h-fold sums from a set with few products

Dedicated to the memory of György Elekes

Ernie Croot
Derrick Hart

January 7, 2010

1 Introduction

Before we state our main theorems, we begin with some notation: given a finite subset A of some commutative ring, we let $A+A$ denote the set of sums $a+b$, where $a,b \in A$; and, we let $A.A$ denote the set of products ab, $a,b \in A$. When three or more sums or products are used, we let kA denote the k-fold sumset $A+A+\cdots+A$, and let $A^{(k)}$ denote the k-fold product set $A.A...A$. Lastly, by $d*A$ we mean the set A dilated by the scalar d, which is just the set da, $a \in A$.

The theory of sum-product inequalities has an interesting history, and began with the theorem of Erdős and Szemerédi [11], which says that for some $\varepsilon > 0$ and $n > n_0(\varepsilon)$, we have that for any set A of n real numbers, either the sumset $A+A$ or the product set $A.A$ has at least $n^{1+\varepsilon}$ elements. Further improvements to this result were achieved by Nathanson [17], Ford [12], Elekes [8], and finally Solymosi [19] and [20].

Another type of theorem that one can prove regarding sums and products is to assume that either the sumset $A+A$ is near to being as small as possible (near to n), and then to show that $A.A$ must be near to n^2; or, one can suppose that the product set $A.A$ is small, and show that the sumset $A+A$ is large. Furthermore, one can consider k-fold sums and products here. Some quite interesting results along these lines were produced by Chang [5], [6], Elekes-Ruzsa [10], Elekes-Nathanson-Ruzsa [9], and Jones-Rudnev [16].

There are also some related analogues in finite fields similar to these just mentioned. For example, [3], [13], [14], [15] and [21].

Continuing with the characteristic 0 case, Chang and Bourgain proved the following results on k-fold sums and products: Chang [4] showed that if A is a set of n integers, and $|A.A| < n^{1+\varepsilon}$, then the sumset $|kA| \gg_{\varepsilon,k} n^{k-\delta}$, where $\delta \to 0$ as $\varepsilon \to 0$. And then Chang and Bourgain [2] showed that for any $b \geq 1$, there exists $k \geq 1$ such that if A is a set of n integers,

$$|kA| \cdot |A^{(k)}| \ \gg \ n^b.$$

In both of these results, we would like to have that they hold for the real numbers (or even the complex numbers), instead of just the integers. Unfortunately, this appears to be out of reach at the moment.

The purpose of the present paper is to present some results towards this end. Specifically, we will prove the following two theorems.

Theorem 1 *For all $h \geq 2$ and $0 < \varepsilon < \varepsilon_0(h)$ we have that the following holds for all $n > n_0(h, \varepsilon)$: if A is a set of n real numbers and*

$$|A.A| \ \leq \ n^{1+\varepsilon},$$

then

$$|hA| \ \geq \ n^{\log(h/2)/2\log 2 + 1/2 - f_h(\varepsilon)},$$

where $f_h(\varepsilon) \to 0$ as $\varepsilon \to 0$.

If instead of showing that hA is large, we just want to show that $h(A.A)$ is large, we can prove a much stronger theorem:

Theorem 2 *Under the same hypotheses on A as in the theorem above, we have that*

$$|h(A.A)| \ = \ |A.A + A.A + \cdots + A.A| \ > \ n^{\Omega((h/\log h)^{1/3})}.$$

Here, and in later sections, the notation $f(x) = \Omega(g(x))$ will simply mean that $g(x) = O(f(x))$; that is, up to a constant factor, $f(x)$ grows at least as fast as $g(x)$ as $x \to \infty$.

1.1 Some remarks

While the methods in the present paper will need substantial modification to come anywhere near to proving an analogue of [4] for the real numbers, we feel that it might be possible to achieve bounds as good in Theorem 1 above as we have in Theorem 2. Although this too will require a lot of work, we feel that we have a few good ideas on how to actually achieve it.

It is also worth remarking that we have several different approaches to proving a theorem of the quality of Theorem 1. In particular, it is possible to use an iterative argument involving the Szemerédi-Trotter theorem, a Szemerédi cube lemma similar to Lemma 3 below, and some "energy arguments", to achieve similar such bounds. However, it is not as easy to see how one might go about modifying such an "incidence proof" of Theorem 1 to achieve bounds as good as in Theorem 2.

2 Preliminary lemmas and results

First, in the proofs of both theorems, we will assume that all the elements of A are positive. The reason we can assume this is that either at least $(n-1)/2$ elements of A are all positive, or at least $(n-1)/2$ are all negative. If we are in the negative case here, we just let A' be the negative of these negative elements; and otherwise, we just let A' be these $(n-1)/2$ positive elements. Then, we simply prove our theorem using A' in place of A. The effect of the lost factor of 2 will be negligible.

The proof of Theorem 2 will require the following result of Wooley [22] (see also Borwein-Erdélyi-Kós [1] for some related results).

Theorem 3 *For every $k \geq 1$, there exist two distinct sets*

$$\{x_1, ..., x_s\},\ \{y_1, ..., y_s\}\ \subseteq\ \mathbb{Z}$$

of

$$s\ <\ (k^2/2)(\log k + \log\log k + O(1))$$

(when $k = 1$ we just delete the $\log\log k$ *term) distinct integers in each, such that*

$$\sum_{i=1}^{s} x_i^j\ =\ \sum_{i=1}^{s} y_i^j,\ \text{for all } j = 1, ..., k,$$

but that

$$\sum_{i=1}^{s} x_i^{k+1} \neq \sum_{i=1}^{s} y_i^{k+1}.$$

For the purposes of our paper, we actually require the following corollary of this theorem.

Corollary 1 *For all integers $j \geq 1$, there exists a monic polynomial $f(x)$, having only the coefficients $0, 1,$ and -1, having at most*

$$j^2(\log j + \log\log j + O(1))$$

(again, if $j = 1$ we just delete the $\log\log j$ term) non-zero terms, such that $f(x)$ vanishes at $x = 1$ to order j, but not to order $j+1$.

Since the number of terms of this polynomial depends only on j, it follows that if one performs a Taylor expansion of this polynomial about $x = 1$, one will find that

$$f(x) \ = \ \sum_{i=j}^{d} c_i(x-1)^i, \ d = \deg(f),$$

where $c_j \neq 0$, and each c_i in turn is either 0 or its absolute value can be bounded from below by some function of j alone (the degree d depends on j).

Proof of the Corollary. Basically, we just use the well-known fact that a polynomial

$$f(x) \ = \ \sum_{i=1}^{s} x^{x_i} \ - \sum_{i=1}^{s} x^{y_i}.$$

vanishes to order j at $x = 1$ if and only if f and its first $j-1$ derivatives vanish at $x = 1$, where the ℓth derivative evaluated at 1 looks like

$$\sum_{i=1}^{s} x_i(x_i - 1)\cdots(x_i - \ell + 1) \ - \ \sum_{i=1}^{s} y_i(y_i - 1)\cdots(y_i - \ell + 1).$$

Clearly, having all these be 0, for $\ell = 0, 1, ..., j-1$, is equivalent to having a solution to the "Tarry-Escott Problem" considered by Wooley in Theorem 3 above.

One small remaining point to consider is the fact that some of the x_i's and y_i's could be negative (meaning that the f above is a Laurent polynomial, not a polynomial). That is easily fixed by multiplying f by an appropriate power of x, which does not affect the vanishing properties at $x = 1$.

The fact that the non-zero coefficients among $|c_j|, ..., |c_d|$ can be bounded from below by a function of j follows from the fact that the degree d of the polynomial is a function of j, along with the fact that for $i = j, ..., d$ we have that if $c_i \neq 0$, then

$$|c_i| \ = \ |f^{(i)}(1)/i!| \ \geq \ 1/i! \ \geq \ 1/d!.$$

■

Another major theorem that we will require is the Ruzsa-Plunnecke inequality [18].

Theorem 4 *Suppose that A is a finite subset of an additive abelian group. Then, if*

$$|A + A| \ \leq \ K|A|,$$

we will have that for all integers $k, \ell \geq 1$,

$$|kA - \ell A| \ = \ |A + A + \cdots + A - A - \cdots - A| \ \leq \ K^{k+\ell}|A|.$$

We will also require the following basic lemmas.

Lemma 1 *Suppose that A is a set of m^2 positive real numbers, say they are*

$$0 \ < \ a_1 \ < \ \cdots \ < \ a_{m^2},$$

such that no dyadic interval $[x, 2x]$ contains m or more of the a_j's. Then, for all integers $k \geq 1$,

$$|kA| \ \gg_k \ m^k.$$

Proof of the lemma. Let

$$B \ := \ \{a_1, a_{2m+1}, a_{4m+1}, ..., a_{m^2-m+1}\}.$$

We claim that all the sums

$$b_1 + \cdots + b_k, \ b_i \in B, \ b_1 \leq \cdots \leq b_k,$$

are distinct, which would prove the lemma.

To see this, suppose we had

$$b_1 + \cdots + b_k \ = \ b'_1 + \cdots + b'_k,$$

and suppose without loss that $b_k \leq b'_k$. If $b_k < b'_k$, then $b_k < b'_k/2$, and we have

$$b'_k \ = \ b_1 + \cdots + b_k - b'_1 - \cdots - b'_{k-1} \ \leq \ b_1 + \cdots + b_k \ < \ 2b_k \ < \ b'_k,$$

a contradiction. So, we can delete b_k and b'_k from both sides; and then, repeating the argument, we get $b_i = b'_i$, $i = 1, 2, ..., k$, and we are done. ■

The following lemma is basically a generalization of a result in [7].

Lemma 2 *For all integers $r, \ell \geq 1$, and for real numbers $0 < c_1 < c_1(r, \ell)$, $0 \leq c_2 < c_2(r, \ell, c_1)$ and $0 < \varepsilon < \varepsilon(r, \ell, c_1, c_2)$, the following holds for all n sufficiently large: Suppose A is a set of n real numbers satisfying*

$$|A.A| \ < \ n^{1+\varepsilon},$$

and suppose that

$$A' \ \subseteq \ A, \ B \ \subseteq \ A^{(r)}/A^{(r)},$$

satisfy

$$|B| \ > \ n^{c_1}, \text{ and } |A'| \ > \ n^{1-c_2}.$$

Then, there are

$$n^{2-O(c_2\ell + r\ell^2\varepsilon)} \text{ pairs } (a_1, a_2) \in A' \times A',$$

such that if we let

$$x \ = \ a_1 a_2,$$

then there exist

$$n^{-O(c_2\ell + r\ell^2\varepsilon)}|B|^2$$

pairs

$$(b_1, b_2) \ \in \ B \times B, \ b_1 > b_2,$$

such that if we let

$$d \ = \ b_1/b_2,$$

then

$$x, \ dx, \ d^2x, \ ..., \ d^\ell x \ \in \ A'.A'.$$

Proof of the lemma. First, note that

$$|A'.A'| \ \le\ |A/A|\ <\ n^{1+\varepsilon}.$$

This implies that there exists $t_1, t_2 \in A'$ such that there are at least

$$n^2/n^{1+\varepsilon}\ =\ n^{1-\varepsilon}$$

solutions $(t_1', t_2') \in A' \times A'$ to the equation

$$t_1 t_2\ =\ t_1' t_2'.$$

Put another way, we have $t_1'/t_1 = t_2/t_2'$ for lots of pairs $(t_1', t_2') \in A' \times A'$. Note that since each solution to this equation corresponds to an element of $(A'/t_1) \cap (t_2/A')$, it follows that there exists $t_1, t_2 \in A'$ such that if we let

$$A''\ :=\ (A'/t_1) \cap (t_2/A'),$$

then $|A''| > n^{1-\varepsilon}$. By ensuring that $0 < \varepsilon < c_2$ (which we are allowed to assume, because the range for ε depends on c_2) we will have

$$|A''|\ >\ n^{1-\varepsilon}\ >\ n^{1-c_2}.$$

Of course, this means that if we let $t = t_1 t_2$ then

$$A'''\ :=\ A' \cap (t/A') \text{ satisfies } |A'''|\ =\ |A''|\ >\ n^{1-c_2}.$$

Note that

$$A'''/A'''\ \subseteq\ t^{-1} * (A'.A').$$

What we will show is that for lots of pairs

$$(e_1, e_2)\ \in\ A''' \times A''',\ \text{and } y = e_1/e_2,$$

the set A'''/A''' contains "lots" of progressions

$$y,\ dy,\ d^2y, ...,\ d^\ell y,\ \text{where } d \in B/B. \tag{1}$$

If we can do this, then

$$x,\ dx,\ d^2x,\ ...,\ d^\ell x\ \in\ A'.A',\ \text{where } x = ty.$$

Showing that A'''/A''' contains such a progression as in (1) amounts to showing that the following system has non-trivial solutions:

$$\frac{b_1}{b_2}\frac{e_1}{e_2} \ = \ \frac{e_3}{e_4},\ \frac{b_1^2}{b_2^2}\frac{e_1}{e_2} \ = \ \frac{e_5}{e_6},\ ...,\ \frac{b_1^\ell}{b_2^\ell}\frac{e_1}{e_2} \ = \ \frac{e_{2\ell+1}}{e_{2\ell+2}}. \tag{2}$$

Note that $d = b_1/b_2 \in B/B$ and the e_i should all belong to A''', making

$$e_1/e_2,\ e_3/e_4,\ e_5/e_6,\ ...,\ e_{2\ell+1}/e_{2\ell+2} \ \in \ A'''/A''',$$

as we require.

Another way to write (2) is as

$$\begin{array}{rcl} b_1e_1e_4 & = & b_2e_2e_3 \\ b_1^2e_1e_6 & = & b_2^2e_2e_5 \\ & \vdots & \\ b_1^\ell e_1e_{2\ell+2} & = & b_2^\ell e_2e_{2\ell+1}. \end{array} \tag{3}$$

Note that since $b_i \in B \subseteq A^{(r)}/A^{(r)}$ and since $e_i \in A''' \subseteq A'$, both sides of each equation of (3) belongs to

$$(A^{(r\ell)}/A^{(r\ell)})(A')^{(2)} \ \subseteq \ A^{(r\ell+2)}/A^{(r\ell)},$$

which has at most

$$n^{1+O(r\ell\varepsilon)}$$

elements, by Ruzsa-Plünnecke.

We now will count solutions to (3) by defining a certain mapping: Let $X := (A''')^{\ell+1} \times B$, and $Y := (B^{(\ell)}(A''')^{(2)})^\ell$, and define the mapping

$$\begin{array}{rcl} \varphi \ : \ X & \rightarrow & Y \\ (e_1,\ e_4,\ e_6,\ e_8,\ ...,\ e_{2\ell+2},\ b_1) & \rightarrow & (b_1e_1e_4,\ b_2^2e_1e_6,\ ...,\ b_1^\ell e_1e_{2\ell+2}), \end{array}$$

Every pair of vectors $v, w \in X$ such that

$$\varphi(v) \ = \ \varphi(w) \tag{4}$$

corresponds to a ('collision') solution to (3).

The total number of solutions to (4), and therefore also to (3), is given by

$$\sum_{z \in Y} |\varphi^{-1}(z)|^2.$$

By Cauchy-Schwarz, this is at least

$$\left(\sum_{z \in Y} |\varphi^{-1}(z)| \right)^2 / |Y| \ = \ |X|^2/|Y|.$$

To bound this from below, we note that

$$|X| \ \geq \ n^{\ell+1-O(\ell c_2)} |B|,$$

and

$$|Y| \ \leq \ (n^{1+O(r\ell\varepsilon)})^\ell \ = \ n^{\ell+O(r\ell^2\varepsilon)}.$$

So, the number of solutions in the b_i's and e_i's to the system (3) is

$$\geq \ |X|^2/|Y| \ > \ n^{\ell+2-O(\ell c_2 + r\ell^2\varepsilon)} |B|^2. \qquad (5)$$

On average, then, a tuple

$$(e_4, e_6, ..., e_{2\ell+2}) \ \in \ (A''')^\ell, \qquad (6)$$

has at least

$$n^{2-O(\ell c_2 + r\ell^2\varepsilon)} |B|^2$$

corresponding four-tuples

$$(e_1, e_2, b_1, b_2) \ \in \ A''' \times A''' \times B \times B,$$

such that the system (3) has a solution (which must be unique, since the remaining e_i's are determined exactly). Clearly this proves the lemma upon choosing the tuple (6) producing the greatest number of four-tuples. Note that having $b_1 > b_2$ can be guaranteed simply by taking reciprocals in (2). ■

And now we state two more general-purpose lemmas, the first of which is perhaps better known as the "Szemeredi cube lemma", and is used in the proof of Theorem 1 only, while the other lemma is used in the proofs of both theorems.

Lemma 3 *The following holds for all $k \geq 2$, $0 < c < c_0(k)$, $0 < \varepsilon < \varepsilon_0(k, c)$ and $n > n_0(k, c, \varepsilon)$: suppose that A is a set of n real numbers such that*

$$|A.A| \ < \ n^{1+\varepsilon},$$

and suppose that $B \subseteq A$ satisfies

$$|B| \ \geq \ n^c.$$

Then, there exists

$$\theta_1, \ ..., \ \theta_k \ \in \ B/B, \ \text{each } \theta_i > 1,$$

such that for at least

$$n^{1-O_k(c)}$$

values $d \in A$ we have that all the numbers

$$\theta_1^{\gamma_1} \cdots \theta_k^{\gamma_i} d, \ \text{where each } \gamma_i \ \in \ \{0, 1\},$$

belong to A. (Note that for each such d, this means that 2^k different elements belong to the set A.)

Proof of the lemma. The proof is inductive: we will construct

$$D_0 \ := \ A, \ D_1, \ ..., \ D_k \ \subseteq \ A,$$

such that

$$D_i \ = \ D_{i-1} \cap (\theta_i^{-1} * D_{i-1}), \ i = 1, 2, ..., k,$$

where $\theta_i \in B/B$, $\theta_i > 1$, is chosen greedily to maximize D_i, given D_{i-1}.

Suppose that we have already shown that

$$|D_{i-1}| \ = \ n^{1-O_k(c)}.$$

Then, consider the product set

$$BD_{i-1} \ = \ \{bd \ : \ b \in B, \ d \in D_{i-1}\} \ \subseteq \ A.A.$$

Since $|A.A| < n^{1+\varepsilon}$, we have that

$$|BD_{i-1}| \ \leq \ n^{1+\varepsilon},$$

and therefore we easily see that there exist

$$s, t \in B,\ \ s/t \neq \theta_1, ..., \theta_{i-1},$$

such that

$$|(s * D_{i-1}) \cap (t * D_{i-1})|\ >\ n^{1-O_k(c)},$$

for $\varepsilon > 0$ sufficiently small in terms of k, c.

So, letting $\theta_i = s/t > 1$, we are done, because

$$|D_{i-1} \cap (\theta_i^{-1} * D_{i-1})|\ =\ |(s * D_{i-1}) \cap (t * D_{i-1})|\ >\ n^{1-O_k(c)},$$

as claimed. ■

Lemma 4 *Suppose that C is a set of real numbers, and*

$$1\ =\ \delta_0\ >\ \delta_1\ >\ \delta_2\ >\ \cdots\ >\ \delta_{k-1}\ >\ 0$$

are positive real numbers such that if we define the ratios

$$\alpha_i\ :=\ \delta_i/\delta_{i-1},\ \ i = 1, 2, ..., k-1,$$

then for all pairs

$$c, d\ \in\ C,\ \ c > d,$$

we have

$$c/d - 1\ >\ 2k\alpha_1,\ ...,\ 2k\alpha_{k-1}.$$

Next, partition C into any disjoint sets

$$C\ =\ C_1\ \cup\ C_2\ \cdots\ \cup\ C_k,$$

where for $i < j$ we have that every element of C_i is greater than every element of C_j. Let us express this as

$$C_i\ >\ C_j,\ \text{for } i < j.$$

Then, we have that all sums

$$c_1 + c_2\delta_1 + \cdots + c_k\delta_{k-1},\ \ c_1 \in C_1, ..., c_k \in C_k,$$

are distinct.

Proof of the lemma. Suppose that, on the contrary, two of these sums are equal. Then, it would mean that

$$c_1 + c_2\delta_1 + \cdots + c_k\delta_{k-1} \ = \ c'_1 + c'_2\delta_1 + \cdots + c'_k\delta_{k-1}. \tag{7}$$

Suppose without loss that $c_1 \geq c'_1$. Now let us suppose that, in fact, $c_1 > c'_1$. Then, we have that

$$c_1/c'_1 - 1 \ = \ \sum_{i=2}^{k}(c'_i/c'_1 - c_i/c'_1)\delta_{i-1}.$$

From the fact that $C_1 > C_2, ..., C_k$, we have that the right-hand-side here is bounded from above in absolute value by

$$\sum_{i=2}^{k} 2\delta_{i-1} \ \leq \ 2k\delta_1 \ \leq \ 2k\alpha_2 \ < \ c_1/c'_1 - 1,$$

which is impossible. We conclude that $c_1 = c'_1$.

Now suppose for proof by induction we have shown that

$$c_i = c'_i, \ i = 1, 2, 3, ..., j, \text{ where } j \leq k - 1.$$

We now show that

$$c_{j+1} \ = \ c'_{j+1},$$

which would clearly prove the lemma.

We begin by deleting the terms $c_i\delta_{i-1}$ and $c'_i\delta_{i-1}$ from both sides of (7), for $i = 1, 2, ..., j$. So, we are left with

$$\sum_{i=j+1}^{k} c_i\delta_{i-1} \ = \ \sum_{i=j+1}^{k} c'_i\delta_{i-1},$$

which can be rewritten as

$$(c_{j+1}/c'_{j+1} - 1) \ = \ \sum_{i=j+2}^{k} (c'_i/c'_{j+1} - c_i/c'_{j+1})\delta'_{i-1}, \tag{8}$$

where

$$\delta'_i \ := \ \delta_i/\delta_j \ \leq \ \alpha_i, \ i = j + 1, ..., k - 1.$$

We assume without loss that $c_{j+1} \geq c'_{j+1}$. If, in fact, $c_{j+1} > c'_{j+1}$, then the absolute value of the right-hand-side of (8) is clearly bounded from above by

$$2k\alpha_{j+1} \ < \ c_{j+1}/c'_{j+1} - 1,$$

which is a contradiction. We conclude that $c_{j+1} = c'_{j+1}$, and therefore the induction step is proved, as is the lemma. ■

3 Proof of Theorem 1

We suppose that the elements of A are

$$a_1 \ < \ a_2 \ < \ \cdots \ < \ a_n,$$

which we assume are all positive by the remarks at the beginning of section 2.

Let $0 < \delta < 1/2$ be some parameter that we will choose as small as needed later, and let $k \geq 2$ be some parameter that we will let depend on h later. Let

$$s \ := \ \lfloor n^\delta \rfloor,$$

and set

$$B \ := \ \{a_j, a_{j+1}, ..., a_{j+s}\},$$

where j is chosen so that

$$a_{j+s}/a_j \text{ is minimal.} \tag{9}$$

We may assume that B lies in some interval

$$B \ \subseteq \ [x, 2x],$$

since otherwise no consecutive block of $s+1$ elements of A lies in an interval of this form; and therefore, by Lemma 1, we could conclude that

$$|kA| \ \geq \ n^{k/2},$$

which would prove our theorem.

Having B lie in a dyadic interval implies that all ratios $\theta = b_2/b_1$, $b_1, b_2 \in B$, $b_1 < b_2$, satisfy

$$\theta - 1 \ \in \ [0, 1).$$

Next, let $c = \delta$ and apply Lemma 3. Let $\theta_1, ..., \theta_{k-1} \in B/B$ denote the numbers that result from this lemma (using $k-1$ in place of k). Let C_0 denote the set of all $n^{1-O_k(\delta)}$ elements $d \in A$ that the lemma produces, and write

$$C_0 \ := \ \{c_1, ..., c_{n'}\}, \ c_1 < c_2 < \cdots < c_{n'}, \ n' \ > \ n^{1-O_k(\delta)}.$$

Then, let

$$C \ := \ \{c_1, c_{1+sk2^k}, c_{1+2sk2^k}, c_{1+3sk2^k}, \ ..., c_{1+\lfloor (n'-1)/sk2^k \rfloor sk2^k}\}$$

be the set of every $sk2^k$th element of C_0. Note that since the elements $\theta_i \in B/B$, and B satisfies (9), we have that

$$\theta_j^{2k} \ < \ c_2/c_1, \ c_1, c_2 \in C, \ c_2 > c_1,$$

and therefore

$$2k(\theta_j - 1) \ < \ \theta_j^{2k} - 1 \ < \ c_2/c_1 - 1.$$

It follows that if we let

$$\delta_i \ := \ (\theta_1 - 1)(\theta_2 - 1)\cdots(\theta_i - 1), \ i = 1, 2, ..., k-1,$$

then we have for $i = 1, 2, ..., k-2$ that

$$\delta_{i+1}/\delta_i \ = \ \theta_{i+1} - 1 \ < \ (c_2/c_1 - 1)/2k.$$

We almost are ready to apply Lemma 4 – all we have to do is partition C, which we do simply by letting

$$C \ = \ C_1 \cup \cdots \cup C_k,$$

where C_1 consists of the largest $\lfloor |C|/k \rfloor$ elements of C, C_2 consists of the next largest $\lfloor |C|/k \rfloor$ elements of C, and so on.

Lemma 4 now tells us that all the sums

$$c_1 + c_2\delta_1 + \cdots + c_k\delta_{k-1}, \ c_i \in C_i, \tag{10}$$

are distinct. This then results in

$$\gg \ (|C|/k)^k \ \gg_k \ n^{k(1-O_k(\delta))}.$$

distinct sums.

These sums, in turn, can be re-written as just sums and differences of elements from A as follows: by expressing the δ_{i-1} back in terms of the θ_j's, we find that

$$c_i\delta_{i-1} \ = \ c_i(\theta_1 - 1)\cdots(\theta_{i-1} - 1) \ = \ (-1)^{i-1}c_i + (-1)^{i-2}\theta_1 c_i + \cdots$$

Each term here looks like

$$\pm c_i\theta_1^{\gamma_1}\cdots\theta_{i-1}^{\gamma_{i-1}}, \text{ where } \gamma_j \in \{0,1\},$$

and we know from our use of Lemma 3 that all such numbers belong to $\pm A$.

It is easy to see, then, that all the sums (10) can be re-expressed as elements of $KA - LA$, where

$$K, L \ < \ 2^{k-2} + 2^{k-3} + \cdots + 1 \ < \ 2^{k-1}.$$

So,

$$|2^{k-1}A|^2 \ > \ |KA|\cdot|LA| \ \geq \ |KA - LA| \ > \ n^{k(1-O_k(\delta))},$$

from which it follows that upon letting $h = 2^{k-1}$,

$$|hA| \ \geq \ n^{\log(h)/2\log 2 + 1/2 - g_h(\delta)},$$

where $g_h(\delta) \to 0$ as $\delta \to 0$. Of course, this only works for when h is a power of 2; by bounding general h between two consecutive powers of 2, we can conclude that

$$|hA| \ \geq \ n^{\log(h/2)/2\log 2 + 1/2 - g_h(\delta)}.$$

This completes the proof of our theorem, by choosing $\delta > 0$ small enough, and then choosing $\varepsilon > 0$ even smaller as appropriate for Lemma 3.

4 Proof of Theorem 2

Write out the elements of A in incresing order as

$$a_1 \ < \ a_2 \ < \ \cdots \ < \ a_n,$$

which we assume are all positive by the remarks at the beginning of section 2.

Let $\delta > 0$ be some parameter that we will choose later as function of h alone, and let s and B be as in the beginning of the proof of Theorem 1. In fact, we may assume that

$$B \ \subseteq\ [x, (1 + 1/\gamma(h))x],$$

for any function $\gamma(h) > 0$ we please. The reason is that if this minimal set B exceeds this interval, and if a_j is the smallest element of B, then

$$[a_j,\ a_{j+Ls}] \ \supseteq\ [x, (1+\gamma(h))^L x] \ \supseteq\ [x, 2x],$$

for L large enough. And so, we may again deduce (as in the proof of Theorem 1), using Lemma 1, that

$$|hA| \ \gg\ n^{\Omega(h^{1/2})},$$

which would prove our theorem.

As in the proof of Theorem 1, we may assume that the elements of B lie in some dyadic interval $[x, 2x]$, upon applying Lemma 1.

Let $k \geq 2$ be some parameter that is to depend on h, that we will choose later.

We now apply Lemma 2 using $\ell = M$, $r = 1$, $c_1 = \delta$, $A' = A$ (so $c_2 = 0$) and $\varepsilon > 0$ as small as needed in terms of M and δ, where the precise value of M will be determined below, and will depend only on h. So, there exists

$$\theta \ \in\ B/B,\ \theta \ >\ 1,$$

such that for at least

$$|A|^{2-O(\ell^2\delta)}$$

pairs

$$(a_1, a_2) \ \in\ A,$$

we have that if we let $y = a_1 a_2$, then

$$y,\ y\theta,\ ...,\ y\theta^\ell \ \in\ A.A. \tag{11}$$

So, there exists $a_1 \in A$ and $\theta \in B/B$, $\theta > 1$, such that there are

$$|A|^{1-O(\ell^2\delta)} \tag{12}$$

values $a_2 \in A$ such that for $y = a_1 a_2$ we have that (11) holds.

If we let the special elements $a_2 \in A$ be

$$\{a_{q_1}, ..., a_{q_{n'}}\},\ n' > n^{1-O(\ell^2\delta)},$$

then we define

$$C\ :=\ \{a_{q_1}, a_{q_{\lfloor\sqrt{n}\rfloor+1}}, a_{q_{2\lfloor\sqrt{n}\rfloor+1}}, ..., a_{\lfloor(n'-1)/\lfloor\sqrt{n}\rfloor\rfloor\cdot\lfloor\sqrt{n}\rfloor+1}\}\ \subseteq\ \{a_{q_1}, ..., a_{q_{n'}}\}. \quad (13)$$

Note that C is basically a "well-separated" subset of those special elements $a_2 \in A$; and, in fact, if $\delta < 1/2$, so that $s < n^{1/2}$, they are so well-separated that that all ratios c_2/c_1, $c_1, c_2 \in C$, $c_2 > c_1$, have the property that

$$c_2/c_1\ >\ \theta. \quad (14)$$

Now we apply Corollary 1, letting

$$f_j(x),\ j = 1, 2..., k-1$$

be polynomials having at most $j^2(\log j + \log\log j + O(1))$, $j = 1, ..., k-1$, terms each, each with coefficients only $0, 1$, or -1, that vanish at $x = 1$ to the orders $1, 2, 3, ..., k-1$, respectively. Then we let

$$M\ =\ \max(\deg(f_1), ..., \deg(f_{k-1})),$$

which is a parameter that came up earlier in the proof of the present theorem (Theorem 2). Note that M does not depend on n – it depends on k, and therefore on h.

Next, we set

$$\delta_i\ :=\ f_i(\theta),\ i = 1, 2, ..., k-1.$$

Since $f_{i+1}(x)/f_i(x)$ vanishes at $x = 1$ to order 1, and since $\theta \in B/B$ and $\theta \in [1, 2)$, we have that if we set

$$\alpha_i\ :=\ \delta_i/\delta_{i-1},\ i = 2, 3, ..., k-1,$$

then for every $c_1, c_2 \in C$, $c_2 > c_1$, we have from (14) that

$$c_2/c_1 - 1\ >\ \theta - 1\ \gg_k\ \alpha_i\ >\ 0.$$

(Note that the implied constant here depends on the sizes of the coefficients c_i in Corollary 1, and we know that these coefficients are rational numbers that depend on k.) But, in fact, if $\delta > 0$ is small enough, then for $c_1, c_2 \in C$, $c_2 > c_1$, we can assume that for any function $\gamma(k)$ of k,

$$\theta^{\gamma(k)} \ < \ c_2/c_1;$$

and so, we may assume

$$c_2/c_1 - 1 \ > \ 2k\alpha_i \ > \ 0.$$

So, if we let C_1 be the largest $\lfloor |C|/k \rfloor$ elements of C, C_2 be the second largest $\lfloor |C|/k \rfloor$ elements of C, and so on, down to C_k, then upon applying Lemma 4, we have that all sums

$$a_1 + a_2 f_1(\theta) + \cdots + a_k f_k(\theta), \ a_i \in C_i, \tag{15}$$

are distinct. Since each C_i satisfies

$$|C_i| \ \gg_k \ n^{1/3},$$

for $\delta > 0$ small enough (and $\varepsilon > 0$ small enough in terms of δ and h), we deduce that this produces $n^{\Omega(k)}$ distinct sums. Now, because

$$a_i, a_i\theta, \ ..., \ a_i\theta^M \ \in \ A.A,$$

by design, we have that upon expanding out these polynomials f_i in (15) into powers of θ, we find that these $n^{\Omega(k)}$ sums are, in fact, elements of $KA - LA$, where

$$K, L \ \leq \ (1^2 + 2^2 + \cdots + (k-1)^2/2)(\log k + \log\log k + O(1)) \ \ll \ k^3 \log k.$$

It follows that

$$|(ck^3 \log k)(A.A)|^2 \ \geq \ |K(A.A) - L(A.A)| \ \geq \ n^{\Omega(k)}.$$

This clearly proves the theorem upon letting $k \gg (h/\log h)^{1/3}$.

5 Acknowledgements

We would like to thank P. Borwein and T. Erdélyi for useful discussions about their paper with G. Kós listed below. We would also like to thank the referees for carefully reading the paper and offering good suggestions.

References

[1] P. Borwein, T. Erdélyi and G. Kós, *Littlewood-type problems on* $[0,1]$, Proc. London Math. Soc. **79** (1999), 22-46.

[2] J. Bourgain and M-C. Chang, *On the size of k-fold sum and product sets of integers*, J. Amer. Math. Soc. **17** (2003), 473-497.

[3] J. Bourgain, *Mordell's exponential sum estimate revisited*, J. of the Amer. Math. Soc. **18** (2005).

[4] M-C. Chang, *Erdős-Szemerédi problem on sum set and product set*, Annals of Math **157** (2003), 939-957.

[5] ———, *Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems*, Geom. and Funct. Anal. **113** (2002), 399-419.

[6] K. Chipeniuk, *Sums and products of distinct sets and distinct elements in fields of characteristic* 0, preprint on ARXIVES.

[7] E. Croot, I. Z. Ruzsa, and T. Schoen, *Arithmetic progressions in sparse sumsets*, INTEGERS **7** (2007).

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

[9] G. Elekes, M. Nathanson and I. Ruzsa, *Convexity and sumsets*, J. Number Theory **83** (2000), 194-201.

[10] G. Elekes and I. Ruzsa, *Few sums, mamy products*, Studia Sci. Math. Hungar. **40** (2003).

[11] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics; To the memory of Paul Turán. P. Erdos, L. Alpar, and G. Halasz, editors. Akademiai Kiado-Birkhauser Verlag, Budapest-Basel-Boston, Mass. 1983, 213-218.

[12] K. Ford, *Sums and products from a finite set of real numbers*, Ramanujan Jour. **2** (1998), 59-66.

[13] A. Glibichuk, *Additive properties of product sets in an arbitrary field*, preprint on ARXIVES.

[14] A. Glibichuk and S. Konyagin, *Additive properties of product sets in fields of prime order*, Centre de Recherches Mathematiques, Proceedings and Lecture Notes, 2006.

[15] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Contemp. Math. **464** (2008).

[16] T. Jones and M. Rudnev, *Solymosi's multiplicative energy bound for complex numbers*, preprint on ARXIVES.

[17] M. Nathanson, *On sums and products of integers*, Proc. Amer. Math. Soc. **125** (1997), 9-16.

[18] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97-109.

[19] J. Solymosi, *On sums-sets and product-sets of complex numbers*, J. Th. Nomb. Bordeaux **17** (2005), 921-924.

[20] ———-, *An upper bound on the multiplicative energy*, preprint.

[21] L. A. Vinh, *The solvability of norm, bilinear and quadratic equations over finite fields via specta of graphs*, preprint on the ARXIVES.

[22] T. Wooley, *Some remarks on Vinogradov's mean value theorem and Tarry's problem*, Monatsh. Math. **122** (1996), 265-273.