

On iterated product sets with shifts

**B. Hanson, O. Roche-Newton, D.
Zhelezov**

RICAM-Report 2018-18

ON ITERATED PRODUCT SETS WITH SHIFTS

BRANDON HANSON, OLIVER ROCHE-NEWTON, AND DMITRII ZHELEZOV

ABSTRACT. We prove that, for any finite set $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$ and any positive integer k , the k -fold product set of the shift $A + 1$ satisfies the bound

$$|\{(a_1 + 1)(a_2 + 1) \cdots (a_k + 1) : a_i \in A\}| \geq \frac{|A|^k}{(8k^4)^{kK}}.$$

This result is essentially optimal when K is of the order $c \log |A|$, for a sufficiently small constant $c = c(k)$.

Our main tool is a multiplicative variant of the Λ -constants used in harmonic analysis, applied to Dirichlet polynomials.

1. INTRODUCTION

Let A be a finite set of integers. The *sum set* and *product set* of A are defined respectively as

$$A + A := \{a + b : a, b \in A\}, \quad AA := \{ab : a, b \in A\}.$$

The sum-product problem is concerned with showing that one of these sets is always large. It was conjectured by Erdős and Szemerédi [7] that, for all $\epsilon > 0$ and any finite $A \subset \mathbb{Z}$,

$$\max\{|A + A|, |AA|\} \geq c(\epsilon)|A|^{2-\epsilon} \tag{1}$$

where $c(\epsilon) > 0$ is an absolute constant. The same conjecture can also be made over the reals, and indeed other fields. The Erdős–Szemerédi conjecture remains open, and it appears to be a deep problem. Konyagin and Shkredov [12] proved that (1) holds with $\epsilon < 2/3$, and the current best bound, due to Rudnev, Shkredov and Stevens [13], has $\epsilon \leq 2/3 - 1/1509 + o(1)$. These bounds hold over real numbers, and their proofs are geometric in nature.

A similar question can also be considered with more variables. The *k -fold sumset* and *k -fold product set* of $A \subset \mathbb{Z}$ are defined respectively as

$$kA := \{a_1 + \cdots + a_k : a_1, \dots, a_k \in A\}, \quad A^{(k)} := \{a_1 \cdots a_k : a_1, \dots, a_k \in A\}.$$

Erdős and Szemerédi also made the even more general conjecture that, for all $\epsilon > 0$ and any finite $A \subset \mathbb{Z}$,

$$\max\{|kA|, |A^{(k)}|\} \geq c(\epsilon)|A|^{k-\epsilon}. \tag{2}$$

Given the state of progress with the $k = 2$ version of this conjecture, it is not surprising that the more general conjecture is also wide open. However, over the rationals, a series of remarkable results concerning unlimited growth does exist. The first of these results is the following theorem of Chang [5].

Theorem 1.1. *Let $A \subset \mathbb{Q}$ be a finite set with $|AA| \leq K|A|$ and let $k \geq 2$ be an integer. Then*

$$|kA| \geq \frac{|A|^k}{(2k^2 - k)^{kK}}. \quad (3)$$

The results proved in [5] were actually somewhat more general. It was established that

$$E_k^+(A) \leq |A|^k (2k^2 - k)^{kK}, \quad (4)$$

where $E_k^+(A)$ is the k -fold additive energy, which is defined as the quantity

$$E_k^+(A) := |\{a_1 + \cdots + a_k = a_{k+1} + \cdots + a_{2k} : a_1, \dots, a_{2k} \in A\}|.$$

Note that the trivial solutions with $a_1 = a_{k+1}, \dots, a_k = a_{2k}$ ensure that $E_k^+(A) \geq |A|^k$ and so (4) is a factor of $(Ck^2)^{kK}$ away from being optimal. Inequality (3) follows from (4) after an application of the Cauchy–Schwarz inequality.

Giving a result with even more generality, Chang in fact proved a version of (4) with weighted energy. See the forthcoming Section 3 for a discussion on energy and weighted energy featuring the relevant definitions.

In the statement of Theorem 1.1, we think of k as a fixed constant. The theorem then gives a very strong lower bound for the size of kA when K is significantly smaller than $\log |A|$. However, if we push to the range $K = |A|^\epsilon$ for some positive ϵ , then Theorem 1.1 gives only a trivial bound.

In a follow-up paper of Bourgain and Chang [4], this method was used as a foundation and developed considerably in order to prove the following result.

Theorem 1.2. *Let $k \geq 2$ be a fixed integer. Given $\gamma > 0$, there is a constant $\Lambda = \Lambda(\gamma, k)$ such that for all finite sets $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$,*

$$|kA| \geq \frac{|A|^{k-\gamma}}{K^\Lambda}.$$

In particular, this now gives an excellent lower bound for $|kA|$ when $K = |A|^\epsilon$, for some small but positive ϵ .

Once again, a more general version of Theorem 1.2 was actually proved in [4], giving an upper bound for the weighted energy of A . This level of generality was important for establishing the main result of [4], which was the following result on unbounded growth of sums or products.

Theorem 1.3. *For all $b \geq 0$, there is an integer $k = k(b)$ such that for all $A \subset \mathbb{Q}$ with $|A| \geq 2$,*

$$\max\{|kA|, |A^{(k)}|\} \geq |A|^b.$$

See Zhelezov [16] for an exposition of the work of [5] and [4].

In this paper, we consider an alternative formulation of the sum-product problem with products and products of shifts. Given an arbitrary $A \subset \mathbb{R}$, sum-product heuristics lead one to believe that $\max\{|AA|, |(A+1)(A+1)|\}$ is large. Roughly speaking, this is an assertion that if A is multiplicatively structured then an additive shift will disturb this structure. A similar problem was

considered in the finite field setting by Bourgain [3], and it was established by Garaev and Shen [9] that for any finite $A \subset \mathbb{R}$,

$$\max\{|AA|, |(A+1)(A+1)|\} \geq c|A|^{5/4}, \quad (5)$$

where $c > 0$ is an absolute constant. See also Jones–Roche-Newton [11] for a slightly improved exponent. In principle, the value of 1 for the shift is not important, and a shift by any non-zero x should give the same outcome. Indeed, the proof of (5) works in exactly the same way if 1 is replaced with any $x \neq 0$.

It seems plausible that the numerology of the Erdős–Szemerédi conjecture holds for this problem too. That is, we expect that $\max\{|A^k|, |(A+1)^k|\}$ should be close to $|A|^k$. The main result of this paper proves a result in this direction, although under the stronger assumption that A has small multiplicative doubling.

Theorem 1.4. *Let $A \subset \mathbb{Q}$ be finite and suppose that $|AA| = K|A|$. Then, for any $k \geq 2$,*

$$|(A+1)^{(k)}| \geq \frac{|A|^k}{(8k^4)^{kK}}.$$

This is an analogue of Theorem 1.1 above, and gives an essentially optimal lower bound for $|(A+1)^k|$ in the case when $K < c \log |A|$. Again, we actually prove a more general result with energies and weights. See Theorem 6.1 for the full statement.

Note that, since this theorem holds for any set of rationals, it follows that the shift value 1 can be replaced by any rational $\lambda \neq 0$. Indeed, if $|AA| = K|A|$ then also $|(\frac{A}{\lambda})(\frac{A}{\lambda})| = K|A|$ for any rational λ . We can therefore apply Theorem 1.4 to the set A/λ and conclude that

$$|(A+\lambda)^{(k)}| = \left| \left(\frac{A}{\lambda} + 1 \right)^{(k)} \right| \geq \frac{|A|^k}{(8k^4)^{kK}}.$$

It seems that an analogue of Theorem 1.3 for products and products of shifts would have several interesting consequences in additive number theory. The authors consider this problem in a forthcoming paper [10].

Finally, it is worth noting that one can prove a weaker version of Theorem 1.4 by using quantitative bounds for the Subspace Theorem [8] similarly to [6]. The resulting bound will be of the form

$$|(A+1)^{(k)}| \geq e^{-c(k)K} |A|^k.$$

Apart from relying on a deep and hard result [8], the main disadvantage of such an approach is that the dependence $c(k)$ turns out to be triply exponential in k (comparing to almost linear in our case). Indeed, the number of terms after expanding the brackets in $(A+1)^k$ grows exponentially in k , while the state-of-the-art quantitative bound for the Subspace Theorem is doubly exponential in the number of variables; see [6],[1] for further details.

On the other hand, the dependence $c(k)$ may be important for applications. We record the following application to S -unit equations as an example.

Corollary 1.5. *Let p_1, \dots, p_r be a set of primes and S be a set of rational numbers of the form*

$$s = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

with $|\alpha_i| \leq H$. Then for any rational $c_1, c_2 \neq 0$ the number of solutions $(s_1, s_2) \in S \times S$ to

$$c_1 s_1 + c_2 s_2 = 1$$

is bounded by $(\log H)^{C2^r}$ with some absolute effective constant $C > 0$.

Corollary 1.5 is much weaker than the celebrated result of Beukers and Schlikewei [2], but may indicate a possible connection between sum-product estimates and Diophantine equations. We prove Corollary 1.5 in Section 7.

1.1. Outline of the proof. Our proof strategy is based on the ideas that Chang used to prove Theorem 1.1. Chang's strategy begins by using Freiman's Lemma to show that the elements of a set A with $|AA| = K|A|$ are determined by the powers of a set $\{p_1, \dots, p_K\}$ of K primes. The aim is to use this information to bound the number of solutions to

$$a_1 + \cdots + a_k = a_{k+1} + \cdots + a_{2k}, \tag{6}$$

such that $a_1, \dots, a_{2k} \in A$. The problem of bounding the number of solutions to (6) is converted into the problem of bounding certain trigonometric sums. The proof then proceeds by induction on K . If $K = 1$ then it follows that some power of the determining prime p must occur more than once in (6). Using this and an application of Hölder's inequality establishes the base case, and closing the induction is then fairly straightforward.

We imitate this argument, with the role of trigonometric sums played instead by Dirichlet polynomials, since we are now bounding the number of solutions to the multiplicative equation

$$(a_1 + 1) \cdots (a_k + 1) = (a_{k+1} + 1) \cdots (a_{2k} + 1). \tag{7}$$

When A is a set of integers things go through rather smoothly. However, the statement of Theorem 1.4 is not so satisfying in this case, since the lack of dilation invariance in our problem restricts the value of the additive shift we can take. The case when A consists of rational numbers, and in particular when the powers of our determining prime may be negative, does not yield to this method immediately, and the major challenge we faced was to tackle this case.

To explain how we overcome this hurdle, let us begin with the base case $K = 1$. We can control the number of solutions to (7) by those solutions consisting only of positive powers of p and those consisting of only negative powers. We can then bound those solutions coming from the first case by treating them as integers. However, we cannot yet say anything about the solutions coming from negative powers of p . We thus get a base case with two separate terms, and this blows up into a rather complicated statement after the induction process. However, once we apply a little extra information coming from Freiman's Lemma, we are able to bound these terms with only negative powers, and after some tricky calculations the desired result follows.

Note that, for the case $k = 2$ of Theorem 1.1, and indeed also that of Theorem 1.2, things are somewhat easier, as the whole proof can be carried out in the “physical space”, without the need for trigonometric sums. See [16] for the details of the modifications to the argument. A similar situation arises here, as the case $k = 2$ of Theorem 1.4 can be proven without using Dirichlet polynomials. However, when $k = 2$, a better version of Theorem 1.4 is available, even over \mathbb{R} ; see Shkredov [14, Theorem 12].

1.2. Notation. For two integers a, b we write, as usual, $(a, b) = 1$ if a and b are coprime. Similarly for $a, b \in \mathbb{Q}$ we say that a and b are coprime if, after writing $a = n_a/d_a$ and $b = n_b/d_b$ as reduced fractions, there is no prime which appears in both a and b . That is, $(n_a, n_b) = (n_a, d_b) = (d_a, n_b) = (d_a, d_b) = 1$.

We write $\mathbb{Z}_{\geq 0}$ for the set of all non-negative integers, and \mathbb{Z}_- for the set of all negative integers.

2. BACKGROUND ON DIRICHLET POLYNOMIALS

Let $(w_n)_{n=1}^N$ be a finite sequence of non-negative reals. The associated Dirichlet polynomial is

$$\sum_n w_n n^s = \sum_n w_n \exp(s(\log n))$$

which is a function of a complex variable s . These polynomials are not periodic in T , but still satisfy similar properties to those of trigonometric polynomials when integrated over a long interval.

Lemma 2.1. *For any $m, n \in \mathbb{Q}$ we have*

$$\int_0^T (m/n)^{it} dt = \begin{cases} T & \text{if } m = n, \\ O_{m,n}(1) & \text{if } m \neq n. \end{cases}$$

Consequently, for $k \geq 1$, we have

$$\frac{1}{T} \int_0^T \left| \sum_n w_n n^{it} \right|^{2k} dt = \sum_{n_1 \cdots n_k = n_{k+1} \cdots n_{2k}} w_{n_1} \cdots w_{n_{2k}} + o_{T \rightarrow \infty}(1)$$

where the implied constants in $o_{T \rightarrow \infty}(1)$ depend on the sequence w_n .

In particular, this leads to the following result which gives a connection between Dirichlet polynomials and the weighted multiplicative energy of A .

Corollary 2.2. *Let A be a finite set of rationals and let $w = \{w_a : a \in A\}$ be a set of weights on A . Then*

$$E_{k,w}(A) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \left| \sum_{a \in A} w_a a^{it} \right|^{2k} dt.$$

We will be interested in the following sorts of Dirichlet polynomials, and only interested at purely imaginary values. For p a prime and a rational number x , let $v_p(x)$ denote the p -adic valuation of x , that is, the power of p when x is expressed in its reduced form as a product of primes:

$$x = \prod_p p^{v_p(x)}.$$

For any $u \in \mathbb{Q}$, write $\mathcal{F}_{p,j,u}$ for the set of those Dirichlet polynomials of the form

$$f_j(t) = \sum_{n \in \mathbb{Q}: v_p(n)=j} w_n (n+u)^{it}.$$

3. WEIGHTED MULTIPLICATIVE ENERGY

A key notion in this paper is that of the *multiplicative energy of order k* of a set A , which is defined as

$$E_k(A) = \sum_n \Gamma_{k,A}^2(n),$$

where $\Gamma_{k,A}(n) = |\{(a_1, \dots, a_k) \in A^k : a_1 \cdots a_k = n\}|$. Alternatively, this is the number of solutions to the equation

$$a_1 \cdots a_k = a_{k+1} \cdots a_{2k}.$$

Good upper bounds for $E_k(A)$ lead to good lower bounds for $|A^k|$, because of the following inequality which is a standard application of the Cauchy-Schwarz inequality;

$$E_k(A) |A^{(k)}| \geq |A|^{2k}.$$

It turns out that a certain weighted version of $E_k(A)$ is more robust for applications. Let A be a finite set of size N with elements a_1, \dots, a_N (the actual ordering is not important). Next, let $w = \{w_1, \dots, w_N\}$ be a set of non-negative real numbers. One can think of w_i as the weight attached to the element a_i . Then define the multiplicative energy of order k with weights w_i as

$$E_{k,w}(A) := \sum w_{i_1} \cdots w_{i_{2k}},$$

where the summation is taken over all $2k$ -tuples (i_1, \dots, i_{2k}) such that

$$a_{i_1} \cdots a_{i_k} = a_{i_{k+1}} \cdots a_{i_{2k}}.$$

Finally, define $\Lambda_k(A)$ as

$$\Lambda_k(A) := \max_w E_{k,w}(A)^{1/k},$$

where the maximum is taken over all weights w such that

$$\sum_{i=1}^N w_i^2 = 1. \tag{8}$$

It is well-defined by compactness. An attentive reader will notice that our definition of Λ_k is a straightforward ‘multiplicative’ adaptation of the Λ -constants widely used in harmonic analysis.

The use of Λ -constants for sum-product type problems was pioneered by Chang and Bourgain (see [5], [4] and references therein). The present note is largely based on the ideas of [5]. In particular, Section 4 is an adaptation of the technique used in [5] to the multiplicative setting.

Now we record some properties of $\Lambda_k(A)$ in order to justify such a quantity. Let $\|\cdot\|_{2k}$ be the standard norm in $L_{2k}[0, T]$, normalised such that $\|1\|_{2k} = 1$. So,

$$\|f\|_{2k} := \left(\frac{1}{T} \int_0^T |f(t)|^{2k} dt \right)^{1/2k}.$$

Lemma 3.1. *Let A be a finite set with some non-negative real numbers w_a assigned to each element $a \in A$. Then*

$$\left\| \sum_{a \in A} w_a a^{it} \right\|_{2k}^2 \leq \Lambda_k(A) \left(\sum_{a \in A} w_a^2 \right) + o_{T \rightarrow \infty}(1). \quad (9)$$

Proof. If $\sum_{a \in A} w_a^2 = 0$ the claim of the lemma is trivial. Otherwise, define new weights

$$w'_a := \frac{w_a}{(\sum_{a \in A} w_a^2)^{1/2}}$$

which satisfy (8). It thus suffices to show that

$$\left\| \sum_{a \in A} w'_a a^{it} \right\|_{2k}^2 \leq \Lambda_k(A) + o_{T \rightarrow \infty}(1),$$

which is a straightforward consequence of our definition of $\Lambda_k(A)$ and Lemma 2.1. \square

A crucial corollary is the following stability property of Λ_k which does not seem to be available when one works with multiplicative energies.

Corollary 3.2. *Let $A' \subset A$. Then*

$$E_k^{1/k}(A') \leq \Lambda_k(A) |A'|.$$

In particular,

$$E_k(A) \leq \Lambda_k^k(A) |A|^k.$$

Proof. Apply Lemma 3.1 with $w_a = 1$ if $a \in A'$ and $w_a = 0$ otherwise. \square

4. THE INTEGER CASE

In this section we restrict ourselves to the integer case and prove the following bound.

Theorem 4.1. *Let A be a sufficiently large but finite set of positive integers, with the property that $|AA| \leq K|A|$ for some integer K . Then, for any u coprime with the elements of A , we have*

$$\Lambda_k(A + u) \leq (2k^2)^K. \quad (10)$$

In particular,

$$|(A + u)^{(k)}| \geq \frac{|A|^k}{(2k^2)^{kK}}. \quad (11)$$

The following is analogous to Proposition 6 of Chang [5]. Here, we have an extra restriction that we are dealing only with positive powers of a given prime p . This makes things rather simpler for us, and we can follow the strategy of Chang, making the appropriate minor alterations.

Lemma 4.2. *Let p be a prime and let \mathcal{J} be a set of positive integers. Let $u \in \mathbb{Z}$ such that $(p, u) = 1$. Suppose $f_j \in \mathcal{F}_{p, j, u}$ for $j \in \mathcal{J}$. Then for $k \geq 1$,*

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_j f_j(t) \right|^{2k} dt \right)^{1/k} \leq 2k^2 \sum_j \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_j(t)|^{2k} dt \right)^{1/k}. \quad (12)$$

Proof. Expanding the k 'th power of the left hand side of (12) gives

$$\sum_{j_1, \dots, j_{2k}} \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T f_{j_1}(t) \cdots f_{j_k}(t) \overline{f_{j_{k+1}}(t)} \cdots \overline{f_{j_{2k}}(t)} dt \quad (13)$$

For fixed j_1, \dots, j_{2k} , the quantity

$$\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T f_{j_1}(t) \cdots f_{j_k}(t) \overline{f_{j_{k+1}}(t)} \cdots \overline{f_{j_{2k}}(t)} dt$$

gives a weighted count of the number of solutions to equations of the form

$$(m_1 p^{j_1} + u) \cdots (m_k p^{j_k} + u) = (m_{k+1} p^{j_{k+1}} + u) \cdots (m_{2k} p^{j_{2k}} + u), \quad (14)$$

with each of the $m_i \in \mathbb{Q}$ coprime to p . We claim that there are no solutions to (14) if all of the j_i are distinct. Indeed, suppose that all of these powers are distinct, and in particular there is a unique smallest power, say $j_1 < j_2, j_3, \dots, j_{2k}$. Then we get (expanding the brackets, subtracting u^k from both sides, and multiplying out all denominators of the m_i) an equation

$$M p^{j_1} + N_1 p^{j_1+1} = N_2 p^{j_1+1} \quad (15)$$

for some integers M, N_1 and N_2 , such that $(M, p) = 1$. This is a contradiction, since the right hand side is divisible by p^{j_1+1} and the left hand side is not. Therefore, there are no contributions to (13) coming from those terms where all of the j_i are distinct.

It remains to consider the cases where two or more of the powers j_1, \dots, j_{2k} are the same. There are three kinds of ways in which this can happen.

- (1) $j_i = j_{i'}$ with $1 \leq i \leq k$ and $k+1 \leq i' \leq 2k$. There are k^2 possible positions for such a pair (i, i') ,
- (2) $j_i = j_{i'}$ with $1 \leq i, i' \leq k$. There are $\binom{k}{2}$ possible positions for such a pair (i, i') ,
- (3) $j_i = j_{i'}$ with $k+1 \leq i, i' \leq 2k$. There are $\binom{k}{2}$ possible positions for such a pair (i, i') .

Suppose we are in situation (1) above. Specifically, suppose that $j_1 = j_{2k}$. The other $k^2 - 1$ cases can be dealt with by the same argument. Then these terms in (13) can be rewritten as

$$\begin{aligned} & \sum_{j_1} \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T f_{j_1}(t) \overline{f_{j_1}(t)} \sum_{j_2, \dots, j_{2k-1}} f_{j_2}(t) \cdots f_{j_k}(t) \overline{f_{j_{k+1}}(t)} \cdots \overline{f_{j_{2k-1}}(t)} dt \\ &= \sum_j \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |f_j(t)|^2 \left| \sum_j f_j(t) \right|^{2(k-1)} dt. \end{aligned}$$

Suppose we are in situation (2). Specifically, suppose that $j_1 = j_2$. The other $\binom{k}{2}$ cases can be dealt with by the same argument. Then these terms in (13) can be rewritten as

$$\begin{aligned}
& \sum_{j_1} \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T f_{j_1}^2(t) \sum_{j_3, \dots, j_{2k}} f_{j_3}(t) \cdots f_{j_k}(t) \overline{f_{j_{k+1}}(t)} \cdots \overline{f_{j_{2k}}(t)} dt \\
& \leq \sum_j \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |f_j(t)|^2 \left| \sum_j f_j(t) \right|^{k-2} \left| \sum_j \overline{f_j(t)} \right|^k dt \\
& = \sum_j \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |f_j(t)|^2 \left| \sum_j f_j(t) \right|^{2(k-1)} dt.
\end{aligned}$$

The same argument also works in case (3). Returning to (13), we then have

$$\begin{aligned}
& \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_j f_j(t) \right|^{2k} dt \right) \\
& \sum_{j_1, \dots, j_{2k}} \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T f_{j_1}(t) \cdots f_{j_k}(t) \overline{f_{j_{k+1}}(t)} \cdots \overline{f_{j_{2k}}(t)} dt \\
& \leq \left(k^2 + 2 \binom{k}{2} \right) \sum_j \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |f_j(t)|^2 \left| \sum_j f_j(t) \right|^{2(k-1)} dt \\
& \leq 2k^2 \sum_j \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |f_j(t)|^2 \left| \sum_j f_j(t) \right|^{2(k-1)} dt.
\end{aligned}$$

Here we have used the fact that the weights are positive and real, which allows us to overcount solutions which may occur in more than one of the three cases above. Finally, an application of Hölder's inequality gives

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_j f_j(t) \right|^{2k} dt \right) \leq 2k^2 \sum_j \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_j(t)|^{2k} dt \right)^{1/k} \left(\frac{1}{T} \int_0^T \left| \sum_j f_j(t) \right|^{2k} dt \right)^{1-1/k}.$$

A rearrangement of this inequality completes the proof. \square

Using an inductive argument, we can extend this result to handle generalized geometric progressions. To that end, for a vector $\mathbf{p} = (p_1, \dots, p_t)$ of prime numbers and a vector $\mathbf{j} = (j_1, \dots, j_t)$ of non-negative integers, let $\mathcal{F}_{\mathbf{p}, \mathbf{j}, u}$ be the set of Dirichlet polynomials of the form

$$f_{\mathbf{j}}(t) = \sum_{n: v_{p_i}(n) = j_i} w_n (n+u)^{it}.$$

Lemma 4.3. *Let $\mathbf{p} = (p_1, \dots, p_K)$ be a vector of prime numbers and let \mathcal{J} be a set of vectors with non-negative entries. Let $u \in \mathbb{Z}$ such that $(u, p_1 \cdots p_K) = 1$. Suppose $f_{\mathbf{j}} \in \mathcal{F}_{\mathbf{p}, \mathbf{j}, u}$ for $\mathbf{j} \in \mathcal{J}$. Then*

for $k \geq 1$, we have

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j \in \mathcal{J}} f_j(t) \right|^{2k} dt \right)^{1/k} \leq (2k^2)^K \sum_{j \in \mathcal{J}} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_j(t)|^{2k} dt \right)^{1/k}. \quad (16)$$

Proof. We establish the convention that f_j is identically zero for all $j \notin \mathcal{J}$. Therefore, we can complete the sum in (16), and the aim is to prove that

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j \in \mathbb{Z}_{\geq 0}^K} f_j(t) \right|^{2k} dt \right)^{1/k} \leq (2k^2)^K \sum_{j \in \mathbb{Z}_{\geq 0}^K} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_j(t)|^{2k} dt \right)^{1/k}.$$

We proceed by induction on K , the base case $K = 1$ being given by Lemma 4.2. Then

$$\begin{aligned} & \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j \in \mathbb{Z}_{\geq 0}^K} f_j(t) \right|^{2k} dt \right)^{1/k} \\ &= \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j_K \in \mathbb{Z}_{\geq 0}} \left(\sum_{j' \in \mathbb{Z}_{\geq 0}^{K-1}} f_{j', j_K}(t) \right) \right|^{2k} dt \right)^{1/k} \\ &\leq 2k^2 \sum_{j_K \in \mathbb{Z}_{\geq 0}} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j' \in \mathbb{Z}_{\geq 0}^{K-1}} f_{j', j_K}(t) \right|^{2k} dt \right)^{1/k} \\ &\leq 2k^2 \sum_{j_K \in \mathbb{Z}_{\geq 0}} (2k^2)^{K-1} \sum_{j' \in \mathbb{Z}_{\geq 0}^{K-1}} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_{j', j_K}(t)|^{2k} dt \right)^{1/k} \\ &= (2k^2)^K \sum_{j \in \mathbb{Z}_{\geq 0}^K} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_j(t)|^{2k} dt \right)^{1/k}. \end{aligned}$$

The first inequality above follows from an application of Lemma 4.2, using the fact that

$$\sum_{j' \in \mathbb{Z}_{\geq 0}^{K-1}} f_{j', j_K}(t) \in \mathcal{F}_{p_K, j_K, u}.$$

The second inequality follows from the induction hypothesis. \square

We are now in a strong position to establish results on the physical side, starting with the following lemma.

Lemma 4.4. *Let $\mathbf{p} = (p_1, \dots, p_K)$ be a vector of prime numbers and let $\mathcal{J} \subset \mathbb{Z}^K$ be a set of vectors with non-negative entries. Let $u \in \mathbb{Z}$ such that $(u, p_1 \dots p_K) = 1$. Suppose that*

$$A = \bigcup_{j=(j_1, \dots, j_K) \in \mathcal{J}} \{p_1^{j_1} \dots p_K^{j_K} x(j)\}$$

with each $x(\mathbf{j}) \in \mathbb{Q}$ coprime to $p_1 \cdots p_K$. Then

$$\Lambda_k(A + u) \leq (2k^2)^K.$$

Proof. For each $\mathbf{j} = (j_1, \dots, j_K) \in \mathcal{J}$, define $a_j = p_1^{j_1} \cdots p_K^{j_K} x(\mathbf{j})$, so that $A = \{a_j : \mathbf{j} \in \mathcal{J}\}$. Define $f_j(t) = w_j(a_j + u)^{it}$ for some weights $w = \{w_j : \mathbf{j} \in \mathcal{J}\}$ satisfying

$$\sum_{\mathbf{j} \in \mathcal{J}} w_j^2 = 1.$$

Note that $f_j(t) \in \mathcal{F}_{p, \mathbf{j}, u}$, because of the divisibility conditions in the statement of the lemma. Note also that

$$\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T |f_j(t)|^{2k} dt = w_j^{2k}.$$

Using this, as well as Theorem 4.3 and Corollary 2.2, we conclude that

$$\begin{aligned} E_{k,w}(A + u)^{1/k} &= \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}} w_j (a_j + u)^{it} \right|^{2k} dt \right)^{1/k} \\ &= \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}} f_j(t) \right|^{2k} dt \right)^{1/k} \\ &\leq (2k^2)^K \sum_{\mathbf{j} \in \mathcal{J}} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |f_j(t)|^{2k} dt \right)^{1/k} \\ &= (2k^2)^K. \end{aligned}$$

Since the bound above does not depend on the weights, we are done. \square

Before completing the proof of Theorem 4.1, we need the following more or less obvious lemma.

Lemma 4.5. *Let L be an affine subspace of \mathbb{F}^l of dimension d . Then, after relabeling the coordinates if necessary, L has the form*

$$L = \{(x_1, \dots, x_d, f_1(x_1, \dots, x_d), \dots, f_{l-d}(x_1, \dots, x_d) : x_1, \dots, x_d \in \mathbb{F}\},$$

where each of the functions f_i have degree at most 1 in variables x_1, \dots, x_d .

In particular, there are d coordinate projections π_1, \dots, π_d such that the map $\pi : \mathbb{F}^l \rightarrow \mathbb{F}^d$ given by $\pi(\mathbf{v}) = (\pi_1(\mathbf{v}), \dots, \pi_d(\mathbf{v}))$ is injective on L .

Proof. By shifting if necessary, we may assume L is a linear subspace without loss of generality. Let v_1, \dots, v_d be d linearly independent vectors in L which we place as rows in a matrix M of dimension $d \times l$ and rank d . Performing row reduction on M and permuting columns if necessary, we get a matrix M' in a row echelon form. Since the rank of M' is d , the left-most minor of M' is a $d \times d$ identity matrix. The rows of M' span L , and this is exactly the claim of the lemma. \square

Let A be a set of positive integers and let $\mathcal{P} = \{p_1, \dots, p_t\}$ be the set of primes dividing any element of A . Abusing notation slightly, we define a map $\mathcal{P} : A \rightarrow \mathbb{Z}^t$ where $\mathcal{P}(a) = (v_{p_1}(a), \dots, v_{p_t}(a))$. Denoting by $\mathcal{P}(X)$ the image of a set X under \mathcal{P} , observe that $\mathcal{P}(AA) = \mathcal{P}(A) + \mathcal{P}(A)$. We define the multiplicative dimension of A to be the least dimension of an affine space L containing $\mathcal{P}(A)$.

Theorem 4.6 (Freiman's Lemma (see Lemma 5.13 in [15])). *Let $A \subset \mathbb{R}^m$ be a finite set not contained in a proper affine subspace. Then*

$$|A + A| \geq (m + 1)|A| - O_m(1).$$

Theorem 4.1 now becomes a simple corollary.

Proof (of Theorem 4.1). It follows from Freiman's Lemma that if $|AA| \leq K|A|$ with $|A|$ sufficiently large, then A has multiplicative dimension at most K . Thus, there is an affine subspace of \mathbb{R}^t containing $v(A)$ and of dimension at most K . Permuting the coordinates if necessary, it follows from an application of Lemma 4.5 that each $a \in A$ can be written as $a = p_1^{v_{p_1}(a)} \dots p_K^{v_{p_K}(a)} n_a$ where n_a is not divisible by any p_i with $1 \leq i \leq K$ and the vector $(v_{p_1}(a), \dots, v_{p_K}(a))$ is unique to a . This is precisely the situation of Lemma 4.4. This proves (10).

From the Cauchy-Schwarz inequality and Corollary 3.2

$$|A|^{2k} \leq |(A + u)^{(k)}| E_k(A + u) \leq (2k^2)^{kK} |A|^k |(A + u)^{(k)}|,$$

whence

$$|A|^k \leq (2k^2)^{kK} |(A + u)^{(k)}|.$$

□

5. THE RATIONAL CASE - THE MAIN LEMMA

In this section, we begin to deal with the rational case, which is rather more complicated. The first aim is prove an analogue of Lemma 4.3. We begin to tackle this by proving the following lemma which helps us to decompose \mathcal{J} suitably.

Lemma 5.1. *Let $\mathcal{J} \subset \mathbb{Z}^K$ and decompose it as $\mathcal{J} = \mathcal{J}_1 \cup \dots \cup \mathcal{J}_N$. Let $\mathbf{p} = (p_1, \dots, p_K)$ be a vector of prime numbers and for each $\mathbf{j} \in \mathcal{J}$ let $f_{\mathbf{j}} \in \mathcal{F}_{\mathbf{j}, \mathbf{p}, 1}$. Then*

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k} \leq N \sum_{n=1}^N \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}_n} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k}. \quad (17)$$

Proof. It suffices to prove the inequality for all sufficiently large T , which we assume fixed for now. Then

$$\left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k} = \left(\left\| \sum_{n=1}^N \sum_{\mathbf{j} \in \mathcal{J}_n} f_{\mathbf{j}} \right\|_{2k} \right)^2 \leq \left(\sum_{n=1}^N \left\| \sum_{\mathbf{j} \in \mathcal{J}_n} f_{\mathbf{j}} \right\|_{2k} \right)^2, \quad (18)$$

by the triangle inequality. By the Cauchy-Schwarz inequality, (18) is bounded by

$$N \sum_{n=1}^N \left\| \sum_{j \in \mathcal{J}_n} f_j \right\|_{2k}^2. \quad (19)$$

Letting $T \rightarrow \infty$ we get the claim of the lemma. \square

We need to introduce some notation which will be convenient for the forthcoming statement and its proof. Let $S \subset [K]$ for a fixed positive integer K . For a set $\mathcal{J} \subset \mathbb{Z}^K$, we write $\mathcal{J}_S \subset \mathcal{J}$ for the set of all vectors in \mathcal{J} whose non-negative entries lie exclusively in the positions corresponding to elements of S . We will let π_S denote the projection onto the coordinates from S . Suppose $\mathbf{j}_S \in \pi_S(\mathcal{J})$, then we define

$$\mathcal{J}_S(\mathbf{j}_S) = \{\mathbf{j} \in \mathcal{J} : \pi_S(\mathbf{j}) = \mathbf{j}_S, \pi_{[K] \setminus S}(\mathbf{j}) \in \mathbb{Z}_-^{K-|S|}\}.$$

Theorem 5.2. *Let $\mathbf{p} = (p_1, \dots, p_K)$ be a vector of prime numbers and let $\mathcal{J} \subset \mathbb{Z}^K$ be a finite set of vectors. Suppose $f_j \in \mathcal{F}_{\mathbf{p}, \mathbf{j}, 1}$ for $\mathbf{j} \in \mathcal{J}$. Then for $k \geq 1$, we have*

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k} \leq (4k^2)^K \sum_{S \subset \{1, \dots, K\}} \sum_{\mathbf{j}_S \in \pi_S(\mathcal{J}_S)} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}_S(\mathbf{j}_S)} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k}.$$

Proof. First we partition

$$\mathcal{J} = \bigcup_{S \subset \{1, \dots, K\}} \mathcal{J}_S.$$

By Lemma 5.1, we have

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k} \leq 2^K \sum_{S \subset \{1, \dots, K\}} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}_S} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k}.$$

Now consider the set $\pi_S(\mathcal{J}_S)$ which consists of vectors in $\mathbb{Z}^{|S|}$, each with non-negative entries. Thus, applying Lemma 4.3 to these, we get

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}_S} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k} \leq (2k^2)^{|S|} \sum_{\mathbf{j}_S \in \pi_S(\mathcal{J}_S)} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{\mathbf{j} \in \mathcal{J}_S(\mathbf{j}_S)} f_{\mathbf{j}}(t) \right|^{2k} dt \right)^{1/k}$$

and the theorem follows. \square

6. THE RATIONAL CASE - CONCLUDING THE PROOF

This section is devoted to proving the main result of this paper, which we now state in full.

Theorem 6.1. *Let $A \subset \mathbb{Q}$ be a finite set, with the property that $|AA| \leq K|A|$ for some integer K . Then we have*

$$\Lambda_k(A+1) \leq (8k^4)^K. \quad (20)$$

In particular,

$$|(A+1)^{(k)}| \geq \frac{|A|^k}{(8k^4)^{kK}}. \quad (21)$$

Proof. Suppose that $A \subset \mathbb{Q}$ and $|AA| \leq K|A|$ and let $\mathcal{P} = \{p_1, \dots, p_l\}$ be the set of all primes that appear in the prime decomposition of the elements of A . So, each element $a \in A$ can be expressed uniquely as $a = p_1^{v_{p_1}(a)} \cdots p_l^{v_{p_l}(a)}$. We have no control over the size of \mathcal{P} , but we do know that \mathcal{P} is finite.

As in the proof of Theorem 4.1, we also let $\mathcal{P} : A \rightarrow \mathbb{Z}^n$ denote the prime evaluation map defined by $\mathcal{P}(p_1^{v_{p_1}(a)} \cdots p_n^{v_{p_n}(a)}) = (v_{p_1}(a), \dots, v_{p_n}(a))$ and note that $|\mathcal{P}(A) + \mathcal{P}(A)| = |AA|$.

By Freiman's Lemma $\mathcal{P}(A)$ has affine dimension at most K . Then, by Lemma 4.5, we have that

$$\mathcal{P}(A) = \{(j_1, \dots, j_K, f_{K+1}(j_1, \dots, j_K), \dots, f_l(j_1, \dots, j_K)) : (j_1, \dots, j_K) \in \pi(\mathcal{P}(A))\},$$

where π is the projection from \mathbb{R}^l to the first K coordinates, and each f_i is either constant, or linear in variables j_1, \dots, j_K .

We then apply the inverse map \mathcal{P}^{-1} and see that A has the form

$$A = \{p_1^{j_1} \cdots p_K^{j_K} x(j_1, \dots, j_K) : (j_1, \dots, j_K) \in \pi(\mathcal{P}(A))\},$$

where $x(j_1, \dots, j_K) = p_{K+1}^{f_{K+1}(j_1, \dots, j_K)} \cdots p_l^{f_l(j_1, \dots, j_K)}$. Note that x is coprime to $p_1 \cdots p_K$. Let $\mathcal{J} = \pi(\mathcal{P}(A))$ and for $\mathbf{j} = (j_1, \dots, j_K) \in \mathcal{J}$, let

$$a_{\mathbf{j}} = p_1^{j_1} \cdots p_K^{j_K} x(\mathbf{j}).$$

Now suppose w is any weight function defined on $A+1$ and we consider

$$\sum_{a \in A} w_{a+1}(a+1)^{it} = \sum_{\mathbf{j} \in \mathcal{J}} w_{a_{\mathbf{j}}+1}(a_{\mathbf{j}}+1)^{it} = \sum_{S \subset \{1, \dots, K\}} \sum_{\mathbf{j}_S \in \pi_S(\mathcal{J}_S)} \sum_{j \in \mathcal{J}_S(\mathbf{j}_S)} w_{a_{\mathbf{j}}+1}(a_{\mathbf{j}}+1)^{it}.$$

By Theorem 5.2,

$$\begin{aligned} & \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{a \in A} w_{a+1}(a+1)^{it} \right|^{2k} dt \right)^{1/k} \\ & \leq (4k^2)^K \sum_{S \subset \{1, \dots, K\}} \sum_{\mathbf{j}_S \in \pi_S(\mathcal{J}_S)} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j \in \mathcal{J}_S(\mathbf{j}_S)} w_{a_{\mathbf{j}}+1}(a_{\mathbf{j}}+1)^{it} \right|^{2k} dt \right)^{1/k}. \quad (22) \end{aligned}$$

If we define

$$A_{S, \mathbf{j}_S} = \{a_{\mathbf{j}} : \mathbf{j} \in \mathcal{J}_S(\mathbf{j}_S)\}$$

and w_{S, \mathbf{j}_S} to be the weights w restricted to $A_{S, \mathbf{j}_S} + 1$ then the innermost quantity above is

$$\lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j \in \mathcal{J}_S(\mathbf{j}_S)} w_{a_{\mathbf{j}}+1}(a_{\mathbf{j}}+1)^{it} \right|^{2k} dt \right)^{1/k} = E_{k, w_{S, \mathbf{j}_S}}(A_{S, \mathbf{j}_S} + 1)^{1/k}.$$

This energy is a weighted count of solutions to the equation

$$(a_{j_1} + 1) \cdots (a_{j_k} + 1) = (a_{j_{k+1}} + 1) \cdots (a_{j_{2k}} + 1). \quad (23)$$

Define \mathbf{l}_S to be the K -dimensional vector obtained from \mathbf{j}_S by adding zero entries to those positions not corresponding to S . We can then write $\mathbf{j} \in \mathcal{J}_S(\mathbf{j}_S)$ as $\mathbf{l}_S + \mathbf{j}'$ where \mathbf{j}' has negative entries on coordinates from $S' = \{1, \dots, K\} \setminus S$ and zeros on coordinates in S . We let \mathbf{p}_S denote the vector of primes with indices from S and \mathbf{q} denote the vector of primes with indices from S' . Finally, if we use the notation $\mathbf{z}^{\mathbf{m}} = z_1^{m_1} \cdots z_K^{m_K}$, then for $\mathbf{j}_i = \mathbf{l}_S + \mathbf{j}'_i$ we have

$$a_{\mathbf{j}_i} = \mathbf{p}_S^{\mathbf{l}_S} \mathbf{q}^{\mathbf{j}'_i} x(\mathbf{j}_i).$$

Now we claim the following:

Claim 6.2. *If (23) holds then*

$$\mathbf{j}'_1 + \cdots + \mathbf{j}'_k = \mathbf{j}'_{k+1} + \cdots + \mathbf{j}'_{2k} \quad (24)$$

and

$$x(\mathbf{j}_1) \cdots x(\mathbf{j}_k) = x(\mathbf{j}_{k+1}) \cdots x(\mathbf{j}_{2k}). \quad (25)$$

In particular

$$a_{\mathbf{j}_1} \cdots a_{\mathbf{j}_k} = a_{\mathbf{j}_{k+1}} \cdots a_{\mathbf{j}_{2k}}.$$

Proof of claim. We begin with (24). We have

$$a_{\mathbf{j}_i} + 1 = \frac{\mathbf{p}_S^{\mathbf{l}_S} x(\mathbf{j}_i) + \mathbf{q}^{-\mathbf{j}'_i}}{\mathbf{q}^{-\mathbf{j}'_i}}.$$

The non-zero entries of $-\mathbf{j}'_i$ are positive and correspond to indices in S' . Furthermore $\mathbf{p}_S^{\mathbf{l}_S} x(\mathbf{j}_i)$ is coprime to p_t for any $t \in S'$. Thus

$$v_{p_t}(a_{\mathbf{j}_i} + 1) = v_{p_t}(\mathbf{q}^{\mathbf{j}'_i}),$$

and from this (24) follows.

Next, we recall that $x(\mathbf{j}_i)$ is of the form $p_{K+1}^{f_{K+1}(\mathbf{j}_i)} \cdots p_l^{f_l(\mathbf{j}_i)}$ for primes p_{K+1}, \dots, p_l and functions f_i which are linear or constant. Thus

$$v_{p_t}(x(\mathbf{j}_1) \cdots x(\mathbf{j}_k)) = f_t(\mathbf{j}_1) + \cdots + f_t(\mathbf{j}_k)$$

and

$$v_{p_t}(x(\mathbf{j}_{k+1}) \cdots x(\mathbf{j}_{2k})) = f_t(\mathbf{j}_{k+1}) + \cdots + f_t(\mathbf{j}_{2k})$$

for any $t \in \{K+1, \dots, l\}$. Writing $f_t = H_t + c_t$ for a linear form H_t and a constant c_t we see

$$v_{p_t}(x(\mathbf{j}_1) \cdots x(\mathbf{j}_k)) = H_t(\mathbf{j}_1 + \cdots + \mathbf{j}_k) + kc_t$$

and

$$v_{p_t}(x(\mathbf{j}_{k+1}) \cdots x(\mathbf{j}_{2k})) = H_t(\mathbf{j}_{k+1} + \cdots + \mathbf{j}_{2k}) + kc_t.$$

In view of the first part of the claim and the the fact that $\mathbf{j}_i = \mathbf{l}_S \oplus \mathbf{j}'_i$, we have

$$\mathbf{j}_1 + \cdots + \mathbf{j}_k = \mathbf{j}_{k+1} + \cdots + \mathbf{j}_{2k}$$

and (25) follows. □

Having established this claim, we can multiply both sides of (23) by

$$\prod_{i=1}^k a_{j_i}^{-1} = \prod_{i=k+1}^{2k} a_{j_i}^{-1}$$

to get the equation

$$(1 + a_{j_1}^{-1}) \cdots (1 + a_{j_k}^{-1}) = (1 + a_{j_{k+1}}^{-1}) \cdots (1 + a_{j_{2k}}^{-1}).$$

Counting such equations with the same weights, we are now evaluating

$$E_{k, w_S, j_S} (A_{S, j_S}^{-1} + 1)^{1/k} = \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{j \in \mathcal{J}_S(j_S)} w_{a_j+1} (a_j^{-1} + 1)^{it} \right|^{2k} dt \right)^{1/k}.$$

Crucially, the powers of primes indexed by S' are now all positive in the above quantity, and we can apply Lemma 4.3. The above is thus at most

$$(2k^2)^{K-|S|} \sum_{j \in \mathcal{J}_S(j_S)} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T |w_{a_j+1} (a_j^{-1} + 1)^{it}|^{2k} dt \right)^{1/k} \leq (2k^2)^K \sum_{j \in \mathcal{J}_S(j_S)} |w_{a_j+1}|^2.$$

Inserting this into (22), we conclude that

$$\begin{aligned} \lim_{T \rightarrow \infty} \left(\frac{1}{T} \int_0^T \left| \sum_{a \in A} w_{a+1} (a+1)^{it} \right|^{2k} dt \right)^{1/k} &\leq (4k^2)^K \sum_{S \subset \{1, \dots, K\}} \sum_{j_S \in \pi_S(\mathcal{J}_S)} (2k^2)^K \sum_{j \in \mathcal{J}_S(j_S)} |w_{a_j+1}|^2. \\ &= (8k^4)^K \sum_{j \in \mathcal{J}} |w_{a_j+1}|^2. \end{aligned}$$

Since the inequality above is true for any set of weights on $A+1$, (20) then follows from the definition of $\Lambda_k(A+1)$.

To prove (21), we apply the Cauchy-Schwarz inequality and Corollary 3.2, just as we did in the conclusion of the proof of Theorem 4.1. This yields

$$|A|^{2k} \leq E_k(A+1) |(A+1)^{(k)}| \leq \Lambda_k^k(A+1) |A|^k |(A+1)^{(k)}| \leq (8k^4)^k K |A|^k |(A+1)^{(k)}|,$$

and a rearrangement of this inequality completes the proof of (21). □

7. PROOF OF COROLLARY 1.5

Recall the statement of Corollary 1.5.

Corollary. *Let p_1, \dots, p_r be a set of primes and S be a set of rational numbers of the form*

$$s = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

with $|\alpha_i| \leq H$. Then for any rational $c_1, c_2 \neq 0$ the number of solutions $(s_1, s_2) \in S \times S$ to

$$c_1 s_1 + c_2 s_2 = 1 \tag{26}$$

is bounded by $(\log H)^{C^{2r}}$ with some absolute effective constant $C > 0$.

Proof. Let S_1 be the set of $s_1 \in S$ such that (s_1, s_2) is a solution to (26) for some $s_2 \in S$. By the hypothesis S_1 is contained in the generalised geometric progression

$$G := \{p_1^{i_1} \dots p_r^{i_r} : i_1, \dots, i_r \in [-H, H]\}.$$

It is straightforward to check that

$$|GG| \leq 2^r |G|,$$

and thus by Corollary 3.2 and Theorem 6.1 applied for the set $c_1 S_1$

$$E_k(c_1 S_1 - 1) \leq \exp(Ck \log k 2^r) |S_1|^k. \quad (27)$$

On the other hand, the shifted set $c_1 S_1 - 1$ is contained in $-c_2 G$, so

$$|(c_1 S_1 - 1)^{(k)}| \leq |G^{(k)}| < \exp(r \log(3kH)). \quad (28)$$

Applying Cauchy-Schwarz to (27) and combining with (28) we have

$$|S_1| < \exp(C \log k 2^r + r \log(3kH)/k).$$

Taking

$$k = \frac{\log H}{\log \log H}$$

and assuming $w \log H \gg r \gg 1$, we get

$$|S_1| \leq \exp(C' 2^r \log \log H) = (\log H)^{C' 2^r}$$

for some absolute $C' > 0$. □

8. ACKNOWLEDGEMENTS

Oliver Roche-Newton was partially supported by the Austrian Science Fund FWF Projects F5509 and P 30405-N32. Dmitrii Zhelezov was partially supported by the Knuth and Alice Wallenberg Foundation Program for Mathematics 2017.

We thank Brendan Murphy and Endre Szemerédi for helpful conversations.

REFERENCES

- [1] F. Amoroso and E. Viada, ‘Small points on subvarieties of a torus’, *Duke Math. J.* 150(3) (2009), 407–442.
- [2] F. Beukers and H. P. Schlickewei, ‘The equation $x + y = 1$ in finitely generated groups’, *Acta Arith.* 78(2) (1996), 186–199.
- [3] J. Bourgain, ‘More on sum-product phenomenon in prime fields and its applications’, *Int. J. Number Theory* 1 (2005), 1–32.
- [4] J. Bourgain and M.-C. Chang, ‘On the size of k -fold sum and product sets of integers’, *J. Amer. Math. Soc.*, 17(2) (2004), 473–497.
- [5] M.-C. Chang, ‘The Erdős-Szemerédi problem on sum set and product set’, *Ann. of Math. (2)* 157 (2003), no. 3, 939–957.
- [6] M.-C. Chang, ‘Sum and product of different sets’, *Contrib. Discrete Math.* 1 no. 1 (electronic) (2006), 47–56.
- [7] P. Erdős and E. Szemerédi, ‘On sums and products of integers’, *Studies in pure mathematics*, Birkhäuser, Basel, (1983), 213–218.
- [8] J.-H. Evertse, H. P. Schlickewei, and W.M. Schmidt, ‘Linear equations in variables which lie in a multiplicative group’, *Ann. of Math.* 155(3) (2002), 807–836.
- [9] M. Garaev and C.-Y. Shen, ‘On the size of the set $A(A+1)$ ’, *Math. Z.* 265(1), (2010), 125–132.
- [10] B. Hanson, O. Roche-Newton and D. Zhelezov, ‘On iterated product sets with shifts II’, *Forthcoming* (2018).
- [11] T. G. F. Jones and O. Roche-Newton, ‘Improved bounds on the set $A(A+1)$ ’, *J. Combin. Theory Ser. A* 120(3) (2013), 515–526.

- [12] S. Konyagin and I. D. Shkredov, ‘On sum sets of sets, having small product set’, *Proc. Steklov Inst. Math.* 290 (2015), 288-299.
- [13] M. Rudnev, I. D. Shkredov and S. Stevens, ‘On the energy variant of the sum-product conjecture’, *arXiv:1607.05053* (2016).
- [14] I. D. Shkredov, ‘Some remarks on sets with small quotient set’, *Sb. Math.* 208(12) (2017), 144-158
- [15] T. Tao, V. Vu. ‘Additive combinatorics’ *Cambridge University Press* (2006).
- [16] D. Zhelezov, ‘Bourgain-Chang’s proof of the weak Erdős-Szemerédi conjecture’, *arXiv:1710.09316* (2017).

PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA, USA
E-mail address: `bwh5339@psu.edu`

JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, LINZ, AUSTRIA
E-mail address: `o.rochenewton@gmail.com`

ALFRÉD RÉNYI INSTITUTE OF MATHEMATICS, HUNGARIAN ACADEMY OF SCIENCES, BUDAPEST, HUNGARY
E-mail address: `dzhelezov@gmail.com`