let $k > 2$ be fixed, and suppose both parts of the theorem have been proved for t variables for each positive integer $t < k$ and for all t-tuples of coefficients $(c_1, ..., c_t)$.

We begin with the equation

$$c_1y_1 + \cdots + c_ky_k = 0, \tag{17}$$

which we rewrite as $c_1y_1 + ... + c_{k-1}y_{k-1} = -c_ky_k$. There are at most n choices for y_k in A, all of which are nonzero. Picking one of these (call it a) and dividing through by the value $-c_ka$, the number of solutions $(y_1, ..., y_{k-1}, a) \in A^k$ to (17) is the number of solutions to the new equation

$$\frac{c_1}{-c_ka}y_1 + \cdots + \frac{c_{k-1}}{-c_ka}y_{k-1} = 1 \tag{18}$$

in $k-1$ variables. There are still n possibilities for each variable in this equation, and each still falls in A.

First suppose k is even. Then $k-1$ is odd, so by the inductive hypothesis there are at most $D_{k-1,m}n^{(k-2)/2}$ solutions in A^{k-1} to (18). Since there are at most n possible values for a, we have at most $D_{k-1,m}n^{k/2}$ solutions in A^k to (17). Since k is even, this is the desired result.

Next, if k is odd, $k-1$ is even, and the equation (18) has fewer than $D_{k-1,m}n^{(k-1)/2-1}$ solutions in A^{k-1}, whereby the (17) has fewer than $D_{k-1,m}n^{(k-1)/2}$ in A^k. This again gives the desired result.

Hence the result for vanishing sums holds in k variables.

To count solutions in A^k to

$$c_1y_1 + \cdots + c_ky_k = 1, \tag{19}$$

we begin by applying Theorem 5. This tells us that the number of nondegenerate solutions in the entirety of the rank $k(m+1)$ group G^k is bounded by $\exp((6k)^{3k}(k(m+1)+1))$. We use the inductive hypothesis to count degenerate solutions.

For each such degenerate solution $(y_1, ..., y_k) \in A^k$ of (19) we have a nonempty proper subset of $\{c_1y_1, ..., c_ky_k\}$ which sums to 0, and the complement of this proper subset sums to 1. From each degenerate solution, then, we obtain a corresponding solution of a system of the form

$$\sum_{j=1}^{t} c_{i_j}y_{i_j} = 0 \qquad\qquad \sum_{j=t+1}^{k} c_{i_j}y_{i_j} = 1 \tag{20}$$

where $2 \le t \le k-1$, and $i_1, \ldots, i_k$ is some permutation of $1, \ldots, k$ with $i_1 < \cdots < i_t$ and $i_{t+1} < \cdots < i_k$. Furthermore, every other solution of (19) in A^k from which we obtain the same solution of (20) in this manner must have components which are a permutation of $(y_1, ..., y_k)$.

It follows that, since there are $\binom{k}{t}$ choices for $\{i_1, \ldots, i_t\}$, the total number of solutions in A^k to (19) is bounded via the inductive hypothesis by

$$2(k!)\sum_{t=2}^{k-1}\binom{k}{t}D_{t,m}D_{k-t,m}n^{\gamma_0(t)+\gamma_1(k-t)} \tag{21}$$

where we have used the extra factor of two to simply account for the small number nondegenerate solutions. We begin by computing the exponent on n. Arguing based on parity of k, for k even we have

$$\gamma_0(t) + \gamma_1(k-t) = k/2 - 1 = \gamma_1(k), \tag{22}$$

independent of the parity of t. Similarly, for k odd, we get

$$\begin{aligned} \gamma_0(t) + \gamma_1(k-t) &= \begin{cases} (k-1)/2, \text{ if } t \text{ is even} \\ (k-3)/2, \text{ if } t \text{ is odd} \end{cases} \\ &\leq \gamma_1(k). \end{aligned}$$

In both cases we see that we can bound (21) by

$$\left(2(k!)\sum_{t=2}^{k-1}\binom{k}{t}D_{t,m}D_{k-t,m}\right)n^{\gamma_1(k)} \tag{23}$$

and we need only compute the constant.

Now,

$$D_{t,m}D_{k-t,m} = \exp\left[(t^{12t} + (k-t)^{12(k-t)})m\right]. \tag{24}$$

The exponent is maximized over all possible values of t for $t = k-1$.

The entire sum is therefore bounded above by

$$2(k!)\exp((1 + (k-1)^{12(k-1)})m)\sum_{t=2}^{k-1}\binom{k}{t} \leq \exp(k^{12k}m)$$

using the fact that $\sum_{t=2}^{k-1}\binom{k}{t} < 2^k$.

The result for unit sums therefore holds for k variables. The lemma now follows by induction. □

In order to prove Proposition 10 we must eliminate the hypothesis $0 \notin A$ from Lemma 12(b) for the case of equations of the form (14).

We continue to use the notation $n = |A|$. Then if $0 \in A$, the number of solutions to (14) we gain is bounded above by

$$\sum_{t=1}^{2h-1} \binom{2h}{t} D_{2h-t,m} n^{\lfloor (2h-t)/2 \rfloor}.$$

Here we have set t variables in the equation (14) equal to 0 and used Lemma 12 to count the number of solutions to the resulting equation, for each t, $1 \leq t \leq 2h-1$. We can further bound the above expression by

$$D_{2h-1,m} n^{h-1} \cdot 2^{2h}.$$

After a short calculation, we see that the total possible number of solutions in A^{2h} to (14) for arbitrary A is therefore

$$\leq \quad \exp(h^{49h} m) n^h$$

if n is sufficiently large. We have therefore proved:

Lemma 13. *Let $A \subset \mathbb{C}$ be finite, and let $\dim_\times(A) = m$. Then for every $h \in \mathbb{N}$ there exists n sufficiently large that if $|A| \geq n$ then the number of additive $2h$-tuples in A is bounded above by $\exp(h^{49h} m) n^h$.*

Combining this with Lemma 11 we obtain Proposition 10.

Remark 14. The above lemma was proved with the bound $e^{(-h^{Ch}(m+1))} n^h$ for some undetermined constant C by Chang in [4]. In fact, Chang's result is somewhat stronger, with a bound of the form $O_h(n^h + e^{(-h^{Ch}(m+1))} n^{h-1})$. Since using this form of the bound makes the following estimates more complicated with no quantitative gains in the final result, we will not use it here.

3. Simple Sums and Simple Products

We are now in a position to consider simple sums and simple products constructed from a finite set $A \subset \mathbb{C}$. The proof of Theorem 2 is similar to that for the integer case, given in [2]. When working with subsets of the complex plane, however, we use our revised definition of multiplicative dimension (8) and the bound in Lemma 13.

For a finite set $A \subset \mathbb{C}$ let $g(A) = |A^+| + |A^\times|$. Then for each positive integer n, we have $g_{\mathbb{C}}(n) = \min_{A \subset \mathbb{C},\ |A|=n} g(A)$, and it is sufficient to show that for any $\epsilon > 0$ and an arbitrary set A of sufficiently large size n we necessarily have $g(A) \geq n^{(1/200-\epsilon)\frac{\log\log(n)}{\log\log\log(n)}}$.

We begin by showing that a large proportion of the iterated sumset hA is included in the set $|hA \cap A^+|$.

Lemma 15. *Let $A \subset \mathbb{C}$ be finite with $\dim_\times(A) = m$ and such that $|A|$ is sufficiently large. Then for any sufficiently large $h \in \mathbb{N}$ with $h \leq |A|$ we have*

$$|hA \cap A^+| \geq \frac{|A|^h}{\exp(h^{50h}m)}.$$

Proof. This follows exactly as in [2]. First we observe that the left-hand side is at least as large as the number of simple sums with exactly h summands. Letting

$$r_{hA}(x) = |\{(a_1, \ldots, a_h) \in A^h : a_1 + \cdots + a_h = x\}|$$

we have

$$\binom{|A|}{h} \leq \sum_{x \in hA \cap A^+} r_{hA}(x). \tag{25}$$

Using Stirling's formula in the form $N! \approx N^{N+1/2}e^{-N}$ on the left side we have

$$\binom{|A|}{h} = \frac{|A|!}{h!(|A|-h)!} \geq C\frac{|A|^{|A|}}{h^{h+1/2}|A|^{|A|-h}} = C(|A|/h^{1+1/2h})^h.$$

for an absolute constant C. Combining the previous two relations and applying the Cauchy-Schwartz inequality followed by Lemma 13 to the right side of (25) we have

$$\begin{aligned} C(|A|/h^{1+1/2h})^h &\leq |hA \cap A^+|^{1/2}\left(\sum_{x \in hA \cap A^+} (r_{hA}(x))^2\right)^{1/2} \\ &\leq |hA \cap A^+|^{1/2}(\exp(h^{49h}m)|A|^h)^{1/2}. \end{aligned}$$

since the bracketed sum after the first inequality is at most the number of additive $2h$ tuples in A. It follows that

$$|hA \cap A^+| \geq C^2\frac{|A|^h}{h^{2h+1}\exp(h^{49h}m)},$$

and absorbing the constant C^2 and the factor h^{2h+1} into the exponential (recalling h is large) we have

$$|hA \cap A^+| \geq \frac{|A|^h}{\exp(h^{50h}m)}.$$

□

The next step is to show that a set with small multiplicative dimension must have a large simple sum.

Lemma 16. *Let $B \subset \mathbb{C}$, and suppose that $\dim_\times(B) = m$. Then for any ϵ_1 with $0 < \epsilon_1 < 1/50$, there exists $n = n(\epsilon_1) \in \mathbb{N}$ sufficiently large such that if*

$$|B| \geq \sqrt{n}$$

and

$$m \leq \left(\frac{1}{50} - \epsilon_1\right) \frac{\log\log(n)}{\log\log\log(n)}$$

then

$$g(B) \geq n^{\frac{\epsilon_1}{3} \frac{\log\log(n)}{\log\log\log(n)}}. \tag{26}$$

Proof. We have

$$g(B) > |B^+| \geq |hB \cap B^+|$$

for any $h \in \mathbb{N}$. Applying Lemma 15 to the right side we therefore have

$$g(B) > \frac{|B|^h}{\exp(h^{50h} m)}$$

provided h is sufficiently large. We take $h = \lfloor \frac{1}{50} \frac{\log\log(n^{1/2})}{\log\log\log(n)} \rfloor$. Then

$$50h \log(h) \leq \log\log(n^{1/2})$$

so

$$\exp(h^{50h} m) \leq n^{m/2}.$$

But then we have

$$g(B) > \frac{|B|^h}{n^{m/2}} \geq n^{h/2 - m/2}.$$

Recalling our condition on m and our choice of h and using the fact that n is large in terms of ϵ_1, we have the result. □

We now use the previous two lemmas to prove Theorem 2. Let $\epsilon > 0$ be sufficiently small. Also, let $A \subset \mathbb{C}$ be finite with $\dim_\times(A) = m$, and let $\epsilon_1, \epsilon_2 < \epsilon$. Let $n = n(\epsilon)$ be sufficiently large in terms of ϵ, and suppose $|A| = n$. We may assume without loss of generality that $0 \notin A$.

By Lemma 16 we may also assume without loss of generality that every subset $B \subset A$ with $|B| \geq \sqrt{n}$ satisfies

$$\dim_\times(B) \geq \left\lfloor \left(\frac{1}{50} - \epsilon_1\right) \frac{\log\log(n)}{\log\log\log(n)} \right\rfloor. \tag{27}$$

We therefore divide A into sets $B_1, \ldots, B_{\lfloor\sqrt{n}\rfloor}$, each with size $|B_i| \geq \sqrt{n}$, and denote

$$A_s = \cup_{i=1}^{s} B_i,$$

so $A_{\lfloor\sqrt{n}\rfloor} = A$.

Taking $B = A$ in equation (27) we apply Lemma 9 to conclude the existence of a map $\nu : zG \to \mathbb{Z}^m$ for some coset zG of a subgroup G of $\mathbb{C}^*$ which contains A and for some $m \geq \lfloor (1/50 - \epsilon_1) \frac{\log\log(n)}{\log\log\log(n)} \rfloor$. Applying (12) we have

$$g(A) > |A^{\times}| \geq \frac{1}{|A|} |\nu(A)^+|. \tag{28}$$

It will therefore be sufficient to prove the bound of Theorem 2 for $|\nu(A)^+|$.

Let

$$\rho = 1 + n^{-1/2+\epsilon_2}.$$

The proof now splits into two cases: first the case in which the simple sums of the sets $\nu(A_s)$ grow quickly with s, followed by a complementary case in which we are able to effectively use the large multiplicative dimension of B_s for some s.

First, if $|\nu(A_s \cup B_{s+1})^+| > \rho|\nu(A_s)^+|$ for every s, we can begin with $A_1 = B_1$ and iterate, gaining a factor of ρ each time, to get

$$|\nu(A)^+| > \rho^{\lfloor\sqrt{n}\rfloor - 1} |\nu(B_1)| > \rho^{\sqrt{n}-2}\sqrt{n}.$$

Hence, using (for x small) $\log(1+x) > x - x^2/2 > x/2$ we have

$$\begin{aligned} |\nu(A)^+| &> \exp\left((\sqrt{n} - 2)\log(\rho) + \frac{1}{2}\log(n) \right) \\ &> \exp\left((\sqrt{n} - 2)(1/2) n^{-1/2+\epsilon_2} + \frac{1}{2}\log(n) \right) \\ &> \exp((1/2) n^{\epsilon_2}) \end{aligned}$$

The last bound is much better than what we are ultimately trying to prove.

We are therefore reduced to the case where $|\nu(A_s \cup B_{s+1})^+| \leq \rho|\nu(A_s)^+|$ for some s. Let $m = \dim_{\times}(B_{s+1})$, so $m \geq \lfloor \left(\frac{1}{50} - \epsilon_1\right) \frac{\log\log(n)}{\log\log\log(n)} \rfloor$ by (27).

Now, since the sets B_i are disjoint, the sets $\nu(B_i)$ are as well, so that

$$\nu(A_s \cup B_{s+1})^+ = (\nu(A_s) \cup \nu(B_{s+1}))^+ = \nu(A_s)^+ + \nu(B_{s+1})^+. \tag{29}$$

We therefore have

$$|\nu(A_s)^+ + \nu(B_{s+1})^+| \leq \rho|\nu(A_s)^+|, \tag{30}$$

so by the Plünnecke-Ruzsa Inequality (Theorem 7) for any $h \in \mathbb{N}$ we have

$$|(h+1)\nu(B_{s+1})^+ - \nu(B_{s+1})^+| \leq \rho^{h+2}|\nu(A_s)^+|. \tag{31}$$

Let $\nu(B_{s+1}) = \{b_1, \ldots, b_k\}$, and define the h-fold simple sum of $\nu(B_{s+1})$ by

$$\nu(B_{s+1})^+[h] := \left\{ \sum_{i=1}^{k} \epsilon_i b_i : \epsilon_i \in \{0, 1, \ldots, h\},\ i = 1, \ldots, k \right\}.$$

Then the left-hand side of (31) is larger than

$$\begin{aligned} |h\nu(B_{s+1})^+| &\geq |\nu(B_{s+1})^+[h]| \\ &\geq h^m. \end{aligned} \tag{32}$$

The second inequality here comes from looking at the h-fold simple sum of a linearly independent set in $\mathbb{R}^m$ chosen from $\nu(B_{s+1})$, since by Lemma 9 (a), $\nu(B_{s+1})$ is at least m-dimensional.

We now take $h = \lfloor n^{1/2-\epsilon_2} \rfloor$, so that

$$\begin{aligned} \rho^{h+2} &\leq (1 + n^{-1/2+\epsilon_2})^{n^{1/2-\epsilon_2}+2} \\ &< \exp((n^{1/2-\epsilon_2} + 2)\log(1 + n^{-1/2+\epsilon_2})) \\ &< e^2. \end{aligned} \tag{33}$$

Combining (31), (32), and (33), we have

$$\begin{aligned} |\nu(A_s)^+| &> e^{-2}h^m \\ &> e^{-2}\lfloor n^{1/2-\epsilon_2} \rfloor^{\lfloor \left(\frac{1}{50}-\epsilon_1\right)\frac{\log\log(n)}{\log\log\log(n)} \rfloor}. \end{aligned}$$

This proves the theorem.

4. Sums of Distinct Sets With Small Productset

4.1. Bounding the Multiplicative Dimension in terms of the Relative Size of the Productset

In this section we begin to prove Theorem 4. Let $A, B \subset \mathbb{C}$ be finite, with $|B| = C|A|$, and suppose that $|AB| < \alpha|A|$. In analogy with the proof of Theorem 3, our strategy is to use the condition $|AB| < \alpha|A|$ to bound the multiplicative dimensions of $|A|$ and $|B|$ in terms of α. However, we no longer have Freiman's theorem at our disposal. Instead, we substitute for it with the following result of Ruzsa [10].

Theorem 17. ([10]) *Let $n \in \mathbb{N}$, and let $X, Y \subset \mathbb{R}^n$ be finite with $|X| \leq |Y|$. Suppose $\dim(X+Y) = n$. Then we have*

$$|X+Y| \geq |Y| + n|X| - \frac{n(n+1)}{2}. \tag{34}$$

We begin by translating the problem to the setting of Ruzsa's result.

Suppose $0 \notin A \cup B$, and let $D = \dim_\times(A \cup B)$. Let $G_{A\cup B}$ be a multiplicative group in $\mathbb{C}^*$ of rank D which has a coset $zG_{A\cup B}$ that contains $A \cup B$. Then by Lemma 9 there is an injective map $\nu : zG_{A\cup B} \to (\mathbb{Z}^D, +) \subset (\mathbb{R}^D, +)$. We set

$$d = \dim(\nu(A) + \nu(B)) \geq \max(\dim \nu(A), \dim \nu(B)) \geq \max(\dim_\times(A), \dim_\times(B)) \tag{35}$$

where the first inequality holds because $\nu(A) + \nu(B)$ contains translates of both $\nu(A)$ and $\nu(B)$ and the second inequality follows from Lemma 9(a).

Now, we may have $d < D$, so we cannot immediately apply Theorem 17. However, as mentioned $\nu(A) + \nu(B)$ contains translates $\nu(A) + \beta$ and $\alpha + \nu(B)$ for $\alpha \in \nu(A)$, $\beta \in \nu(B)$. Let $\mathbb{A}^d$ be the real affine space containing $\nu(A) + \nu(B)$, and let $\gamma \in \mathbb{A}^d$. Then $\mathbb{A}^d - \gamma$ is a subspace of $\mathbb{R}^D$ of dimension d, and so there is an isomorphism $\eta : (\mathbb{A}^d - \gamma) \to \mathbb{R}^d$. Setting $X = \eta(\nu(A) + \beta - \gamma)$ and $Y = \eta(\nu(B) + \alpha - \gamma)$ we find that

$$\begin{aligned} |X+Y| &= |\eta(\nu(A) + \nu(B) + \alpha + \beta - 2\gamma)| \\ &= |\nu(A) + \nu(B) + \alpha + \beta - 2\gamma| \\ &= |\nu(A) + \nu(B)| \\ &\leq 2|AB| \end{aligned} \tag{36}$$

where in the last step we applied Lemma 9(b). In addition, we have

$$\dim(X+Y) = d. \tag{37}$$

Combining (35), (36), and (37) we have now proven the following.

Lemma 18. *Let $A, B \subset \mathbb{C}\backslash\{0\}$ be finite. Then there exists $d \geq \max(\dim_\times(A), \dim_\times(B))$ and sets $X, Y \subset \mathbb{R}^d$ with $|X| = |A|$ and $|Y| = |B|$ such that*

$$\dim(X+Y) = d$$

and

$$|X+Y| \leq 2|AB|.$$

Theorem 17 now applies to the sets X and Y. Rewriting the result in terms of A and B by using the above lemma, we get

Corollary 19. *Let $A, B \subset \mathbb{C} \setminus \{0\}$ be finite. Then there exists $d \geq \max(\dim_\times(A), \dim_\times(B))$ such that*

$$2|AB| \geq |B| + d|A| - \frac{d(d+1)}{2}. \tag{38}$$

In order to bound the multiplicative dimensions of A and B in terms of α, we need to handle the trailing term of $-d(d+1)/2$. Since, recalling (9), $\dim(X+Y) \leq \dim(X) + \dim(Y)$, we have

$$|A| + |B| = |X| + |Y| \geq d + 2.$$

Then if we let $K = (|A| + |B|)/(d+2)$ we therefore have

$$K \geq 1. \tag{39}$$

We can now rewrite Corollary 19 in terms of α, C, and K.

Lemma 20. *Let $A, B \subset \mathbb{C} \setminus \{0\}$ be finite, with $|B| = C|A|$ for some $C > 1$ and $|AB| < \alpha|A|$, and let $m = \max(\dim_\times(A), \dim_\times(B))$. Then there exists $d \geq m$ such that if $K = \frac{|A|+|B|}{d+2}$ then*

$$m < \frac{2\alpha - C}{1 - \frac{C}{K}}. \tag{40}$$

Proof. Let $d \geq m$ be any value given by the conclusion of Corollary 19. It suffices to prove the bounds for d.

By Corollary 19 we have

$$2\alpha|A| > 2|AB| \geq |B| + d|A| - \frac{d(d+1)}{2}.$$

Rearranging,

$$2\alpha \geq C + d - \frac{d(d+1)}{2|A|}.$$

Now, we have $2C|A| = 2|B| > |A| + |B|$, so this gives

$$2\alpha - C \geq d - \frac{Cd(d+1)}{K(d+2)} \geq d\left(1 - \frac{C}{K}\right).$$

Dividing, we see the result. □

For our application of this lemma, we need to avoid the singular behavior when $K = C$. The following will allow us to bound C/K away from 1.

Lemma 21. *Let $d \in \mathbb{N}$ be a sufficiently large integer and suppose that $X, Y \subset \mathbb{R}^d$ are sufficiently large and satisfy*

$$|Y| = C|X|, \qquad 1 \leq C \ll \log^2 |X|$$

and

$$\dim(X + Y) = d.$$

Set $K = (|X| + |Y|)/(d + 2)$. Then if $K \leq \log^2 |X|$ we have

$$|X + Y| \gg \frac{|X||Y|}{\log^4 |X|}. \tag{41}$$

Proof. We begin by recalling (10) to assert that $\dim(X \cup Y) = d$. Hence there are linearly independent vectors $x_1, \ldots, x_r$ and $y_1, \ldots, y_{d-r}$ for some $1 \leq r \leq d$ and a point $x_0 \in X$ such that $x_0 + x_i \in X$ for $1 \leq i \leq r$ and $x_0 + y_j \in Y$ for $1 \leq j \leq d - r$.

First, suppose that $r \geq d/2$. Then let Y' be any subset of Y with $|Y'| = \lfloor |Y|/(8 \log^2 |X|) \rfloor$. Note that $|Y| \geq |X|$, so $|Y'| \neq 0$ since $|Y|$ is taken to be sufficiently large, but that (from the definition of K)

$$|Y'| \leq (d + 2)/8 = d/8 + 1/4 < d/4.$$

Hence we may choose $X' \subset x_0 + \{x_1, \ldots, x_r\}$ such that

$$|X'| = \lfloor d/4 \rfloor \geq |Y'| \geq |X|/(16 \log^2 |X|)$$

and such that the spans of $X' - x_0$ and $Y' - x_0$ do not intersect. Since $x + y = x' + y'$ implies $y - y' = x' - x$, it follows that

$$|X + Y| \geq |X' + Y'| \gg (|X|/(2^5 \log^2 |X|))(|Y|/(2^5 \log^2 |X|)).$$

If $r \leq d/2$, then $d - r \geq d/2$, and the argument is the same with the sets exchanged. □

The following summarizes the results of this section as they will apply in the proof of Theorem 4:

Proposition 22. *Let $A, B \subset \mathbb{C} \backslash \{0\}$ be finite with $|A|$ sufficiently large, and suppose that $|B| = C|A|$ for some $1 \leq C \ll \log^2 |A|$ and $|AB| < \alpha |A|$. Assume that*

$$\alpha \ll \log |A|.$$

and let

$$m = \max(\dim_\times(A), \dim_\times(B)).$$

Then

$$m < 4\alpha$$

Proof. By Lemma 18 there is $d \geq \max(\dim_\times(A), \dim_\times(B))$ and sets $X, Y \subset \mathbb{R}^d$ with $|X| = |A|$ and $|Y| = |B|$ such that

$$|X + Y| \leq 2|AB| \leq 2\alpha|A| \ll 2|A| \log |A|.$$

Letting $K = (|X| + |Y|)/(d + 2) = (|A| + |B|)/(d + 2)$, Lemma 21 therefore implies that

$$K > \log^2 |X|.$$

Now, by Lemma 20 we have

$$m < \frac{2\alpha - C}{1 - \frac{C}{K}},$$

and since $C|A| = |B| \leq |AB| \leq \alpha|A|$ we get $C \ll \log |A|$. Hence

$$C/K \leq 1/2$$

since $|A|$ is sufficiently large and we get

$$m < \frac{2\alpha - C}{1 - \frac{1}{2}} < 4\alpha.$$

□

With Propostion 22 proven, we could proceed by induction (albeit with more bookeeping) as in Section 2 (or [4]) to complete the proof of Theorem 4. However, the alternative proof in the next section leads to a better dependence on the numbers of iterates k and l.

4.2. Conclusion of the Proof of Theorem 4

We have once again reduced our problem involving the relative productset size $|AB|/|A|$ into one involving multiplicative dimension. Theorem 4 is now a corollary of the following lemma.

Lemma 23. *Let $A, B \subset \mathbb{C}$ be finite sets and suppose that $|B| = C|A|$ for some $C > 1$. Let*

$$m = \max(\dim_\times(A), \dim_\times(B)),$$

and let $k, l \in \mathbb{N}_0$. Assume that $m \ll \log |A|$. Then there is an absolute constant c_1 such that

$$|kA + lB| \geq c_1 \frac{|A|^k |B|^l}{(k + l)^{4(k+l)}} - O_{k,l,m}(|B|^{k+l-1})$$

where the implicit constant in the O term can be taken as $c_2 e^{(k+l)^{15(k+l)}m}$ for an absolute constant c_2.

Lemma 23 will in turn follow from a lemma which places slightly stronger hypotheses on the sets A and B, with small losses in the k and l dependence when these hypotheses are removed.

Lemma 24. *Let $A, B \subset \mathbb{C} \setminus \{0\}$ be finite sets and suppose that $|B| = C|A|$ for some $C > 1$. Let*

$$m = \max(\dim_\times(A), \dim_\times(B)),$$

and let $k, l \in \mathbb{N}_0$. Assume that $m \ll \log |A|$. In addition, suppose that

$$A \cap (-A) = B \cap (-B) = A \cap B = A \cap (-B) = \emptyset. \tag{42}$$

Then

$$|kA + lB| \geq \binom{|A|}{k}\binom{|B|}{l} - O_{k,l,m}(|B|^{k+l-1}),$$

where the implicit constant in the O term can be taken as $ce^{(k+l)^{15(k+l)}m}$ for an absolute constant c.

Once we have Lemma 24 we can arrive at Lemma 23 as follows. Let $A, B \subset \mathbb{C}$ be finite, and suppose that they do not satisfy one or more of the hypotheses in (42). First, we let A' and B' be such that

$$\begin{aligned} A' \subset A \qquad & B' \subset B \\ |A'| \geq |A|/4 \qquad & |B'| \geq |B|/4 \\ a \in A' \Longrightarrow -a \notin A' \qquad & b \in B' \Longrightarrow -b \notin B' \end{aligned}$$

If $|A' \cap B'| < |B'|/2$, we let

$$A'' = A', \qquad B'' = B' \setminus A'.$$

Next, if in addition $|A'' \cap (-B'')| < |B''|/2$, we let

$$A''' = A'', \qquad B''' = B'' \setminus (-A''), \qquad k''' = k, \qquad l''' = l,$$

and Lemma 24 applies with A''' in place of A, B''' in place of B, k''' in place of k, and l''' in place of l to give

$$\begin{aligned} |kA+lB| &\geq |k'''A'''+l'''B'''| \\ &\geq \binom{|A'''|}{k}\binom{|B'''|}{l} - O_{k,l,m}(|B|^{k+l-1}) \\ &\gg \frac{|A|^k|B|^l}{16^{k+l}k^kl^l} - O_{k,l,m}(|B|^{k+l-1}), \end{aligned}$$

which is better than the bound in Lemma 23.

On the other hand, if in addition $|A''\cap(-B'')|\geq |B''|/2$, we let

$$A''' = A''\cap(-B''), \qquad k''' = k+l, \qquad l''' = 0.$$

Then Lemma 24 applies with A''' in place of A, k''' in place of k, and l''' in place of l to give

$$\begin{aligned} |kA+lB| &\geq |k'''A'''| \\ &\geq \binom{|A'''|}{k+l} - O_{k,l,m}(|B|^{k+l-1}) \\ &\gg \frac{|B|^{k+l}}{16^{k+l}(k+l)^{(k+l)}} - O_{k,l,m}(|B|^{k+l-1}) \end{aligned}$$

Lastly, if $|A'\cap B'|\geq |B'|/2$ then we let

$$A'' = A'\cap B', \qquad k'' = k+l, \qquad l'' = 0.$$

Then Lemma 24 applies with A'' in place of A, k'' in place of k, and l'' in place of l to give

$$\begin{aligned} |kA+lB| &\geq |k''A''| \\ &\geq \binom{|A''|}{k+l} - O_{k,l,m}(|B|^{k+l-1}) \\ &\gg \frac{|B|^{k+l}}{8^{k+l}(k+l)^{(k+l)}} - O_{k,l,m}(|B|^{k+l-1}) \end{aligned}$$

In any of the above cases we have the bound in Lemma 23. Notice in particular that the above computations did not worsen the constant in the O term.

It remains to prove Lemma 24. To proceed, we introduce some notation. Let A_k denote the k element subsets of A and let B_l denote the l element subsets of B. That is,

$$A_k = \{S \subset A : |S| = k\} \qquad B_l = \{T \subset B : |T| = l\}.$$

Next, for each $x \in kA + lB$, let

$$S_x = \left\{ (S,T) \in A_k \times B_l : \sum_{a \in S} a + \sum_{b \in T} b = x \right\}.$$

Observe that

$$|kA + lB| \geq |A_k||B_l| - |\cup_{x \in kA+lB} E_x|, \tag{43}$$

where

$$E_x = \left\{ \Big((S,T), (S',T') \Big) \in S_x \times S_x : (S,T) \neq (S',T') \right\}.$$

Denote the union on the right side of (43) by E.

The first term in (43) has size $\binom{|A|}{k}\binom{|B|}{l}$, so we have only to estimate $|E|$. It is sufficient to prove the following bound:

$$|E| \leq ce^{(k+l)^{15(k+l)}m}|B|^{k+l-1}. \tag{44}$$

We will have use of the following definition:

Definition 25. Let M be an r by n complex matrix with at least one nonzero entry in every column. Denote the entry in the ith row and jth column of M by M_{ij}. Then for any $b \in \mathbb{C}$ we say that $a = (a_1, ..., a_n) \in \mathbb{C}^n$ is a nondegenerate solution of $Mx = b$ if it is a solution such that for each i, $1 \leq i \leq r$ there is no proper subset J of $\{j : 1 \leq j \leq n, M_{ij} \neq 0\}$ such that $\sum_{j \in J} M_{ij} a_j = 0$.

We can use Theorem 5 to show that, within a finite subset of a low-rank multiplicative subgroup of $(\mathbb{C}^*)^n$, there are not many solutions to a system of equations.

Lemma 26. *Let M be an r by n complex matrix, and let Y be a finite set contained in a subgroup of $\mathbb{C}^*$ of rank s. Then there are at most*

$$\left(\exp((6n)^{3n}(ns+1))|Y|\right)^r$$

nondegenerate solutions to $Mx = 0$ in Y^n.

Proof. Letting the component of M in the ith row and jth column be M_{ij}, we can rewrite $Mx = 0$ as

$$\sum_{j=1}^{n} M_{ij}x_j = 0, \qquad 1 \le i \le r. \tag{45}$$

Now, let $J(i) = \max\{j : M_{ij} \neq 0\}$. Then, fixing a value of $x_{J(i)}$ for each i, say $x_{J(i)} = Y_i \in Y$, we can rearrange (45) to get

$$\sum_{j=1}^{n-1} \frac{M_{ij}}{-M_{iJ(i)}Y_i} y_j = 1, \qquad 1 \le i \le r. \tag{46}$$

For each nondegenerate solution $(y_1, ..., y_n)$ of (45) with $y_{J(i)} = Y_i$ for each i, there corresponds an r-tuple $(\mathbf{z}_1, ..., \mathbf{z}_r)$ such that $\mathbf{z}_i \in Y^{n-1}$ is a nondegenerate solution of the ith equation in (46) with $(\mathbf{z}_i)_j = 0$ for all indices j such that $M_{ij} = 0$ and $(\mathbf{z}_i)_j = y_j$ otherwise. As well, this correspondence is one-to-one, so we need only count the number of such r-tuples.

However, for a fixed i, the nonzero components of $\mathbf{z}_i$ make up a nondegenerate solution of the equation

$$\sum_{\substack{1 \le j \le n-1 \\ M_{ij} \neq 0}} \frac{M_{ij}}{-M_{iJ(i)}Y_i} x_j = 1.$$

Now Theorem 5 applies, and we see that for a fixed i there are at most $e^{(6n)^{3n}(ns+1)}$ possibilities for $\mathbf{z}_i$. Hence the number of r-tuples $(\mathbf{z}_1, ..., \mathbf{z}_r)$ is this value raised to the rth power. Since there are $|Y|$ choices for Y_i, $i = 1, ..., r$, this gives the result of the lemma. □

To prove (44), we would like to use the above lemma to count elements of E. To do so, we will first demonstrate a low-multiplicity correspondence between E and nondegenerate solutions of $Mx = 0$ for a small number of matrices M. Such will be the content of the next lemma.

Lemma 27. *Let $A, B \subset \mathbb{C} \setminus \{0\}$ satisfy the hypotheses of Lemma 24. Let $\mathcal{M}$ be the set of matrices with $r \le k + l - 1$ rows and $2k + 2l$ columns and with each column containing exactly one nonzero entry, which is one of the values $0, \pm 1$. Lastly, let*

$$Z = \left\{x \in (A \cup B)^{2k+2l} : \begin{array}{l} x \text{ is a nondegenerate solution of } Mx = 0 \\ \text{for some } \ M \in \mathcal{M} \end{array}\right\}.$$

Then with E as in (43) we have

$$|E| \le (2k)!(2l)!|Z|.$$

Proof. By definition of E, for each element $\Big((S,T),(S',T')\Big)$ of E we have

$$\sum_{a\in S} a + \sum_{b\in T} b = \sum_{a'\in S'} a' + \sum_{b'\in T'} b'.$$

Choose any ordering of the elements of each of the sets S, S', T, T', say $S = \{c_1, ...c_k\}$, $S' = \{c_{k+1}, ..., c_{2k}\}$, $T = \{c_{2k+1}, ..., c_{2k+l}\}$, and $T' = \{c_{2k+l+1}, ..., c_{2k+2l}\}$. This gives a one-to-one correspondence between E and a subset of the solutions in $(A \cup B)^{2k+2l}$ of the equation

$$x_1 + ... + x_k - x_{k+1} - ... - x_{2k} + x_{2k+1} + ... + x_{2k+l} - x_{2k+l+1} - ... - x_{2k+2l} = 0. \quad (47)$$

Let d_i denote the ith coefficient in the expression (47); then for $1 \le i \le k$ and $2k+1 \le i \le 2k+l$ we have $d_i = 1$, whereas for $k+1 \le i \le 2k$ and $2k+l+1 \le i \le 2k+2l$ we have $d_i = -1$.

Now, there is a partition of $\{1, 2, ..., 2k+2l\}$ into sets $J_1, ..., J_r$ such that

$$\sum_{j\in J_t} d_j c_j = 0, \qquad 1 \le t \le r \quad (48)$$

and

$$\sum_{j\in J'_t} d_j c_j \ne 0, \qquad 1 \le t \le r$$

for each proper subset $J'_t \subset J_t$ with $J'_t \ne \emptyset$.

Let M be the matrix of the system (48) (so the entry in row t and column j is d_j if $j \in J_t$ and is 0 otherwise). Then $(c_1, ..., c_{2k+2l})$ is a nondegenerate solution of the system $Mx = 0$.

Recalling that $0 \notin A \cup B$, we see that each of the equations in (48) has at least two terms on the left. Furthermore, applying (42) and the condition that $(S,T) \ne (S',T')$ one equation must have at least three. It follows that M has at most $k+l-1$ rows, and hence $(c_1, ..., c_{2k+2l}) \in Z$. The desired correspondence therefore takes $\Big((S,T),(S',T')\Big)$ to the constructed value of $(c_1, ..., c_{2k+2l})$.

It remains only to show that this correspondence above has low multiplicity. But any particular $(2k+2l)$-tuple $(c'_1, ..., c'_{2k+2l}) \in Z$ is mapped to from at most $(2k)!(2l)!$ elements of E, one for each possible rearrangement of the components $c'_1, ..., c'_{2k+2l}$. This gives the result. □

Now, applying Lemmas 26 and 27 to sets A and B satisfying the hypotheses of Lemma 24, we find that

$$|E| \le (2k)!(2l)! \left(2\exp\left((12(k+l))^{6(k+l)}((2k+2l)(m+1)+1)\right)|B|\right)^{k+l-1} |\mathcal{M}|. \quad (49)$$

But we certainly have

$$|\mathcal{M}| \leq 3^{(2k+2l)^2}, \tag{50}$$

since each element of $\mathcal{M}$ is a matrix with three possible values for each entry and with fewer than $2k+2l$ rows and $2k+2l$ columns. Combining (49) and (50) and absorbing extraneous factors into a single dominating constant, we have (44), and Lemma 24 follows. □

Now, let $A, B \subset \mathbb{C}$ be finite, with $|B| = C|A|$, and suppose that $|AB| < \alpha|A|$. Fix integers k and l, and assume that

$$\alpha \ll \log |A|.$$

By Lemma 23, there are absolute constants c_1 and c_2 such that we have

$$|kA + lB| \geq \frac{c_1|A|^k|B|^l}{(k+l)^{4(k+l)}} - c_2 e^{(k+l)^{15(k+l)}m}|B|^{k+l-1} \tag{51}$$

where $m = \max(\dim_\times(A), \dim_\times(B))$. By Proposition 22 we have

$$m < 4\alpha.$$

Substituting this into (51), we have proved Theorem 4.

Acknowledgements. I would like to thank József Solymosi for pointing out and providing the reference [7] and for his suggestions for improving the argument, and Izabella Łaba for her constant support throughout the production of this work. I would also like to thank Mariah Hamel for her help, and Boris Bukh for his suggestions.

References

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

[2] M.-C. Chang. Erdös-Szemerédi problem on sum set and product set. *Annals of Math.*, 157:939–957, 2003.

[3] M.-C. Chang. On sums and products of distinct numbers. *J. Combin. Theory Ser. A*, 105(2):349–354, 2004.

[4] M.-C. Chang. Sum and product of different sets. *Contrib. Discrete Math.*, 1(1):47–56, 2006.

[5] Gy. Elekes. On the number of sums and products. *Acta. Arith.*, 81:365–367, 1997.

[6] P. Erdös and E. Szemerédi. On sums and products of integers. In *Studies in Pure Mathematics*, pages 213–218. Birkhauser, Switzerland, 1983.

[7] J.-H. Evertse, H.P. Schlickewei, and W.M. Schmidt. Linear equations in variables which lie in a multiplicative group. *Annals of Math.*, 155(3):807–836, 2002.

[8] K. Ford. Sums and products from a finite set of real numbers. *Ramanujan J.*, 2:59–66, 1998.

[9] M.B. Nathanson. On sums and products of integers. *Proc. Amer. Math. Soc.*, 125:9–16, 1997.

[10] I. Z. Ruzsa. Sum of sets in several dimensions. *Combinatorica*, 14(4):485–490, 1994.

[11] I. Z. Ruzsa. Sums of finite sets. In *Number Theory (New York, 1991-1995)*. Springer-Verlag, New York, 1996.

[12] J. Solymosi. An upper bound on the multiplicative energy. *Preprint*.

[13] J. Solymosi. On the number of sums and products. *Bull. London Math. Soc.*, 37(4):491–494, 2005.

[14] T. Tao. The sum-product phenomenon in arbitrary rings. *Contrib. Discrete Math.*, to appear.

[15] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, Cambridge, UK, 2006.