Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences (ÖAW)

On iterated product sets with shifts II

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

RICAM-Report 2018-19

ON ITERATED PRODUCT SETS WITH SHIFTS II

BRANDON HANSON, OLIVER ROCHE-NEWTON, AND DMITRII ZHELEZOV

Abstract. 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 non-zero $u \in \mathbb{Q}$. Here, $|A^{(k)}|$ denotes the k-fold product set $\{a_1 \cdots a_k : a_1, \dots, a_k \in A\}$.

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.

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 non-zero. In this article we wish to investigate the sizes of the k-fold product sets

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

and

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

This is an instance of a sum-product problem. Recall that the Erdős-Szemerédi [7] 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 $A \subset \mathbb{Z}$,

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

where $kA := \{a_1 + \cdots + a_k : a_1, \dots, a_k \in A\}$ 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, [12], [13], [16], [17] and the references contained therein 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

[6] and Bourgain-Chang [4]. This culminated in the main theorem of [4]: 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 non-zero u, at least one of $|A^{(k)}|$ or $|(A+u)^{(k)}|$ is large. The $k = 2$ version of this problem was considered in [9] and [11]. 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 non-zero rational u,*

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

This paper is a sequel to [10], 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 non-zero $u \in \mathbb{Q}$ 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 [6] 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 $0 < \gamma < 1/2$, there exists a positive constant $C = C(\gamma, k)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and any non-zero 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 3.7 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 generalised 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 [8] which, after quantitative improvements by Amoroso and Viada [1], 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[1] of rank r. 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 non-empty $J \subsetneq \{1, \dots, k\}$

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

Theorem 1.4 (The Subspace Theorem, [8] [1])**.** *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 generalises to K-almost subgroups with K taken as a proxy for the group rank. A straightforward corollary of Theorem 1.5 and Theorem 1.4 is as follows.

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

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

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

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

Similarly to Theorem 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.

[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've 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.

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

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

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 [3].

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 non-zero $c_1, c_2 \in \mathbb{Q}$ 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

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

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 $|AA| \leq K|A|$ then $|A+A| \geq K^{-C}|A|^2$ for some positive absolute constant C. For $A \subset \mathbb{Z}$, this result was proved in [4], 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 [6] and [4], the latter of which showed[3] that, for all $\gamma > 0$, there is a constant $C = C(\gamma)$ such that for any $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$,

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

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.

[3]This is something of an over-simplification, as [4] in fact proved a much more general result which bounded the multi-fold additive energy with weights attached.

Remark. *It is highly probable that our method can be combined with the ideas of* [5] *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

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

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 10.

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 [15]. We can significantly improve the bound in the rational setting, pushing the exponent in (6) from $1/2 + 1/442 - o_{\epsilon}(1)$ to $2/3 - o_{\epsilon}(1)$ 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 $B, B' \subset \mathbb{Q}$,*

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

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 10.

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 [2] 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 10.

1.4. **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 multiplicative doubling K is of the order $c \log |A|$ for a sufficiently small constant c. The structure of these arguments are similar to those introduced by Chang in [6], and also used by the authors in [10]. We also introduce the notion of separating constants in section 2, which generalises that of the aforementioned mixed energy.

Section 3 begins by stating the crucial Theorem 3.1, which states that is $|AA|$ is small then there is a large subset $A' \subset A$ with a good separating constant. The rest of the section introduces the language of Λ-constants and some of their crucial properties. These properties are then used in section 4 to conclude the proofs of the main results of this paper, Theorems 1.1, 1.3 and 1.7, using Theorem 3.1 as a black box.

It then remains to prove Theorem 3.1. This is a long and technical proof, where we need to amplify the bounds obtained in section 2 in several stages. This process happens in sections 5, 6, 7,

8 and 9, and closely follows the exposition in [18].[4] Finally, in section 10, 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 [6] and Bourgain-Chang [4], as well as [10]. In [6], it was proved that, for any finite set of rationals A with $|AA| \leq K|A|$, the *k-fold additive energy*, which is defined as the number of solutions to

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

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

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

Bound (7) is close to optimal when $K = c \log |A|$, but becomes trivial when $K = |A|^{\varepsilon}$. In [4], (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 [10], we followed a similarly strategy to that of [6], proving that for any finite set of rationals A with $|AA| \leq K|A|$ and any non-zero rational u, the *k-fold multiplicative energy* of $A + u$, which is defined as the number of solutions to

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

is at most $(Ck^2)^{kK}|A|^k$. Unfortunately, in adapting the approach of [6] in order to bound the number of solutions to (8) in [10], 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 [4] to obtain a strong bound when K is of order $|A|^{\varepsilon}$.

In this paper, we modify the approach of [10] by working with a different form of energy. Consider the following representation function:

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

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

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

The innermost sum is the quantity

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

[4] We recommend that the reader consult [18] for more information about the proof of the Bourgain-Chang Theorem, and particularly the early parts of [18], where an attempt is made to outline some heuristics of the proof.

We summarise 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 $k \geq 2$, we have*

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

In particular,

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

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 [6]. There are also clear similarities with the prequel to this paper [10].

To do this, as in [10], 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 non-negative 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 non-zero rational number. Then, for any integer $k \geq 2$, we have*

$$\tilde{E}_{k,w}(A;u) = \lim_{T\to\infty}\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{a\in A} w_a a^{it_1}(a+u)^{it_2}\right|^{2k} dt_1dt_2.$$

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

$$\sum_{a_1,\dots,a_k\in A}\sum_{b_1,\dots,b_k\in A} w_{a_1}\cdots w_{a_k}w_{b_1}\cdots w_{b_k}\cdot$$
$$\cdot\int_0^T(a_1\cdots a_kb_1^{-1}\cdots b_k^{-1})^{it_1}dt_1\int_0^T((a_1+u)\cdots(a_k+u)(b_1+u)^{-1}\cdots(b_k+u)^{-1})^{it_2}dt_2.$$

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 $L^{2k}[0,T]^2$, normalised 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 $L^{2k}\left(\mathbb{R}^2\right)$ for every integer $k \geq 2$. Then, for every integer $k \geq 2$,*

$$\lim_{T\to\infty} \left(\frac{1}{T^2} \int_0^T \int_0^T \left| \sum_{j\in\mathcal{J}} f_j(t_1,t_2) \right|^{2k} dt_1 dt_2 \right)^{1/k} \leq N \sum_{n=1}^{N} \lim_{T\to\infty} \left(\frac{1}{T^2} \int_0^T \int_0^T \left| \sum_{j\in\mathcal{J}_n} f_j(t_1,t_2) \right|^{2k} dt_1 dt_2 \right)^{1/k}. \quad (10)$$

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

$$\left(\frac{1}{T^2} \int_0^T \int_0^T \left| \sum_{j\in\mathcal{J}} f_j(t_1,t_2) \right|^{2k} dt_1 dt_2 \right)^{1/k} = \left(\left\| \sum_{n=1}^{N} \sum_{j\in\mathcal{J}_n} f_j \right\|_{2k} \right)^2 \leq \left(\sum_{n=1}^{N} \left\| \sum_{j\in\mathcal{J}_n} f_j \right\|_{2k} \right)^2, \quad (11)$$

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 non-negative weights, and let u be a non-zero 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 non-zero rational number. Then for any w, a set of non-negative 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

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

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

$$\tilde{E}_{k,w}(A_+;u) = \lim_{T\to\infty}\frac{1}{T^2}\int_0^T\int_0^T \left|\sum_{d\geq v_p(u)} f_d(t_1,t_2)\right|^{2k} dt_1dt_2.$$

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 $1\leq i\leq k$ and $k+1\leq i'\leq 2k$. There are k^2 possible positions for such a pair (i,i'),
(2) $d_i = d_i'$ with $1\leq i,i'\leq k$. There are $\binom{k}{2}$ possible positions for such a pair (i,i'),
(3) $d_i = d_i'$ 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 $d_1 = d_{2k}$. The other $k^2 - 1$ cases can be dealt with by the same argument. Then these terms in (14) can be rewritten as

$$\sum_{d_1 \geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T f_{d_1}(t_1,t_2)\overline{f_{d_1}(t_1,t_2)} \sum_{d_2,\dots,d_{2k-1} \geq v_p(u)} f_{d_2}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k-1}}(t_1,t_2)}dt_1dt_2$$

$$= \sum_{d \geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \left| \sum_{d \geq v_p(u)} f_d(t_1,t_2) \right|^{2(k-1)} dt_1dt_2. \quad (19)$$

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

$$\sum_{d_1 \geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T f_{d_1}^2(t_1,t_2) \sum_{d_3,\dots,d_{2k} \geq v_p(u)} f_{d_3}(t_1,t_2)\cdots f_{d_k}(t_1,t_2)\overline{f_{d_{k+1}}(t_1,t_2)}\cdots\overline{f_{d_{2k}}(t_1,t_2)}dt_1dt_2$$

$$\leq \sum_{d \geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \left| \sum_{d \geq v_p(u)} f_d(t_1,t_2) \right|^{k-2} \left| \sum_d \overline{f_d(t_1,t_2)} \right|^k dt_1dt_2$$

$$= \sum_{d \geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \left| \sum_{d \geq v_p(u)} f_d(t_1,t_2) \right|^{2(k-1)} dt_1dt_2.$$

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

$$\tilde{E}_{k,w}(A_+;u) \leq \binom{2k}{2} \sum_{d \geq v_p(u)} \lim_{T\to\infty} \frac{1}{T^2} \int_0^T \int_0^T |f_d(t_1,t_2)|^2 \left| \sum_{d \geq v_p(u)} f_d(t_1,t_2) \right|^{2(k-1)} dt_1dt_2$$

$$\leq \binom{2k}{2} \sum_{d \geq v_p(u)} \tilde{E}_{k,w}(A_d;u)^{1/k} E_{k,w}(A_+;u)^{1-1/k},$$

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

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

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

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

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

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 [5] , 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

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

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 non-zero 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 non-negative weights on A, and for any integer $k\geq 2$,

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

Proof. The aim is to prove that

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

[5]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

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

$$=\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{d_K\in\mathbb{Z}}\left(\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\sum_{a\in A_{(\boldsymbol{d}',d)}}w_a a^{it_1}(a+u)^{it_2}\right)\right|^{2k}dt_1dt_2\right)^{1/k}$$

$$\leq 2\binom{2k}{2}\sum_{d_K\in\mathbb{Z}}\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\sum_{a\in A_{(\boldsymbol{d}',d)}}w_a a^{it_1}(a+u)^{it_2}\right|^{2k}dt_1dt_2\right)^{1/k}$$

$$\leq 2\binom{2k}{2}\sum_{d_K\in\mathbb{Z}}\left(2\binom{2k}{2}\right)^{K-1}\sum_{\boldsymbol{d}'\in\mathbb{Z}^{K-1}}\lim_{T\to\infty}\left(\frac{1}{T^2}\int_0^T\int_0^T\left|\sum_{a\in A_{(\boldsymbol{d}',d)}}w_a a^{it_1}(a+u)^{it_2}\right|^{2k}dt_1dt_2\right)^{1/k}$$

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

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

2.1. **Separating constants.** The following definition, which follows the terminology used in [18], is central to this paper. Let ψ be an arbitrary real number. A set $X \subset \mathbb{Q}$ is said[6] to be *ψ-separating* if for any non-zero $u \in \mathbb{Q}$, any set finite $Z \subset \mathbb{Q}$ of the form

$$Z = \bigcup_{x\in X} xY_x$$

such that $(x, Y_{x'}) = 1$ for all $x, x' \in X$, and any set of weights w on Z

$$\tilde{E}_{k,w}(Z;u)^{1/k} \leq \psi\sum_{x\in X}\tilde{E}_{k,w}(xY_x;u)^{1/k}.$$

A first observation about separating constants comes in the form of the following claim.

Claim 2.7. *Any finite $A \subset \mathbb{Q}$ is $|A|$-separating.*

This claim follows immediately from Corollary 2.4. Combining this new definition with Lemma 2.5, we can also record the following corollary.

Corollary 2.8. *Let p be a prime number. Suppose A is of the form $A = \{p^h : h \in H\}$ for some finite set $H \subset \mathbb{Z}$. Then A is $2\binom{2k}{2}$-separating.*

[6]Strictly speaking, we should perhaps include k in this definition and say that a set is (ψ, k)-separating if it satisfied the stated conditions. In order to simplify the notation we do not do this. Instead, we can think of $k \geq 2$ as a fixed integer throughout the remainder of the paper, unless stated otherwise. Henceforth, this condition on k will be omitted from statements of results.

With this definition of the separating constant, we can use Lemma 2.6 to get a first bound for the separating constant of a set with small product set. Once again, this bound is good when $K \leq c \log |A|$ for a sufficiently small constant c.

To do this, we recall an argument of Chang [6] which uses Freiman's Lemma to show that a set of rationals with small product set is determined by a small number of prime factors. Let A be a set of rationals and let

$$\mathcal{P} := \{p : p \text{ is prime and there exists } a \in A, v_p(a) \neq 0\} = \{p_1, \dots, p_t\}$$

be the set of primes dividing some element of A. Abusing notation slightly, we define a map $\mathcal{P} : A \to \mathbb{Z}^t$ 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 $A \subset Q$ to be the least dimension of an affine space L containing $\mathcal{P}(A)$.

Theorem 2.9 (Freiman's Lemma)**.** *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 2.10. *Let $A \subset \mathbb{Q}$ be finite with $|AA| = K|A|$. Then, A is $\left(2\binom{2k}{2}\right)^K$-separating.*

Proof. It follows from Freiman's Lemma that if $|AA| \leq K|A|$ with $|A|$ sufficiently large, then A has multiplicative dimension at most K.

This means that there is a set of $\{p_1, \dots, p_K\}$ of primes and a set of vectors $\mathcal{J} \subset \mathbb{Z}^K$ such that

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

where each $x_{\boldsymbol{j}}$ is a rational number coprime[7] to $p_1 \cdots p_K$. For $\boldsymbol{j} = (j_1, \dots, j_K) \in \mathcal{J}$, write $a_{\boldsymbol{j}} = p_1^{j_1} \cdots p_K^{j_K} x_{\boldsymbol{j}}$.

Now, let

$$Z = \bigcup_{\boldsymbol{j}\in\mathcal{J}} a_{\boldsymbol{j}} Y_{\boldsymbol{j}} \subset \mathbb{Q}$$

with the $(Y_{\boldsymbol{j}}, a_{\boldsymbol{j}'}) = 1$ for all $\boldsymbol{j}, \boldsymbol{j}' \in \mathcal{J}$. In particular, $Y_{\boldsymbol{j}}$ is coprime to $p_1 \cdots p_K$. Therefore, in the notation of Lemma 2.6

$$Z_{\boldsymbol{j}} = a_{\boldsymbol{j}} Y_{\boldsymbol{j}}.$$

Then, by Lemma 2.6,

$$\tilde{E}_{k,w}(Z; u)^{1/k} \leq \left(2\binom{2k}{2}\right)^K \sum_{\boldsymbol{j}\in\mathbb{Z}^K} \tilde{E}_{k,w}(a_{\boldsymbol{j}} Y_{\boldsymbol{j}}; u)^{1/k}.$$

□

We recall now the Plünnecke-Ruzsa Theorem. See [14] for a simple inductive proof. Following convention, we state it using additive notation, although it will be used in the multiplicative setting.

[7]We say that two rational numbers a and b are comprime if at least one of $v_p(a)$ and $v_p(b)$ is zero for all prime p. As with the case of integers, we write $(a, b) = 1$.

Theorem 2.11. *Let A be a subset of a commutative additive group G with $|A+A| \leq K|A|$. Then for any $h \in \mathbb{N}$,*

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

One may think of the separating constant of X as a generalisation of the notion of the mixed energy $\tilde{E}_k(X;u)$. Indeed, if X is ψ-separating then take $Y_x = \{1\}$ for all $x \in X$ and $w(x) = 1$ for all $x \in X$. Then it follows that $\tilde{E}_k(X;u) \leq \psi^k|X|^k$. In particular, Theorem 2.10 implies the following result.

Theorem 2.12. *Let A be a finite set of rational numbers and let $u \in \mathbb{Q}$ be non-zero. Suppose that $|AA| \leq K|A|$. Then, for any integer $k \geq 2$,*

$$|(A+u)^k| \geq \frac{|A|^{k-1}}{K^k\left(2\binom{2k}{2}\right)^{Kk}}$$

Proof. By Theorem 2.10,

$$\tilde{E}_k(A;u) \leq \left(2\binom{2k}{2}\right)^{Kk}|A|^k.$$

Also, by Theorem 2.11, $|A^{(k)}| \leq K^k|A|$. Inserting these two bounds into Lemma 2.1 completes the proof. □

A stronger version of Theorem 2.12 was the main result of [10], which used the standard k-fold multiplicative energy of the set $A+u$.

A key goal of this paper is to amplify this approach in order to give a good bound for the case when $K = |A|^{\varepsilon}$. The advantage of working with this generalised notion of energy is that it has a crucial "chaining property" which will be important in the forthcoming analysis for pushing to get results for larger K.

Lemma 2.13. *Let A be a finite set of rationals which can be decomposed as a disjoint union*

$$A = \bigcup_{b\in B} bC_b$$

and with $(b, C_{b'}) = 1$ for all $b, b' \in B$. Assume also that B is ψ_1-separating and that each C_b is ψ_2-separating. Then A is $\psi_1\psi_2$-separating.

Proof. Let Z be a set of rationals which decomposes as

$$Z = \bigcup_{a\in A} aY_a$$

with $(a, Y_{a'}) = 1$ for all $a, a' \in A$. Then for any $u \in \mathbb{Q}$ and weights w on Z,

$$\tilde{E}_{w,u}(Z;u)^{1/k} = \tilde{E}_{w,u}\left(\bigcup_{b\in B} b\left(\bigcup_{c\in C_b} cY_{bc}\right);u\right)^{1/k} \leq \psi_1 \sum_{b\in B}\tilde{E}_{w,u}\left(b\left(\bigcup_{c\in C_b} cY_{bc}\right);u\right)^{1/k}.$$

In the inequality above we have used the fact that B is ψ_1 separating and that

$$\left(b, \bigcup_{c\in C_{b'}} cY_{b'c}\right) = 1$$

for any $b, b' \in B$. Indeed, take an arbitrary product cy with $c \in C_{b'}$ and $y \in Y_{b'c}$. Then b is coprime to c by the hypothesis of the lemma. Also, y is coprime to each element of A by the definition of Z, which implies that y is coprime to b by the hypothesis of the lemma.

We therefore have

$$\begin{aligned}\tilde{E}_{w,u}(Z;u)^{1/k} \leq \psi_1 \sum_{b\in B} \tilde{E}_{w,u}\left(\bigcup_{c\in C_b} c(bY_{bc}); u\right)^{1/k} &\leq \psi_1 \sum_{b\in B} \psi_2 \sum_{c\in C_b} \tilde{E}_{w,u}\left(c(bY_{bc}); u\right)^{1/k} \\ &= \psi_1\psi_2 \sum_{a\in A} \tilde{E}_{w,u}\left(aY_a; u\right)^{1/k}.\end{aligned}$$

The inequality above uses fact that C_b is ψ_2-separating and that $(c, bY_{bc'}) = 1$ for any $c, c' \in C_b$. This can be verified in the same way as the previous inequality. □

3. Lambda-constants

We will soon begin the process of amplifying Theorem 2.10 from the previous section in order to get a better separating factor which leads to strong bound when $K = |A|^{\varepsilon}$. At the conclusion of this process we will prove the following result.

Theorem 3.1. *Given $0 < \tau, \gamma < 1/2$, there exist positive constants $C_1 = C_1(\tau, \gamma, k)$ and $C_2 = C_2(\tau, \gamma, k)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| = K|A|$, there exists $A' \subset A$ with $|A'| \geq K^{-C_1}|A|^{1-\tau}$ such that A' is $K^{C_2}|A|^{\gamma}$-separating.*

In fact, one can check that the proof of Theorem 3.1 goes through in a more general setting. Let $S : 2^{\mathbb{Q}} \to \mathbb{R}$ be a function defined on rational sets with the following properties:

(1) (Trivial bound) For an arbitary set $A \subset \mathbb{Q}$

$$S(A) \leq |A|.$$

(2) (Stability) If $A' \subset A$ then

$$S(A') \leq S(A).$$

(3) (p-adic separation) There is an absolute constant $s \geq 0$ such that for any prime p and $I \subset \mathbb{Z}$,

$$S(\bigcup_{i\in I} p^i) \leq s.$$

(4) (Nesting) Let $A \subset \mathbb{Q}$ and $\{B_a\}_{a\in A}$ is a collection of sets such that $(a, B_{a'}) = 1$ for any $a, a' \in A$. Further assume that $aB_a, a \in A$ are pairwise disjoint. Then

$$S(\bigcup_{a\in A} aB_a) \leq S(A) \max_{a\in A} S(aB_a).$$

Note that our definition of the separating constant satisfies (1)-(4).

Theorem 3.2. *Let S be a function with the properties above. Given $0 < \tau, \gamma < 1/2$, there exist positive constants $C_1 = C_1(\tau, \gamma, s)$ and $C_2 = C_2(\tau, \gamma, s)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| = K|A|$, there exists $A' \subset A$ with $|A'| \geq K^{-C_1}|A|^{1-\tau}$ such that*

$$S(A') \leq K^{C_2}|A|^{\gamma}.$$

The proof of Theorem 3.1 is essentially borrowed from [4]. We present here a proof adapted to our setting to make the paper self-contained. The same proof applies to Theorem 3.2 with cosmetic modifications, but we expect that it might be useful to have such a general 'black-box' version for future use.

Before we begin the lengthy proof of Theorem 3.1, we will take some time to see how it implies the two main theorems of this paper. To do this, it will be convenient to use the language of Λ-*constants*, and to introduce some of their key properties. The main motivation behind Λ-constants is the stability property given by the forthcoming Corollary 3.4, which is absent in the non-weighted version of the energy.

We also encourage the interested reader to consult our preceding paper [10] 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 non-zero 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

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

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

Lemma 3.3. *Let $A \subset \mathbb{Q}$ be a finite set with some non-negative real weights w_a assigned to each element $a \in A$ and let u be a non-zero 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

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

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 3.4. *Suppose that $A \subset \mathbb{Q}$, that u is a non-zero rational and $A' \subset A$. Then*

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

In particular,

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

and

$$\tilde{E}_k(A;u) \leq \Lambda_k^k(A;u)|A|^k.$$

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 3.3. □

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

Lemma 3.5. *Let $A \subset \mathbb{Q}$ be ψ-separating. Then for any $u \in \mathbb{Q} \setminus \{0\}$*

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

Proof. Let w be any set of weights on A that satisfy (23). Write

$$A = \bigcup_{a\in A} aY_a$$

with $Y_a = \{1\}$ for all $a \in A$. Then by the definition of ψ-separating, it follows that for any non-zero $u \in \mathbb{Q}$

$$\tilde{E}_{k,w}(A;u)^{1/k} \leq \psi \sum_{a\in A} \tilde{E}_{k,w}(\{a\};u)^{1/k} = \psi \sum_{a\in A} (w(a)^{2k})^{1/k} = \psi.$$

□

Lemma 3.6. *Let $A \subset \mathbb{Q}$ be a finite set with $|AA| \leq K|A|$ and let u be a non-zero rational number. Suppose that $A' \subset A$ and A' is ψ-separating. Then*

$$\Lambda_k(A;u) \leq K^4 \left(\frac{|A|}{|A'|-1} \right)^2 \psi.$$

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 $R_{(A/A'),A'}(x) \geq |A'| - 1$ for all $x \in A$. This is because, for all non-zero $a' \in A'$, $x = (\frac{x}{a'})a'$. Therefore,

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

On the other hand, by the triangle inequality and Lemma 3.3

$$\begin{aligned}\left\| \sum_{z \in A/A'} \sum_{a' \in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \right\|_{2k} &\leq \sum_{z \in A/A'} \left\| \sum_{a' \in A'} w^{(z)}(za')(za')^{it_1}(za'+u)^{it_2} \right\|_{2k} \\ &\leq \sum_{z \in A/A'} \Lambda_k(zA';u)^{1/2} + o_{T\to\infty}(1).\end{aligned}$$

Since A' is ψ-separating, it follows from Lemma 3.5 that $\Lambda_k(zA';u) = \Lambda_k(A';u/z) \leq \psi$. We also have

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

by the Ruzsa Triangle Inequality (see [17]). It therefore follows that

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

and the result follows. □

Combining this with Theorem 3.1 gives the following, which is our main result concerning Λ-constants.

Theorem 3.7. *Given $0 < \gamma < 1/2$, there exists a positive constants $C = C(\gamma,k)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| = K|A|$ and any non-zero rational u,*

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

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. Both theorems are restated below for the convenience of the reader.

Theorem 4.1. *For all $b \in \mathbb{Z}$, there exists $k = k(b)$ such that for any finite set $A \subset \mathbb{Q}$ and any non-zero 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

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

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

$$|BB| < |B||A|^{\frac{b-1}{l}}.$$

Also, for any non-zero $\lambda \in \mathbb{Q}$, $|(\lambda B)(\lambda B)| < |B||A|^{\frac{b-1}{l}}$. Therefore, by Theorem 3.7,

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

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 3.4 and Lemma 2.1

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

This rearranges to

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

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

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

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

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

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.

□

Theorem 3.7 also implies Theorem 1.3. The statement is repeated below for the convenience of the reader.

Theorem 4.2. *Given $0 < \gamma < 1/2$ 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 non-zero 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,

$$\tilde{E}_{k,w}(A;u) = \frac{\tilde{E}_k(A;u)}{|A|^k} \geq \frac{|A|^k}{|A^{(k)}||(A+u)^{(k)}|}, \tag{25}$$

where the inequality comes from Lemma 2.1. It follows from Theorem 3.7 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 (25), it follows that

$$|A^{(k)}||(A+u)^{(k)}| \geq \frac{|A|^{k(1-\gamma)}}{K^{Ck}}. \tag{26}$$

Finally, since $|AA| \leq K|A|$, it follows from the Plünnecke-Ruzsa Theorem that $|A^{(k)}| \leq K^k|A|$. Inserting this into (26) completes the proof.

□

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

Theorem 4.3. *For any $\gamma > 0$ there is $C(\gamma) > 0$ such that for any K-almost subgroup $A \subset \mathbb{Q}$ and fixed non-zero $c_1, c_2 \in \mathbb{Q}$ 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

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

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 3.7 and Corollary 3.4 for any non-zero u

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

with the parameters $0 < \gamma' < 1/2, k \geq 2$ to be taken in due course.

In particular, by Lemma 2.1

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

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

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

We then have

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

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

□

5. Graph Fibering

Suppose Z_1 and Z_2 abelian groups, with finite subsets $A, B \subset Z_1 \times Z_2$. We will write $z_1 \oplus z_2$ for an element of $Z_1 \times Z_2$. We will write, for $x \in X \subset Z_1 \times Z_2$ with $\pi_1(x) = x_1$,

$$X_2(x_1) = \{x_2 \in \pi_2(X) : x_1 \oplus x_2 \in X\}.$$

Suppose $G \subset A \times B$. Denote by π_1 and π_2 the projections onto the first and second coordinates of $Z_1 \times Z_2$ respectively. The set G is interpreted as a bipartite graph on A and B, and it can be decomposed into a union by considering the fibers of π_1. Indeed, let

$$G_1 = \{(\pi_1(a), \pi_1(b)) : (a, b) \in G\}$$

and for $(a_1, b_1) \in G_1$, let

$$G_2(a_1, b_1) = \{(a_2, b_2) : (a_1 \oplus a_2, b_1 \oplus b_2) \in G\} \subset \pi_2(A) \times \pi_2(B).$$

Recall the notation

$$A +_G B = \{a + b : (a, b) \in G\}.$$

One of the primary reasons for decomposing a graph this way is that it behaves nicely with addition along the graph.

Lemma 5.1. *Suppose A and B are finite subsets of $Z_1 \times Z_2$. Then for $G \subset A \times B$ we have*

$$|A +_G B| \geq |\pi_1(A) +_{G_1} \pi_1(B)| \min_{(a_1,b_1) \in \pi_1(A) \times \pi_1(B)} |A_2(a_1) +_{G_2(a_1,b_1)} B_2(b_1)|.$$

Proof. Write

$$A +_G B \supseteq \bigcup_{s \in \pi_1(A +_G B)} \bigcup_{\substack{(a_1 \oplus a_2, b_1 \oplus b_2) \in G \\ a_1 + b_1 = s}} \{(s \oplus (a_2 + b_2))\}.$$

Next, from the observation that the first union above is disjoint, and the fact that $\pi_1(A +_G B) = \pi_1(A) +_{G_1} \pi_1(B)$, we have

$$|A +_G B| \geq \sum_{s \in \pi_1(A) +_{G_1} \pi_1(B)} \Big| \bigcup_{\substack{(a_1 \oplus a_2, b_1 \oplus b_2)) \in G \\ a_1 + b_1 = s}} \{(s \oplus (a_2 + b_2))\} \Big|.$$

Since, for fixed a_1, b_1,

$$\bigcup_{\substack{(a_1 \oplus a_2, b_1 \oplus b_2) \in G \\ a_1 + b_1 = s}} \{a_2 + b_2\} \supseteq A_2(a_1) +_{G_2(a_1,b_1)} B_2(b_1)$$

the lemma follows. □

Lemma 5.2 (Regularized decomposition)**.** *Let Z_1 and Z_2 be abelian groups and let $A, B \subset Z_1 \times Z_2$ be finite sets. Suppose that $\delta > 0$, $K \geq 1$ and $G \subset A \times B$ are such that*

$$|G| \geq \delta |A||B|,$$

and

$$|A +_G B| \leq K(|A||B|)^{1/2}.$$

There are absolute constants $c, C > 0$, subsets $A' \subset A$ and $B' \subset B$, and a subset $G' \subset A' \times B'$ with the following properties.

(1) (Uniform fibers) If

$$M_A = |\pi_1(A)|,\ M_B = |\pi_1(B)| \tag{27}$$

then there are numbers m_A and m_B satisfying

$$M_A m_A \geq c\delta^2(\log(K/\delta))^{-1}|A|, \tag{28}$$

$$M_B m_B \geq c\delta^2(\log(K/\delta))^{-1}|B|, \tag{29}$$

$$m_A, m_B \geq c\delta^{10}K^{-4}\max_{a_1\in\pi_1(A),b_1\in\pi_1(B_1)}(|A_2(a_1)| + |B_2(b_1)|), \tag{30}$$

and such that we have approximately uniform fibers:

$$|(A')_2(a_1)| \approx m_A,\ |(B')_2(b_1)| \approx m_B \tag{31}$$

for $a_1 \in \pi_1(A')$ and $b_1 \in \pi_1(B')$.

(2) (Uniform graph fibering) For some $\delta_1, \delta_2 > 0$ satisfying

$$\delta_1\delta_2 > c(\log(K/\delta))^{-3}\delta \tag{32}$$

we have that the first coordinate subgraph is dense:

$$|G_1'| \geq \delta_1 M_A M_B, \tag{33}$$

and that the subgraph has dense fibers: for each $(a_1, b_1) \in G_1'$ we have

$$|G_2'(a_1, b_1)| \geq \delta_2 m_A m_B. \tag{34}$$

(3) (Bounded doubling) For some $K_1, K_2 > 0$ with

$$K_1K_2 \leq C\delta^{-2}(\log K)K \tag{35}$$

we have

$$|\pi_1(A') +_{G_1'} \pi_1(B')| = K_1(M_A M_B)^{1/2}, \tag{36}$$

and for each $(a_1, b_1) \in G_1'$,

$$|\pi_2(A') +_{G_2'(a_1,b_1)} \pi_2(B')| \approx K_2(m_A m_B)^{1/2}. \tag{37}$$

5.1. **Proof of Theorem 5.2.** We will produce the sets A' and B' after a sequence of refinements. One such refinement comes from the following lemma. Here, and in what follows, when $G \subseteq A \times B$ we write $\deg_G a$ (respectively, $\deg_G b$) for the size of $\{b' \in B : (a, b') \in G\}$ (respectively, the size of $\{a' \in A : (a', b) \in G\}$).

Lemma 5.3. *Let A and B be finite sets and $G \subseteq A \times B$ of size $\delta|A||B|$. Then there exist $A' \subset A, B' \subset B$ and $G' \subset G \cap (A' \times B')$ such that*

- $\deg_{G'} a \geq \frac{\delta}{4}|B|$,
- $\deg_{G'} b \geq \frac{\delta}{4}|A|$,
- $|A'| \geq \frac{\delta}{2}|A|$,

- $|B'| \geq \frac{\delta}{2}|B|$, *and*
- $|G'| \geq \frac{\delta}{2}|A||B|$

for any $a \in A', b \in B'$.

Proof. Remove from A (respectively, B) one by one all vertices with degree less than $\delta|A|/4$ (respectively, $\delta|B|/4$), until both A and B contain only vertices of degree at least $\delta|A|/4$ (respectively, $\delta|B|/4$) in the remaining graph. At the end of this process, we cannot have removed more than $\delta|A||B|/2$ edges. Indeed, we remove at any stage at most $\delta|B|/4$ edges adjacent to a vertex in $|A|$ (and we can remove at most $|A|$ such vertices) or else at most $\delta|A|/4$ edges adjacent to a vertex in B (and we can remove at most $|B|$ such vertices). Take A' and B' to be the sets of survived vertices in A and B respectively and $G' := G \cap (A' \times B')$. □

Now, set $|A| = N_A$ and $|B| = N_B$. In view of the above lemma, and passing to subsets if necessary, we may assume

$$|A| \geq \frac{1}{2}\delta N_A,\ |B| \geq \frac{1}{2}\delta N_B,$$
$$|G| \geq \frac{1}{2}\delta N_A N_B$$

and that for any $a \in A$ and $b \in B$ we have

$$\deg_G a \geq \frac{1}{4}\delta|B|,\ \deg_G b \geq \frac{1}{4}\delta|A|.$$

First, we may assume without loss of generality that

$$n_A = \max_{a_1 \in \pi_1(A)} |A_2(a_1)| \geq \max_{b_1 \in \pi_1(B)} |B_2(b_1)|$$

It is also useful to observe that, if $a \in A$ then $|\{a\} +_G B| = \deg_G a$, where $\deg_G a$ is the number of neighbours of a in G. So,

$$\delta N_B \leq \frac{1}{N_A}\sum_{a \in A} \deg_G a \leq |A +_G B| \leq K(N_A N_B)^{1/2}.$$

We can apply the same argument, reversing the roles of A and B, and we have proved

$$\delta N_B^{1/2} \leq K N_A^{1/2},\ \delta N_A^{1/2} \leq K N_B^{1/2}. \tag{38}$$

Having assumed this, our first order of business is to establish property (1) for B'.

5.1.1. *Regularization of* B. Let $a_1 \in \pi_1(A)$ be such that $|A_2(a_1)| = n_A$. Then $a_1 \oplus A_2(a_1)$ consists of n_A elements of A each with at least $\frac{1}{4}\delta|B|$ neighbours in B. Thus

$$|(a_1 \oplus A_2(a_1) \times B) \cap G| \geq \frac{1}{4}\delta n_A |B|.$$

Let

$$B' = \left\{ b \in B : |\{a_2 : (a_1 \oplus a_2, b) \in G\}| \geq \frac{1}{8}\delta n_A \right\}$$
$$|B'| \geq \frac{1}{8}\delta|B| \geq \frac{1}{16}\delta^2 N_B \tag{39}$$

and such that for each $b \in B'$ we have

$$|((a_1 \oplus A_2(a_1)) \times \{b\}) \cap G| \geq \frac{1}{8}\delta n_A.$$

Moreover, since every element in B has at least $\frac{1}{4}\delta N_A$ neighbours in A, we have

$$|(A \times B') \cap G| \geq \frac{1}{4}\delta N_A |B'|.$$

If $k = |\pi_1(B')|$ then there are elements $b_1 \oplus b_1', \dots, b_k \oplus b_k'$ with the b_i distinct, and for each of them the sets

$$a_1 \oplus A_2(a_1) + b_i \oplus b_i'$$

are disjoint, since their first coordinates are $a_1 + b_i$ and are distinct. Each of these sets contains at least $\frac{1}{8}\delta n_A$ distinct elements of $A +_G B$ since each element of B' has that many neighbours in G. From this it follows that

$$|a_1 \oplus A_2(a_1) +_G B'| \geq \frac{1}{8}\delta n_A |\pi_1(B')|$$

and so

$$\frac{1}{8}\delta n_A |\pi_1(B')| \leq |A +_G B| \leq K(N_A N_B)^{1/2} \leq \frac{K^2}{\delta} N_B.$$

Here we have used the inequality (38). Next, we define

$$B'' = \bigcup_{\substack{1 \leq i \leq k \\ |B_2'(b_i)| \geq 10^{-4}\delta^5 K^{-2} n_A}} b_i \oplus B_2'(b_1). \tag{40}$$

By (40) and (39),

$$|B' \setminus B''| \leq |\pi_1(B')| 10^{-4}\delta^5 K^{-2} n_A \leq 10^{-3}\delta^3 N_B \leq \frac{\delta}{10}|B'|.$$

Now, we have already assumed that $\max_{b_1 \in \pi_1(B)} |B_2(b_1)| \leq n_A$, so applying a dyadic partition to the range $10^{-4}\delta^5 K^{-2} n_A \leq m \leq n_A$, we find a value of m_B in this range and a subset

$$B''' = \bigcup_{\substack{b_1 \in \pi_1(B') \\ m_B \leq |B_2''(b_1)| \leq 2m_B}} b_1 \oplus B_2'(b_1)$$

which has size $|B'''| \gg \log(K/\delta)^{-1}|B''|$. Thus

$$|B'''| \gg \frac{|B''|}{\log(K/\delta)} \gg \frac{|B'|}{\log(K/\delta)} \gg \frac{\delta^2}{\log(K/\delta)} N_B.$$

Since each element of B has at $\frac{1}{8}\delta N_A$ neighbours in G, we further have

$$|(A \times B''') \cap G| \geq \frac{1}{8}\delta N_A |B'''|.$$

If $M_B = |\pi_1(B''')|$, then because each element of $\pi_1(B''')$ has about m_B fibers, we have

$$|B'''| \approx m_B M_B.$$

Redefine $B' = B'''$ and $N_B' = |B'|$. Then we have shown that

$$N_B' \gg \frac{\delta^2}{\log(K/\delta)} N_B.$$

5.1.2. *Regularization of A.* Let

$$A' = \bigcup_{\substack{a_1 \in \pi_1(A) \\ |A_2(a_1)| \geq 10^{-5}\delta^3 K^{-2} m_B}} a_1 \oplus A_2(a_1).$$

We first estimate $|A \setminus A'|$. We write $A'' = A \setminus A'$, so that for each $a \in A''$ we have

$$|A_2(a_1)| < 10^{-5}\delta^3 K^{-2} m_B. \tag{41}$$

We will show $|(A'' \times B') \cap G| \leq \frac{\delta}{40} N_A N'_B$. To see why, assume the contrary. Then there is a $b_1 \in \pi_1(B')$ with

$$|(A'' \times b_1 \oplus B'_2(b_1)) \cap G| \geq \frac{\delta}{100} N_A m_B.$$

Indeed, each of the vertex sets $b_1 \oplus B'_2(b_1)$ are disjoint and have size m_B up to a factor of 2. Now let $A''' \subset A''$ be the set of those a for which

$$|(\{a\} \times b_1 \oplus B'_2(b_1)) \cap G| \geq \frac{\delta}{200} m_B.$$

From the definition, it follows that

$$|A'''| \geq \frac{\delta}{200} N_A. \tag{42}$$

Let

$$M = \max_{a_1 \in \pi_1(A''')} |A'''_2(a_1)|.$$

We have

$$|A''' +_G (b_1 \oplus B'_2(b_1)))| \leq |A +_G B| \leq K(N_A N_B)^{1/2} \leq \frac{K^2}{\delta} N_A.$$

Because every element of A''' has at least $(\delta/200)m_B$ neighbours in $b_1 \oplus B'_2(b_1)$, and because for each $a_1 \in \pi_1(A''')$ the sets $(a_1 \oplus A'''_2(a_1)) +_G (b_1 \oplus B'_2(b_1))$ are disjoint, we get

$$|A''' +_G (b_1 \oplus B'_2(b_1)))| \geq (\delta/200) m_B |\pi_1(A''')|.$$

In view of (42)

$$|\pi_1(A''')| \geq \frac{|A'''|}{M} \geq \frac{\delta}{200M} N_A,$$

we obtain the bound

$$\frac{\delta^2}{4 \cdot 10^4 M} N_A m_B \leq \frac{K^2}{\delta} N_A$$

whence

$$M > \frac{\delta^3 m_B}{10^5 K^2},$$

which contradicts (41) and the definition of M. By what we have just shown,

$$|(A' \times B') \cap G| \geq \frac{\delta}{8} N_A N'_B.$$

Now, for each $a \in A'$, we certainly have

$$|A_2(a_1)| \leq n_A \leq 10^4 m_B \delta^{-5} K^2$$

the final estimate coming from the bounds on the range range of m_B. Thus we partition the range

$$10^{-5}\delta^3 K^{-2} m_B \leq |A_2(a_1)| \leq 10^4 m_B \delta^{-5} K^2$$

dyadically, to find an m_A in this range such that

$$A'''' = \bigcup_{\substack{a_1 \in \pi_1(A) \\ m_A \leq |A_2(a_1)| \leq 2m_A}} a_1 \oplus A_2(a_1)$$

satisfies

$$|(A'''' \times B') \cap G| \gg \frac{\delta}{\log(K/\delta)} N_A N'_B.$$

Moreover, since $|(A'''' \times B') \cap G| \leq |A''''|N'_B$ we have $|A''''| \gg \delta(\log(K/\delta))^{-1}N_A$. If we define $M_A = |\pi_1(A'''')|$ then we have

$$|A''''| \approx M_A m_A$$

as needed. We relabel $A' = A''''$ and $N'_A = |A'|$, observing that

$$N'_A \gg \frac{\delta}{\log(K/\delta)} N_A$$

and we are ready to proceed to the next step.

5.1.3. *Regularizing the graph fibers.* So far we have found subsets A' and B', and an absolute constant $c > 0$, satisfying

$$|(A' \times B') \cap G| \geq c\frac{\delta}{\log(K/\delta)}|A'||B'|,$$

$$|A'| \approx m_A M_A \geq c\frac{\delta}{\log(K/\delta)} N_A,$$

and

$$|B'| \approx m_B M_B \geq c\frac{\delta^2}{\log(K/\delta)} N_B.$$

Furthermore, each of A' and B' have fibers above π_1 of size roughly m_A and m_B respectively. Recall that for $(a_1, b_1) \in \pi_1(A') \times \pi_1(B')$ we have the graph

$$G_2(a_1, b_1) = \{(a_2, b_2) \in A'_2(a_1) \times B'_2(b_1) : (a_1 \oplus a_2, b_1 \oplus b_2) \in G\}.$$

Because we have regularized the fibers of A' and B', each of these graphs has cardinality obeying

$$|G_2(a_1, b_1)| \leq 4m_A m_B.$$

By a slight abuse of notation, we let

$$G_1 = \{(\pi_1(a), \pi_1(B)) : (a, b) \in (A' \times B') \cap G\}$$

and define

$$G'_1 = \left\{(a_1, b_1) \in \pi_1(A') \times \pi_1(B') : |G_2(a_1, b_1)| \geq \frac{c\delta}{16\log(K/\delta)} m_A m_B\right\}.$$

Since

$$\sum_{(a_1,b_1) \in \pi_1(A') \times \pi_1(B')} |G_2(a_1, b_1)| = |(A' \times B') \cap G| \geq c\frac{\delta}{\log(K/\delta)}|A'||B'|$$

it follows that

$$\sum_{(a_1,b_1) \in G'_1} |G_2(a_1, b_1)| \geq c\frac{\delta}{2\log(K/\delta)}|A'||B'|.$$

By a dyadic pigeon-holing for δ' in the range $c\delta(\log(K/\delta))^{-1} \leq \delta' \leq 4$, we can find $\delta' \gg \delta(\log(K/\delta))^{-1}$ such that

$$G_1'' = \big\{(a_1,b_1) \in G_1' : \delta' m_A m_B \leq |G_2(a_1,b_1)| \leq 2\delta' m_A m_B\big\}$$

certainly satisfies

$$\sum_{(a_1,b_1)\in G_1''} |G_2(a_1,b_1)| \gg c\frac{\delta}{(\log(K/\delta))^2}|A'||B'|.$$

From this estimate, it also follows that

$$|G_1''| \gg \frac{\delta}{\delta'(\log(K/\delta))^2} M_A M_B.$$

Let us relabel G_1'' as G_1' and set

$$G' = \{(a,b) \in A' \times B' : (\pi_1(a),\pi_1(b)) \in G_1'\}.$$

We move on to the final step of the lemma.

5.1.4. *Regularizing the doubling constant.* For $(a_1,b_1) \in \pi_1(A') \times \pi_1(B')$ we define

$$K_+(G_2(a_1,b_1)) = \frac{|A_2'(a_1) +_{G_2(a_1,b_1)} B_2'(b_1)|}{(|A_2'(a_1)||B_2'(b_1)|)^{1/2}}.$$

This quantity measure the growth of sumsets on the fibres lying above a pair (a_1,b_1). Now define

$$H = \{(a_1,b_1) \in G_1' : K_+(G_2(a_1,b_1)) > C(\log(K/\delta))^3\delta^{-10}K\}.$$

Provided C is large enough we have $H \leq \frac{1}{10}|G_1'|$. To see this, first observe the trivial bound

$$|\pi_1(A') +_H \pi_1(B)| \geq \frac{|H|}{\min\{|\pi_1(A')|,|\pi_1(B')|\}} \geq \frac{|H|}{(M_A M_B)^{1/2}}. \tag{43}$$

Let

$$G_H = \{(a_1,a_2) \in G : (\pi_1(a_1),\pi_1(a_2)) \in H\} \subset G.$$

Also, for $(a_1,b_1) \in H$ we have

$$(G_H)_2(a_1,b_1) = G_2(a_1,b_1)$$

so that by Lemma 5.1

$$|A' +_G B'| \geq |\pi_1(A') +_H \pi_1(B')| \min_{(a_1,b_1)\in H}(|A_2'(a_1) +_{G_2(a_1,b_1)} B_2'(b_1)|).$$

By the definition of H and (43) we see

$$K(N_A N_B)^{1/2} \geq |A' +_G B'| \geq C\frac{|H|}{(M_A M_B)^{1/2}}(\log(K/\delta))^3\delta^{-10}K(m_A m_B)^{1/2}.$$

Using our estimates for $m_A M_A$, $m_B M_B$ and G_1', the right hand side is

$$C\frac{|H|}{M_A M_B}(\log(K/\delta))^3\delta^{-10}K(M_A m_A M_B m_B)^{1/2} \geq cCK(N_A N_B)^{1/2}\frac{|H|}{|G_1'|}.$$

Thus for C sufficiently large in terms of c (which was absolute), we have $|H| \leq \frac{1}{10}|G_1'|$. Now let $G_1'' = G_1' \setminus H$. We perform yet another dyadic pigeon-holing to find $K' \leq C(\log(K/\delta))^3\delta^{-10}K$ such that

$$G_1''' = \{(a_1,b_1) \in G_1'' : K' \leq K_+(G_2(a_1,b_1)) \leq 2K'\}$$

has cardinality

$$|G_1'''| \gg \frac{|G_1'|}{\log(K/\delta)}.$$

Now, by Lemma 5.1 along the subgraph of G with first projection equal to G_1''' we have

$$K(N_AN_B)^{1/2} \geq |\pi_1(A') +_{G_1'''} \pi_1(B')|K'(m_Am_B)^{1/2} = K_+(G_1''')K'(M_Am_AM_Bm_B)^{1/2},$$

where $K_+(G_1''') = |\pi_1(A') +_{G_1'''} \pi_1(A_2')|(M_AM_B)^{-1/2}$. By the established bounds on m_AM_A and m_BM_B, we get

$$K(N_AN_B)^{1/2} \gg K_+(G_1''')K'\delta^{3/2}\log(K/\delta)(N_AN_B)^{1/2}.$$

From this we see

$$K_+(G_1''')K' \ll K\log(K/\delta)\delta^{3/2} \ll K\log(K)\delta^2.$$

Now let $G' = \{(a,b) \in A' \times B' : (\pi_1(a), \pi_1(b)) \in G_1'''\}$. Define $K_1 = K_+(G_1''')$ and $K_2 = K'$. Let $\delta_2 = \delta'$ and $\delta_1 = c\delta(\delta_2(\log(K/\delta))^3)^{-1}$. One then verifies that with these parameters, the claims of the lemma have all been justified.

6. Iteration scheme

In this section we will use Lemma 5.2 in order to setup an iteration scheme. At each step we have a pair of sets $(\mathcal{A}, \mathcal{B})$ which correspond to a pair of additive sets $(A, B) := (\mathcal{P}(\mathcal{A}), \mathcal{P}(\mathcal{B}))$ and a graph G on $A \times B$, together with the data (N, δ, K) such that:

(1) $|A||B| = N$
(2) $|A +_G B| \leq KN^{1/2}$
(3) $|G| \geq \delta N$.

Apart from that, the setup above is equipped with a pair of functions $\psi(N,\delta,K)$, $\phi(N,\delta,K)$ (which are called *admissible* in [4]). These functions are technical aids to carry out an induction type argument.

Definition 6.1 (Admissible pair of functions)**.** *A pair of functions $\psi(N,\delta,K)$, and $\phi(N,\delta,K)$ is said to be* admissible *if for arbitrary sets $A, B \subset \mathbb{Z}^{[n]}$ and a graph G on $A \times B$ satisfying (1)-(3) the following holds.*

There is a graph $G' \subseteq G$ such that

(G) Graph size is controlled by ϕ:

$$|G'| \geq \phi(N,\delta,K)$$

(S) Separation of G'-neigborhoods is controlled by ψ:

For any $a \in A$ (resp. $b \in B$) the $\mathcal{P}$-preimage of the G'-neighborhood

$$\mathcal{P}^{-1}\left[G'(a)\right] := \mathcal{P}^{-1}\left[\{b \in B : (a,b) \in G'\}\right].$$

(resp. of $G'(b)$) is $\psi(N,\delta,K)$-separating.

Furthermore, we will assume that the following technical conditions hold for $\phi(N,\delta,K), \psi(N,\delta,K)$:

(A1) ϕ, ψ are non-decreasing in N

(A2) ϕ *is non-decreasing in* δ*, non-increasing in* K *and for each* δ *and* K*, we have* $\phi(N,\delta,K) \leq N$*.*

(A3) ψ *is non-decreasing in* K

(A4) If $N \geq M$ *then*

$$\frac{\phi(N,\delta,K)}{N} \leq \frac{\phi(M,\delta,K)}{M}$$

Note that, by Claim 2.7, the pair $\psi(N,\delta,K) := N; \phi(N,\delta,K) := \delta N$ is trivially admissible with much room to spare.

The following lemma gives a Freiman-type pair of admissible functions which is better than trivial in the regime $K = o(\log N)$, and will be used later to bootstrap the argument.

Lemma 6.2 (Freiman-type admissible functions)**.** *There is an absolute constant* $C > 0$ *such that the pair of functions*

(1) $\psi(N,\delta,K) := \min\left\{(2k^2)^{\left(\frac{K}{\delta}\right)^C}, N\right\}$

(2) $\phi(N,\delta,K) := \left(\frac{\delta}{K}\right)^C N$

is admissible.

Proof. This pair is easily seen to satisfy (A1) through (A4). Thus it remains to check (G) and (S). By the setup, we are given two sets $\mathcal{A}$ and $\mathcal{B}$ of sizes N_A and N_B respectively, and a graph G of size $\delta N_A N_B$ such that

$$|A +_G B| \leq K\sqrt{N_A N_B} \tag{44}$$

Assume without loss of generality that $N_A \geq N_B$ and take $X = A \cup B$, which is of size $\approx N_A$. Since by (44)

$$\frac{K^2}{\delta^2} N_B \geq N_A$$

we have

$$|G| \gg \frac{\delta^3}{K^2}|X|^2$$

and

$$|X +_G X| \ll K|C|.$$

By a variant of the Balog-Szemerédi-Gowers theorem (see e.g. [17], Exercise 6.4.10) there is $X' \subseteq X$ such that $|X' + X'| < K'|X'|$ and $|G \cap (X' \times X')| > \delta' N_A^2$ with

$$\delta' > \left(\frac{\delta}{K}\right)^C \tag{45}$$

$$K' < \left(\frac{K}{\delta}\right)^C. \tag{46}$$

By Theorem 2.9 any subset of X has rank at most K' and by Theorem 2.10, the $\mathcal{P}$-preimage of any subset of X' is at most $(2k^2)^{K'^C}$-separating for some $C > 0$. Thus, taking $G' := G \cap (X' \times X')$ by (45) and (46) we verify that the pair (1), (2) is admissible. □

The goal is to find a better pair of admissible functions. The lemma below implements the 'induction on scales' approach, which allows one to cook up a new pair $\phi_*(N,\cdot,\cdot),\psi_*(N,\cdot,\cdot)$ from a given pair of admissible functions, but taken at the smaller scale $\approx N^{1/2}$.

Lemma 6.3. *Let ψ and ϕ be an admissible pair of functions. Then for some absolute constant $C>0$ the pair of functions*

$$\psi_*(N,\delta,K) := Ck^2 \max \psi(N',\delta',K')\psi(N'',\delta'',K'') \quad (47)$$

$$\phi_*(N,\delta,K) := \min \phi(N',\delta',K')\phi(N'',\delta'',K'') \quad (48)$$

is admissible.

Here min *and* max *is taken over the data $(N',\delta',K'),(N'',K'',\delta'')$ such that*

$$\left(c\frac{\delta^9}{\log^{22}(K/\delta)}\right)N \leq N'N'' \leq N \quad (49)$$

$$N'+N'' \leq \left(C\frac{K^{11}}{\delta^{45}}\right)N^{1/2} \quad (50)$$

$$K'K'' \leq \left(C\frac{\log^{15}K}{\delta^{20}}\right)K \quad (51)$$

$$\delta'\delta'' \geq \left(c\frac{1}{\log^{6}(K/\delta)}\right)\delta. \quad (52)$$

Proof. Let us first check that (ϕ_*,ψ_*) given by (47) and (48) indeed satisfy (A1) through (A4). Assume $N_1<N_2$ and δ,K are fixed. Then $\psi_*(N_1,\cdot,\cdot)<\psi_*(N_2,\cdot,\cdot)$ since for $\psi_*(N_2,\cdot,\cdot)$ the maximum is taken over the larger range of parameters

$$N'N''\leq N_2,\quad N'+N''\leq C\delta^{-45}K^{11}N_2^{1/2}.$$

Similarly,

$$\phi_*(N_1,\cdot,\cdot)<\phi_*(N_2,\cdot,\cdot)$$

since the minimum is now taken over the smaller set

$$c\delta^9\log^{-22}(K/\delta)N_2\leq N'N''.$$

Note, that here we have used the fact that ϕ and ψ are both increasing. This proves (A1).

In order to prove (A2) it suffices to note that when δ increases (resp. K decreases) the range of parameters $N',N'',\delta',\delta'',K',K''$ over which the minimum in ϕ_* is taken is getting more narrow. Similarly, when K increases the maximum in ψ_* is taken over a larger set which proves (A3).

It remains to verify (A4). Let M,δ,K be fixed and $M',M'',\delta',\delta'',K',K''$ be such that the minimum for $\phi_*(M,\delta,K)$ in (49) is achieved. Let $c>0$ be a parameter. Then $cM',cM'',\delta',\delta'',K',K''$ are in the admissible range for $\phi_*(c^2M,\delta,K)$ so

$$\begin{aligned}\phi_*(c^2M,\delta,K) &\leq \phi(cM',\delta',K')\phi(cM'',\delta'',K'')\\ &\leq c^2\phi(M',\delta',K')\phi(M'',\delta'',K'')\\ &= c^2\phi_*(M,\delta,K).\end{aligned}$$

Taking c such that $c^2M = N$ we get (A4).

Let $A, B \subset \mathbb{Z}^n$ of sizes N_A, N_B respectively, $G \subseteq A \times B$ and suppose that the conditions (1)-(3) are satisfied with parameters (N, δ, K) where $N = N_A N_B$. Our ultimate goal is to find a subgraph of G of size at least

$$\phi(N', \delta', K')\phi(N'', \delta'', K'')$$

such that the $\mathcal{P}$-preimage of any its neighbourhoods is

$$Ck^2\psi(N', \delta', K')\psi(N'', \delta'', K'') - \text{separating},$$

for some $N', N'', K', K'', \delta', \delta''$ satisfying (49). Once this is done, the proof will be complete. In order to achieve this goal, we will apply Lemma 5.2 and then use the hypothesis that the pair ψ, ϕ is admissible for much smaller sets.

Define a function $f(t)$ for $0 \leq t \leq n$ as

$$f(t) = \max_{(a_1,b_1)\in\pi_{[t]}(A)\times\pi_{[t]}(B)} \{|A_2(a_1)| + |B_2(b_1)|\},$$

where $\pi_{[t]}$ is the projection onto the first t coordinates, and $A_2(a_1)$ and $B_2(b_1)$ are the fibres above a_1 and b_1 respectively. Note that f is decreasing, $f(0) = |A| + |B| \geq N^{1/2}$, and $f(n) = 0$. Thus there is t' such that

$$f(t') \geq N^{1/4} \tag{53}$$

but

$$f(t' + 1) < N^{1/4}. \tag{54}$$

We use the t' defined above for the decomposition $\mathbb{Z}^n = \mathbb{Z}^{t'} \times \mathbb{Z}^{n-t'}$ and let π_1 and π_2 denote the projection onto the first and second factor respectively. We now apply Lemma 5.2 and get sets $A' \subseteq A$ and $B' \subseteq B$ together with a graph $G' \subseteq G \cap (A' \times B')$ such that

$$A' = \bigcup_{a_1\in\pi_1(A')} a_1 \oplus A_2'(a_1) \tag{55}$$

$$B' = \bigcup_{b_1\in\pi_1(B')} b_1 \oplus B_2'(b_1) \tag{56}$$

and the fibers $A_2'(a_1), B_2'(b_1)$ together with the fiber graphs $G_2'(a_1, b_1)$ are uniform as defined in the statement of Lemma 5.2. Note that it is possible that $t' = 0$, in which case the sets split trivially with $\pi_1(A') = \pi_1(B') = \{0\}$.

Using the notation of Lemma 5.2 we have

$$|\pi_1(A') +_{G_1'} \pi_1(B)| \leq K_1(M_A M_B)^{1/2}. \tag{57}$$

Since ϕ, ψ is an admissible pair, there is $G_1'' \subseteq G_1'$ of size at least $\phi(M_1M_2, \delta_1, K_1)$ such that all $\mathcal{P}$-preimages of its vertex neighbourhoods are $\psi(M_1M_2, \delta_1, K_1)$-separating. Next, since $G_1'' \subseteq G_1'$, for each edge $(a_1, b_1) \in G_1''$, there is a graph $G_2'(a_1, b_1) \subseteq A_2'(a_1) \times B_2'(b_1)$ such that $|G_2'(a_1, b_1)| \geq \delta_2 m_A m_B$ and

$$|A_2'(a_1) +_{G_2'(a_1,b_1)} B_2'(b_1)| \leq K_2(m_A m_B)^{1/2}. \tag{58}$$

Again, by admissibility of ϕ, ψ, there is $G_2''(a_1,b_1) \subseteq G_2'(a_1,b_1)$ of size at least $\phi(m_A m_B, \delta_2, K_2)$ such that all $\mathcal{P}$-preimages of its vertex neighbourhoods are $\psi(m_A m_B, \delta_2, K_2)$-separating.

Now define $G'' \subseteq G \cap (A' \times B')$ as

$$G'' := \{(a_1 \oplus a_2, b_1 \oplus b_2) : (a_1,a_2) \in G_1'', (a_2,b_2) \in G_2''(a_1,b_1)\}.$$

It is clear by construction that indeed all vertices of G'' belong to A' and B' respectively. Moreover, we have

$$|G''| \geq \phi(M_A M_B, \delta_1, K_1)\phi(m_A m_B, \delta_2, K_2). \tag{59}$$

Now let's estimate the separating constant for the $\mathcal{P}$-preimage of a neighbourhood $\mathcal{P}^{-1}[G''(u)]$ of some $u \in V(G'')$. Without loss of generality assume that $n \in B'$ and $b = b_1 \oplus b_2$. We can write

$$G''(b) = \bigcup_{a_1 \in G_1''(b_1)} \bigcup_{a_2 \in G_2''(a_1,b_1)} \{a_1 \oplus a_2\}. \tag{60}$$

Thus,

$$\mathcal{P}^{-1}[G''(b)] = \bigcup_{a_1 \in G_1''(b_1)} p_1^{a_1} \cdot \left\{ \bigcup_{a_2 \in G_2''(a_1,b_1)} p_2^{a_2} \right\}. \tag{61}$$

Here we are using the notation $q^r = q_1^{r_1} \cdots q_l^{r_l}$ for a vector q of primes and a vector r of integers, and p_1 and p_2 are respectively the first t primes from the map $\mathcal{P}$ and the remaining primes. Now, since $G_1''(b_1)$ and $G_2''(a_1,b_1)$ are orthogonal as linear sets we conclude that $(p_1^{a_1}, p_2^{a_2}) = 1$. Thus, by Lemma 2.13 and the admissibility of ϕ, ψ applied to G_1'' and $G_2''(a_1,b_1)$ we conclude that $\mathcal{P}^{-1}[G''(b)]$ is at most $\psi(M_A M_B, \delta_1, K_1)\psi(m_A m_B, \delta_2, K_2)$-separating.

We now record the bounds for the various parameters following from Lemma 5.2. We have

$$\delta_1\delta_2 \geq \left(c\frac{1}{\log^3(K/\delta)}\right)\delta. \tag{62}$$

$$K_1 K_2 \leq \left(C\frac{\log K}{\delta^2}\right)K \tag{63}$$

$$M_A m_A \geq \left(c\frac{\delta^2}{\log(K/\delta)}\right)N_A \tag{64}$$

$$M_B m_B \geq \left(c\frac{\delta^2}{\log(K/\delta)}\right)N_B \tag{65}$$

$$m_A, m_B \geq \left(c\frac{\delta^{10}}{K^4}\right)N^{1/4} \tag{66}$$

In particular, we have

$$M_A M_B < \frac{N_A N_B}{m_A m_B} < \left(c\frac{K^8}{\delta^{20}}\right)N^{1/2}. \tag{67}$$

As a first attempt, we set $N' = M_A M_B$ and $N'' = m_A m_B$, $\delta' = \delta_1$, $K' = K_1$, $\delta'' = \delta_2$ and $K'' = K_2$. If $N'' = m_A m_B$ is less than $N^{1/2}$, one can verify that all of the above bounds comply with the statement of this lemma, and we can stop. If N'' is too big, we will apply Lemma 5.2 again.

To further reduce the size we apply Lemma 5.2 again for each pair of sets $(A_2'(a_1), B_2'(b_1))$ such that $(a_1, b_1) \in G_1'$, stripping off only a single coordinate as explained below. Assume the base point (a_1, b_1) is fixed henceforth.

We split the coordinates $\{t'+1, \dots, n\}$ as $\mathbb{Z} \times \mathbb{Z}^{n-t'-2}$. We apply Lemma 5.2, this time with to the pair of sets $A_2'(a_1)$ and $B_2'(b_1)$ and the graph $G_2'(a_1, b_1)$. To ease notation, let us set $U = A_2'(a_1)$, $V = B_2'(b_1)$, and $H = G_2'(a_1, b_1)$. Here, it is worth noting that U, V and H depend on the base point (a_1, b_1). This time, we have the estimates

$$|U| \approx m_A, |V| \approx m_B$$

and

$$|U +_H V| \leq K_2 \left(|U||V|\right)^{1/2}$$

where $|H| \geq \frac{\delta_2}{4}|U||V|$. We will again denote by π_1 the projection onto the first coordinate, and by π_2 the projection onto the remaining $n - t' - 2$ coordinates. We then get

$$U' \subseteq U, \;\; V' \subseteq V$$

such that

$$U' = \bigcup_{u_1 \in \pi_1(U')} u_1 \oplus U_2'(u_1) \tag{68}$$

$$V' = \bigcup_{y_1 \in \pi_1(V')} v_1 \oplus V_2'(v_1) \tag{69}$$

and the fibers $U_2'(u_1)$ and $V_2'(v_1)$ are of approximately the same size, say m_U and m_V respectively. We also write $M_U = |\pi_1(U)|$ and $M_V = |\pi_1(V)|$. Note again that, for instance, the fiber $U_2'(u_1)$ may be trivial (i.e. $\{0\}$), which simply means that $m_U \approx 1$. By (28), (29) we have the estimates

$$M_U m_U \geq c\delta_2^2 (\log(K_2/\delta_2))^{-1}|U|, \;\; M_V m_V \geq c\delta_2^2 (\log(K_2/\delta_2))^{-1}|V|$$

Next, we have a graph

$$H' \subseteq (U' \times V') \cap H$$

with uniform fibers as defined in Lemma 5.2. The graph H' splits into the base graph $H_1' \subset \pi_1(U') \times \pi_1(V')$ such that

$$|\pi_1(U') +_{H_1'} \pi_1(V')| \leq K_3 (M_U M_V)^{1/2},$$

and fiber graphs $H_2'(u_1, v_1)$ such that for $(u_1, v_1) \in H_1'$

$$|U_2'(u_1) +_{H_2'(u_1, v_1)} V_2'(v_1)| \leq K_4 (m_U m_V)^{1/2}, \tag{70}$$

with

$$|U_2'(u_1)| \approx m_U \tag{71}$$

$$|V_2'(v_1)| \approx m_V \tag{72}$$

$$|H_2'(u_1, v_1)| \geq \delta_4 m_U m_V. \tag{73}$$

The parameters $m_U, m_V, \delta_3, \delta_4, K_3, K_4$ as well as the sizes of H_1' and $H_2'(u_1, v_1)$ are controlled by Lemma 5.2. By the assumption that the original pair (ϕ, ψ) is admissible, for each such a graph $H_2'(u_1, v_1)$ there is a subgraph $H_2''(u_1, v_1) \subseteq H_2'(u_1, v_1)$ with

$$|H_2''(u_1, v_1)| \geq \phi(m_U m_V, \delta_4, K_4) \tag{74}$$

such that the $\mathcal{P}$-preimage of each neighborhood of $H_2''(u_1, v_1)$ is $\psi(m_U m_V, \delta_4, K_3)$-separating. Define $H'' \subset H'$ as

$$H'' = \{(u_1 \oplus u_1, v_1 \oplus v_2) : (u_1, v_1) \in H_1', (u_2, v_2) \in H_2''(u_1, v_1)\}. \tag{75}$$

The size of H'' is at least $|H_1'|\phi(m_U m_V, \delta_4, K_4)$. Next, the set of vertices of H_1' all lie in a one-dimensional affine subspace, so combining Corollary 2.8 and Lemma 2.13 one concludes that the $\mathcal{P}$-preimage of each neighborhood of H'' is $Ck^2\psi(m_U m_V, \delta_4, K_4)$-separating with some absolute constant $C > 0$. Putting together all of the details, we conclude that, for $G_2'(a_1, b_1) \subset A'(a_1) \times B'(b_1)$, there is a subgraph $H'' \subseteq G_2'(a_1, b_1)$ of size at least

$$\phi_{a_1,b_1} := |H_1'|\phi(m_U m_V, \delta_4, K_4) \tag{76}$$

such that the $\mathcal{P}$-preimage of each neighbourhood in H'' is ψ_{a_1,b_1}-separating, where

$$\psi_{a_1,b_1} := Ck^2\psi(m_U m_V, \delta_4, K_4).$$

Since the the graph H'' depends on the pair (a_1, b_1), we now rename this graph H''_{a_1,b_1}.

In turn, substituting ψ_{a_1,b_1} and ϕ_{a_1,b_1} into the argument leading to (59) and Lemma 2.13, we construct a graph

$$G''' := \{(a_1 \oplus a_2, b_1 \oplus b_2) : (a_1, b_1) \in G_1', (a_2, b_2) \in H''_{a_1,b_1}\}.$$

The graph G''' has size at least

$$\phi(M_A M_B, \delta_1, K_1) \cdot \min_{(a_1,b_1)\in G_1'} \phi_{a_1,b_1}, \tag{77}$$

and the separating factors are at most

$$\psi(M_A M_B, \delta_1, K_1) \cdot \max_{(a_1,b_1)\in G_1'} \psi_{a_1,b_1}, \tag{78}$$

With G''' we have now found a large subgraph with good separating factors. In the remaining calculations, we show that the existence of this G''' is good enough to imply the theorem. Essentially it remains to check that the quantities (77) and (78) can indeed be bounded respectively by (48) and (47). Note that the quantities (77) and (78) do depend on the structure of A and B. We are going to show, however, that they are uniformly bounded by (48) and (47) which are functions of (N, δ, K) only. We remark here that we will make use of the following fact: if $|X +_G Y| \leq K(|X||Y|)^{1/2}$ for some $G \subset X \times Y$ of size at least $\delta|X||Y|$, then $K/\delta \geq 1$.

First, since $(a_1, b_1) \in G_1'$ we have by (32)

$$\delta_4 \geq \delta_3\delta_4 > c\log^{-3}(K_2/\delta_2)\delta_2. \tag{79}$$

By (35) and (32)

$$\frac{K_2}{\delta_2} \leq \frac{K_1 K_2}{\delta_1 \delta_2} < \frac{CK \log(K) \log^3(K/\delta)}{\delta^3} \tag{80}$$

and so

$$\log(K_2/\delta_2) < C \log(K/\delta). \tag{81}$$

Consequently,

$$\delta_1 \delta_4 \overset{(79),(81)}{>} c \log^{-3}(K/\delta) \delta_1 \delta_2 \overset{(62)}{>} c \log^{-6}(K/\delta) \delta. \tag{82}$$

Next, by (35)

$$K_4 \leq \frac{K_3 K_4}{\delta_3 \delta_4} \leq C K_2 \log^2(K_2) \delta_2^{-4} \tag{83}$$

and by (32)

$$\delta_2 > c \log^{-3}(K/\delta) \delta \tag{84}$$

$$K_2 < C \delta^{-4} K \log^2 K. \tag{85}$$

Therefore

$$\begin{aligned} \log^2(K_2) \delta_2^{-4} &\leq C \log^{14}(K/\delta) \delta^{-4} \\ &= C(\delta^{14} \log^{14}(K/\delta)) \delta^{-18} < C(\log^{14} K) \delta^{-18} \end{aligned} \tag{86}$$

and

$$K_1 K_4 \overset{(83)}{\leq} C K_1 K_2 \log^2(K_2) \delta_2^{-4} \overset{(63),(86)}{\leq} C \frac{K \log^{15} K}{\delta^{20}}. \tag{87}$$

Finally, we have by (28), (32), (33) and (34) that

$$\begin{aligned} |H_1'| m_U m_V &\geq c \log^{-3}(K_2/\delta_2) \delta_2 (\delta_2^4 \log^{-2}(K_2/\delta_2)) |A_2(a_1)| |B_2(b_1)| \\ &\geq c \log^{-5}(K/\delta) \delta_2^5 m_A m_B \overset{(84)}{\geq} c \log^{-20}(K/\delta) \delta^5 m_A m_B. \end{aligned} \tag{88}$$

Define

$$N'' := \min\{N^{1/2}, \max\{m_U m_V, c \log^{-20}(K/\delta) \delta^5 m_A m_B\}\}. \tag{89}$$

By our choice of t' it follows that $m_U m_V \leq N''$. By (A4) we have

$$\frac{m_U m_V}{N''} \phi(N'', \delta_3, K_3) \leq \phi(m_U m_V, \delta_4, K_4). \tag{90}$$

Defining

$$N' := \frac{M_A M_B m_U m_V}{N''} |H_1'|, \tag{91}$$

we have by (88) and (89) that $M_A M_B \leq N'$, so by (A4) again

$$\frac{M_A M_B}{N'} \phi(N', \delta_1, K_1) \leq \phi(M_A M_B, \delta_1, K_1), \tag{92}$$

so

$$\begin{aligned}\phi(N',\delta_1,K_1)\phi(N'',\delta_3,K_3) &\leq \frac{N'}{M_AM_B}\phi(M_AM_B,\delta_1,K_1)\frac{N''}{m_Um_V}\phi(m_Um_V,\delta_3,K_3)\\ &\overset{(76)}{=} \phi(M_AM_B,\delta_1,K_1)\phi_{a_1,b_1}. \end{aligned} \tag{93}$$

On the other hand,

$$\begin{aligned} N'N'' &= M_AM_Bm_Um_V|H_1'| && (94)\\ &\overset{(88)}{\geq} c\log^{-20}(K/\delta)\delta^5 M_AM_Bm_Am_B && (95)\\ &\overset{(28),(29)}{\geq} c\delta^9\log^{-22}(K/\delta)N. && (96)\end{aligned}$$

Also, since

$$m_Am_B \overset{(66)}{>} c\delta^{20}K^{-8}N^{1/2},$$

it follows from the definition of N'' in (89) that

$$c\delta^{45}K^{-11}N^{1/2}\leq N''\leq N^{1/2}.$$

Then, since $N''N'\leq N$,

$$N'\leq C\delta^{-45}K^{11}N^{1/2},$$

and so

$$N'+N''\leq C\delta^{-45}K^{11}N^{1/2}. \tag{97}$$

We now have all the estimates to finish the proof. The bounds (82), (87), (94), (97) verify that the parameters

$$\begin{aligned}\delta' &:= \delta_1,\ \ \delta'':=\delta_4\\ K' &:= K_1,\ \ K'':=K_4\end{aligned} \tag{98}$$

and N',N'' indeed satisfy the constraints (49). Recall that by (A1) $\psi(\cdot,\delta,K)$ is increasing in the first argument, so by (67) and (54)

$$\begin{aligned}\psi_*(N,\delta,K) &\geq Ck^2\psi\left(\max\left\{N^{1/2},\frac{N}{m_Am_B}\right\},\delta_1,K_1\right)\psi\left(\min\{N^{1/2},m_Am_B\},\delta_4,K_4\right)\\ &\geq \psi(M_AM_B,\delta_1,K_1)\psi_{x,y}.\end{aligned} \tag{99}$$

In the previous inequality, we have used monotonicity (A1) and the information that $\frac{N}{m_Am_B}\geq M_AM_B$, $N^{1/2}\geq m_Um_V$, $m_A\geq m_U$ and $m_B\geq m_V$.

Also, (93) and (77) verify that

$$\begin{aligned}\phi_*(N,\delta,K) &\leq \phi(N',\delta_1,K_1)\phi(N'',\delta_4,K_4)\\ &\leq \phi(M_AM_B,\delta_1,K_1)\phi_{a_1,b_1}.\end{aligned} \tag{100}$$

It follows that the pair (ψ_*,ϕ_*) is indeed admissible since (99) and (100) hold for all base points $(a_1,b_1)\in G_1'$ and thus uniformly bound (78) and (77) respectively. □

7. A better admissible pair

With Lemma 6.3 at our disposal we can start with the data (N, δ, K) and reduce the problem to the case of smaller and smaller N and K with reasonable losses in δ. The process can be described by a binary a tree where each node with the data (N, δ, K) splits into two children with the attached data being approximately equal to $(N^{1/2}, \delta', K')$ and $(N^{1/2}, \delta', K'')$, with $K'K''$ roughly equal to K and $\delta'\delta''$ roughly equal to δ. Thus, when the height of the tree is about $\log\log K$, the K's in the most of the nodes should be small enough so that Lemma 6.2 becomes non-trivial. Going from the bottom to the top we then recover an improved admissible pair of functions at the root node.

Lemma 7.1. *For any $\gamma > 0$ there exists $C(\gamma) > 0$ such that the pair*

$$\phi(N, \delta, K) := \left(\frac{\delta}{K}\right)^{C \log\log(K/\delta)} N \tag{101}$$

$$\psi(N, \delta, K) := k^{\log(K/\delta)^{C/\gamma}} N^{\gamma} \tag{102}$$

is admissible.

Proof. Let N, δ, K be fixed. Take an integer $t = 2^l$ to be specified later (l is going to be the height of the tree and t the total number of nodes).

Let (ϕ_0, ψ_0) be the Freiman-type admissible pair given by Lemma 6.2. We apply recursively Lemma 6.3 and obtain admissible pairs for $i = 1, \dots, l$ as follows

$$\psi_i := \max Ck^2 \psi_{i-1}(N', \delta', K')\psi_{i-1}(N'', \delta'', K'') \tag{103}$$

$$\phi_i := \min \phi_{i-1}(N', \delta', K')\phi_{i-1}(N'', \delta'', K''), \tag{104}$$

(with the max and min taken over the set of parameters constrained by (49)). Thus, at the root node we have the admissible pair $\psi := \psi_{l-1}, \phi := \phi_{l-1}$ given by

$$\psi(N, \delta, K) := (Ck^2)^{2^l} \prod_{\nu \in \{0,1\}^l} \psi_0(N'_\nu, \delta'_\nu, K'_\nu) \tag{105}$$

$$\phi(N, \delta, K) := \prod_{\nu \in \{0,1\}^l} \phi_0(N_\nu, \delta_\nu, K_\nu) \tag{106}$$

for some data $(N_\nu, \delta_\nu, K_\nu)$ and (possibly different) $(N'_\nu, \delta'_\nu, K'_\nu)$ at the leaf nodes of the tree which attain the respective maxima and minima. For intermediate tree nodes ν, denoting by $\{\nu, 0\}$ and $\{\nu, 1\}$ the left and right child of ν respectively, one has

$$c_1 \delta_\nu^9 \log^{-22}(K_\nu/\delta_\nu) N_\nu \le N_{\nu,0} N_{\nu,1} \le N_\nu \tag{107}$$

$$N_{\nu,0} + N_{\nu,1} \le C_1 \delta_\nu^{-45} K_\nu^{11} N_\nu^{1/2} \tag{108}$$

$$K_{\nu,0} K_{\nu,1} \le C_1 \frac{\log^{15} K_\nu}{\delta_\nu^{20}} K_\nu \tag{109}$$

$$\delta_{\nu,0}\delta_{\nu,1} \ge c_1 \log^{-6}(K_\nu/\delta_\nu)\delta_\nu, \tag{110}$$

and similarly for $(N'_\nu, \delta'_\nu, K'_\nu)$. The absolute constants c_1 and C_1 are exactly those given in the statement of Lemma 6.3 as c and C respectively. They have been relabelled here in an attempt to distinguish them.

In what follows we assume that N is large enough so that $\log K_\nu > C$ and $\log(\delta_\nu^{-1}) > c^{-1}$ and the constants C, c can be swallowed by an extra power of $\log(K/\delta)$.

We have

$$\log \frac{K_{\nu,0}}{\delta_{\nu,0}} + \log \frac{K_{\nu,1}}{\delta_{\nu,1}} < 20 \log \frac{K_\nu}{\delta_\nu}$$

so for an arbitrary $1 < l' \leq l$

$$\max_{\nu \in \{0,1\}^{l'}} \log \frac{K_\nu}{\delta_\nu} \leq \sum_{\nu \in \{0,1\}^{l'}} \log \frac{K_\nu}{\delta_\nu} < 20^{l'} \log \frac{K}{\delta}. \tag{111}$$

Next, it follows from (110) and (111) that

$$\begin{aligned} \prod_{\nu \in \{0,1\}^{l'}} \delta_\nu = \prod_{\nu \in \{0,1\}^{l'-1}} \delta_{\nu,0}\delta_{\nu,1} &\geq \prod_{\nu \in \{0,1\}^{l'-1}} c_1 \left(\log \frac{K_\nu}{\delta_\nu}\right)^{-6} \delta_\nu \\ &> \prod_{\nu \in \{0,1\}^{l'-1}} c_1 \left(20^{l'} \log \frac{K}{\delta}\right)^{-6} \prod_{\nu \in \{0,1\}^{l'-1}} \delta_\nu \\ &= \left(\frac{20}{c_1}\right)^{-3l' \cdot 2^{l'}} \left(\log \frac{K}{\delta}\right)^{-3 \cdot 2^{l'}} \prod_{\nu \in \{0,1\}^{l'-1}} \delta_\nu. \end{aligned} \tag{112}$$

Applying (112) iteratively then yields

$$\prod_{\nu \in \{0,1\}^{l'}} \delta_\nu > \left(\frac{20}{c_1}\right)^{-6l' \cdot 2^{l'}} \left(\log \frac{K}{\delta}\right)^{-6 \cdot 2^{l'}} \delta. \tag{113}$$

Using similar arguments, we obtain the following bounds:

$$\prod_{\nu \in \{0,1\}^{l'}} K_\nu < \left(\frac{20C_1}{c_1}\right)^{280 \cdot l' 2^{l'}} \left(\log \frac{K}{\delta}\right)^{280 \cdot 2^{l'}} \delta^{-20l'} K \tag{114}$$

and

$$\prod_{\nu \in \{0,1\}^{l'}} N_\nu > \left(\frac{20}{c_1}\right)^{-160 \cdot l' 2^{l'}} \left(\log \frac{K}{\delta}\right)^{-160 \cdot 2^{l'}} \delta^{9l'} N. \tag{115}$$

For more details on how these bounds are obtained, see [4, p. 492].

Substituting (113), (114), (115) into (106) and Lemma 6.2 (2) we get

$$\begin{aligned} \phi(N, \delta, K) = \prod_{\nu \in \{0,1\}^l} \phi_0(N_\nu, \delta_\nu, K_\nu) &= \prod_{\nu \in \{0,1\}^l} \left(\frac{\delta_\nu}{K_\nu}\right)^C N_\nu \\ &\geq e^{-C' l 2^l} \left(\log \frac{K}{\delta}\right)^{-C' 2^l} \delta^{lC'} K^{-C'} N, \end{aligned}$$

for some suitable $C' > 0$. Taking[8]

$$l := \log\log(K/\delta)$$

we obtain

$$\phi(N, \delta, K) \geq \left(\frac{\delta}{K}\right)^{C \log\log(K/\delta)} N$$

for some suitable $C > 0$.

We now turn to ψ. For the sake of notation we use again $(N_\nu, \delta_\nu, K_\nu)$ instead of $(N'_\nu, \delta'_\nu, K'_\nu)$. The bounds above, however, still hold.

By (105) and Lemma 6.2

$$\psi(N, \delta, K) = (Ck^2)^{2^l} \prod_{\nu \in \{0,1\}^l} \min\left\{(2k^2)^{\left(\frac{K_\nu}{\delta_\nu}\right)^C}, N_\nu\right\}. \tag{116}$$

In order to bound the quantity of the right hand side effectively, we will need a suitable uniform bound for individual N_ν, which we deduce below.

It follows from (110) that

$$\delta_{\nu,0}, \delta_{\nu,1} \geq c_1 \left(\log \frac{K_\nu}{\delta_\nu}\right)^{-6} \delta_\nu. \tag{117}$$

Applying this bound as well as (111), it follows that for any $1 \leq l' \leq l$ and $\nu \in \{0,1\}^{l'}$,

$$\delta_\nu = \delta_{\nu',\cdot} \geq c_1 \left(\log \frac{K_{\nu'}}{\delta_{\nu'}}\right)^{-6} \delta_{\nu'} \geq (20C)^{-6l'} \left(\log \frac{K}{\delta}\right)^{-6} \delta_{\nu'}. \tag{118}$$

Iteratively applying (118) yields

$$\delta_\nu \geq (20C)^{-6l'^2} \left(\log \frac{K}{\delta}\right)^{-6l'} \delta. \tag{119}$$

Similarly, since $K_\nu \geq \delta_\nu$, it follows from (109) and (117) that

$$K_{\nu,0} \leq C_1 \frac{K_\nu \log^{15} K_\nu}{\delta_\nu^{20} \delta_{\nu,1}} \leq C'_1 \frac{\left(\log \frac{K_\nu}{\delta_\nu}\right)^{21}}{\delta_\nu^{21}} K_\nu.$$

The same argument implies that $K_{\nu,1} \leq C'_1 \frac{K_\nu \left(\log \frac{K_\nu}{\delta_\nu}\right)^{21}}{\delta_\nu^{21}}$. Therefore, by applying (111) and (119), it follows that for any $\nu \in \{0,1\}^{l'}$,

$$K_\nu = K_{\nu',*} \leq C'_1 \frac{K_{\nu'} \left(\log \frac{K_{\nu'}}{\delta_{\nu'}}\right)^{21}}{\delta_{\nu'}^{21}} \leq \frac{(20C)^{147l'^2} \left(\log \frac{K}{\delta}\right)^{147l'}}{\delta^{21}} K_{\nu'}. \tag{120}$$

Iterating (120) yields

$$K_\nu \leq \frac{(20C)^{147l'^3} \left(\log \frac{K}{\delta}\right)^{147l'^2}}{\delta^{21l'}} K. \tag{121}$$

To bound N_ν, first note that (108), (119) and (121) together imply that for any $\nu' \in \{0,1\}^{l'}$,

$$N_{\nu,0} + N_{\nu,1} \leq C_1 \delta_\nu^{-45} K_\nu^{11} N_\nu^{1/2} \leq \frac{(20C_1)^{1887l'^3} \left(\log \frac{K}{\delta}\right)^{1887l'^2} K^{11}}{\delta^{276l'}} N_\nu^{1/2}.$$

[8]Strictly speaking we should ensure that l is an integer by taking $l := \lfloor \log\log(K/\delta) \rfloor$. In order to simplify calculations and avoid adding further multiplicative constants, we assume that l as defined here is already an integer.

Applying this bound iteratively yields (with some rather crude estimates)

$$N_\nu \leq \frac{(20C_1)^{4000l'^3}\left(\log\frac{K}{\delta}\right)^{4000l'^2}K^{22}}{\delta^{4000l'}}N^{\frac{1}{2^{l'}}}. \tag{122}$$

Before inserting (122) into (116), we split the data $(N_\nu, \delta_\nu, K_\nu)$ into two parts, $I \cup J = \{0,1\}^l$, such that

$$I = \left\{\nu : \frac{K_\nu}{\delta_\nu} < T\right\}$$

and

$$J = \left\{\nu : \frac{K_\nu}{\delta_\nu} \geq T\right\},$$

with the threshold T specified later.

By (113) and (114) we see that $|J|$ is rather small:

$$T^{|J|} \leq \prod_{\nu\in\{0,1\}^l}\frac{K_\nu}{\delta_\nu} < \left(\frac{20C_1}{c_1}\right)^{286\cdot l2^l}\log(\frac{K}{\delta})^{286\cdot 2^l}\delta^{-21l}K. \tag{123}$$

Set $t := 2^l$, so it follows from (123) that for an appropriate constant C_2,

$$|J|\log T \leq C_2 lt.$$

Choose

$$\log T := C_2\gamma^{-1}l = \frac{C_2\log\log(K/\delta)}{\gamma}. \tag{124}$$

Thus

$$\frac{|J|}{t} \leq \frac{C_2 l}{\log T} = \gamma. \tag{125}$$

We are finally ready to put everything together:

$$\begin{aligned}
\psi(N,\delta,K) &\overset{(116)}{=} (Ck^2)^{2^l}\prod_{\nu\in\{0,1\}^l}\min\left\{(2k^2)^{\left(\frac{K_\nu}{\delta_\nu}\right)^C}, N_\nu\right\}.\\
&\leq (Ck^2)^{2^l}\prod_{\nu\in I}(2k^2)^{T^C}\prod_{\nu\in J}N_\nu\\
&\overset{(122)}{\leq} (C'k^2)^{tT^C}\left(\frac{(20C_1)^{4000l^3}\left(\log\frac{K}{\delta}\right)^{4000l^2}K^{22}}{\delta^{4000l}}N^{\frac{1}{t}}\right)^{|J|}\\
&\overset{(125)}{\leq} k^{\left(\log\frac{K}{\delta}\right)^{\frac{C''}{\gamma}}}N^\gamma.
\end{aligned}$$

□

8. A strong admissible pair

Finally, in this section we will use Lemma 7.1 to get an even better pair of admissible functions.

Lemma 8.1. *Given $0 < \tau, \gamma < 1/2$ there exist positive constants $\alpha_i(\tau,\gamma,k), \beta_i(\tau,\gamma,k), i = 1,2,3$ such that for all sufficiently large N, the pair*

$$\phi(N,\delta,K) := K^{-\alpha_1}\delta^{\alpha_2\log\log N}e^{\alpha_3(\log\log N)^2}N^{1-\tau} \tag{126}$$

$$\psi(N,\delta,K) := K^{\beta_1}\delta^{-\beta_2\log\log N}e^{-\beta_3(\log\log N)^2}N^{\gamma} \tag{127}$$

is admissible.

Proof. The strategy of the proof is as follows. We start with the already not-so-bad admissible pair given by Lemma 7.1 and improve it by repeated application of Lemma 6.3.

Let $P_N[\phi,\psi]$ be the predicate that the pair (ϕ,ψ) given by (126) and (127) is admissible in the sense of Definition 6.1 for all graphs of size at most N and at least $N^{1/2}$.

We are going to prove that

(1) The base case: $P_{N_0}[\phi,\psi]$ is true for some $N_0(\tau,\gamma)$.
(2) The inductive step: $P_N[\phi,\psi] \Rightarrow P_{N^{3/2}}[\phi,\psi]$.

The exponent $3/2$ is of little importance here and is taken with much room to spare. Lemma 8.1 will then follow by induction, for all $N \geq N_0$.

In order to prove (1) it suffices to find a fixed threshold $N_0(\tau,\gamma)$ such that the pair (126), (127) is either trivial or worse than that given by Lemma 7.1 if $N \leq N_0$. One can achieve this by fine-tuning the constants α_1, β_1, which we now explain.

Apply Lemma 7.1 with $\gamma = \gamma/4$ to obtain an admissible pair given by (101), (102). We seek to choose α_1, β_1 and $N_0(\delta,\gamma)$ such that for each N in the range $N_0^{1/2} \leq N \leq N_0$

$$\left(\frac{\delta}{K}\right)^{C(\gamma)\log\log(K/\delta)} N \geq K^{-\alpha_1}\delta^{\alpha_2 \log\log N} e^{\alpha_3(\log\log N)^2} N^{1-\tau} \tag{128}$$

$$\min\{N, \exp\left(\log k \cdot \log(K/\delta)^{C(\gamma)/\gamma}\right) N^{\gamma/4}\} \leq K^{\beta_1}\delta^{-\beta_2\log\log N} e^{-\beta_3(\log\log N)^2} N^{\gamma}. \tag{129}$$

To ensure (128) holds it is sufficient to take $\alpha_1 = \frac{C(\gamma)}{2}\log\log N_0$ with $C(\gamma) > 0$ from Lemma 7.1 and to take $\alpha_2 = C_2\alpha_1$ and $\alpha_3 = C_3\alpha_1$ for some absolute constants $C_2, C_3 \geq 1$. Indeed,

$$\begin{aligned} K^{-\alpha_1}\delta^{\alpha_2\log\log N} e^{\alpha_3(\log\log N)^2} N^{1-\tau} &\leq \left(\frac{\delta}{K}\right)^{\alpha_1} e^{\alpha_3(\log\log N)^2} N^{1-\tau} \\ &\leq \left(\frac{\delta}{K}\right)^{C(\gamma)\log\log N} e^{\alpha_3(\log\log N)^2} N^{1-\tau} \\ &\leq \left(\frac{\delta}{K}\right)^{C(\gamma)\log\log N} N, \end{aligned}$$

where the last inequality holds as long as we take N_0 sufficiently large (and thus also N is sufficiently large). Inequality (128) then follows since the inequality $N \geq \frac{K}{\delta}$ holds by definition of N, δ and K.

Ensuring (129) is more involved, as later on want to impose the further constraint $\beta_3 > \beta_2 > \beta_1$. For now, it suffices to guarantee that

$$\log k \cdot \log\left(\frac{K}{\delta}\right)^{\frac{C}{\gamma}} < \frac{\gamma}{4}\log N \tag{130}$$

and

$$e^{\beta_3(\log\log N)^2} < N^{\frac{\gamma}{2}}. \tag{131}$$

However, the bound (130) fails only if K/δ is rather large, namely

$$\frac{K}{\delta} > e^{\log^{c\gamma} N}$$

for some $c(C,\gamma,k)>0$. In this case it suffices to take β_1 so large that

$$K^{\beta_1}\delta^{-\beta_2\log\log N}e^{-\beta_3(\log\log N)^2}N^{\gamma}>N$$

and thus (129) holds. To this end, we set

$$\beta_1:=(\log N_0)^{1-c\gamma}$$

and make the constraint that, say,

$$\beta_3,\beta_2<10\beta_1\log\log N_0.$$

Moreover, this constraint on β_3 also ensures that (131) holds for N sufficiently large.

Summing up, we have found some fixed threshold $N_0(\tau,\gamma)$ at which (126), (127) become admissible with fixed α_1,β_1 and still some freedom to define the constants $\alpha_2,\beta_2,\alpha_3$, and β_3.

We now turn to part (2) of the induction scheme, the inductive step. Assuming that N',N'' are at the scale so that (126), (127) are admissible with the data (N',δ',K'); (N'',δ'',K'') we will show that (126), (127) are also admissible for the data (N,δ,K) with $N\approx N'N''$.

Assuming β_1 (or N_0) is large enough we may assume that

$$\frac{K}{\delta}<N^{10^{-4}}, \tag{132}$$

as otherwise (127) $>N$ which is trivially admissible.

We need to estimate

$$\psi(N',\delta',K')\psi(N'',\delta'',K'')$$

from above and

$$\phi(N',\delta',K')\phi(N'',\delta'',K''),$$

from below in order to verify that (126), (127) are admissible for (N,δ,K). By (132), the constraints (49) can be relaxed to

$$N\geq N'N'' > N\left(\frac{\delta}{\log N}\right)^{40}>N^{99/100} \tag{133}$$

$$N'+N'' < N^{1/2}\left(\frac{K}{\delta}\right)^{45}<N^{1/2+1/40} \tag{134}$$

$$\delta'\delta'' > \frac{\delta}{\log^6 N} \tag{135}$$

$$K'K'' < \delta^{-20}(\log N)^{15}K. \tag{136}$$

From (133) and (134) we have (with room to spare)

$$N^{1/2-1/20}<N',N''<N^{1/2+1/20} \tag{137}$$

and so assuming N is large enough

$$\frac{99}{100}\log\log N<\log\log N',\ \log\log N''<\log\log N-\log\frac{20}{11}. \tag{138}$$

With the constraints above, it suffices to verify (writing ll for log log as in [4]) that

$$(K'K'')^{-\alpha_1}(\delta')^{\alpha_2 llN'}(\delta'')^{\alpha_2 llN''}e^{\alpha_3[(llN')^2+(llN'')^2]}(N'N'')^{1-\tau} \tag{139}$$

is indeed always bounded below by (126). We can bound (139) by

$$K^{-\alpha_1}\delta^{\alpha_2 llN}e^{\alpha_3(llN)^2}N^{1-\tau}u\cdot v \tag{140}$$

where

$$u = (\log N)^{-15\alpha_1-6\alpha_2 llN-40}e^{\frac{9}{10}\alpha_3(llN)^2} \tag{141}$$

$$v = \delta^{20\alpha_1-\log\frac{20}{11}\alpha_2+40}. \tag{142}$$

For suitable choices of $\alpha_2,\alpha_3>\alpha_1$ both $u,v>1$ so (126) is admissible.

Similarly for (127) we have

$$(K'K'')^{\beta_1}(\delta')^{-\beta_2 llN'}(\delta'')^{-\beta_2 llN''}e^{-\beta_3[(llN')^2+(llN'')^2]}(N'N'')^{\gamma} \tag{143}$$

$$< K^{\beta_1}\delta^{-\beta_2 llN}e^{-\beta_3(llN)^2}N^{\gamma}u\cdot v \tag{144}$$

with

$$u = (\log N)^{15\beta_1+6\beta_2 llN}e^{-\frac{9}{10}\beta_3(llN)^2} \tag{145}$$

$$v = \delta^{-20\beta_1+\log\frac{20}{11}\beta_2}. \tag{146}$$

Again, by taking suitable $\beta_3>\beta_2>\beta_1$ we make $u,v<1$ so (127) is admissible. This closes the induction on scales argument and finishes the proof.

□

9. Concluding the proof of Theorem 3.1

We are finally ready to finish the proof of Theorem 3.1. Recall that the aim is to show that, given $0<\tau,\gamma<1/2$, there are positive constants $C_1=C_1(\tau,\gamma,k)$ and $C_2=C_2(\tau,\gamma,k)$, such that for any $A\subset\mathbb{Q}$ with $|AA|\leq K|A|$, there exists $A'\subset A$ with $|A'|\geq K^{-C_1}|A|^{1-\tau}$, such that A' is $K^{C_2}|A|^{\gamma}$-separating.

Since $|AA|\leq K|A|$, after applying the prime evaluation map, we have $|\mathcal{P}(A)+\mathcal{P}(A)|\leq K|\mathcal{P}(A)|$. Fix $\gamma'=\gamma/2$, $\tau'=\tau/2$, and apply Lemma 8.1 for this choice of γ',τ', with the full graph $G=\mathcal{P}(A)\times\mathcal{P}(A)$. It follows that there is a subgraph $G'\subset G$ such

$$|G'|\geq K^{-\alpha_1}e^{\alpha_3(\log\log|A|)^2}|A|^{2-2\tau'}\geq K^{-\alpha_1}|A|^{2-2\tau'}$$

and such that for each $v\in V(G)$ the $\mathcal{P}$-preimages of $N_{G'}(v)$ is

$$K^{\beta_1}e^{-\beta_3(\log\log|A|)^2}|A|^{2\gamma'}\leq K^{\beta_1}|A|^{2\gamma'}$$

separating.[9]

Then, by the pigeonhole principle, there is a vertex $v\in V(G)$ such that $|N_{G'}(v)|\geq|A|^{1-2\tau'}$. Write $A'=\mathcal{P}^{-1}(N_{G'}(v))$ for the preimage of the neighbourhood of v. Then this is a subset of A with the required properties.

[9]Note here that we have discarded the extra information coming from the terms of the form $e^{\pm C(\log\log|A|)^2}$.

10. Further Applications

Proof of Theorem 1.8. Recall that Theorem 1.8 is the following statement. For all $\gamma \geq 0$ there exists a constant $C = C(\gamma)$ such that for any finite $A \subset \mathbb{Q}$ with $|AA| \leq K|A|$ and any finite set L of lines in the plane, $I(P, L) \leq 3|P| + |A|^{\gamma} K^{C} |L|$, 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 $m, c \neq 0$. 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 $m = \frac{y-y'}{x-x'}$. 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 $|l_{m,c} \cap P| \leq K^{C} |A|^{\gamma}$. 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 $B, B' \subset \mathbb{Q}$,

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

We will prove that

$$S \leq 2|A|^{\gamma} K^{C} (|B'|^{1/2}|B| + |B'|). \tag{147}$$

Since the roles of B and B' are interchangeable, (147) 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,

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

Therefore,

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

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

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

□

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, Imre Ruzsa 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] A. Balog, O. Roche-Newton and D. Zhelezov, 'Expanders with superquadratic growth', *Electron. J. Combin.* **24** (2017), no. 3, Paper 3.14, 17 pp.
[3] F. Beukers and H. P. Schlickewei, 'The equation $x+y=1$ in finitely generated groups', *Acta Arith.* 78(2) (1996), 186–199.
[4] J. Bourgain and M.-C. Chang, 'On the size of k-fold sum and product sets of integers', *J. Amer. Math. Soc.* **17**, no. 2, (2004), 473-497.
[5] J. Bourgain and M.-C. Chang, 'Sum-product theorems in algebraic number fields' *J. Anal. Math.* **109** (2009), 253-277.
[6] M.-C. Chang, 'The Erdős-Szemerdi problem on sum set and product set', *Ann. of Math. (2)* **157**, no. 3, (2003), 939-957.
[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, no. 1, (2010), 125-132.**
[10] B. Hanson, O. Roche-Newton and D. Zhelezov, 'On iterated product sets with shifts', *arXiv:1801.07982 (2018).*
[11] T. G. F. Jones and O. Roche-Newton, 'Improved bounds on the set $A(A+1)$', *J. Combin. Theory Ser. A* **120**, no. 3, (2013), 515-526.
[12] S. V. Konyagin and I. D. Shkredov, 'On sum sets of sets, having small product set', *Proc. Steklov Inst. Math.* **290** (2015), 288-299.
[13] S. V. Konyagin and I. D. Shkredov, 'New results on sums and products in $\mathbb{R}$', *Proc. Steklov Inst. Math.* **294** (2016), 87-98.
[14] G. Petridis, 'New proofs of Plünnecke-type estimates for product sets in groups', *Combinatorica* **32**, no. 6, (2012), 721-733.
[15] I. D. Shkredov and D. Zhelezov, 'On additive bases of sets with small product set', *IMRN* **2018**, no. 5, (2018), 1585-1599.
[16] J. Solymosi, 'Bounding multiplicative energy by the sumset', *Adv. Math.* **222** (2009), 402-408.
[17] T. Tao, V. Vu. 'Additive combinatorics' *Cambridge University Press* (2006).
[18] 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