On the discretized sum-product problem

Larry Guth[*]   Nets Hawk Katz[†]   Joshua Zahl[‡]

December 5, 2019

Abstract

We give a new proof of the discretized ring theorem for sets of real numbers. As a special case, we show that if $A \subset \mathbb{R}$ is a $(\delta, 1/2)_1$-set in the sense of Katz and Tao, then either $A + A$ or $A.A$ must have measure at least $|A|^{1-\frac{1}{68}}$.

1 Introduction

A $(\delta, \sigma)_1$-set is a discretized analog of a σ-dimensional subset of $\mathbb{R}$. More precisely, for $\delta > 0$ we say that a set $A \subset \mathbb{R}$ is δ-discretized if it is a union of closed intervals of length δ. We say that a δ-discretized set $A \subset [1, 2]$ is a $(\delta, \sigma)_1$-set if $|A| \approx \delta^{1-\sigma}$ and if it satisfies the non-concentration condition $|A \cap I| \lesssim |I|^{\sigma}|A|$ for all intervals I.

In [10], Katz and Tao conjectured that a $(\delta, 1/2)_1$ set cannot be approximately closed under both addition and multiplication. Specifically, they conjectured that there exists an absolute constant $c > 0$ so that if $A \subset [1, 2]$ is a $(\delta, 1/2)_1$-set, then

$$|A + A| + |A.A| \gtrapprox \delta^{-c}|A|. \tag{1}$$

This conjecture was proved by Bourgain [1], who established (1) whenever A is a $(\delta, \sigma)_1$ set, $0 < \sigma < 1$. In [1], the constant $c = c(\sigma) > 0$ is not explicitly computed, but an examination of [1] suggests that the constant is very small. Subsequent work by Bourgain-Gamburd and Bourgain [4, 2], and work in progress by Lindenstrauss-Varjú and Bateman-Lie proved variants of (1) where the set A satisfies weaker non-concentration conditions.

In this paper, we obtain a short new proof of (1) that establishes an explicit value of c.

Theorem 1.1. *Let $0 < \sigma < 1$. Let $A \subset [1, 2]$ be a δ-discretized set of measure $\delta^{1-\sigma}$. Suppose that for all intervals I, we have the non-concentration estimate*

$$|A \cap I| \leq C|I|^{\sigma}|A|. \tag{2}$$

Then for every $c < \frac{\sigma(1-\sigma)}{4(7+3\sigma)}$, we have

$$|A + A| + |A.A| \gtrsim C^{-O(1)}\delta^{-c}|A|. \tag{3}$$

In [1, Section 4], Bourgain proved that Theorem 1.1 (with any value $c > 0$) establishes the Erdős-Volkmann ring conjecture [7]: there does not exist a measurable subring of the reals of Hausdorff dimension strictly between 0 and 1. This was first proved by Edgar and Miller in [6].

Remark 1.2. In [4], Bourgain and Gamburd established a variant of Theorem 1.1 where the non-concentration hypothesis (2) was replaced by the weaker requirement

$$|A \cap I| \leq C|I|^\tau |A| \tag{4}$$

for some $\tau > 0$ (in particular, τ may be smaller than σ). They obtained their result by reducing the general case $\tau > 0$ to the special case $\tau = \sigma$, and then applying the previously established discretized sum-product theorem from [1]. A similar reduction can be used to obtain a variant of Theorem 1.1 where A satisfies the weaker non-concentration hypothesis (4). When this is done, the constant c in (3) will depend on both σ and τ.

Our proof of Theorem 1.1 uses many of the ideas from Garaev's sum-product theorem in $\mathbb{F}_p$ from [8]. In [8], Garaev proved that if $A \subset \mathbb{F}_p$ with $|A| < p^{7/13}(\log p)^{-4/13}$, then $|A + A| + |A.A| \gtrsim |A|^{15/14}/(\log|A|)^{2/7}$. By refining Garaev's arguments, the exponent of $15/14$ was improved to $14/13$ by Shen and the second author [9]; to $13/12$ by Bourgain and Garaev [3]; and to $12/11$ by Rudnev [13].

Glossing over several technical details, Garaev's proof proceeds as follows. Either $\frac{A-A}{A-A} = \mathbb{F}_p$, or there is an element $x \in \frac{A-A}{A-A}$ so that $x + 1 \notin \frac{A-A}{A-A}$. If the former occurs, then Plünnecke's inequality (discussed further in Section 3 below) implies that $|A + A| + |A.A|$ must be large. In our proof, we will call this situation the "dense case." If the latter occurs, then we can write $x = \frac{a-b}{c-d}$, where $a, b, c, d \in A$. Since $x + 1 \notin \frac{A-A}{A-A}$, we have $|A + (x+1)A| = |A|^2$, and this in turn implies that $|(a-b)A + (c-d)A + (c-d)A| \geq |A|^2$. Plünnecke's inequality now implies that $|A + A| + |A.A|$ must be large. In our proof, we will call this situation the "gap case."

When mimicking Garaev's argument for discretized subsets of $\mathbb{R}$, we run into several issues. First, if $A \subset [1, 2]$ is a δ-discretized set, then the "denominators" in the set $\frac{A-A}{A-A}$ might be very small. Rather than considering the entire set $\frac{A-A}{A-A}$, we pick a cutoff and look at quotients where the denominator is not too small. Several steps in the argument have to be tuned or adjusted to take account of the size of the denominator.

If the set of quotients is sufficiently dense, then we proceed as in the "dense case" of Garaev's argument. Otherwise, there is a fairly large gap in our set of quotients. Suppose that we had an element x in our set of quotients and $x + 1$ was in the middle of the fairly large gap. Then we could adapt Garaev's argument from the "gap case" described above. Unfortunately, there is no guarantee that this will happen. Instead, we show that if our set of quotients has a fairly large gap, we can find a x in our set of quotients so that either $x/2$ or $(x+1)/2$ is in the middle of the large gap, and we can use this element in the same way that Garaev uses $x + 1$.

1.1 Notation

If $X \subset \mathbb{R}$ and $t > 0$, we will write $\mathcal{E}_t(X)$ to denote the t-covering number of X, that is, the cardinality of the smallest covering of X by intervals of length t. We will write $\mathcal{N}_t(X)$ to denote the closed t neighborhood of X, and we will write X_t to denote $\mathcal{N}_t(X) \cap t\mathbb{Z}$; this is the discretization of X at scale t. We say a set $X \subset \mathbb{R}$ is t-separated if every pair of points in X have distance at least t. In particular, the set X_t is always t-separated.

With this terminology, we will state an equivalent formulation of Theorem 1.1 that will be slightly easier to work with

Theorem 1.1'. Let $0 < \sigma < 1$. Let $A \subset [1,2]$ be a δ-separated set of cardinality $\delta^{-\sigma}$. Suppose that for all intervals I of length at least δ, we have the non-concentration estimate

$$\#(A \cap I) \leq C|I|^{\sigma}(\#A). \tag{5}$$

Then for every $c < \frac{\sigma(1-\sigma)}{4(7+3\sigma)}$, we have

$$\mathcal{E}_{\delta}(A + A) + \mathcal{E}_{\delta}(A.A) \gtrsim C^{-O(1)}\delta^{-c}(\#A). \tag{6}$$

1.2 Thanks

2 Preprocessing of δ-separated sets with good additive properties.

In this section, we deal with the following technical problem. Let $X \subset [1,2]$ be a δ-separated set. We will be in the situation where X has good additive properties at scale δ namely,

$$\mathcal{E}_{\delta}(X + X) \leq K(\#X).$$

We would like to know that in absolute terms, the set X has the same additive properties at each scale $t > \delta$, that is

$$\mathcal{E}_t(X + X) \leq K\mathcal{E}_t(X).$$

This is not necessarily true about X but is true about a fairly large subset. The following lemma, which is closely related to Lemma 5.2 from [5] will make this statement precise.

Lemma 2.1. *Let $X \subset [1,2]$ be a δ-separated subset and suppose $\#X = \delta^{-\sigma}$ for some $0 < \sigma < 1$. Suppose that*

$$\mathcal{E}_{\delta}(X + X) \leq K(\#X).$$

Then for every $\epsilon > 0$, there is a subset $\tilde{X} \subset X$ with

$$\#\tilde{X} \gtrsim \delta^{\epsilon}(\#X),$$

so that

$$\mathcal{E}_t(\tilde{X} + \tilde{X}) \lesssim \delta^{-10\epsilon} K\mathcal{E}_t(\tilde{X}) \quad \text{for all } \delta < t < 1, \tag{7}$$

with the implicit constants depending on σ and ϵ.

Proof. We will pick j, a large natural number depending only on σ and ϵ. Without loss of generality, we may assume that $\delta = 2^{-mj}$ for m a natural number. Indeed, reducing to this case will only affect our constants by factor of $2^{O(j)}$; since j depends only on σ and ϵ, this is acceptable.

3

We will subdivide the interval $[1, 2]$ into the 2^j-adic intervals. That is, for each natural number $0 \le l \le m$, we let

$$\mathcal{D}_l([1, 2]) = \{[1 + k2^{-lj}, \ 1 + (k+1)2^{-lj}] : 0 \le k \le 2^{lj} - 1\}.$$

The collection of intervals

$$\mathcal{D} = \bigcup_{l=0}^{m} \mathcal{D}_l([1, 2])$$

is a tree with $m + 1$ levels under containment. We will find our subset $\tilde{X}$ by following an algorithm that goes up the tree. We let X_l be the set of intervals in $\mathcal{D}_l([1, 2])$ which contain a point of X. We now will pick subsets Z_l of each X_l, starting with $Z_m = X_m$.

Next we observe that once Z_{l+1} has been chosen we have that

$$\#Z_{l+1} = \sum_{I \in X_l} \#\{J \in Z_{l+1} : J \subset I\}.$$

We know that each positive summand is between 1 and 2^j. Thus

$$\#Z_{l+1} = \sum_{k=1}^{j} \sum_{\substack{I \in X_l \\ 2^{k-1} \le \#\{J \in Z_{l+1} : J \subset I\} < 2^k}} \#\{J \in Z_{l+1} : J \subset I\}.$$

We pick the value of k contributing most to the sum and let

$$Z_l = \{I \in X_l : 2^{k-1} \le \#\{J \in Z_{l+1} : J \subset I\} < 2^k\}.$$

What we have basically done is found a large piece of X which is an essentially uniform tree. We keep track of our losses. We let $\tilde{X}_l$ be the set of $x \in X$ so that x is in an interval of Z_k for each $k > l$. We have that

$$\#\tilde{X}_l \ge \frac{1}{(2j)^{m-l}}(\#X).$$

We observe that by making j large enough, we have ensured that $(2j)^m \le 2^{jm\epsilon} = \delta^{-\epsilon}$. Because a fortiori, we also have $2^m \le \delta^{-\epsilon}$, we know that each interval in Z_l contains at least $\delta^{2\epsilon} \frac{\#X}{\#Z_l}$ elements of X (recall that these intervals have length 2^{-lj}). Thus each interval in $Z_l + Z_l$ of length 2^{-lj+1} contains at least $\delta^{2\epsilon} \frac{\#X}{\#Z_l}$ elements of $X + X$ which are δ-separated. Thus we must have

$$\#(Z_l + Z_l) \lesssim \delta^{-10\epsilon} K(\#Z_l),$$

because otherwise $\mathcal{E}_\delta(X + X) \gtrsim \delta^{-8\epsilon} K(\#X)$, a contradiction. We let

$$\tilde{X} = \bigcap \tilde{X}_l,$$

and the lemma is proved.

$\square$

3 Plünnecke's inequality and its implications

In this section we will begin the proof of Theorem 1.1′. Let $A \subset [1, 2]$ be a δ-separated set of cardinality $\delta^{-\sigma}$ that satisfies (5). Fix a number $c < \frac{\sigma(1-\sigma)}{4(7+3\sigma)}$, and let $\epsilon > 0$ be a small constant to be chosen later. In the arguments below, we will see terms of the form $\delta^{O(\epsilon)}$. The implicit constant will depend only on σ.

Apply Lemma 2.1 to A with ϵ as above to obtain a set A' that satisfies (7). Define K by

$$K = \frac{\mathcal{E}_\delta(A' + A') + \mathcal{E}_\delta(A'.A')}{(\#A')}.$$

Then we have that $\mathcal{E}_\delta(A' + A') + \mathcal{E}_\delta(A'.A') \leq K(\#A')$; our goal will be to obtain a lower bound for K. Because $\#(A') \gtrsim \delta^{O(\epsilon)} \#A$, and, of course,

$$A' + A' \subset A + A,$$

and

$$A'.A' \subset A.A,$$

an appropriate lower bound on K implies inequality (6).

Our next task is to find a large subset $A_1 \subset A'$ that has small expansion (in the δ-covering sense) under certain types of repeated addition and multiplication. Our main tool will be Plünnecke's inequality:

Proposition 3.1 (Plünnecke). *Let G be an Abelian group and let $X, Y_1, \ldots, Y_k$ be subsets of G. Suppose that $\#(X + Y_i) \leq K_i(\#X)$ for each $i = 1, \ldots, k$. Then there exists a subset $X' \subset X$ so that*

$$\#(X' + Y_1 + \ldots + Y_k) \leq \left(\Pi_{i=1}^k K_i\right)(\#X').$$

An inequality of this form was first proved by Plünnecke [12]. The current formulation is due to Ruzsa [14]. More recently, Petridis [11] obtained a short and elementary proof of Plünnecke's inequality.

Observe that if $X, Y_1, \ldots, Y_k$ are subsets of G with $\#(X + Y_i) \leq K_i(\#X)$ for each $i = 1, \ldots, k$, then whenever $X_0 \subset X$ with $\#X_0 \geq (\#X)/2$, we have $\#(X_0 + Y_i) \leq 2K_i(\#X_0)$ for each $i = 1, \ldots, k$. By repeatedly applying this observation to the set $X_0 = X \backslash X'$ that is "left over" after applying Proposition 3.1, we can obtain the following slight strengthening of Plünnecke's inequality:

Corollary 3.2. *Let G be an Abelian group and let $X, Y_1, \ldots, Y_k$ be subsets of G. Suppose that $\#(X + Y_i) \leq K_i(\#X)$ for each $i = 1, \ldots, k$. Then there exists a subset $X' \subset X$ with $\#X' \geq (\#X)/2$ so that*

$$\#(X' + Y_1 + \ldots + Y_k) \lesssim \left(\Pi_{i=1}^k K_i\right)(\#X').$$

We will also need Ruzsa's triangle inequality:

Proposition 3.3 (Ruzsa triangle inequality). *Let G be an Abelian group and let $X, Y, Z \subset G$ be finite subsets. Then*

$$\#(X - Z) \leq \frac{\#(X - Y) \ \#(Y - Z)}{\#Y}.$$

Proof. Let $s = x - z \in X - Z$. Then there are at least $\#Y$ distinct representations of s as a sum of an element of $X - Y$ with an element of $Y - Z$. Namely, $s = (x - y) + (y - z)$ for each $y \in Y$. $\quad\square$

If $X \subset [1,2]$ is a set, we will call a set X' a δ-*refinement* of X if $X' \subset X$, and $\mathcal{E}_\delta(X') \geq \mathcal{E}_\delta(X)/2$. We shall extend Proposition 3.1, Corollary 3.2 and Proposition 3.3 to the δ-covering setting, by replacing any set X by X_δ and observing that $\#X_\delta \sim \mathcal{E}_\delta(X)$.

Corollary 3.4. *Let* $X, Y_1, \ldots, Y_k$ *be subsets of* $\mathbb{R}$. *Suppose that* $\mathcal{E}_\delta(X + Y_i) \leq K_i \mathcal{E}_\delta(X)$ *for each* $i = 1, \ldots, k$. *Then there is a* δ-*refinement* X' *of* X *so that*

$$\mathcal{E}_\delta(X' + Y_1 + Y_2 + \ldots + Y_k) \lesssim \left(\Pi_{i=1}^k K_i\right)\mathcal{E}_\delta(X').$$

In particular,

$$\mathcal{E}_\delta(Y_1 + Y_2 + \ldots + Y_k) \lesssim \left(\Pi_{i=1}^k K_i\right)\mathcal{E}_\delta(X).$$

To obtain Corollary 3.4, replace each of the sets $X, Y_1, \ldots, Y_k$ by $X_\delta, (Y_1)_\delta, \ldots, (Y_k)_\delta$. Observe that for any subset Z of X_δ, we have

$$\#\left(Z + (Y_1)_\delta + \ldots + (Y_k)_\delta\right) \sim \mathcal{E}_\delta(Z + Y_1 + \ldots + Y_k),$$

with the implicit constant depending on k. Apply Corollary 3.2 to the finite sets $X_\delta, (Y_1)_\delta, \ldots, (Y_k)_\delta$, and let R be the resulting refinement of X_δ. Finally, take X' to be the set $\mathcal{N}_\delta(R) \cap X$.

In the same way, we obtain the following δ-covering version of the triangle inequality.

Proposition 3.5. *Let* X, Y, Z *be subsets of* $\mathbb{R}$. *Then*

$$\mathcal{E}_\delta(X - Z) \lesssim \frac{\mathcal{E}_\delta(X - Y)\ \mathcal{E}_\delta(Y - Z)}{\mathcal{E}_\delta(Y)}.$$

We are now ready to proceed. Observe that for any $x \in A'$, we have that

$$\#\left((xA')_\delta\right) \sim \mathcal{E}_\delta(xA').$$

First, by Cauchy-Schwarz, the condition $\mathcal{E}_\delta(A'.A') \leq K(\#A')$ implies that

$$\sum_{x,y \in A'} \#\left((xA')_\delta \cap (yA')_\delta\right) \gtrsim (\#A')^3 K^{-1}.$$

Select an element $b \in A'$ so that

$$\sum_{x \in A'} \#\left((xA')_\delta \cap (bA')_\delta\right) \gtrsim (\#A')^2 K^{-1}. \tag{8}$$

By dyadic pigeonholing, we can select a set $\bar{A} \subset A'$ and a number $K^{-1} \leq \rho \leq 1$ with $\#\bar{A} \gtrsim (\log K)\rho(\#A') \gtrsim |\log \delta|^{-1}\rho(\#A')$ so that

$$\#\left((aA')_\delta \cap (bA')_\delta\right) \sim (\#A')K^{-1}\rho^{-1} \quad \text{for each } a \in \bar{A}.$$

At the end of our argument, we will see that the worst-case occurs when $\rho = 1$. Thus a casual reader may safely set $\rho = 1$. We will consider the δ-covering number $\mathcal{E}_\delta(aA' \pm bA')$ when $a \in \bar{A}$. Let $X = (aA')_\delta \cap (bA')_\delta$, so $\#X \geq K^{-1}\rho^{-1}(\#A')$. We have

$$\mathcal{E}_\delta(X + aA') \lesssim K(\#A') \leq K^2\rho(\#X),$$
$$\mathcal{E}_\delta(X + bA') \lesssim K(\#A') \leq K^2\rho(\#X).$$

By Corollary 3.4, we obtain

$$\mathcal{E}_\delta\big(aA' + bA'\big) \lesssim K^4\rho^2(\#X) \lesssim K^3\rho(\#A'). \tag{9}$$

By Proposition 3.5, substituting aA' for X, bA' for Z and $-X$ for Y, we obtain

$$\mathcal{E}_\delta\big(aA' - bA'\big) \lesssim K^4\rho^2(\#X) \lesssim K^3\rho(\#A'). \tag{10}$$

Combining the results (9) and (10), we obtain

$$\mathcal{E}_\delta\big(aA' \pm bA'\big) \lesssim K^4\rho^2(\#X) \lesssim K^3\rho(\#A'). \tag{11}$$

So far elements of $\bar{A}$ have good properties for multiplying A' and adding such dilates, but we would like to take advantage as well of the additive properties of $\bar{A}$. To wit, we have that $\bar{A} + \bar{A} \subset A' + A'$ so that

$$\mathcal{E}_\delta(\bar{A} + \bar{A}) \leq \mathcal{E}_\delta(A' + A') \leq K(\#A') \leq K|\log\delta|\rho^{-1}(\#\bar{A}).$$

However, we might have liked to have estimates on $\mathcal{E}_t(\bar{A} + \bar{A})$ for $t > \delta$. To fulfill our desires, we apply Lemma 2.1 to $\bar{A}$ with ϵ as above to obtain a set $A_1 = \tilde{\bar{A}}$. We immediately obtain the estimate

$$\mathcal{E}_t(A_1 + A_1) \leq K|\log\delta|\rho^{-1}\delta^{-O(\epsilon)}\mathcal{E}_t(A_1) \quad \text{for all } \delta < t < 1.$$

In the next two lemmas, we will obtain estimates for the cardinality of various sums involving A_1 and A'. These lemmas constitute an ingredient of our argument that does not occur in Garaev's finite field argument. We lose some resolution when we multiply A' by a number much smaller than 1 and then calculate δ-covering number, but we win some of this back by considering nonconcentration for A'.

Lemma 3.6. *Let $d_1 = a_1 - b_1$, $d_2 = a_2 - b_2$, with $a_1, a_2, b_1, b_2 \in A_1$. Then*

$$\mathcal{E}_\delta(d_1 A' + d_2 A') \lesssim C\delta^{-\epsilon}K^{12}\rho^4 \max(|d_1|, |d_2|)^\sigma(\#A'). \tag{12}$$

Proof. By Corollary 3.4 and (11), there is a refinement A'' of A' so that

$$\mathcal{E}_\delta(bA'' + d_1 A' + d_2 A') \leq \mathcal{E}_\delta(bA'' + a_1 A' - b_1 A' + a_2 A' - b_2 A') \lesssim K^{12}\rho^4(\#A'), \tag{13}$$

where $b \in A'$ is the element satisfying (8).

Next, observe that $d_1 A' + d_2 A'$ is contained in an interval of length $d \lesssim \max(|d_1|, |d_2|)$. Thus

$$\mathcal{E}_\delta(d_1 A' + d_2 A') \lesssim \big(\mathcal{E}_d(bA'')\big)^{-1} \mathcal{E}_\delta(bA'' + d_1 A' + d_2 A') \lesssim \big(\mathcal{E}_d(bA'')\big)^{-1} K^{12}\rho^4(\#A').$$

Since $\#A'' \sim \#A'$ and A' satisfies the non-concentration estimate $\#(A' \cap I) \lesssim C\delta^{-\epsilon}d^\sigma(\#A')$ for each interval I of length d, following from the comparison of the size of A' to that of A and the non-concentration estimate for A given in (5), we must have that

$$\mathcal{E}_d(bA'') \gtrsim \frac{\#A''}{C\delta^{-\epsilon}d^\sigma(\#A')} = C^{-1}\delta^\epsilon d^{-\sigma}.$$

This completes the proof of the lemma. $\qquad\square$

Lemma 3.7. *Let $d_1 = a_1 - b_1$, $d_2 = a_2 - b_2$, with $a_1, a_2, b_1, b_2 \in A_1$. Then for each $k \geq 2$, there is a set $A_2 \subset A_1$ with $\#A_2 \geq (\#A_1)/4$ so that*

$$\mathcal{E}_\delta\big(d_1 A_2 + \underbrace{d_2 A_2 + \ldots + d_2 A_2}_{k \ times}\big) \lesssim C\delta^{-O(\epsilon)} |\log \delta|^{O(1)} K^{11+k} \rho^{5-k} \max(|d_1|, |d_2|)^\sigma (\#A'). \tag{14}$$

The implicit constant in the $|\log \delta|^{O(1)}$ and $\delta^{-O(\epsilon)}$ terms depend on k.

Proof. As in the proof of Lemma 3.6, select a refinement A'' of A' so that $\mathcal{E}_\delta(bA'' + d_1 A' + d_2 A') \lesssim K^{12} \rho^4 (\#A')$. This implies that

$$\mathcal{E}_\delta(bA'' + d_1 A_1 + d_2 A_1) \lesssim \delta^{-O(\epsilon)} K^{12} \rho^3 (\#A_1).$$

We have that

$$\mathcal{E}_\delta(d_2 A_1 + d_2 A_1) = \mathcal{E}_{\frac{\delta}{d_2}}(A_1 + A_1) \leq K\delta^{-O(\epsilon)} \rho^{-1} |\log \delta| \, \mathcal{E}_\delta(d_2 A_1),$$

and thus by Corollary 3.4, there is a refinement A_1' of A_1 so that the k-fold sum

$$\mathcal{E}_\delta(d_2 A_1' + \ldots + d_2 A_1') \leq K^{k-1} \delta^{-O(\epsilon))} \rho^{1-k} |\log \delta|^{k-1} \mathcal{E}_\delta(d_2 A_1').$$

Apply Corollary 3.4 with $X = d_2 A_1'$, $Y_1 = d_2 A_1' + \ldots + d_2 A_1'$ (this is a $(k-1)$-fold sum), and $Y_2 = bA'' + d_1 A_1$. We conclude that there is a refinement A_2 of A_1' so that

$$\mathcal{E}_\delta(bA'' + d_1 A_2 + d_2 A_2 + \ldots + d_2 A_2) \lesssim (K^{12}\rho^3)\delta^{-O(\epsilon)}(K^{k-1}\rho^{1-k}|\log \delta|^{k-1})(\#A_1)$$
$$= K^{11+k}\rho^{4-k}\delta^{-O(\epsilon)}|\log \delta|^{k-1}(\#A_1).$$

We now proceed as in the proof of Lemma 3.6. Observe that $d_1 A_2 + d_2 A_2 + \ldots + d_2 A$ is contained in an interval of length $d \lesssim (k+1) \max(|d_1|, |d_2|)$. Thus

$$\mathcal{E}_\delta(d_1 A_2 + d_2 A_2 + \ldots + d_2 A_2) \lesssim \big(\mathcal{E}_d(bA'')\big)^{-1} \mathcal{E}_\delta(bA'' + d_1 A_2 + d_2 A_2 + \ldots + d_2 A_2)$$
$$\lesssim \big(\mathcal{E}_d(bA'')\big)^{-1} K^{11+k} \rho^{4-k} \delta^{-O(\epsilon)} |\log \delta|^{O(1)} (\#A_1).$$

Since $\#A'' \sim \#A'$ and A' satisfies the non-concentration estimate $\#(A' \cap I) \leq C\delta^{-\epsilon} d^\sigma (\#A')$ for each interval I of length d, we must have that $\mathcal{E}_d(bA'') \gtrsim \frac{\#A''}{C\delta^{-\epsilon}d^\sigma(\#A')} = C^{-1}\delta^\epsilon d^{-\sigma}$. Since $\#A' \geq \delta^\epsilon \#A_1$, we have

$$\mathcal{E}_\delta(d_1 A_2 + d_2 A_2 + \ldots + d_2 A_2) \lesssim C\delta^{-O(\epsilon)} |\log \delta|^{O(1)} d^\sigma K^{11+k} \rho^{4-k} (\#A'). \qquad \square$$

4 The structure of $\frac{A-A}{A-A}$: dense versus gap cases

Let A_1 be the set constructed in the previous section, and let $\gamma \in (0, 1/2)$ be a parameter we will specify later. Consider the set

$$B = \left\{ \frac{a_1 - a_2}{a_3 - a_4} : a_i \in A_1, |a_3 - a_4| > \delta^\gamma \right\}.$$

Since $A_1 \subset [1, 2]$, we have that $B \subset [-\delta^{-\gamma}, \delta^{-\gamma}]$. We also have $0, 1 \in B$. Choose a positive integer m so that $2^{-m} \sim \delta^{1-2\gamma}$. Define $s = 2^{-m}$.

Lemma 4.1. *At least one of the following two things must happen.*

(A): There exists a point $b \in B \cap [0,1]$ with

$$\max\left(\operatorname{dist}(b/2,\ B),\ \ \operatorname{dist}\left(\frac{b+1}{2},\ B\right)\right) \geq s.$$

(B): $\mathcal{E}_s(B \cap [0,1]) \gtrsim s^{-1}$.

Proof. Suppose that Item (A) does not occur. Let $\tilde{b} \in B_{2s}$ and let $b \in B$ be the corresponding point with $|b - \tilde{b}| \leq 2s$. Then there is an element $b' \in B$ with $|b' - b/2| < s$, and thus

$$|b' - \tilde{b}/2| \leq |b' - b/2| + |b/2 - \tilde{b}/2| < s + s = 2s,$$

so $\tilde{b}/2 \in B_{2s}$.

Similarly, there is an element $b'' \in B$ with $|b'' - \frac{b+1}{2}| < s$, and thus

$$\left| b'' - \frac{\tilde{b}+1}{2} \right| \leq \left| b'' - \frac{b+1}{2} \right| + \left| \frac{b+1}{2} - \frac{\tilde{b}+1}{2} \right| < s + s = 2s,$$

so $\frac{\tilde{b}+1}{2} \in B_{2s}$.

We will now prove by induction that for each $n = 1, \ldots, m-1$, every dyadic rational of the form $p/2^n \in [0,1]$ is contained in B_{2s}. Indeed, if $n = 0$ then the result holds since $0, 1 \in B$ implies that $0, 1 \in B_{2s}$. Now suppose the result has been proved for some value of $n \leq m-2$, and let $p/2^{n+1} \in [0,1]$. If $p < 2^n$, then by the induction hypothesis $p/2^n \in B_{2s}$, and thus $\frac{1}{2}p/2^n = p/2^{n+1} \in B_{2s}$. If $p \geq 2^n$, then by the induction hypothesis, $(p - 2^n)/2^n = p/2^n - 1 \in B_{2s}$, and thus $p/2^{n+1} = \frac{p/2^n - 1}{2} + \frac{1}{2} \in B_{2s}$. This completes the induction. We conclude that Item (B) holds. □

We say we are in the *gap case* if Item (A) holds and in the *dense case* if Item (B) holds. Note that these are not mutually exclusive.

5   The dense case

By pigeonholing, we can select $b_1, b_2, b_3, b_4 \in A_1$ with $|b_3 - b_4| > \delta^\gamma$ and $|b_1 - b_2| \leq |b_3 - b_4|$ so that

$$\#\left\{ (a_1, ..., a_4) \in A_1^4 \colon \left| \frac{a_1 - a_2}{a_3 - a_4} - \frac{b_1 - b_2}{b_3 - b_4} \right| < \delta^{1-2\gamma},\ |a_3 - a_4| > \delta^\gamma \right\} \lesssim (\#A_1)^4 \delta^{1-2\gamma}. \tag{15}$$

By Lemma 3.6, we have

$$\mathcal{E}_\delta\left((b_1 - b_2)A_1 + (b_3 - b_4)A_1 \right) \leq \mathcal{E}_\delta\left((b_1 - b_2)A' + (b_3 - b_4)A' \right) \lesssim C\delta^{-\epsilon} K^{12} \rho^4 |b_3 - b_4|^\sigma (\#A'). \tag{16}$$

We will now establish a lower bound on $\mathcal{E}_\delta\left((b_1 - b_2)A_1 + (b_3 - b_4)A_1 \right)$. Define $Q \subset A_1^4$ to be the set of quadruples obeying

$$(b_3 - b_4)a_1 + (b_1 - b_2)a_4 = (b_3 - b_4)a_2 + (b_1 - b_2)a_3 + O(\delta). \tag{17}$$

9

Cauchy-Schwarz gives $\mathcal{E}_\delta\big((b_1 - b_2)A_1 + (b_3 - b_4)A_1\big) \gtrsim (\#A_1)^4/(\#Q)$, so our goal is now to find an upper bound for Q. Note that (17) implies that

$$a_1 + \frac{b_1 - b_2}{b_3 - b_4}a_4 = a_2 + \frac{b_1 - b_2}{b_3 - b_4}a_3 + O(\delta|b_3 - b_4|^{-1}),$$

which implies that

$$\left|\frac{a_1 - a_2}{a_3 - a_4} - \frac{b_1 - b_2}{b_3 - b_4}\right| \lesssim \delta|b_3 - b_4|^{-1}|a_2 - a_4|^{-1}. \tag{18}$$

We first consider quadruples $(a_1, ..., a_4) \in Q$ where $|a_3 - a_4| \geq \delta^\gamma$. For each such quadruple, (18) implies that

$$\left|\frac{a_1 - a_2}{a_3 - a_4} - \frac{b_1 - b_2}{b_3 - b_4}\right| \lesssim \delta^{1-2\gamma}.$$

Comparing with (15), we see that the number of such quadruples is $\lesssim (\#A_1)^4 \delta^{1-2\gamma} \lesssim (\#A_1)^3 \delta^{(1-\sigma)-2\gamma-O(\epsilon)}$. Thus if at least half the quadruples from Q are of this form, then

$$\mathcal{E}_\delta\big((b_1 - b_2)A_1 + (b_3 - b_4)A_1\big) \gtrsim (\#A_1)\delta^{2\gamma+\sigma-1+O(\epsilon)} \gtrsim \rho|\log\delta|^{-1}\delta^{2\gamma+\sigma-1}(\#A').$$

By (16), we conclude that if at least half the quadruples from Q are of this form, then

$$K \gtrsim (C|\log\delta|)^{-O(1)}\rho^{-1/4}\delta^{\frac{2\gamma+\sigma-1}{12}+O(\epsilon)} \gtrsim (C|\log\delta|)^{-O(1)}\delta^{\frac{2\gamma+\sigma-1}{12}+O(\epsilon)}. \tag{19}$$

On the other hand, we consider quadruples $(a_1, ..., a_4) \in Q$ where $|a_3 - a_4| \leq \delta^\gamma$. We begin by choosing elements $a_1, a_4 \in A_1$. By our non-concentration hypothesis (2) and the requirement $|a_3 - a_4| \leq \delta^\gamma$, the number of admissible a_3 is at most $C\delta^{\gamma\sigma}(\#A)$. Next, a_2 must lie in an interval of length $\leq \delta|b_3 - b_4|^{-1}$. By our non-concentration hypothesis, the number of admissible a_2 is at most $C\delta^\sigma(\#A)|b_3 - b_4|^{-\sigma} = C|b_3 - b_4|^{-\sigma}$. Thus the set of quadruples of this type has size at most $(\#A_1)^2\big(C\delta^{\gamma\sigma}(\#A)\big)\big(C|b_3 - b_4|^{-\sigma}\big)$. Thus if at least half the quadruples from Q are of this form, then

$$\mathcal{E}_\delta\big((b_1 - b_2)A_1 + (b_3 - b_4)A_1\big) \gtrsim \frac{(\#A_1)^4}{(\#A_1)^2\big(C\delta^{\gamma\sigma}(\#A)\big)\big(C|b_3 - b_4|^{-\sigma}\big)}$$
$$\gtrsim C^{-O(1)}\rho^2|\log\delta|^{-1}\delta^{-\gamma\sigma+O(\epsilon)}|b_3 - b_4|^\sigma(\#A').$$

By (16), we conclude that if at least half the quadruples from Q are of this form, then

$$K \gtrsim (C|\log\delta|)^{-O(1)}\rho^{-1/6}\delta^{\frac{-\gamma\sigma}{12}+O(\epsilon)} \gtrsim (C|\log\delta|)^{-O(1)}\delta^{\frac{-\gamma\sigma}{12}+O(\epsilon)}. \tag{20}$$

If we are in the dense case, then

$$K \gtrsim \delta^{O(\epsilon)}(C|\log\delta|)^{-O(1)}\min\big(\delta^{\frac{2\gamma+\sigma-1}{12}},\ \delta^{\frac{-\gamma\sigma}{12}}\big). \tag{21}$$

10

6   The gap case

In this section, we will suppose that we are in the gap case. This means that there exists $b = \frac{b_1 - b_2}{b_3 - b_4} \in B \cap [0,1]$ so that either (A.1): $b/2$ is at least s-separated from B or (A.2): $\frac{b+1}{2}$ is at least s-separated from B (recall $s \sim \delta^{1-2\gamma}$). The reader should recall that by the definition of B, we have that $|b_3 - b_4| \geq \delta^\gamma$. In Case (A.1), write $b/2 = e_1/e_2$, while in Case (A.2), write $\frac{b+1}{2}$ as e_1/e_2. In Case (A.1) we can write $e_1 = d_1$, $e_2 = d_2 + d_2$, where $d_1, d_2 \in A_1 - A_1$. In Case (A.2) we can write $e_1 = d_1 + d_2$, $e_2 = d_2 + d_2$, where $d_1, d_2 \in A_1 - A_1$.

We will prove a lower bound on $\mathcal{E}_\delta(e_1 A_1 + e_2 A_1)$. Define $Q \subset A_1^4$ to be the set of quadruples obeying

$$e_2 a_1 + e_1 a_4 = e_2 a_2 + e_1 a_3 + O(\delta). \tag{22}$$

Cauchy-Schwarz gives $\mathcal{E}_\delta(e_1 A_1 + e_2 A_1) \gtrsim (\#A_1)^4/(\#Q)$, so our goal is now to find an upper bound for Q. Note that (22) implies that

$$a_1 + \frac{e_1}{e_2} a_4 = a_2 + \frac{e_1}{e_2} a_3 + O\big(\delta|e_2|^{-1}\big), \tag{23}$$

which implies that

$$\left| \frac{a_1 - a_2}{a_3 - a_4} - \frac{e_1}{e_2} \right| \lesssim \delta |e_2|^{-1} |a_2 - a_4|^{-1}. \tag{24}$$

We first consider quadruples $(a_1, ..., a_4) \in Q$ where $|a_3 - a_4| \geq \delta^\gamma$. For each such quadruple, (24) implies that

$$\left| \frac{a_1 - a_2}{a_3 - a_4} - \frac{e_1}{e_2} \right| \lesssim \delta^{1-2\gamma}.$$

Now since we are in the gap case, e_1/e_2 is at least $s \sim \delta^{1-2\gamma}$ separated from B. But since $|a_3 - a_4| \geq \delta^\gamma$, $\frac{a_1 - a_2}{a_3 - a_4} \in B$. This shows that there are no quadruples in Q with $|a_3 - a_4| \geq \delta^\gamma$.

We conclude that every quadruple in Q has $|a_3 - a_4| \leq \delta^\gamma$. Select elements $a_1, a_4 \in A_1$. By the non-concentration hypothesis (2), the set of admissible a_3 has size at most $C\delta^{\gamma\sigma}(\#A)$. Finally, a_2 must lie in an interval of length $\delta|e_2|^{-1}$; again by the non-concentration hypothesis, the set of admissible a_2 has size at most $C(\delta/|e_2|)^\sigma(\#A') = C|e_2|^{-\sigma}$. All together, we have

$$|Q| \lesssim C^{O(1)} (\#A_1)^2 (\#A') \delta^{\gamma\sigma} |e_2|^{-\sigma}.$$

This gives us the lower bound

$$\mathcal{E}_\delta(e_1 A_1 + e_2 A_1) \gtrsim C^{-O(1)} \rho^2 \delta^{O(\epsilon)} |\log \delta|^{-2} \delta^{-\gamma\sigma} |e_2|^\sigma (\#A'). \tag{25}$$

Note that nothing in the argument obtaining this lower bound would change if we replaced A_1 by a refinement of A_1. We conclude that

$$\mathcal{E}_\delta(e_1 A_2 + e_2 A_2) \gtrsim C^{-O(1)} \rho^2 \delta^{O(\epsilon)} |\log \delta|^{-2} \delta^{-\gamma\sigma} |e_2|^\sigma (\#A') \tag{26}$$

whenever A_2 is a refinement of A_1. Applying Lemma 3.7 with $d_1 = b_1 - b_2$, $d_2 = b_3 - b_4$, and $k = 2$ (in Case (A.1)) and $k = 3$ (in Case (A.2), which is worse), we obtain the bound

$$\mathcal{E}_\delta(e_1 A_2 + e_2 A_2) \lesssim C\delta^{-O(\epsilon)} |\log \delta|^{O(1)} K^{14} \rho^2 |e_2|^\sigma (\#A'). \tag{27}$$

11

Combining (25) and (27), we have

$$C^{-O(1)}\rho^2\delta^{O(\epsilon)}|\log\delta|^{-1}\delta^{-\gamma\sigma}|e_2|^\sigma(\#A') \lesssim C\delta^{-O(\epsilon)}|\log\delta|^{O(1)}K^{14}\rho^2|e_2|^\sigma(\#A'),$$

and thus

$$K \gtrsim \delta^{O(\epsilon)}(C|\log\delta|)^{-O(1)}\delta^{\frac{-\gamma\sigma}{14}}. \tag{28}$$

By Lemma 4.1, at least one of (21) or (28) must hold. Selecting $\gamma = \frac{7(1-\sigma)}{2(7+3\sigma)}$, we conclude that

$$K \gtrsim \delta^{O(\epsilon)}(C|\log\delta|)^{O(1)}\delta^{-\frac{\sigma(1-\sigma)}{4(7+3\sigma)}}.$$

Since

$$\mathcal{E}_\delta(A' + A') + \mathcal{E}_\delta(A'.A') \leq \mathcal{E}_\delta(A + A) + \mathcal{E}_\delta(A.A),$$

we conclude that

$$\mathcal{E}_\delta(A + A) + \mathcal{E}_\delta(A.A) \gtrsim \delta^{O(\epsilon)}(C|\log\delta|)^{O(1)}\delta^{-\frac{\sigma(1-\sigma)}{4(7+3\sigma)}}(\#A).$$

Thus if $\epsilon > 0$ is selected sufficiently small (depending only on c and σ), then (6) holds.

References

[1] J. Bourgain. On the Erdős-Volkmann and Katz-Tao ring conjectures. *Geom. Funct. Anal* 15(1): 334–365. 2003.

[2] J. Bourgain. The discretized sum-product and projection theorems. *J. Anal. Math.* 112(1): 193–236. 2010.

[3] J. Bourgain and M.Z. Garaev. On a variant of sum-product estimates and explicit exponential sum bounds in prime fields. *Math. Proc. Cambridge Philos. Soc.* 146: 1–21. 2009.

[4] J. Bourgain and A. Gamburd. On the spectral gap for finitely-generated subgroups of $SU(2)$. *Invent. Math.* 171: 83–121. 2008.

[5] J. Bourgain, A. Gamburd, and P. Sarnak. Affine linear sieve, expanders, and sum-product. *Invent. Math.* 179, 559–644. 2010.

[6] G.A. Edgar and C. Miller. Borel subrings of the reals. *Proc. Amer. Math. Soc.* 131(4): 1121–1129. 2003.

[7] P. Erdős and B. Volkmann. Additive gruppen mit vorgegebener Hausdorffscher dimension. *J. Reine Angew. Math.* 221: 203–208. 1966.

[8] M.Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. *Int. Math. Res. Notices.* rnm035. 2007.

[9] N. Katz and C.Y. Shen. A slight improvement to Garaev's sum product estimate. *Proc. Amer. Math. Soc.* 136(7): 2499–2504. 2008.

[10] N. Katz and T. Tao. Some connections between Falconer's distance set conjecture and sets of Furstenburg type. *New York J. Math.* 7: 149–187. 2001.

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

[12] H. Plünnecke. Eine zahlentheoretische anwendung der graphentheorie. *J. Reine Angew. Math.* 243: 171–183. 1970.

[13] M. Rudnev. An improved sum-product inequality in fields of prime order. *Int. Math. Res. Notices.* 2012(16): 3693–3705. 2012.

[14] I.Z. Ruzsa. An application of graph theory to additive number theory. *Scientia, Ser. A*. 3: 97–109. 1989.