Algebra & Number Theory

Volume 14
2020
No. 8

On iterated product sets with shifts, II

Brandon Hanson, Oliver Roche-Newton and Dmitrii Zhelezov

msp

msp

ALGEBRA AND NUMBER THEORY 14:8 (2020)
https://doi.org/10.2140/ant.2020.14.2239

On iterated product sets with shifts, II

Brandon Hanson, Oliver Roche-Newton and Dmitrii Zhelezov

The main result of this paper is the following: for all $b \in \mathbb{Z}$ there exists $k = k(b)$ such that

$$\max\{|A^{(k)}|, |(A+u)^{(k)}|\} \geq |A|^b,$$

for any finite $A \subset \mathbb{Q}$ and any nonzero $u \in \mathbb{Q}$. Here, $|A^{(k)}|$ denotes the k-fold product set $\{a_1 \cdots a_k : a_1, \ldots, a_k \in A\}$.

Furthermore, our method of proof also gives the following l_∞ sum-product estimate. For all $\gamma > 0$ there exists a constant $C = C(\gamma)$ such that for any $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$ and any $c_1, c_2 \in \mathbb{Q} \setminus \{0\}$, there are at most $K^C|A|^\gamma$ solutions to

$$c_1 x + c_2 y = 1, \quad (x, y) \in A \times A.$$

In particular, this result gives a strong bound when $K = |A|^\epsilon$, provided that $\epsilon > 0$ is sufficiently small, and thus improves on previous bounds obtained via the Subspace Theorem.

In further applications we give a partial structure theorem for point sets which determine many incidences and prove that sum sets grow arbitrarily large by taking sufficiently many products.

We utilize a query-complexity analogue of the polynomial Freiman–Ruzsa conjecture, due to Pälvölgyi and Zhelezov (2020). This new tool replaces the role of the complicated setup of Bourgain and Chang (2004), which we had previously used. Furthermore, there is a better quantitative dependence between the parameters.

1. Introduction

1.1. ***Background and statement of main results.*** Let A be a finite set of rational numbers and let $u \in \mathbb{Q}$ be nonzero. In this article we wish to investigate the sizes of the k-fold product sets

$$A^{(k)} := \{a_1 \cdots a_k : a_1, \ldots, a_k \in A\} \quad \text{and} \quad (A+u)^{(k)} = \{(a_1+u)\cdots(a_k+u) : a_1, \ldots, a_k \in A\}.$$

This is an instance of a sum-product problem. Recall that the Erdős and Szemerédi [1983] sum-product conjecture states that, for all $\epsilon > 0$ there exists a constant $c(\epsilon) > 0$ such that

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

holds for any $A \subset \mathbb{Z}$. Here $A + A := \{a + b : a, b \in A\}$ is the *sum set* of A, and AA is another notation for $A^{(2)}$. Erdős and Szemerédi also made the more general conjecture that for any finite $A \subset \mathbb{Z}$,

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

MSC2010: primary 11B99; secondary 11D72.
Keywords: sum-product problem, S-units, weak Erdős–Szemerédi, unbounded growth conjecture, subspace theorem.

where $kA := \{a_1 + \cdots + a_k : a_1, \ldots, a_k \in A\}$ is the *k-fold sum set*. Both of these conjectures are wide open, and it is natural to also consider them for the case when A is a subset of $\mathbb{R}$ or indeed other fields. The case when $k = 2$ has attracted the most interest. See, for example, [Konyagin and Shkredov 2015; 2016; Solymosi 2009; Tao and Vu 2006] for more background on the original Erdős–Szemerédi sum-product problem.

Most relevant to our problem is the case of general (large) k. Little is known about the Erdős–Szemerédi conjecture in this setting, with the exception of the remarkable series of work of Chang [2003] and Bourgain and Chang [2004]. This culminated in the main theorem of [Bourgain and Chang 2004]: for all $b \in \mathbb{R}$ there exists $k = k(b) \in \mathbb{Z}$ such that

$$\max\{|kA|, |A^k|\} \geq |A|^b \tag{1}$$

holds for any $A \subset \mathbb{Q}$. On the other hand, it appears that we are not close to proving such a strong result for $A \subset \mathbb{R}$.

In the same spirit as the Erdős–Szemerédi conjecture, it is expected that an additive shift will destroy multiplicative structure present in A. In particular, one expects that, for a nonzero u, at least one of $|A^{(k)}|$ or $|(A+u)^{(k)}|$ is large. The $k = 2$ version of this problem was considered in [Garaev and Shen 2010] and [Jones and Roche-Newton 2013]. The main result of this paper is the following analogue of the Bourgain–Chang theorem.

Theorem 1.1. *For all $b \in \mathbb{Z}$, there exists $k = k(b)$ such that for any finite set $A \subset \mathbb{Q}$ and any nonzero rational u,*

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

This paper is a sequel to [Hanson et al. 2019], in which the main result was the following:

Theorem 1.2. *For any finite set $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$, any nonzero $u \in \mathbb{Q}$ and any positive integer k,*

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

The proof of this result was based on an argument that Chang [2003] introduced to give similar bounds for the k-fold sum set of a set with small product set. Theorem 1.2 is essentially optimal when K is of the order $c \log|A|$, for a sufficiently small constant $c = c(k)$. However, the result becomes trivial when K is larger, for example if $K = |A|^\epsilon$ and $\varepsilon > 0$. The bulk of this paper is devoted to proving the following theorem, which gives a near optimal bound for the size of $(A+u)^{(k)}$ when $K = |A|^\varepsilon$, for a sufficiently small but positive ε.

Theorem 1.3. *Given $0 < \gamma < \frac{1}{2}$, there exists a positive constant $C = C(\gamma, k)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and any nonzero rational u,*

$$|(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)-1}}{K^{Ck}}.$$

In fact, we prove a more general version of Theorem 1.3 in terms of certain weighted energies and so-called Λ-constants (see Theorem 3.6 for the general statement that implies Theorem 1.3 — see Sections 2 and 3 for the relevant definitions of energy and Λ-constants). This more general result is what allows us to deduce Theorem 1.1.

1.2. ***A subspace type theorem — an l_∞ sum-product estimate.*** It appears that Theorem 1.1, as well as the forthcoming generalized form of Theorem 1.3, lead to some interesting new applications. To illustrate the strength of these sum-product results, we present three applications in this paper.

Our main application concerns a variant of the celebrated subspace theorem by Evertse, Schmidt and Schlikewei [Evertse et al. 2002] which, after quantitative improvements by Amoroso and Viada [2009], reads as follows: Suppose $a_1, \dots, a_k \in \mathbb{C}^*$, $\alpha_1, \dots, \alpha_r \in \mathbb{C}^*$ and define

$$\Gamma = \{\alpha_1^{z_1} \cdots \alpha_r^{z_r}, z_i \in \mathbb{Z}\},$$

so Γ is a free multiplicative group of rank r.[1] Consider the equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = 1 \tag{2}$$

with $a_i \in \mathbb{C}^*$ viewed as fixed coefficients and $x_i \in \Gamma$ as variables. A solution $(x_1, \dots, x_k)$ to (2) is called *nondegenerate* if for any nonempty $J \subsetneq \{1, \dots, k\}$

$$\sum_{i \in J} a_i x_i \neq 0.$$

Theorem 1.4 (the subspace theorem [Evertse et al. 2002; Amoroso and Viada 2009]). *The number $A(k, r)$ of nondegenerate solutions to (2) satisfies the bound*

$$A(k, r) \leq (8k)^{4k^4(k+kr+1)}. \tag{3}$$

The subspace theorem dovetails nicely to the following version of the Freiman lemma.

Theorem 1.5. *Let $(G, \cdot)$ be a torsion-free abelian group and $A \subset G$ with $|AA| < K|A|$. Then A is contained in a subgroup $G' < G$ of rank at most K.*

Now assume for simplicity that $A \subset \mathbb{Q}$ and $|AA| \leq K|A|$. Let us call such sets (this definition generalizes of course to an arbitrary ambient group) *K-almost subgroups*.[2]

We now show that it is natural to expect that the subspace theorem generalizes to K-almost subgroups with K taken as a proxy for the group rank. A straightforward corollary of Theorems 1.5 and 1.4 is as follows.

[1] The original theorem is formulated in a more general setting, namely for the division group of Γ, but we will stick to the current formulation for simplicity.

[2] One could have used a more general framework of *K-approximate subgroups* introduced by Tao. We decided to introduce a simpler definition in order to avoid technicalities. However, in the abelian setting the definitions are essentially equivalent.

Corollary 1.6 (subspace theorem for K-almost subgroups). *Let A be a K-almost subgroup. Then the number $A(k, K)$ of nondegenerate solutions $(x_1, x_2, \dots, x_k) \in A^k$ to*

$$c_1x_1 + c_2x_2 + \cdots + c_kx_k = 1$$

with fixed coefficients $c_i \in \mathbb{C}^*$ is bounded by

$$A(k, K) \le (8k)^{4k^4(k+kK+1)}.$$

Similarly to (1), the bound of Corollary 1.6 becomes trivial when A is large and K is larger than $c \log|A|$ for some small $c > 0$.

We conjecture that a much stronger polynomial bound holds.

Conjecture 1. There is a constant $c(k)$ such that Corollary 1.6 holds with the bound

$$A(k, K) \le K^{c(k)}.$$

We can support Conjecture 1 with a special case $k = 2$ and $A \subset \mathbb{Q}$, $c_i \in \mathbb{Q}$ and a somewhat weaker estimate, which we see as a proxy for the Beukers–Schlikewei theorem [Beukers and Schlickewei 1996].

Theorem 1.7 (weak Beukers–Schlikewei for K-almost subgroups). *For any $\gamma > 0$ there is $C(\gamma) > 0$ such that for any K-almost subgroup $A \subset \mathbb{Q}$ and fixed nonzero $c_1, c_2 \in \mathbb{Q}$ the number $A(2, K)$ of solutions $(x_1, x_2) \in A^2$ to*

$$c_1x_1 + c_2x_2 = 1$$

is bounded by

$$A(2, K) \le |A|^\gamma K^C.$$

One can view Theorem 1.7 as an l_∞ version of the weak Erdős–Szemerédi sum-product conjecture. The *weak Erdős–Szemerédi conjecture* is the statement that, if $|AA| \le K|A|$ then $|A + A| \ge K^{-C}|A|^2$ for some positive absolute constant C. For $A \subset \mathbb{Z}$, this result was proved in [Bourgain and Chang 2004], but the conjecture remains open over the reals.

A common approach to proving sum-product estimates is to attempt to show that, for a set A with small product set, the *additive energy* of A, which is defined as the quantity

$$E_+(A) := |\{(a, b, c, d) \in A^4 : a + b = c + d\}|,$$

is small. Indeed, this was the strategy implemented in [Chang 2003] and [Bourgain and Chang 2004], the latter of which showed that,[3] for all $\gamma > 0$, there is a constant $C = C(\gamma)$ such that for any $A \subset \mathbb{Q}$ with $|AA| \le K|A|$,

$$E_+(A) \le K^C|A|^{2+\gamma}. \tag{4}$$

[3]This is something of an over-simplification, as [Bourgain and Chang 2004] in fact proved a much more general result which bounded the multifold additive energy with weights attached.

Since there are at least $|A|^2$ trivial solutions when $\{a, b\} = \{c, d\}$, this bound is close to best possible. It then follows from a standard application of the Cauchy–Schwarz inequality that

$$|A + A| \geq \frac{|A|^{2-\gamma}}{K^C}.$$

Defining the representation function $r_{A+A}(c) = |\{(a_1, a_2) \in A \times A : a_1 + a_2 = c\}|$, it follows that

$$E_+(A) = \sum_x r_{A+A}(x)^2,$$

and so bounds for the additive energy can be viewed as l_2 estimates for this representation function.

Theorem 1.7 gives the stronger l_∞ estimate: it says that, if $|AA| \leq K|A|$ then $r_{A+A}(c) \leq K^C|A|^\gamma$ for all $c \neq 0$. This implies (4), and thus in turn the weak Erdős–Szemerédi sum-product conjecture. We prove Theorem 1.7 in Section 4.

Remark. It is highly probable that our method can be combined with the ideas of [Bourgain and Chang 2009] which would generalize Theorem 1.7 to K-almost subgroups consisting of algebraic numbers of degree at most d (though not necessarily contained in the same field extension). The upper power C is going to depend on d then, so the putative bound (using the notation of Theorem 1.7) is

$$A(2, K) \leq C'(d)|A|^\gamma K^{C(\gamma,d)}$$

with some $C, C' > 0$. We are going to consider this matter in detail elsewhere. Note, however, that proving a similar statement with no dependence on d seems to be a significantly harder problem.

1.3. *Further applications.*

1.3.1. *An inverse Szemerédi–Trotter theorem.* Theorem 1.7 can be interpreted as a partial inverse to the Szemerédi–Trotter theorem. The Szemerédi–Trotter theorem states that, if P is a finite set of points and L is a finite set of lines in $\mathbb{R}^2$, then the number of incidences $I(P, L)$ between P and L satisfies the bound

$$I(P, L) := |\{(p, l) \in P \times L : p \in l\}| = O(|P|^{2/3}|L|^{2/3} + |P| + |L|). \tag{5}$$

The term $|P|^{2/3}|L|^{2/3}$ above is dominant unless the sizes of P and L are rather imbalanced. The Szemerédi–Trotter theorem is tight, up to the multiplicative constant.

It is natural to consider the inverse question: for what sets P and L is it possible that $I(P, L) = \Omega(|P|^{2/3}|L|^{2/3})$? The known constructions of point sets which attain many incidences appear to all have some kind of lattice like structure. This perhaps suggests the loose conjecture that point sets attaining many incidences must always have some kind of additive structure, although such a conjecture seems to be far out of reach to the known methods.

However, with an additional restriction that $P = A \times A$ with $A \subset \mathbb{Q}$, Theorem 1.1 leads to the following partial inverse theorem, which states that if A has small product set then $I(P, L)$ cannot be maximal.

Theorem 1.8. *For all $\gamma \geq 0$ there exists a constant $C = C(\gamma)$ such that the following holds. Let A be a finite set of rationals such that $|AA| \leq K|A|$ and let $P = A \times A$. Then, for any finite set L of lines in the plane, $I(P, L) \leq 3|P| + |A|^{\gamma} K^{C} |L|$.*

In fact, not only does this show that $I(A \times A, L)$ cannot be maximal when $|AA|$ is small, but better still the number of incidences is almost bounded by the trivial linear terms in (5). The insistence that the point set is a direct product is rather restrictive. However, since many applications of the Szemerédi–Trotter Theorem make use of direct products, it seems likely that Theorem 1.8 could be useful. The proof is given in Section 5.

1.3.2. *Improved bound for the size of an additive basis of a set with small product set.* Theorem 1.7 also yields the following application concerning the problem of bounding the size of an additive basis considered in [Shkredov and Zhelezov 2018]. We can significantly improve the bound in the rational setting, pushing the exponent in (6) from $\frac{1}{2} + \frac{1}{442} - o_{\epsilon}(1)$ to $\frac{2}{3} - o_{\epsilon}(1)$ in the limiting case $K = |A|^{\epsilon}$.

Theorem 1.9. *For any $\gamma > 0$ there exists $C(\gamma)$ such that for an arbitrary $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and $B, B' \subset \mathbb{Q}$,*

$$S := |\{(b, b') \in B \times B' : b + b' \in A\}| \leq 2|A|^{\gamma} K^{C} \min\{|B|^{1/2}|B'| + |B|, |B'|^{1/2}|B| + |B'|\}.$$

In particular, for any $\gamma > 0$ there exists $C(\gamma)$ such that if $A \subset B + B$ then

$$|B| \geq |A|^{2/3-\gamma} K^{-C}. \tag{6}$$

The proof of Theorem 1.9 is given in Section 5.

Remark. During the preparation of the manuscript we became aware that Cosmin Pohoata has independently proved Theorem 1.9 using an earlier result of Chang and by a somewhat different method.

1.3.3. *Unlimited growth for products of difference sets.* It was conjectured in [Balog et al. 2017] that for any $b \in \mathbb{R}$ there exists $k = k(b) \in \mathbb{N}$ such that for all $A \subset \mathbb{R}$

$$|(A - A)^{k}| \geq |A|^{b}.$$

In another application of Theorem 1.1, we give a positive answer to this question under the additional restriction that $A \subset \mathbb{Q}$. In fact, we prove the following stronger statement.

Theorem 1.10. *For any $b \in \mathbb{R}$ there exists $k = k(b) \in \mathbb{N}$ such that for all $A \subset \mathbb{Q}$ and $B \subset \mathbb{Q}$ with $|B| \geq 2$,*

$$|(A + B)^{k}| \geq |A|^{b}.$$

The proof is given in Section 5.

1.4. ***Asymptotic notation.*** Throughout the paper, the standard notation $\ll$, $\gg$ is applied to positive quantities in the usual way. Saying $X \gg Y$ or $Y \ll X$ means that $X \geq cY$, for some absolute constant $c > 0$. The expression $X \approx Y$ means that both $X \gg Y$ and $X \ll Y$ hold.

1.5. ***The structure of the rest of this paper.*** In Section 2, we introduce a new kind of mixed energy, and establish some initial bounds on this energy which are strong when the set A is defined by relatively few primes ($c\log|A|$ for a sufficiently small constant c). The structure of these arguments are similar to those introduced by Chang [2003], and also used by the authors in [Hanson et al. 2019].

The goal of Section 3 is to prove the main technical result of the paper, Theorem 3.6. The statement uses the language of Λ-constants, which is a robust generalization of additive energy, and so we must first define what these constants are and identify some of their crucial properties. We also introduce the notion of query complexity, which is nicely tuned in to the techniques used and results established in Section 2. An essential tool in converting the bounds from Section 2 into strong bounds for Λ-constants is a deep new result of Zhelezov and Pálvölgyi [2020].

In Section 4, we use Theorem 3.6 to conclude the proofs of the main results of this paper, Theorems 1.1, 1.3 and 1.7. Finally, in Section 5, we give proofs of further applications of our main results.

2. A Chang-type bound for the mixed energy

Different kinds of energies play a pivotal role in the work of Chang [2003] and Bourgain and Chang [2004], as well as [Hanson et al. 2019]. In [Chang 2003], it was proved that, for any finite set of rationals A with $|AA| \le K|A|$, the *k-fold additive energy*, which is defined as the number of solutions to

$$a_1 + \cdots + a_k = a_{k+1} + \cdots a_{2k}, \quad (a_1, \dots, a_{2k}) \in A^{2k}, \tag{7}$$

is at most $(2k^2-k)^{kK}|A|^k$. A simple application of the Cauchy–Schwarz inequality then implies that the *k-fold sum set* satisfies the bound

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

Bound (7) is close to optimal when $K = c\log|A|$, but becomes trivial when $K = |A|^\varepsilon$. In [Bourgain and Chang 2004], (a weighted version of) this bound was used as a foundation, and developed considerably courtesy of some intricate decoupling arguments, in order to prove a bound for the k-fold additive energy which remains very strong when K is of the order $|A|^\varepsilon$.

In [Hanson et al. 2019], we followed a similarly strategy to that of [Chang 2003], proving that for any finite set of rationals A with $|AA| \le K|A|$ and any nonzero rational u, the *k-fold multiplicative energy* of $A+u$, which is defined as the number of solutions to

$$(a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u), \quad (a_1, \dots, a_{2k}) \in A^{2k}, \tag{8}$$

is at most $(Ck^2)^{kK}|A|^k$. Unfortunately, in adapting the approach of [Chang 2003] in order to bound the number of solutions to (8) in [Hanson et al. 2019], we encountered some difficulties with dilation invariance which made the argument rather more complicated, and we were unable to marry our methods with those of [Bourgain and Chang 2004] to obtain a strong bound when K is of order $|A|^\varepsilon$.

In this paper, we modify the approach of [Hanson et al. 2019] by working with a different form of energy. Consider the following representation function:

$$r_k(x, y) = |\{(a_1, \dots, a_k) \in A^k : a_1 \cdots a_k = x,\ (a_1 + u) \cdots (a_k + u) = y\}|.$$

Then, because r_k is supported on $A^{(k)} \times (A+u)^{(k)}$, it follows from the Cauchy–Schwarz inequality that

$$|A|^{2k} = \Bigg(\sum_{(x,y) \in A^{(k)} \times (A+u)^{(k)}} r_k(x, y) \Bigg)^2 \le |A^{(k)}||(A+u)^{(k)}| \sum_{(x,y) \in A^{(k)} \times (A+u)^{(k)}} r_k(x, y)^2. \tag{9}$$

The latter sum is the quantity

$$\tilde{E}_k(A; u) := \left| \left\{ (a_1, \dots, a_k, b_1, \dots, b_k) \in A^{2k} : \prod_{i=1}^k a_i = \prod_{i=1}^k b_i,\ \prod_{i=1}^k (a_i + u) = \prod_{i=1}^k (b_i + u) \right\} \right|.$$

We summarize this in the following lemma.

Lemma 2.1. *For any finite set $A \subset \mathbb{R}$, any $u \in \mathbb{R} \setminus \{0\}$ and any integer $k \ge 2$, we have*

$$|A|^{2k} \le |A^{(k)}||(A+u)^{(k)}|\tilde{E}_k(A; u).$$

In particular,

$$\frac{|A|^k}{\tilde{E}_k(A; u)^{1/2}} \le \max\{|A^{(k)}|, |(A+u)^{(k)}|\}.$$

Our goal is to estimate this energy and to show that, at least for sets of rationals, it cannot ever be too big.

In this section we seek to give an initial upper bound for $\tilde{E}_k(A; u)$. The strategy is close to that of Chang [2003]. There are also clear similarities with the prequel to this paper [Hanson et al. 2019].

To do this, as in [Hanson et al. 2019], we will write $\tilde{E}_k(A; u)$ in terms of Dirichlet polynomials. In this case, our Dirichlet polynomials will be functions of the form

$$F(s_1, s_2) = \sum_{(a,b) \in \mathbb{Q}^2} \frac{f(a, b)}{a^{s_1} b^{s_2}}$$

where $f : \mathbb{Q}^2 \to \mathbb{C}$ is some function of finite support. It will also be more convenient to count weighted energy. For w_a a sequence of nonnegative weights on A, let

$$\tilde{E}_{k,w}(A; u) = \sum_{\substack{a_1 \cdots a_k = b_1 \cdots b_k \\ (a_1+u) \cdots (a_k+u) = (b_1+u) \cdots (b_k+u)}} w_{a_1} \cdots w_{a_k} w_{b_1} \cdots w_{b_k}.$$

Lemma 2.2. *Let A be a finite set of rational numbers and let u be a nonzero rational number. Then, for any integer $k \ge 2$, we have*

$$\tilde{E}_{k,w}(A; u) = \lim_{T \to \infty} \frac{1}{T^2} \int_0^T \int_0^T \left| \sum_{a \in A} w_a a^{it_1} (a+u)^{it_2} \right|^{2k} dt_1 dt_2.$$

Proof. Expanding, the double integral on the right hand side is equal to

$$\sum_{a_1,\dots,a_k\in A}\sum_{b_1,\dots,b_k\in A} w_{a_1}\cdots w_{a_k}w_{b_1}\cdots w_{b_k}$$
$$\cdot\int_0^T (a_1\cdots a_k b_1^{-1}\cdots b_k^{-1})^{it_1}\,dt_1\int_0^T ((a_1+u)\cdots(a_k+u)(b_1+u)^{-1}\cdots(b_k+u)^{-1})^{it_2}\,dt_2.$$

Now

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

From this, the lemma follows. □

Let $\|\cdot\|_{2k}$ be the standard norm in $L^{2k}([0,T]^2)$, normalized such that $\|1\|_{2k}=1$. So,

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

Lemma 2.3. *Let $\mathcal{J}$ be a set of integers and decompose it as $\mathcal{J}=\mathcal{J}_1\cup\cdots\cup\mathcal{J}_N$. For each $j\in\mathcal{J}$ let $f_j:\mathbb{R}\times\mathbb{R}\to\mathbb{C}$ be a function belonging to $L^{2k}(\mathbb{R}^2)$ for every integer $k\geq 2$. Then, for every integer $k\geq 2$,*

$$\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{j\in\mathcal{J}} f_j(t_1,t_2)\right|^{2k}dt_1dt_2\right)^{1/k}$$
$$\leq N\sum_{n=1}^N\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{j\in\mathcal{J}_n} f_j(t_1,t_2)\right|^{2k}dt_1dt_2\right)^{1/k}. \quad (10)$$

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

$$\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{j\in\mathcal{J}} f_j(t_1,t_2)\right|^{2k}dt_1dt_2\right)^{1/k}=\left(\left\|\sum_{n=1}^N\sum_{j\in\mathcal{J}_n} f_j\right\|_{2k}\right)^2\leq\left(\sum_{n=1}^N\left\|\sum_{j\in\mathcal{J}_n} f_j\right\|_{2k}\right)^2, \quad (11)$$

by the triangle inequality. By the Cauchy–Schwarz inequality, (11) is bounded by

$$N\sum_{n=1}^N\left\|\sum_{j\in\mathcal{J}_n} f_j\right\|_{2k}^2. \quad (12)$$

Letting $T\to\infty$ we get the claim of the lemma. □

Corollary 2.4. *Let A be a finite set of rational numbers, partitioned as $A=A_1\cup\cdots\cup A_N$, let w be a set of nonnegative weights, and let u be a nonzero rational number. Then for any integer $k\geq 2$*

$$\tilde{E}_{k,w}(A;u)^{1/k}\leq N\sum_{j=1}^N\tilde{E}_{k,w}(A_j;u)^{1/k}.$$

Now let p be a fixed prime. For $a\in\mathbb{Q}$, let $v_p(a)$ denote the p-adic valuation of a. For a set A of rational numbers and an integer t, we let $A_t=\{a\in A: v_p(a)=t\}$.

Lemma 2.5. *Let p be a prime number. Suppose A is a finite set of rational numbers and let u be a nonzero rational number. Then for any w, a set of nonnegative weights on A, and any integer $k \geq 2$,*

$$\tilde{E}_{k,w}(A;u)^{1/k} \leq 2\binom{2k}{2} \sum_{d\in\mathbb{Z}} \tilde{E}_{k,w}(A_d;u)^{1/k}.$$

Proof. First, let $A = A_+ \cup A_-$ where $A_+ = \{a \in A : v_p(a) \geq v_p(u)\}$ and $A_- = \{a \in A : v_p(a) < v_p(u)\}$. By Corollary 2.4, we have

$$\tilde{E}_{k,w}(A;u)^{1/k} \leq 2\tilde{E}_{k,w}(A_+;u)^{1/k} + 2\tilde{E}_{k,w}(A_-;u)^{1/k}. \tag{13}$$

These two terms will be dealt with in turn, starting with $E_{k,w}(A_+;u)^{1/k}$. To do this, we first set up some more notation. For an integer d, define the function

$$f_d(t_1,t_2) := \sum_{a\in A_d} w_a a^{it_1}(a+u)^{it_2}.$$

Then, by Lemma 2.2

$$\tilde{E}_{k,w}(A_+;u) = \lim_{T\to\infty} \frac{1}{T^2}\int_0^T \int_0^T \Big|\sum_{d\geq v_p(u)} f_d(t_1,t_2)\Big|^{2k} dt_1 dt_2.$$

Expanding this expression, as in the proof of Lemma 2.2, we obtain that $\tilde{E}_{k,w}(A_+;u)$ is equal to

$$\sum_{d_1,\dots,d_{2k}\geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2}\int_0^T \int_0^T f_{d_1}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k}}(t_1,t_2)}\,dt_1dt_2. \tag{14}$$

For fixed $d_1,\dots,d_{2k}$, the quantity

$$\lim_{T\to\infty} \frac{1}{T^2}\int_0^T \int_0^T f_{d_1}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k}}(t_1,t_2)}\,dt_1dt_2.$$

gives a weighted count of the number of solutions to the system of simultaneous equations

$$a_1\cdots a_k = a_{k+1}\cdots a_{2k} \tag{15}$$

$$(a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u), \tag{16}$$

such that $a_i \in A_{d_i}$.

We claim that there are no solutions to (16), and thus also no solutions to the above system, if all of the d_i are distinct. Indeed, suppose we have a solution

$$(a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u)$$

and so

$$(a_1u^{-1}+1)\cdots(a_ku^{-1}+1) = (b_{k+1}u^{-1}+1)\cdots(b_{2k}u^{-1}+1). \tag{17}$$

Since $v_p(a_iu^{-1}) \geq 0$, expanding out both sides of (17) and simplifying gives

$$u^{-1}(a_1+\cdots+a_k) + \text{higher terms} = u^{-1}(b_{k+1}+\cdots+b_{2k}) + \text{higher terms}. \tag{18}$$

If all of the d_i are distinct, then there is some unique smallest d_i, and thus a unique smallest value of $v_p(a_i)$. But then the left hand side and the right hand side are divisible by distinct powers of p, a contradiction.

So returning to (14), we need only consider the cases in which one or more of the d_i are repeated. There are three kinds of ways in which this can happen:

(1) $d_i = d_i'$ with $1 \le i \le k$ and $k+1 \le i' \le 2k$. There are k^2 possible positions for such a pair (i, i').

(2) $d_i = d_i'$ with $1 \le i, i' \le k$. There are $\binom{k}{2}$ possible positions for such a pair (i, i').

(3) $d_i = d_i'$ with $k+1 \le i, i' \le 2k$. There are $\binom{k}{2}$ possible positions for such a pair (i, i').

Suppose we are in situation (1) above. Specifically, suppose that $d_1 = d_{2k}$. The other $k^2 - 1$ cases can be dealt with by the same argument. Then these terms in (14) can be rewritten as

$$\sum_{d_1 \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T f_{d_1}(t_1,t_2)\overline{f_{d_1}(t_1,t_2)} \sum_{d_2,\dots,d_{2k-1} \ge v_p(u)} f_{d_2}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k-1}}(t_1,t_2)}\,dt_1dt_2$$
$$= \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1,t_2)\Big|^{2(k-1)} dt_1dt_2. \quad (19)$$

Suppose we are in situation (2). Specifically, suppose that $d_1 = d_2$. The other $\binom{k}{2} - 1$ cases can be dealt with by the same argument. Then these terms in (14) can be rewritten as

$$\sum_{d_1 \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T f_{d_1}^2(t_1,t_2) \sum_{d_3,\dots,d_{2k} \ge v_p(u)} f_{d_3}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k}}(t_1,t_2)}\,dt_1dt_2$$
$$\le \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1,t_2)\Big|^{k-2} \Big|\sum_{d} f_d(\bar{t_1},t_2)\Big|^{k} dt_1dt_2$$
$$= \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1,t_2)\Big|^{2(k-1)} dt_1dt_2.$$

The same argument also works in case (3). Returning to (14), we then have

$$\tilde{E}_{k,w}(A_+;u) \le \binom{2k}{2} \sum_{d \ge v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \Big| \sum_{d \ge v_p(u)} f_d(t_1,t_2)\Big|^{2(k-1)} dt_1dt_2$$
$$\le \binom{2k}{2} \sum_{d \ge v_p(u)} \tilde{E}_{k,w}(A_d;u)^{1/k} E_{k,w}(A_+;u)^{1-1/k},$$

the last inequality being Hölder's. It therefore follows that

$$\tilde{E}_{k,w}(A_+;u)^{1/k} \le \binom{2k}{2} \sum_{d \ge v_p(u)} \tilde{E}_{k,w}(A_d;u)^{1/k}. \quad (20)$$

Now we proceed to $E_{k,w}(A_-;u)^{1/k}$. For any solution to the pair of equations

$$a_1\cdots a_k = a_{k+1}\cdots a_{2k} \quad \text{and} \quad (a_1+u)\cdots(a_k+u) = (a_{k+1}+u)\cdots(a_{2k}+u)$$

we have a solution to the equation

$$(1+ua_1^{-1})\cdots(1+ua_k^{-1}) = (1+ua_{k+1}^{-1})\cdots(1+ua_{2k}^{-1}).$$

Again, we expand and simplify, using this time that $v_p(ua_i^{-1})$ is positive, and get

$$u(a_1^{-1}+\cdots a_k^{-1}) + \text{higher terms} = u(a_{k+1}^{-1}+\cdots a_{2k}^{-1}) + \text{higher terms}.$$

As in the previous case,[4] we cannot have a unique smallest $v_p(ua_i^{-1})$. We can therefore repeat the arguments that gave us (20) in order to deduce that

$$\tilde{E}_{k,w}(A_-;u)^{1/k} \le \binom{2k}{2} \sum_{d<v_p(u)} \tilde{E}_{k,w}(A_d;u)^{1/k}. \tag{21}$$

Inserting (20) and (21) into (13) completes the proof. □

Next, this is used as a base case to give an analogous result with more primes.

Lemma 2.6. *Let $p_1,\dots,p_K$ be a prime numbers. Suppose A is a finite set of rational numbers and let u be a nonzero rational number. For a vector $\boldsymbol{d}=(d_1,\dots,d_K)$, define*

$$A_{\boldsymbol{d}} = \{a\in A : v_{p_1}(a)=d_1,\dots,v_{p_K}(a)=d_K\}.$$

Then for any w, a set of nonnegative weights on A, and for any integer $k\ge 2$,

$$\tilde{E}_{k,w}(A;u)^{1/k} \le \left(2\binom{2k}{2}\right)^K \sum_{\boldsymbol{d}\in\mathbb{Z}^K} \tilde{E}_{k,w}(A_{\boldsymbol{d}};u)^{1/k}.$$

Proof. The aim is to prove that

$$\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T \left|\sum_{\boldsymbol{d}\in\mathbb{Z}^K}\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\right|^{2k} dt_1dt_2\right)^{1/k}$$
$$\le \left(2\binom{2k}{2}\right)^K \sum_{\boldsymbol{d}\in\mathbb{Z}^K} \lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T \left|\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\right|^{2k} dt_1dt_2\right)^{1/k}. \tag{22}$$

[4] Note that here we have used the information that $a_1\cdots a_k = a_{k+1}\cdots a_{2k}$, whereas we did not use this when bounding $\tilde{E}_{k,w}(A_+;u)$.

We proceed by induction on K, the base case $K = 1$ being given by Lemma 2.5. Then

$$\begin{aligned}
&\lim_{T\to\infty}\Bigg(\frac{1}{T^2}\int_0^T\int_0^T\Bigg|\sum_{\boldsymbol{d}\in\mathbb{Z}^K}\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\Bigg|^{2k} dt_1 dt_2\Bigg)^{1/k}\\
&\quad= \lim_{T\to\infty}\Bigg(\frac{1}{T^2}\int_0^T\int_0^T\Bigg|\sum_{d_K\in\mathbb{Z}}\Bigg(\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\sum_{a\in A_{(\boldsymbol{d}',d)}} w_a a^{it_1}(a+u)^{it_2}\Bigg)\Bigg|^{2k} dt_1 dt_2\Bigg)^{1/k}\\
&\quad\le 2\binom{2k}{2}\sum_{d_K\in\mathbb{Z}}\lim_{T\to\infty}\Bigg(\frac{1}{T^2}\int_0^T\int_0^T\Bigg|\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\sum_{a\in A_{(\boldsymbol{d}',d)}} w_a a^{it_1}(a+u)^{it_2}\Bigg|^{2k} dt_1 dt_2\Bigg)^{1/k}\\
&\quad\le 2\binom{2k}{2}\sum_{d_K\in\mathbb{Z}}\Bigg(2\binom{2k}{2}\Bigg)^{K-1}\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\lim_{T\to\infty}\Bigg(\frac{1}{T^2}\int_0^T\int_0^T\Bigg|\sum_{a\in A_{(\boldsymbol{d}',d)}} w_a a^{it_1}(a+u)^{it_2}\Bigg|^{2k} dt_1 dt_2\Bigg)^{1/k}\\
&\quad= \Bigg(2\binom{2k}{2}\Bigg)^{K}\sum_{\boldsymbol{d}\in\mathbb{Z}^K}\lim_{T\to\infty}\Bigg(\frac{1}{T^2}\int_0^T\int_0^T\Bigg|\sum_{a\in A_{\boldsymbol{d}}} w_a a^{it_1}(a+u)^{it_2}\Bigg|^{2k} dt_1 dt_2\Bigg)^{1/k}.
\end{aligned}$$

The first inequality above follows from an application of Lemma 2.5. The second inequality follows from the induction hypothesis. □

3. Lambda-constants and query complexity

3.1. ***Lambda constants.*** In order to extract as much as possible from the Lemma 2.6, it will be convenient to use the language of Λ-*constants*. The main motivation behind Λ-constants is the stability property given by the forthcoming Corollary 3.2, which is absent in the nonweighted version of the energy.

We also encourage the interested reader to consult our preceding paper [Hanson et al. 2019] for a slightly more gentle introduction to Λ-constants in the setting of Dirichlet polynomials and more in-depth motivation behind this concept.

Let $A \subset \mathbb{Q}$ be a finite set and let u be a nonzero rational. Define

$$\Lambda_k(A; u) := \max \tilde{E}_{k,w}(A; u)^{1/k},$$

where the maximum is taken over all weights w on A such that

$$\sum_{a\in A} w(a)^2 = 1. \tag{23}$$

An equivalent definition is

$$\Lambda_k(A; u) := \max \lim_{T\to\infty}\Bigg\|\sum_{a\in A} w_a a^{it_1}(a+u)^{it_2}\Bigg\|_{2k}^2.$$

where the maximum is taken over the same range of weights.

Lemma 3.1. *Let $A \subset \mathbb{Q}$ be a finite set with some nonnegative real weights w_a assigned to each element $a \in A$ and let u be a nonzero rational. Then*

$$\left\| \sum_{a \in A} w_a a^{it_1} (a+u)^{it_2} \right\|_{2k}^2 \leq \Lambda_k(A;u) \left(\sum_{a \in A} w_a^2 \right) + o_{T \to \infty}(1). \tag{24}$$

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

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

which satisfy (23). It thus suffices to show that

$$\left\| \sum_{a \in A} w_a' a^{it_1} (a+u)^{it_2} \right\|_{2k}^2 \leq \Lambda_k(A;u) + o_{T \to \infty}(1),$$

which is a straightforward consequence of our definition of $\Lambda_k(A;u)$. □

We will use the following stability property of Λ-constants which helps us to work with subsets.

Corollary 3.2. *Suppose that $A \subset \mathbb{Q}$, that u is a nonzero rational and $A' \subset A$. Then*

$$\Lambda_k(A';u) \leq \Lambda_k(A;u).$$

In particular,

$$\tilde{E}_k^{1/k}(A';u) \leq \Lambda_k(A;u)|A'| \quad \text{and} \quad \tilde{E}_k(A;u) \leq \Lambda_k^k(A;u)|A|^k.$$

Proof. The first claim follows from the observation that any set of weights $\{w_a\}_{a \in A'}$ with $\sum w_a^2 = 1$ can be trivially extended to a set of weights $\{w_a\}_{a \in A}$ by assigning zero weight to the elements in $A \setminus A'$. Next observe that E_k is just $E_{k,w}$ with all the weights being one and apply Lemma 3.1. □

3.2. ***Query complexity.*** The ideas of Section 2 dovetail perfectly with the notion of the *query-complexity* of a set of rationals. Given a set $A \subset \mathbb{Q}$, we define its query complexity $q(A)$ to be the smallest integer t such that there are functions $f_i : \mathbb{Z} \to \mathbb{P}$, $i = 1, \dots, t-1$ and a fixed prime p_0 such that the vectors

$$(v_{p_0}(a), v_{p_1}(a), \dots, v_{p_{t-1}}(a)), \quad a \in A$$

are pairwise distinct, with the primes p_i defined recursively as

$$p_i = f_i(v_{p_{i-1}}(a)). \tag{25}$$

In the language of computational complexity, suppose that Alice and Bob agree on a set $A \subset \mathbb{Q}$, and then Alice secretly chooses an element $a \in A$. Bob can recover the value $a \in A$ by querying Alice iteratively at most t times, at step i evaluating p_i using (25) and asking Alice for $v_{p_i}(a)$.

The following result was recently proven by Zhelezov and Pálvölgyi [2020], building on work of Matolsci, Ruzsa, Shakan and Zhelezov [Matolcsi et al. 2020].[5]

[5] We state a version of the result which is geared towards the particular considerations of our problem; see [Zhelezov and Pálvölgyi 2020, Theorem 1.1] for a more general statement.

Theorem 3.3. *For any $\epsilon > 0$, and any set $A \subset \mathbb{Q}$ with $|AA| \le K|A|$, there exists a subset $A' \subset A$ with $|A'| \ge K^{-2/\epsilon}|A|$ and $q(A) \le \epsilon \log_2 |A|$.*

The next lemma records that any set with small query complexity also has a small Λ-constant.

Lemma 3.4. *Let $A \subset \mathbb{Q}$ with $q(A) \le t$. Then for any $u \in \mathbb{Q} \setminus \{0\}$*

$$\Lambda_k(A; u) \le \left(2\binom{2k}{2}\right)^t.$$

Proof. Write $t = q(A)$. Let w be any set of weights on A that satisfy (23). Let $a \in A$ be arbitrary. In the notation of Lemma 2.6, we have a list of primes $p_1, p_2, \dots, p_t$ defined by (25) such that the set

$$A_{\boldsymbol{d}} = \{a' \in A : v_{p_1}(a') = v_{p_1}(a), \dots, v_{p_t}(a') = v_{p_t}(a)\}$$

has cardinality exactly 1. For any singleton $\{a\} \in A$, $\tilde{E}_{k,w}(\{a\}; u) = w_a^{2k}$. Therefore, by Lemma 2.6,

$$\tilde{E}_{k,w}(A'; u)^{1/k} \le \left(2\binom{2k}{2}\right)^t \sum_{a \in A'} w_a^2 = \left(2\binom{2k}{2}\right)^t. \qquad \square$$

The following result is important generalization of the previous one; it shows that if A contains a large subset with small query complexity then A itself has small Λ-constant.

Lemma 3.5. *Let $A \subset \mathbb{Q}^*$ be a finite set with $|AA| \le K|A|$ and let u be a nonzero rational number. Suppose that $A' \subset A$ and $q(A') = t$. Then*

$$\Lambda_k(A; u) \le K^4 \left(\frac{|A|}{|A'|}\right)^2 \left(2\binom{2k}{2}\right)^t.$$

Proof. Let w be an arbitrary set of weights on A such that $\sum_{a \in A} w(a)^2 = 1$. We seek a suitable upper bound for

$$\left\| \sum_{a \in A} w_a a^{it_1} (a+u)^{it_2} \right\|_{2k}^2.$$

For a fixed $z \in A/A'$, define a set of weights $w^{(z)}$ on zA' by taking $w^{(z)}(za') = w(za')$ if $za' \in A$ and $w^{(z)}(za') = 0$ otherwise. Define

$$R_{(A/A'),A'}(x) := |\{(s, a) \in (A/A') \times A' : sa = x\}|$$

and note that $R_{(A/A'),A'}(x) \ge |A'|$ for all $x \in A$. This is because, for all $a' \in A'$, $x = (x/a')a'$. Therefore,

$$\begin{aligned} \left\| \sum_{z \in A/A'} \sum_{a' \in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \right\|_{2k} &= \left\| \sum_{a \in A} R_{(A/A'),A'}(a) w(a) a^{it_1} (a+u)^{it_2} \right\|_{2k} \\ &\ge |A'| \left\| \sum_{a \in A} w_a a^{it_1} (a+u)^{it_2} \right\|_{2k}. \end{aligned}$$

On the other hand, by the triangle inequality and Lemma 3.1

$$\Big\| \sum_{z\in A/A'} \sum_{a'\in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \Big\|_{2k} \le \sum_{z\in A/A'} \Big\| \sum_{a'\in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \Big\|_{2k}$$
$$\le \sum_{z\in A/A'} \Lambda_k(zA';u)^{1/2} + o_{T\to\infty}(1).$$

Since $q(A') = t$, it follows from Lemma 3.4 that $\Lambda_k(zA';u) = \Lambda_k(A';u/z) \le \big(2\binom{2k}{2}\big)^t$. We also have

$$|A/A'| \le |A/A| \le \frac{|AA|^2}{|A|} \le K^2|A|,$$

by the Ruzsa triangle inequality (see [Tao and Vu 2006]). It therefore follows that

$$\Big\| \sum_{a\in A} w_a a^{it_1}(a+u)^{it_2} \Big\|_{2k} \le K^2 \left(\frac{|A|}{|A'|}\right) \left(2\binom{2k}{2}\right)^{t/2} + o_{T\to\infty}(1),$$

and the result follows. □

Combining this with Theorem 3.3 gives the following, which is our main result concerning Λ-constants.

Theorem 3.6. *Given $0 < \gamma < \frac{1}{2}$, there exists a positive constants $C = C(\gamma, k)$ such that for any finite $A \subset \mathbb{Q}^*$ with $|AA| = K|A|$ and any nonzero rational u,*

$$\Lambda_k(A;u) \le K^C |A|^\gamma.$$

Proof. Apply Theorem 3.3 with $\epsilon = \gamma/\log_2(4k)$. There exists $A' \subset A$ with $|A'| \ge K^{-2/\epsilon}|A|$ and $q(A) \le \epsilon \log_2|A|$. Then by Lemma 3.5

$$\Lambda_k(A;u) \le K^4 \left(\frac{|A|}{|A'|}\right)^2 \left(2\binom{2k}{2}\right)^{\epsilon \log_2|A|} \le K^{4+4/\epsilon}|A|^{\epsilon \log_2(4k)}.$$ □

Observe that we can in fact take $C(\gamma, k)$ in Theorem 3.6 to be $4 + 4\log_2(4k)/\gamma$.

4. Concluding the proofs

In this section we conclude the proof of Theorem 1.1, which is the main theorem of this paper, and Theorem 1.7 announced in the introduction.

We will use the Plünnecke–Ruzsa theorem. See [Petridis 2012] for a simple inductive proof. Following convention, we state it using additive notation, although it will be used in the multiplicative setting.

Theorem 4.1. *Let A be a subset of a commutative additive group G with $|A + A| \le K|A|$. Then for any $h \in \mathbb{N}$,*

$$|hA| \le K^h |A|.$$

For the convenience of the reader, we restate Theorem 1.1.

Theorem 4.2. *For all $b \in \mathbb{Z}$, there exists $k = k(b)$ such that for any finite set $A \subset \mathbb{Q}^*$ and any nonzero rational u,*

$$\max\{|A^{(k)}|, |(A+u)^{(k)}|\} \geq |A|^b$$

Proof. Fix b and assume that

$$|A^{(k)}| < |A|^b$$

for some sufficiently large $k = 2^l$. The value of l (and thus also that of k) will be specified at the end of the proof. Since $|A^{(2^l)}| < |A|^b$, it follows that

$$\frac{|A^{(2^l)}|}{|A^{(2^{l-1})}|}\frac{|A^{(2^{l-1})}|}{|A^{(2^{l-2})}|}\cdots\frac{|A^{(2)}|}{|A|} < |A|^{b-1}$$

and thus there is some integer $l_0 \leq l$ such that

$$\frac{|A^{(2^{l_0+1})}|}{|A^{(2^{l_0})}|} < |A|^{(b-1)/l}.$$

Therefore, writing $k_0 = 2^{l_0}$ and $B = A^{(k_0)}$, we have

$$|BB| < |B||A|^{(b-1)/l}.$$

Also, for any nonzero $\lambda \in \mathbb{Q}$, $|(\lambda B)(\lambda B)| < |B||A|^{(b-1)/l}$. Therefore, by Theorem 3.6,

$$\Lambda_h(\lambda B; u) \leq |A|^{C(b-1)/l}|B|^{\gamma} \leq |A|^{C(b-1)/l+\gamma b}$$

where $C = C(h, \gamma)$ and h, γ will be specified later.

Now, for some $\lambda \in \mathbb{Q}$, we have $A \subset \lambda B$, and thus by Corollary 3.2 and Lemma 2.1

$$\frac{|A|^2}{\max\{|A^{(h)}|, |(A+u)^{(h)}|\}^{2/h}} \leq \tilde{E}_h^{1/h}(A; u) \leq |A|\Lambda_h(\lambda B; u) \leq |A|^{1+C(b-1)/l+\gamma b}.$$

This rearranges to

$$\max\{|A^{(h)}|, |(A+u)^{(h)}|\} \geq |A|^{h/2(1-C(b-1)/l-\gamma b)}.$$

Choose $\gamma = 1/100b$ and $h = 4b$. Then $C = C(h, \gamma) = C(b)$ and we have

$$\max\{|A^{(h)}|, |(A+u)^{(h)}|\} \geq |A|^{h/2(99/100-C(b)(b-1)/l)}.$$

Then choose $l = (b-1)4C$ to get

$$\max\{|A^{(h)}|, |(A+u)^{(h)}|\} \geq |A|^{h/4} = |A|^b.$$

Note that the choice of l depends only on b and thus $k = 2^{4C(b-1)} = k(b)$. In particular, since $k > h$, we conclude that

$$\max\{|A^{(k)}|, |(A+u)^{(k)}|\} \geq |A|^b,$$

as required. □

If we use the value of $C(\gamma, k)$ indicated at the end of the proof of Theorem 3.6 to keep track of the constants in this argument, it follows that we can take $k = 2^{O(b^2 \log b)}$. To be even more precise, it gives

$$k = (16b)^{1616b^2}.$$

This compares favorably with the dependency in the corresponding sum-product bound of Bourgain and Chang [2004], where they commented that it was possible to take $k = 2^{O(b^4)}$. A similar quantitative improvement for the classical iterated sum-product problem is possible by studying the recent paper of Zhelezov and Pálvölgyi [2020] and filling in some extra details.

Theorem 3.6 also implies Theorem 1.3. The statement is repeated below for the convenience of the reader.

Theorem 4.3. *Given $0 < \gamma < \frac{1}{2}$ and any integer $k \geq 2$, there exists a positive constant $C = C(\gamma, k)$ such that for any finite $A \subset \mathbb{Q}^*$ with $|AA| = K|A|$ and any nonzero rational u,*

$$|(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)-1}}{K^{Ck}}.$$

Proof. Define $w(a) = 1/|A|^{1/2}$ for all $a \in A$ and note that (23) is satisfied. Furthermore, for this set of weights w,

$$\tilde{E}_{k,w}(A; u) = \frac{\tilde{E}_k(A; u)}{|A|^k} \geq \frac{|A|^k}{|A^{(k)}||(A+u)^{(k)}|}, \tag{26}$$

where the inequality comes from Lemma 2.1. It follows from Theorem 3.6 that there exists a constant $C = C(\gamma, k)$ such that for any $u \in \mathbb{Q} \setminus \{0\}$, $\Lambda_k(A; u) \leq K^C |A|^\gamma$. Consequently, by the definition of $\Lambda_k(A; u)$,

$$\tilde{E}_{k,w}(A; u) \leq K^{Ck}|A|^{\gamma k}.$$

Combining this with (26), it follows that

$$|A^{(k)}||(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)}}{K^{Ck}}. \tag{27}$$

Finally, since $|AA| \leq K|A|$, it follows from the Plünnecke–Ruzsa Theorem that $|A^{(k)}| \leq K^k|A|$. Inserting this into (27) completes the proof. □

We now turn to the proof of Theorem 1.7. Recall its statement.

Theorem 4.4. *For any $\gamma > 0$ there is $C(\gamma) > 0$ such that for any K-almost subgroup $A \subset \mathbb{Q}^*$ and fixed nonzero $c_1, c_2 \in \mathbb{Q}$ the number $A(2, K)$ of solutions $(x_1, x_2) \in A^2$ to*

$$c_1 x_1 + c_2 x_2 = 1$$

is bounded by

$$A(2, K) \leq |A|^\gamma K^C.$$

Proof. Let $S \subset A$ be the set of $x_1 \in A$ such that $c_1x_1 + c_2x_2 = 1$ for some $x_2 \in A$. Since the projection $(x_1, x_2) \to x_1$ is injective, it suffices to bound the size of S.

Since $S \subset A$, by Theorem 3.6 and Corollary 3.2 for any nonzero u

$$\tilde{E}_k(S; u) \le K^{kC(\gamma',k)}|A|^{k\gamma'}|S|^k$$

with the parameters $0 < \gamma' < \frac{1}{2}$, $k \ge 2$ to be taken in due course.

In particular, by Lemma 2.1

$$|S|^k \le (K^{kC(\gamma',k)}|A|^{k\gamma'}|S|^k)^{1/2} \max\{|S^k|, |(S - 1/c_1)^k|\}.$$

On the other hand, $S \subseteq A$ and $(S - 1/c_1) \subseteq -(c_2/c_1)A$, so by the Plünnecke–Ruzsa inequality

$$\max\{|S^k|, |(S - 1/c_1)^k|\} \le |A^{(k)}| \le K^k|A|.$$

We then have

$$|S| \le |A|^{\gamma'+2/k}K^{C+2},$$

and taking $k = \lfloor 2/\gamma' \rfloor + 1$ and $\gamma' = \gamma/2$, the claim follows. □

5. Further applications

Proof of Theorem 1.8. Recall that Theorem 1.8 is the following statement. For all $\gamma \ge 0$ there exists a constant $C = C(\gamma)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| \le K|A|$ and any finite set L of lines in the plane, $I(P, L) \le 3|P| + |A|^\gamma K^C|L|$, where $P = A \times A$.

First of all, observe that horizontal and vertical lines contribute a total of at most $2|P|$. This is because each point $p \in P$ can belong to at most one horizontal and one vertical line. Similarly, lines through the origin contribute at most $|P| + |L|$ incidences, since each point aside from the origin belongs to at most one such line, and the origin itself may contribute $|L|$ incidences.

It remains to bound incidences with lines of the form $y = mx + c$, with $m, c \ne 0$. Let $l_{m,c}$ denote the line with equation $y = mx + c$. Note that, if $m \notin \mathbb{Q}$ then $l_{m,c}$ contains at most one point from P. Indeed, suppose $l_{m,c}$ contains two distinct points (x, y) and (x', y') from P. In particular, since $A \subset \mathbb{Q}$, $x, y, x', y' \in \mathbb{Q}$. Then $l_{m,c}$ has direction $m = (y - y')/(x - x')$. Therefore, lines $l_{m,c}$ with irrational slope m contribute at most $|L|$ incidences.

Next, suppose that $m \in \mathbb{Q}$ and $c \notin \mathbb{Q}$. Then $l_{m,c}$ does not contain any points from P, since if it did then we would have a solution to $y = mx + c$, but the left hand side is rational and the right hand side is irrational.

It remains to consider the case when $m, c \in \mathbb{Q}^*$. An application of Theorem 1.7 implies that $|l_{m,c} \cap P| \le K^C|A|^\gamma$. Therefore, these lines contribute a total of at most $|L|K^C|A|^\gamma$ incidences.

Adding together the contributions from these different types of lines completes the proof. □

Proof of Theorem 1.9. Recall that Theorem 1.9 states that, for any $\gamma > 0$ there exists $C(\gamma)$ such that for an arbitrary $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and $B, B' \subset \mathbb{Q}$,

$$S := |\{(b, b') \in B \times B' : b + b' \in A\}| \leq 2|A|^{\gamma} K^{C} \min\{|B|^{1/2}|B'| + |B|, |B'|^{1/2}|B| + |B'|\}.$$

We will prove that

$$S \leq 2|A|^{\gamma} K^{C}(|B'|^{1/2}|B| + |B'|). \tag{28}$$

Since the roles of B and B' are interchangeable, (28) also implies that $S \leq 2|A|^{\gamma} K^{C}(|B|^{1/2}|B'| + |B|)$, and thus completes the proof.

Let $\gamma > 0$ and $C(\gamma)$, given by Theorem 1.7, be fixed. Without loss of generality assume that $S \geq 2|B'|$ as otherwise the claimed bound is trivial.

For each $b \in B$ define

$$S_b := \{b' \in B' : b + b' \in A\},$$

and similarly for $b' \in B'$

$$T_{b'} := \{b \in B : b' + b \in A\}.$$

It follows from Theorem 1.7 that for $b_1, b_2 \in B$ with $b_1 \neq b_2$

$$|S_{b_1} \cap S_{b_2}| \leq |A|^{\gamma} K^{C}$$

since each $x \in S_{b_1} \cap S_{b_2}$ gives a solution $(a, a') := (b_1 + x, b_2 + x)$ to

$$a - a' = b_1 - b_2$$

with $a, a' \in A$.

On the other hand, by double-counting and the Cauchy–Schwarz inequality,

$$\sum_{b \in B} |S_b| + \sum_{b_1, b_2 \in B : b_1 \neq b_2} |S_{b_1} \cap S_{b_2}| = \sum_{b' \in B'} |T_{b'}|^2 \geq |B'|^{-1} \Big(\sum_{b' \in B'} |T_{b'}|\Big)^2 = |B'|^{-1} S^2.$$

Therefore,

$$\sum_{b_1, b_2 \in B : b_1 \neq b_2} |S_{b_1} \cap S_{b_2}| \geq |B'|^{-1} S^2 - \sum_{b \in B} |S_b| = |B'|^{-1} S^2 - S \geq \tfrac{1}{2} |B'|^{-1} S^2$$

by our assumption.

The left-hand side is at most $|B|^2 |A|^{\gamma} K^{C}$, and so

$$S \leq (2|A|^{\gamma} K^{C})^{1/2} |C|^{1/2} |B'|,$$

which completes the proof. □

Proof of Theorem 1.10. Recall that Theorem 1.10 states that for all b there exists k such that for all $A, B \subset \mathbb{Q}$ with $|B| \geq 2$, $|(A + B)^k| \geq |A|^b$.

Since $|B| \geq 2$, there exist two distinct elements $b_1, b_2 \in B$. Apply Theorem 1.1 to conclude that for all b there exists $k = k(b)$ with

$$|(A+B)^k| \geq \max\{|(A+b_1)^k|, |((A+b_1)+(b_2-b_1))^k|\} \geq |A|^b. \qquad \square$$

Acknowledgements

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

We thank Brendan Murphy, Cosmin Pohoata, Imre Ruzsa and Endre Szemerédi for helpful conversations.

References

[Amoroso and Viada 2009] F. Amoroso and E. Viada, "Small points on subvarieties of a torus", *Duke Math. J.* **150**:3 (2009), 407–442. MR Zbl

[Balog et al. 2017] A. Balog, O. Roche-Newton, and D. Zhelezov, "Expanders with superquadratic growth", *Electron. J. Combin.* **24**:3 (2017), art. id. 3.14. MR Zbl

[Beukers and Schlickewei 1996] F. Beukers and H. P. Schlickewei, "The equation $x + y = 1$ in finitely generated groups", *Acta Arith.* **78**:2 (1996), 189–199. MR Zbl

[Bourgain and Chang 2004] 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. MR Zbl

[Bourgain and Chang 2009] J. Bourgain and M.-C. Chang, "Sum-product theorems in algebraic number fields", *J. Anal. Math.* **109** (2009), 253–277. MR Zbl

[Chang 2003] M.-C. Chang, "The Erdős–Szemerédi problem on sum set and product set", *Ann. of Math.* (2) **157**:3 (2003), 939–957. MR Zbl

[Erdős and Szemerédi 1983] P. Erdős and E. Szemerédi, "On sums and products of integers", pp. 213–218 in *Studies in pure mathematics*, edited by P. Erdős, Birkhäuser, Basel, 1983. MR Zbl

[Evertse et al. 2002] J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, "Linear equations in variables which lie in a multiplicative group", *Ann. of Math.* (2) **155**:3 (2002), 807–836. MR Zbl

[Garaev and Shen 2010] M. Z. Garaev and C.-Y. Shen, "On the size of the set $A(A+1)$", *Math. Z.* **265**:1 (2010), 125–132. MR Zbl

[Hanson et al. 2019] B. Hanson, O. Roche-Newton, and D. Zhelezov, "On iterated product sets with shifts", *Mathematika* **65**:4 (2019), 831–850. MR Zbl

[Jones and Roche-Newton 2013] 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. MR Zbl

[Konyagin and Shkredov 2015] S. V. Konyagin and I. D. Shkredov, "On sum sets of sets having small product set", *Proc. Steklov Inst. Math.* **290**:1 (2015), 288–299. MR Zbl

[Konyagin and Shkredov 2016] S. V. Konyagin and I. D. Shkredov, "New results on sums and products in $\mathbb{R}$", *Proc. Steklov Inst. Math.* **294**:1 (2016), 78–88. Zbl

[Matolcsi et al. 2020] D. Matolcsi, I. Ruzsa, G. Shakan, and D. Zhelezov, "An analytic approach to cardinalities of sumsets", preprint, 2020. arXiv

[Petridis 2012] G. Petridis, "New proofs of Plünnecke-type estimates for product sets in groups", *Combinatorica* **32**:6 (2012), 721–733. MR Zbl

[Shkredov and Zhelezov 2018] I. D. Shkredov and D. Zhelezov, "On additive bases of sets with small product set", *Int. Math. Res. Not.* **2018**:5 (2018), 1585–1599. MR Zbl

[Solymosi 2009] J. Solymosi, "Bounding multiplicative energy by the sumset", *Adv. Math.* **222**:2 (2009), 402–408. MR Zbl

[Tao and Vu 2006] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math. **105**, Cambridge Univ. Press, 2006. MR Zbl

[Zhelezov and Pálvölgyi 2020] D. Zhelezov and D. Pálvölgyi, "Query complexity and the polynomial Freiman–Ruzsa conjecture", preprint, 2020. arXiv

Communicated by Andrew Granville
Received 2020-01-28 Revised 2020-03-30 Accepted 2020-05-01

brandon.w.hanson@gmail.com *Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, GA, United States*

o.rochenewton@gmail.com *Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria*

dzhelezov@gmail.com *Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, Budapest, Hungary*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2020 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 14 No. 8 2020