Sums, Differences and Dilates

Jonathan Cutler Luke Pebody Amites Sarkar

September 10, 2024

Abstract

Given a set of integers A and an integer k, write $A+k\cdot A$ for the set $\{a+kb : a\in A, b\in A\}$. Hanson and Petridis [6] showed that if $|A+A|\leq K|A|$ then $|A+2\cdot A|\leq K^{2.95}|A|$ and also that $|A+2\cdot A|\leq (K|A|)^{4/3}$. We present a new construction, the *Hypercube+Interval construction*, which lies close to these upper bounds and which shows in particular that, for all $\epsilon>0$, there exist A and K with $|A+A|\leq K|A|$ but with $|A+2\cdot A|\geq K^{2-\epsilon}|A|$.

Further, we analyse a method of Ruzsa [15], and generalise it to give fractional analogues of the sizes of sumsets, difference sets and dilates. We apply this method to a construction of Hennecart, Robert and Yudin [3] to prove that, for all $\epsilon>0$, there exists a set A with $|A-A|\geq |A|^{2-\epsilon}$ but with $|A+A|<|A|^{1.7354+\epsilon}$.

The second author would like to thank E. Papavassilopoulos for useful discussions about how to improve the efficiency of his computer searches.

1 Introduction and Definitions

The study of the size of the sumset $|A+A|$ and difference set $|A-A|$ (sometimes denoted DA) in terms of $|A|$ is a central theme in additive combinatorics. For instance, *Freiman's theorem* states that if $|A+A|\leq K|A|$, then A must be a large fraction of a *generalized arithmetic progression*, and the *Balog-Szemerédi-Gowers theorem* states that if A has large *additive energy*, then A must contain a large subset A' such that $|A'+A'|/|A'|$ is small. For the precise definitions and statements, we refer the reader to [16].

For a finite set $A\subset\mathbb{Z}$, with $|A|=n$, we have that

$$|A+A|\leq \frac{n(n+1)}{2} \quad \text{and} \quad |A-A|\leq n^2-n+1,$$

with equality in both cases precisely when A is a *Sidon set*, that is, a set containing no nontrivial *additive quadruple* $(a,b,c,d)\in A^4$ with $a+b=c+d$ (and consequently no nontrivial (a,b,c,d) with $a-b=c-d$). In other words, if $|A+A|$ is as large as it can possibly be, then so is $|A-A|$, and conversely. In 1992, Ruzsa [15] showed, using an ingenious probabilistic construction, that $|A+A|$ can be small, while $|A-A|$ can be almost as large as possible, and vice-versa. In particular, he showed the following.

Theorem 1 (Ruzsa, 1992)**.** *For every large enough n, there is a set A such that $|A|=n$ with*

$$|A+A|\leq n^{2-c} \qquad \text{and} \qquad |A-A|\geq n^2-n^{2-c},$$

where c is a positive absolute constant. Also, there is a set B with $|B|=n$,

$$|B-B|\leq n^{2-c} \qquad \text{and} \qquad |B+B|\geq \frac{n^2}{2}-n^{2-c}.$$

A few years later, Hennecart, Robert and Yudin [3] constructed a set A of size n with $|A+A| \sim n^{1.4519}$ but $|A-A| \sim n^{1.8462}$. Their construction was inspired by convex geometry, specifically the *difference body inequality* of Rogers and Shephard [13]. In the other direction, the study and classification of *MSTD sets* (sets with more sums than differences) began with Conway in 1967, and has now attracted a large literature (see [7] for a recent survey).

Note that Hennecart, Robert and Rudin in fact constructed a set $A \subset \mathbb{Z}^d$. But any such construction in $\mathbb{Z}^d$ can be easily translated to a construction in $\mathbb{Z}$ using an appropriately chosen *Freiman homomorphism*, i.e., a map ϕ of the form

$$\phi(x_1, \dots, x_d) = \lambda_1 x_1 + \cdots + \lambda_d x_d,$$

for an appropriate choice of integers λ_i.

Another line of investigation was opened by Bukh [2] in 2008. Given a set of integers A and an integer k, define the *dilate set* $A + k \cdot A$ by

$$A + k \cdot A = \{a_1 + k a_2 : a_1, a_2 \in A\}.$$

For $k = 1$, this is just the sumset, $A + A$, and for $k = -1$ it is the difference set, $A - A$. Note that, for example, the dilate set $A + 2 \cdot A$ is generally a strict subset of $A + A + A$, where each of the three summands can be distinct.

Bukh proved many results on general sums of dilates $\lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ (for arbitrary integers $\lambda_1, \dots, \lambda_k$), including lower and upper bounds on their sizes. Some of these results were phrased in terms of sets with *small doubling*, namely, sets $A \subset \mathbb{Z}$ with $|A+A| \leq K|A|$, for some fixed constant K (known as the *doubling constant*). For such a set A, *Plünnecke's inequality* [12] (see also [10]) shows that

$$|A + 2 \cdot A| \leq |A + A + A| \leq K^3 |A|,$$

and Bukh asked if the exponent 3 could be improved. This question was answered affirmatively in 2021 by Hanson and Petridis [6], who proved the following.

Theorem 2 (Hanson-Petridis, 2021)**.** *If $A \subset \mathbb{Z}$ and $|A + A| \leq K|A|$, then*

$$|A + 2 \cdot A| \leq K^{2.95} |A|.$$

They were also able to prove a result that improves Theorem 2 when K is large.

Theorem 3 (Hanson-Petridis, 2021)**.** *If $A \subset \mathbb{Z}$ and $|A + A| \leq K|A|$, then*

$$|A + 2 \cdot A| \leq (K|A|)^{4/3}.$$

Our contributions in this paper are best understood in the context of *feasible regions* of the plane, and so we make the following definition.

Definition. For fixed integers k and l, we define the *feasible region* $F_{k,l}$ to be the closure of the set $E_{k,l}$ of *attainable points*

$$E_{k,l} = \left\{ \left(\frac{\log |A + k \cdot A|}{\log |A|}, \frac{\log |A + l \cdot A|}{\log |A|} \right) \right\},$$

as A ranges over finite sets of integers.

Note that for any k and l, we have that $E_{k,l} \subset [1,2]^2$, which follows from the fact that $|A| \leq |A+k\cdot A| \leq |A|^2$ for all A. For every k and l, each A produces a point in $E_{k,l}$. With A fixed, we can generate a sequence of sets, indexed by the dimension d, by taking a Cartesian product $A^d \subset \mathbb{Z}^d$, and then we will have $|A^d + k\cdot A^d| = |A + k\cdot A|^d$. The advantage of the logarithmic measure we are using is that all examples in this sequence, generated from the same set A, correspond to the same point $(x,y) \in E_{k,l}$. Another useful fact is that the set $F_{k,l}$ is convex. We prove this in Section 2.

The first series of results in this paper concerns the size of the dilate set $A + 2\cdot A$. We present a construction, the *Hypercube+Interval construction*, which improves all previous bounds, and is close to the above upper bounds of Hanson and Petridis. Specifically, this construction shows that the graph of the piecewise-linear function

$$y = \min\left(2x-1, (\log_3 4)x\right) = \begin{cases} 2x-1 & 1 \leq x \leq \log_{\frac{9}{4}} 3 = 1.3548\ldots \\ (\log_3 4)x & \log_{\frac{9}{4}} 3 \leq x \leq 2 \end{cases}$$

is entirely contained in $F_{1,2}$. This will allow us to prove a partial converse to Theorem 2, namely that for any $\epsilon > 0$, there exists a positive constant K and a set A with $|A + A| \leq K|A|$ but $|A+2\cdot A| \geq K^{2-\epsilon}|A|$. Thus the true bound here is between 2 and 2.95. We also give some negative results, showing that neither Sidon Sets, nor subsets of $\{0,1\}^d \subset \mathbb{Z}^d$, can give rise to feasible points outside the regions already proved feasible. Finally, we give a lower bound for the region $F_{1,2}$, which is an easy consequence of Plünnecke's inequality. All these bounds and constructions are illustrated in Figure 2.

Our next series of results concerns the relationship between the sizes of $A + A$ and $A - A$, and thus relates to the feasible region $F_{1,-1}$. This is one of the oldest topics in additive combinatorics, with results going back to Freiman and Pigarev [11] and Ruzsa [14] in the 1970s (and indeed Conway in the 1960s).

Our starting point is a 1992 paper of Ruzsa [15]. Ruzsa constructed sets $A \subset \mathbb{Z}^d$ for which $A - A$ is very large, but $A + A$ is very small, in the following way. Start with a finite set $S \subset \mathbb{Z}$ with $|S + S| < |S - S|$. Then, for a fixed probability $0 < q < 1$, select a random subset $A \subset \mathbb{Z}^d$ by taking each element of S^d independently with probability q^d. For an appropriate choice of q, this "boosts" the discrepancy between $|S + S|$ and $|S - S|$ enough to prove the first part of Theorem 1. The second part is proved in a similar way.

In Section 4, we analyse and generalise Ruzsa's method from [15], leading to the following concept, which can be seen as a continuous analogue of the size of a sumset and that of a dilate.

Definition. A *fractional dilate* γ is a map $\gamma : \mathbb{Z} \to \mathbb{R}^+ \cup \{0\}$ with finite support $\mathrm{supp}(\gamma)$. We define the *size of a fractional dilate* to be

$$\|\gamma\| = \inf_{0\leq p\leq 1} \sum_{n\in \mathrm{supp}(\gamma)} \gamma(n)^p.$$

A *fractional set* is a fractional dilate α for which $\alpha(n) \leq 1$ for all $n \in \mathbb{Z}$.

Note that, if α is a fractional set, then $\|\alpha\| = \sum_{n\in\mathbb{Z}} \alpha(n)$, i.e., the above infimum is attained at $p = 1$. On the other hand, if γ is a dilate for which $\gamma(n) \geq 1$ for all $n \in \mathbb{Z}$, then $\|\gamma\| = |\mathrm{supp}(\gamma)|$, and the infimum is attained at $p = 0$. In general, we describe a fractional dilate as being *opulent*, *spartan* or *p-comfortable* if the above infimum is attained at $p = 0$, $p = 1$ or $0 < p < 1$ respectively. Theorem 20 gives a useful alternative characterization of fractional dilates.

We can identify an actual subset S of $\mathbb{Z}$ with the fractional set $\mathbb{1}_S$, which is both spartan and opulent. For any such sets S and T, $\mathbb{1}_S + k\cdot\mathbb{1}_T$ will be opulent, so that

$$\|\mathbb{1}_S + k\cdot\mathbb{1}_T\| = |S + k\cdot T|.$$

Given a fractional set α, let us say that a random set $S_n \subseteq \mathbb{Z}^n$ is *drawn from* α^n if each element of $\mathbb{Z}^n$ is chosen independently, and the probability that $(i_1, i_2, \ldots, i_n)$ is selected is $\alpha(i_1)\alpha(i_2)\ldots\alpha(i_n)$. Moreover, for fractional sets α, β and an integer k, let $\alpha + k \cdot \beta$ denote the fractional dilate defined by the formula

$$(\alpha + k \cdot \beta)(n) = \sum_{\substack{(i,j) \\ i+kj=n}} \alpha(i)\beta(j).$$

The point of these definitions is the following pair of theorems, which we prove in Section 4.3.

Theorem 4. *Let α be a fractional set with $\|\alpha\| > 1$, and suppose $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n. Then*

$$\mathbb{E}|S_n| = \|\alpha\|^n \qquad \mathrm{Var}|S_n| \leq \|\alpha\|^n$$

and

$$\lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot S_n|)^{1/n} = \|\alpha + k \cdot \alpha\|.$$

Theorem 5. *Let α be a fractional set with $\|\alpha\| > 1$, and suppose $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n. If $\alpha + k \cdot \alpha$ is "strictly spartan" (see later for an explanation of this terminology), in the sense that*

$$\sum_{n \in \mathrm{supp}(\gamma)} \gamma(n) \log \gamma(n) < 0,$$

then, with probability tending to 1,

$$|S_n + k \cdot S_n| \geq \tfrac{1}{2}|S_n|^2 \text{ if } k \neq 1$$
$$|S_n + k \cdot S_n| \geq \tfrac{1}{4}|S_n|^2 \text{ if } k = 1.$$

From now on, the phrase "with high probability", abbreviated to **whp**, means "with probability tending to 1 as the dimension (usually denoted by n) tends to infinity".

In Section 4.4, we apply these theorems to a construction of Hennecart, Robert and Yudin [3], to construct a fractional set α for which $\alpha - \alpha$ is spartan, but $\alpha + \alpha$ is not.

Theorem 6. *There exists a fractional set α for which $\|\alpha\| > 1$, $\alpha - \alpha$ is strictly spartan (so that $\|\alpha - \alpha\| = \|\alpha\|^2$), and $\|\alpha + \alpha\| \leq \|\alpha\|^{1.7354}$.*

This will allow us to prove that $(1.7354, 2)$ is feasible for $F_{1,-1}$.

Corollary 7. *For all $\epsilon > 0$, there exists a finite subset $A \subseteq \mathbb{Z}$ such that $|A - A| \geq |A|^{2-\epsilon} > 1$ but $|A + A| \leq |A|^{1.7354+\epsilon}$.*

Proof. Let α be the fractional set with properties as in Theorem 6, and let S_n be drawn from α^n. First, from Theorem 4 and Chebyshev's inequality

$$\mathbb{P}(||S_n| - \|\alpha\|^n| > 0.1\|\alpha\|^n) \leq 100\mathrm{Var}|S_n|/\|\alpha\|^{2n} \leq 100/\|\alpha\|^n \to 0,$$

so that with high probability

$$||S_n| - \|\alpha\|^n| \leq 0.1\|\alpha\|^n. \tag{1}$$

Second, since $\alpha - \alpha$ is strictly spartan, Theorem 5 shows that with high probability

$$|S_n - S_n| \geq \tfrac{1}{2}|S_n|^2. \tag{2}$$

Finally, Theorem 4 shows that

$$\lim_{n\to\infty} \mathbb{E}|S_n + S_n|^{1/n} \to \|\alpha + \alpha\| = \|\alpha\|^{1.7354}.$$

Consequently, for all $\epsilon > 0$, we will have

$$\mathbb{E}|S_n + S_n| \leq \|\alpha\|^{(1.7354+\epsilon)n}$$

for all sufficiently large n, and for such n

$$\mathbb{P}(|S_n + S_n| > \|\alpha\|^{(1.7354+2\epsilon)n}) \to 0$$

by Markov's inequality. Invoking (1), we have that for sufficiently large n

$$\mathbb{P}(|S_n + S_n| > |S_n|^{1.7354+3\epsilon}) \to 0,$$

so that with high probability

$$|S_n + S_n| \leq |S_n|^{1.7354+3\epsilon}. \tag{3}$$

The conclusion of the corollary follows from (1), (2) and (3). □

In the other direction, it follows from results of Freiman and Pigarev [11] and Ruzsa [14] that $(x, 2)$ is not attainable for any $x < 3/2$. All these results are illustrated in Figure 1.

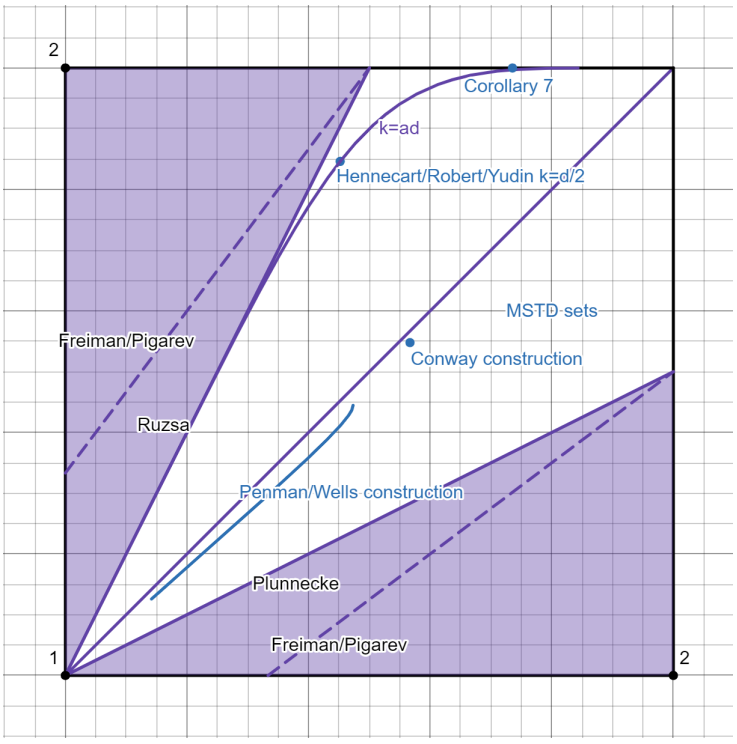

Figure 1: The feasible region $F_{1,-1}$

Finally, in Section 5, we discuss many open questions about $F_{1,-1}$ and $F_{1,2}$, and about feasible regions in general.

2 Feasible Regions

We remind the reader of the definition of a feasible region. For fixed integers k and l, the *feasible region* $F_{k,l}$ is defined as the closure of the set $E_{k,l}$ of *attainable points*

$$E_{k,l} = \left\{ \left(\frac{\log|A + k \cdot A|}{\log|A|}, \frac{\log|A + l \cdot A|}{\log|A|} \right) \right\} \subset [1,2]^2,$$

as A ranges over finite sets of integers. Note once again that the inclusion follows from the fact that $|A| \leq |A + k \cdot A| \leq |A|^2$ for all such A. Since $E_{k,l} \subset [1,2]^2$, we have also $F_{k,l} \subset [1,2]^2$. As mentioned in the introduction, we now prove that $F_{k,l}$ is convex.

Theorem 8. *For all nonzero k, l, the feasible region $F_{k,l}$ is convex, and contains the diagonal $D = \{(x,x) : 1 \leq x \leq 2\}$.*

Proof. First we prove the convexity. To do this, we first consider points $(x,y), (x',y') \in E_{k,l}$, and take $t \in [0,1]$. We will show that $(tx + (1-t)x', ty + (1-t)y') \in F_{k,l}$. Since $(x,y) \in E_{k,l}$, there exists a set $A \subset \mathbb{Z}$ with

$$|A + k \cdot A| = |A|^x \text{ and } |A + l \cdot A| = |A|^y.$$

Likewise, since $(x',y') \in E_{k,l}$, there exists a set $B \subset \mathbb{Z}$ with

$$|B + k \cdot B| = |B|^{x'} \text{ and } |B + l \cdot B| = |B|^{y'}.$$

Setting $\beta = \log|B| / \log|A|$, choose a sequence $q_1, q_2, \ldots$ of rational numbers such that

$$\lim_{i \to \infty} q_i = \frac{t\beta}{1 - t + t\beta}.$$

For each such $q_i = r/s$, we consider a set $A_i \subset \mathbb{Z}^s$, defined as

$$A_i = \underbrace{A \times A \times \cdots \times A}_{r} \times \underbrace{B \times B \times \cdots \times B}_{s-r},$$

in which there are r factors of A and $s - r$ factors of B. We have

$$\begin{aligned} |A_i| &= |A|^r |B|^{s-r}, \\ |A_i + k \cdot A_i| &= |A|^{rx} |B|^{(s-r)x'}, \text{ and} \\ |A_i + l \cdot A_i| &= |A|^{ry} |B|^{(s-r)y'}. \end{aligned}$$

Therefore,

$$\begin{aligned} \frac{\log|A_i + k \cdot A_i|}{\log|A_i|} &= \frac{rx \log|A| + (s-r)x' \log|B|}{r \log|A| + (s-r) \log|B|} \\ &= \frac{q_i x + (1 - q_i)x'\beta}{q_i + (1 - q_i)\beta}, \end{aligned}$$

which tends to $tx + (1-t)x'$ as $i \to \infty$. Similarly,

$$\frac{\log|A_i + l \cdot A_i|}{\log|A_i|} \to ty + (1-t)y',$$

as $i \to \infty$. Consequently, $(tx + (1-t)x', ty + (1-t)y') \in F_{k,l}$.

Now, given points $(x,y),(x',y') \in F_{k,l}$, we may take sequences of points (x_j,y_j) and (x'_j,y'_j) from $E_{k,l}$ tending to (x,y) and (x',y') respectively. For each j, the above argument shows that

$$(tx_j + (1-t)x'_j, ty_j + (1-t)y'_j) \in F_{k,l}.$$

Consequently, letting $j \to \infty$, we have that

$$(tx + (1-t)x', ty + (1-t)y') \in F_{k,l},$$

and the convexity is proved.

To show that $(1,1) \in F_{k,l}$, we consider the set $A := A_N = \{1,2,\dots,N\}$ for $N \gg \max(k,l)$. We have

$$|A + k\cdot A| = (k+1)(N-1)+1 \quad \text{and} \quad |A + l\cdot A| = (l+1)(N-1)+1,$$

so that, as $N \to \infty$,

$$\left(\frac{\log|A+k\cdot A|}{\log|A|}, \frac{\log|A+l\cdot A|}{\log|A|}\right) \to (1,1).$$

To show that $(2,2) \in F_{k,l}$, let $b > \max(|k|,|l|)+1$, and consider the set $B = \{1,b,b^2,\dots,b^N\}$. We have

$$|B + k\cdot B| \geq \tfrac{1}{2}|B|^2 \quad \text{and} \quad |B + l\cdot B| \geq \tfrac{1}{2}|B|^2,$$

so that, as $N \to \infty$,

$$\left(\frac{\log|B+k\cdot B|}{\log|B|}, \frac{\log|B+l\cdot B|}{\log|B|}\right) \to (2,2).$$

It now follows by convexity that $D = \{(x,x) : 1 \leq x \leq 2\} \subset F_{k,l}$. □

This result easily generalises to higher dimensions.

3 A construction for $F_{1,2}$

In this section, we present various results about the feasible region $F_{1,2}$. In particular, as stated in the introduction, we give a partial converse to a result of Hanson and Petridis (Theorem 2).

Our construction, the *Hypercube + Interval construction*, is very simple. Let

$$H_n = \left\{ \sum_{i=0}^{n-1} a_i 4^i : \ a_i \in \{0,1\} \right\}, \qquad I_k = \left\{0,1,\dots,\frac{4(4^{k-1}-1)}{3}\right\} \quad \text{and} \quad A_{n,k} = H_n \cup I_k.$$

In other words, H_n denotes the set of all natural numbers whose base 4 representation has length at most n and contains only 0s and 1s (the hypercube), and I_k is just an interval. We begin by giving bounds on the sizes of various sumsets and dilates related to H_n and I_k.

Theorem 9. *For $n \geq k > \frac{n+1}{2}$, and with notation as above, we have:*

$$\begin{aligned}
|I_k| &= \frac{4^k-1}{3} \geq |H_n| = 2^n \\
|H_n + H_n| &= 3^n \\
|H_n + I_k| &= 2^{n-k+1}\frac{4^k-1}{3} \geq |I_k + I_k| \\
|H_n + 2\cdot H_n| &= 4^n \geq \max\{|H_n + 2\cdot I_k|, |I_k + 2\cdot H_n|, |I_k + 2\cdot I_k|\}.
\end{aligned}$$

Proof. The first assertion is trivial. For $H_n + H_n$, note that

$$H_n + H_n = \left\{ \sum_{i=0}^{n-1} a_i 4^i : \ a_i \in \{0,1,2\} \right\}.$$

In other words, $H_n + H_n$ consists of the natural numbers whose base 4 representation has length at most n and contains only 0s, 1s, and 2s. Thus $|H_n + H_n| = 3^n$. Similarly, $H_n + 2 \cdot H_n$ consists of those natural numbers whose base 4 representation has length at most n and contains only 0s, 1s, 2s and 3s, but this is just $\{0, 1, \ldots, 4^n - 1\}$. Further, since $\max H_n \geq \max I_k$, all of the sets $H_n + 2 \cdot I_k$, $I_k + 2 \cdot H_n$ and $I_k + 2 \cdot I_k$ are subsets of $\{0, 1, \ldots, 4^n - 1\}$, and are therefore of size at most 4^n.

It remains to bound $|H_n + I_k|$. To this end, note that

$$H_n = \{0,1\} + \{0,4\} + \{0,4^2\} + \cdots + \{0,4^{n-1}\}.$$

Also, if $p \geq q$ are positive integers, then

$$\{0, 1, \ldots, p-1\} + \{0, q\} = \{0, 1, \ldots, p+q-1\}.$$

Consequently,

$$\begin{aligned}
H_n + I_k &= I_k + \{0,1\} + \{0,4\} + \cdots + \{0,4^{k-1}\} + \{0,4^k\} + \cdots + \{0,4^{n-1}\} \\
&= \left\{0, 1, \ldots, \frac{4(4^{k-1}-1)}{3}\right\} + \{0,1\} + \{0,4\} + \cdots + \{0,4^{k-1}\} + \{0,4^k\} + \cdots + \{0,4^{n-1}\} \\
&= \left\{0, 1, \ldots, \frac{4(4^{k-1}-1)}{3} + 1\right\} + \{0,4\} + \cdots + \{0,4^{k-1}\} + \{0,4^k\} + \cdots + \{0,4^{n-1}\} \\
&\ \ \vdots \\
&= \left\{0, 1, \ldots, \frac{2(4^{k}-1)}{3} - 1\right\} + \{0,4^k\} + \cdots + \{0,4^{n-1}\} \supseteq I_k + I_k.
\end{aligned}$$

Moreover, the set $\{0,4^k\} + \cdots + \{0,4^{n-1}\}$ consists of multiples of 4^k, which are all further than $2\left(\frac{4^k-1}{3}\right)$ apart. It follows that $H_n + I_k$ consists of 2^{n-k} intervals of length $2\left(\frac{4^k-1}{3}\right)$. □

Recall that $A_{n,k} = H_n \cup I_k$. Using Theorem 9, we can show the following.

Corollary 10. *Fix $\alpha \in \left(\frac{1}{2}, 1\right)$, and set $k = \lfloor \alpha n \rfloor$. Then, as $n \to \infty$,*

$$\begin{aligned}
\frac{\log |A_{n,k}|}{n} &\to \alpha \log 4 \\
\frac{\log |A_{n,k} + A_{n,k}|}{n} &\to \max\left\{\log 3, \frac{1+\alpha}{2}\log 4\right\} \\
\frac{\log |A_{n,k} + 2 \cdot A_{n,k}|}{n} &\to \log 4.
\end{aligned}$$

Proof. For the first part, Theorem 9 gives

$$\lim_{n\to\infty} \frac{\log |H_n|}{n} = \log 2 < \lim_{n\to\infty} \frac{\log |I_k|}{n} = \alpha \log 4.$$

Since $I_k \subseteq A_{n,k}$ and $|A_{n,k}| \leq |H_n| + |I_k|$, it follows that $\lim_{n\to\infty} \log|A_{n,k}|/n = \alpha \log 4$. In other words, for the given range of parameters, the interval I_k makes the dominant contribution to the size of $A_{n,k}$.

For the sumsets, we note that (again using Theorem 9)

$$\lim_{n\to\infty} \frac{\log|H_n + H_n|}{n} = \log 3$$

and

$$\lim_{n\to\infty} \frac{\log|H_n + I_k|}{n} = \frac{1+\alpha}{2}\log 4 > \lim_{n\to\infty} \frac{\log|I_k + I_k|}{n}.$$

Since $H_n + H_n$ and $H_n + I_k$ are both subsets of $A_{n,k} + A_{n,k}$, and

$$|A_{n,k} + A_{n,k}| \leq |H_n + H_n| + |H_n + I_k| + |I_k + I_k|$$

it follows that

$$\lim_{n\to\infty} \frac{\log|A_{n,k} + A_{n,k}|}{n} = \max\left\{\log 3, \frac{1+\alpha}{2}\log 4\right\}.$$

In other words, the dominant contribution to the size of $A_{n,k} + A_{n,k}$ comes from $H_n + H_n$ if $\alpha < \log 3/\log 2 - 1 \approx 0.585$, and from $H_n + I_k$ otherwise.

Finally, for the dilates, we have

$$\lim_{n\to\infty} \frac{\log|A_{n,k} + 2\cdot A_{n,k}|}{n} = \lim_{n\to\infty} \frac{\log|H_n + 2\cdot H_n|}{n} = \log 4.$$

□

We can now use Corollary 10 to expand the known feasible region $F_{1,2}$. Define $f : [1,2] \to [1,2]$ by

$$f(x) = \begin{cases} \frac{1}{2}(\beta+1) & \text{if } 1 \leq x \leq \frac{\log 2}{\log(3/2)} \\ (\log_4 3)x & \text{if } \frac{\log 2}{\log(3/2)} \leq x \leq 2. \end{cases}$$

Corollary 11. *For all $1 < \beta < 2$, $(f(\beta), \beta) \in F_{1,2}$.*

Proof. Let $\alpha = 1/\beta$, and set $k = \lfloor \alpha n \rfloor$. Then

$$\begin{aligned} \alpha \log 4 f(\beta) &= \alpha \log 4 \max\left\{\frac{1}{2}(\beta+1), (\log_4 3)\beta\right\} \\ &= \alpha \log 4 \max\left\{\frac{1+\alpha}{2\alpha}, \frac{\log 3}{\alpha \log 4}\right\} \\ &= \max\left\{\frac{1+\alpha}{2}\log 4, \log 3\right\}. \end{aligned}$$

Thus Corollary 10 provides sets $A_{n,k}$ with

$$\begin{aligned} \frac{\log|A_{n,k}|}{n} &\to \alpha \log 4 \\ \frac{\log|A_{n,k} + A_{n,k}|}{n} &\to \alpha f(\beta) \log 4 \\ \frac{\log|A_{n,k} + 2\cdot A_{n,k}|}{n} &\to \alpha\beta \log 4, \end{aligned}$$

proving the result. □

A simple change of variable shows that the graph of the piecewise-linear function

$$y = \min(2x-1, (\log_3 4)x) = \begin{cases} 2x-1 & 1 \le x \le \log_{\frac{9}{4}} 3 = 1.3548\ldots \\ (\log_3 4)x & \log_{\frac{9}{4}} 3 \le x \le 2 \end{cases}$$

is entirely contained in $F_{1,2}$.

As mentioned above, this gives a partial converse to Theorem 2.

Corollary 12. *For all $\epsilon > 0$, there exist sets S and numbers $K > 1$ with $|S+S| \le K|S|$ but with $|S + 2 \cdot S| > K^{2-\epsilon}|S|$.*

Proof. Take $\alpha > \log 3/\log 2 - 1$ in Corollary 10. □

Let us quickly discuss a lower bound on the feasible region.

Theorem 13. *For all sets A, $|A||A+A| \le |A + 2 \cdot A|^2$.*

Proof. Corollary 7.3.6 of [16], which is an easy conseqeunce of Plünnecke's inequality, states that for any three sets A, B, C,

$$|A||B+C| \le |A+B||A+C|.$$

Setting $B = C = 2 \cdot A$ gives

$$|A||A+A| = |A||2 \cdot A + 2 \cdot A| \le |A + 2 \cdot A|^2.$$

□

These results are all illustrated in Figure 2. First, the two results of Hanson and Petrridis (Theorems 2 and 3) show that the regions $y > 2.95x - 1.95$ and $y > 4x/3$ are both *infeasible* (i.e., none of the points in those regions is attainable). Likewise, Theorem 13 shows that the region $y < 1 + x/2$ is also infeasible. In the other direction, Corollary 11 shows that the lines OD and DC are feasible, while Theorem 8 shows that the line OE is feasible. Consequently, the entire quadrilateral $ODCE$ is feasible.

These results leave three regions unexplored: triangles OAB, BCD and OEF. More precisely, we can ask three questions:

Question 14. *Is (the interior of) triangle OAB infeasible? In other words, does $|A+A| = |A|^{1+t}$ imply $|A+2\cdot A| \le |A|^{1+2t}$? Alternatively, is it true that, for all A, $|A||A+2\cdot A| \le |A+A||A+A|$?*

Question 15. *Are there no attainable points above the extension of line CD? In other words, is it true that, if $|A+A| = 3^t$, then $|A+2\cdot A| \le 4^t$?*

Question 16. *Is (the interior of) triangle OEF infeasible? In other words, is it true that, for all A, $|A+2\cdot A| \ge |A+A|$?*

We coin the term *MST2D sets* (or *more sums than 2-dilates sets*) for counterexamples to Question 16. A natural candidate for an MST2D set is a Sidon set (that is, a set for which $|A+A|$ is as large as possible). However, one can easily show that a Sidon set cannot be an MST2D set.

Lemma 17. *If A is a Sidon set with at least two elements, then $|A+2\cdot A| > |A+A|$.*

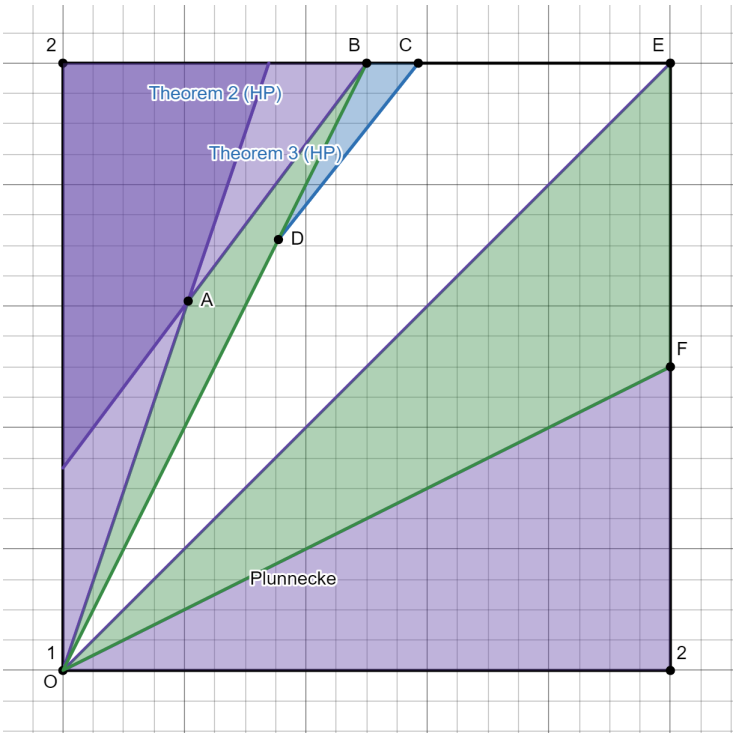

Figure 2: The feasible region $F_{1,2}$

Proof. Adding and multiplying non-zero constants to A does not change $|A+A|$ or $|A+2\cdot A|$. Thus we can assume that $0 \in A$ and $\gcd(A) = 1$.

Let $n = |A|$. If X_1, X_2 are independent and identically distributed (IID) random variables, drawn from any distribution on a finite set S, then $\mathbb{P}(X_1 = X_2) \geq 1/|S|$. Thus if A_1, A_2, A_3, A_4 are IID drawn from the uniform (or indeed any) distribution on A, then

$$|A + 2\cdot A| \geq \mathbb{P}(A_1 + 2\cdot A_2 = A_3 + 2\cdot A_4)^{-1}.$$

Now, since A is a Sidon set,

$$\mathbb{P}(A_4 - A_2 = k) = \mathbb{P}(A_1 - A_3 = k) = \begin{cases} 1/n, \text{ if } k = 0 \\ 0, \text{ if } k \notin A - A \\ 1/n^2, \text{ otherwise.} \end{cases}$$

Thus

$$\mathbb{P}(A_1 + 2\cdot A_2 = A_3 + 2\cdot A_4) = \mathbb{P}(A_1 - A_3 = 2(A_4 - A_2)) = \frac{1}{n^2} + \frac{K}{n^4},$$

where K is the number of non-zero elements of $A - A$ which are double some other element of $A - A$. Now there are $n^2 - n$ non-zero elements of $A - A$, but A contains elements of both parities (since $0 \in A$ and $\gcd(A) = 1$). Therefore, $A - A$ contains at least $2(n-1)$ odd elements, so

$K \leq n^2 - 3n + 2$. Consequently,

$$\begin{aligned}
|A + 2 \cdot A| &\geq \left(\frac{1}{n^2} + \frac{n^2 - 3n + 2}{n^4} \right)^{-1} \\
&= \frac{n^2}{2} \left(1 - \frac{3}{2n} + \frac{1}{n^2} \right)^{-1} \\
&\geq \frac{n^2}{2} \left(1 + \frac{3}{2n} - \frac{1}{n^2} \right) \\
&= \frac{n^2}{2} + \frac{3n}{4} - \frac{1}{2} \geq \frac{n^2 + n}{2} = |A + A|.
\end{aligned}$$

□

Similarly, a natural candidate for a counterexample to Question 15 is a "2-Sidon" set (i.e., one where $|A + 2 \cdot A|$ is as large as possible). An easy way to construct such sets is as subsets of the hypercube $\{0, 1\}^n$. But it follows from Theorem 2.3 of [5] that such sets in fact satisfy the condition of Question 15.

Lemma 18. *[Green [5]] Suppose A and B are subsets of the hypercube $\{0, 1\}^n$. Then*

$$|A + 2 \cdot B| = |A||B| \leq |A + B|^p,$$

where $p = \log 4 / \log 3$.

This lemma has an interesting history, going back to the 1970s. Details are in Appendix B of [5].

Very recently, Becker, Ivanisvili, Krachun and Madrid [1] proved that subsets of $\{0, 1\}^n$ also satisfy the conditions of Question 14; however, since in their result $|A+2\cdot A| = |A|^2$, their Corollary 2 is also a corollary of Lemma 18 above.

Lemma 19 (Becker et al. [1], Corollary 2)**.** *Suppose A is a subset of the hypercube $\{0, 1\}^n$. Then*

$$\frac{|A + 2 \cdot A|}{|A|} \leq \left(\frac{|A + A|}{|A|} \right)^q,$$

where $q = \log 2 / \log(3/2)$.

4 Fractional Dilates

4.1 General results on norms

We remind the reader of the following definitions. A *fractional dilate* γ is a map $\gamma : \mathbb{Z} \to \mathbb{R}^+ \cup \{0\}$ with finite support $\mathrm{supp}(\gamma)$. We define the *size of a fractional dilate* to be

$$\|\gamma\| = \inf_{0 \leq p \leq 1} \sum_{n \in \mathrm{supp}(\gamma)} \gamma(n)^p.$$

A *fractional set* is a fractional dilate α for which $\alpha(n) \leq 1$ for all $n \in \mathbb{Z}$. Finally, we describe a fractional dilate as being *opulent*, *spartan* or *p-comfortable* if the above infimum is attained at $p = 0$, $p = 1$ or $0 < p < 1$ respectively, so that, for instance, all fractional sets are spartan.

First, we give a simple characterisation of fractional dilates, which enables us to easily decide whether a fractional dilate is opulent, spartan or p-comfortable.

Theorem 20. *A fractional dilate γ with support $S = \operatorname{supp}(\gamma)$ is*

$$\begin{cases} \textit{spartan,} & \textit{if } \sum_{n\in S} \gamma(n)\log\gamma(n) \le 0 \\ \textit{opulent,} & \textit{if } \sum_{n\in S} \log\gamma(n) \ge 0 \\ \textit{p-comfortable,} & \textit{if } \sum_{n\in S} \gamma(n)^p \log\gamma(n) = 0. \end{cases}$$

Proof. For a fixed γ with support S, define a function $f : [0,1] \to \mathbb{R}$ by

$$f(p) = \sum_{n\in S} \gamma(n)^p,$$

so that $\|\gamma\| = \inf_{0\le p\le 1} f(p)$. f is twice-differentiable, and also strictly convex, since

$$f''(p) = \sum_{n\in S} (\log\gamma(n))^2 \gamma(n)^p > 0.$$

Suppose first that

$$f'(1) = \sum_{n\in S} \gamma(n)\log\gamma(n) \le 0.$$

Then we must have $f'(p) \le 0$ for all $0 < p < 1$, and hence $\|\gamma\| = f(1)$, i.e., γ is spartan.

Suppose next that

$$f'(0) = \sum_{n\in S} \log\gamma(n) \ge 0.$$

Then we must have $f'(p) \ge 0$ for all $0 < p < 1$, and hence $\|\gamma\| = f(0)$, i.e., γ is opulent.

Otherwise, $f'(0) < 0 < f'(1)$, and hence there is a unique $p \in (0,1)$ for which

$$f'(p) = \sum_{n\in S} \gamma(n)^p \log\gamma(n) = 0.$$

It follows that $\|\gamma\| = f(p)$, i.e., γ is p-comfortable. □

Next we give yet another characterisation of $\|\gamma\|$. Recall that, for positive numbers $y_1, \dots, y_n$ summing to 1, the entropy function $H(y_1, \dots, y_n)$ is defined to be

$$H(y_1, \dots, y_n) = -\sum_{i=1}^{n} y_i \log_2 y_i.$$

Gibbs' inequality (see for instance [4]) states that

$$H(y_1, \dots, y_n) \le -\sum y_i \log_2 z_i$$

for any sequence of positive z_i summing to 1, with equality if and only if $y_i = z_i$ for all i.

Lemma 21. *Suppose γ is a fractional dilate with support $S = \{s_1, \dots, s_n\}$. Then*

$$\|\gamma\| = \max_{y_1+\cdots+y_n=1} 2^{H(y_1,\dots,y_n)} \min\left\{1, \prod_{i=1}^{n} \gamma(s_i)^{y_i}\right\}.$$

Proof. First we observe that, for real x and $0 \le p \le 1$, we have $\min\{0, x\} \le px$, with equality exactly when either

1. $p = 0$ and $x \geq 0$,
2. $p = 1$ and $x \leq 0$, or
3. $0 < p < 1$ and $x = 0$.

Next, fix $0 \leq p \leq 1$, and let

$$z_i = \frac{\gamma(s_i)^p}{\sum_i \gamma(s_i)^p}.$$

Clearly $\sum z_i = 1$. Then, for all positive y_i summing to 1, we have

$$\begin{aligned}
H(y_1, \ldots, y_n) + \min\left\{0, \sum_i y_i \log_2 \gamma(s_i)\right\} &\leq H(y_1, \ldots, y_n) + \sum_i p y_i \log_2 \gamma(s_i) \\
&= H(y_1, \ldots, y_n) + \sum_i y_i \log_2 \gamma(s_i)^p \\
&= H(y_1, \ldots, y_n) + \sum_i y_i \left(\log_2 z_i + \log_2 \sum_i \gamma(s_i)^p\right) \\
&= H(y_1, \ldots, y_n) + \sum_i y_i \log_2 z_i + \log_2 \sum_i \gamma(s_i)^p \\
&\leq \log_2 \sum_i \gamma(s_i)^p,
\end{aligned}$$

with the last inequality being Gibbs' inequality.

Raising 2 to both sides shows that, for all positive $y_1, \ldots, y_n$ summing to 1, and all $0 \leq p \leq 1$,

$$2^{H(y_1,\ldots,y_n)} \min\left\{1, \prod_i \gamma(s_i)^{y_i}\right\} \leq \sum_i \gamma(s_i)^p. \tag{1}$$

To prove the theorem, we only need show that we can choose the y_i and p to achieve equality in (1). For this, revisiting the derivation of (1), we require that $y_i = z_i$ for all i and also that

$$\min\left\{0, \sum_i y_i \log_2 \gamma(s_i)\right\} = \sum_i p y_i \log_2 \gamma(s_i).$$

From the definition of z_i, this means we require exactly that

$$p \sum_i \gamma(s_i)^p \log \gamma(s_i) = \min\left\{0, \sum_i \gamma(s_i)^p \log \gamma(s_i)\right\}.$$

As discussed at the start of this proof, this holds exactly when

1. $p = 0$ and $\sum_i \log \gamma(s_i) \geq 0$, i.e., when γ is opulent,
2. $p = 1$ and $\sum_i \gamma(s_i) \log \gamma(s_i) \leq 0$, i.e., when γ is spartan, or
3. $0 < p < 1$ and $\sum_i \gamma(s_i)^p \log \gamma(s_i) = 0$, i.e., when γ is p-comfortable;

here, we have also used Theorem 20. Consequently, we can indeed achieve equality in (1), so the theorem is proved. □

4.2 Results for two sets

We recall some more definitions from the introduction. Given a fractional set α, we say that a random set $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n if each element of $\mathbb{Z}^n$ is chosen independently, and the probability that $(i_1, i_2, \ldots, i_n)$ is selected is $\alpha(i_1)\alpha(i_2)\ldots\alpha(i_n)$. Moreover, for fractional sets α, β and an integer k, let $\alpha + k \cdot \beta$ denote the fractional dilate defined by the formula

$$(\alpha + k \cdot \beta)(n) = \sum_{\substack{(i,j) \\ i+kj=n}} \alpha(i)\beta(j).$$

First we prove two simple lemmas that we will use repeatedly. In the proof of both we use the fact that fractional sets are spartan.

Lemma 22. *Suppose α and β are fractional sets, and $\gamma = \alpha + \beta$ is spartan. Then*

$$\|\gamma\| = \|\alpha\|\|\beta\|.$$

Proof. If γ is spartan with support S, then

$$\|\gamma\| = \sum_{n\in S} \gamma(n) = \sum_{n\in S} \sum_{\substack{(i,j) \\ i+j=n}} \alpha(i)\beta(j) = \sum_{i\in\mathbb{Z}} \alpha(i) \sum_{j\in\mathbb{Z}} \beta(j) = \|\alpha\|\|\beta\|.$$

□

Lemma 23. *Let α be a fractional set, and suppose that $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n. Then*

$$E|S_n| = \|\alpha\|^n.$$

Proof. Writing $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, we have

$$\mathbb{E}|S_n| = \sum_{v\in\mathbb{Z}^n} \mathbb{P}(v \in S_n) = \sum_{v\in\mathbb{Z}^n} \alpha(v_1)\cdots\alpha(v_n) = \prod_{i=1}^{n} \sum_{v_i\in Z} \alpha(v_i) = \|\alpha\|^n.$$

□

Our aim is to prove Theorems 4 and 5, which concern just one fractional set α and a single random set $S_n \subseteq \mathbb{Z}^n$ drawn from α^n. However, it is easier to start with *two* fractional sets α and β, and let $S_n, T_n \subseteq \mathbb{Z}^n$ be drawn independently from α^n and β^n respectively. In this section, we consider two such sets, and prove the following "two-set" versions of Theorems 4 and 5.

Theorem 24. *Let α and β be fractional sets, and suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively. Then*

$$\lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot T_n|)^{1/n} = \|\alpha + k \cdot \beta\|.$$

Theorem 25. *Let α and β be fractional sets, and suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively. If $\gamma = \alpha + k \cdot \beta$ is strictly spartan, in the sense that*

$$\sum_{n\in\mathrm{supp}(\gamma)} \gamma(n)\log\gamma(n) < 0,$$

then with high probability

$$|S_n + k \cdot T_n| \geq \tfrac{1}{2}|S_n||T_n|.$$

Let us first prove the upper bound in Theorem 24. For this, we require a definition. For two sets $A, B \subseteq \mathbb{Z}^n$, the *multiplicity* $\mathrm{Mult}_{A+k\cdot B}(x)$ of x in $A + k \cdot B$ is defined by the formula

$$\mathrm{Mult}_{A+k\cdot B}(x) = |A \cap (x - k \cdot B)| = |\{(a, b) : a \in A, b \in B, a + kb = x\}|.$$

In other words, $\mathrm{Mult}_{A+k\cdot B}(x)$ is the number of ways of writing $x = a + kb$ with $a \in A$ and $b \in B$.

By replacing $k \cdot \beta$ by β in Theorem 24, it is enough to prove the theorem for $k = 1$. In the rest of this subsection, we will make this simplification.

Theorem 26. *Let α and β be fractional sets, suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively, and let $\gamma = \alpha + \beta$. Then*

$$\mathbb{E}|S_n + T_n| \leq \|\gamma\|^n.$$

Proof. Let X be the support of γ. Then the possible elements of $S_n + T_n$ are the elements of X^n. Given a particular element $x \in X^n$, we have, for all $0 \leq p \leq 1$,

$$\begin{aligned}\mathbb{P}(x \in S_n + T_n) &= \mathbb{P}(\mathrm{Mult}_{S_n+T_n}(x) > 0)\\ &\leq \min\{1, \mathbb{E}(\mathrm{Mult}_{S_n+T_n}(x))\}\\ &\leq (\mathbb{E}(\mathrm{Mult}_{S_n+T_n}(x)))^p.\end{aligned}$$

Now for $x = (x_1, \ldots, x_n) \in X^n$, we have

$$\begin{aligned}\mathbb{E}(\mathrm{Mult}_{S_n+T_n}(x)) &= \sum_{\substack{z_1+y_1=x_1\\ \vdots\\ z_n+y_n=x_n}} \alpha(z_1)\cdots\alpha(z_n)\beta(y_1)\cdots\beta(y_n)\\ &= \left(\sum_{z_1+y_1=x_1} \alpha(z_1)\beta(y_1)\right)\cdots\left(\sum_{z_n+y_n=x_n} \alpha(z_n)\beta(y_n)\right)\\ &= \gamma(x_1)\gamma(x_2)\cdots\gamma(x_n).\end{aligned}$$

It follows that

$$\begin{aligned}\mathbb{E}|S_n + T_n| &= \sum_{x\in X^n} \mathbb{P}(x \in S_n + T_n)\\ &\leq \sum_{x\in X^n} (\mathbb{E}(\mathrm{Mult}_{S_n+T_n}(x)))^p\\ &= \sum_{(x_1,\ldots,x_n)\in X^n} \gamma(x_1)^p\gamma(x_2)^p\cdots\gamma(x_n)^p\\ &= \left(\sum_{x\in X} \gamma(x)^p\right)^n\end{aligned}$$

for all $0 \leq p \leq 1$. Since $\|\gamma\| = \inf_{0\leq p\leq 1} \sum_x \gamma(x)^p$, the result follows. □

Next we prove that $\|\gamma\|$ is a lower bound for the limit. We will require a series of lemmas.

Lemma 27. *Suppose that $X = \sum_{i=1}^N Z_i$, where the Z_i are independent Bernoulli random variables. Then*

$$\mathbb{P}(X > 0) \geq \mathbb{E}(X) - \tfrac{1}{2}\mathbb{E}(X)^2.$$

Proof. We have

$$\mathbb{E}(X)^2 = \sum_{i=1}^{N}\sum_{j=1}^{N}\mathbb{E}(Z_i)\mathbb{E}(Z_j) = \sum_{i=1}^{N}\sum_{j=1}^{N}\mathbb{E}(Z_iZ_j) \geq 2\sum_{i<j}\mathbb{E}(Z_iZ_j) = 2\mathbb{E}\binom{X}{2},$$

so that, since $n - \binom{n}{2} \leq \mathbb{1}_{n>0}$ for all $n \geq 0$,

$$\mathbb{E}(X) - \tfrac{1}{2}\mathbb{E}(X)^2 \leq \mathbb{E}\left(X - \binom{X}{2}\right) \leq \mathbb{E}(\mathbb{1}_{X>0}) = \mathbb{P}(X > 0).$$

□

Lemma 28. *Suppose that $(X_n)_{n=1}^{\infty}$ is a collection of random variables, each of which can be written as the sum of a finite number of independent Bernoulli random variables. If*

$$\lim_{n\to\infty}\mathbb{E}(X_n)^{1/n} = t$$

then

$$\lim_{n\to\infty}\mathbb{P}(X_n > 0)^{1/n} = \min(1, t).$$

Proof. Suppose first that $t < 1$. Lemma 27 implies that

$$\limsup_{n\to\infty}\left(\mathbb{E}(X_n) - \mathbb{P}(X_n > 0)\right)^{1/n} \leq \lim_{n\to\infty}\left(\tfrac{1}{2}\mathbb{E}(X_n)^2\right)^{1/n} = t^2.$$

Consequently, for all $\epsilon > 0$, if $n \geq n_0(\epsilon)$, we have both

$$(t-\epsilon)^n \leq \mathbb{E}(X_n) \leq (t+\epsilon)^n$$

and

$$\mathbb{E}(X_n) - \mathbb{P}(X_n > 0) \leq (t^2 + \epsilon)^n$$

so that also

$$(t-2\epsilon)^n \leq \mathbb{P}(X_n > 0) \leq (t+\epsilon)^n$$

which proves that $\mathbb{P}(X_n > 0)^{1/n} \to t$.

Next suppose that $t \geq 1$. Given any $0 < u < 1$, write $Y_n = X_nW_n$, where the W_i are new independent Bernoulli random variables with $\mathbb{P}(W_n = 1) = (u/t)^n$. Then

$$\lim_{n\to\infty}\mathbb{E}(Y_n)^{1/n} = \lim_{n\to\infty}(\mathbb{E}(X_n)\mathbb{E}(W_n))^{1/n} = u,$$

and so by the above argument

$$u = \lim_{n\to\infty}\mathbb{P}(Y_n > 0)^{1/n} \leq \liminf_{n\to\infty}\mathbb{P}(X_n > 0)^{1/n} \leq 1.$$

Since this is true for all $u < 1$, we must have $\mathbb{P}(X_n > 0)^{1/n} \to 1$. □

We can use Lemma 28 to calculate the asymptotic behaviour of the probability that a randomly chosen vector lies in $S_n + T_n$.

Corollary 29. *Let α and β be fractional sets, suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively, and let $\gamma = \alpha + \beta$. Fix $N > 0$, and suppose that*

- $x_1, \ldots, x_N \in \mathbb{Z}$
- $y_1, \ldots, y_N \geq 0$ *with* $\sum y_i = 1$
- *for each n, $z_{1,n}, \ldots, z_{N,n} \in \mathbb{Z}_{\geq 0}$ with $\sum_i z_{i,n} = n$ and $z_{i,n}/n \to y_i$ for each i*
- *for each n, $v_n \in \mathbb{Z}^n$ is such that $z_{i,n}$ coordinates of v_n are equal to x_i.*

Then, if

$$t = \gamma(x_1)^{y_1} \ldots \gamma(x_N)^{y_N}$$

we have

$$\lim_{n\to\infty} \mathbb{P}(v_n \in S_n + T_n)^{1/n} = \min\{1, t\}.$$

Proof. For a fixed sequence v_n, let

$$X_n = \mathrm{Mult}_{S_n+T_n}(v_n) = \sum_{z\in\mathbb{Z}^n} \mathbb{1}_{z\in S_n, v_n - z\in T_n},$$

so that each X_n is a sum of a finite number of independent Bernoulli random variables. As in the proof of Theorem 26,

$$\mathbb{E}(X_n) = \gamma(x_1)^{z_{1,n}}\gamma(x_2)^{z_{2,n}} \ldots \gamma(x_N)^{z_{N,n}},$$

so $\mathbb{E}(X_n)^{1/n} \to t$. Applying Lemma 28, we get that

$$\mathbb{P}(v_n \in S_n + T_n)^{1/n} = \mathbb{P}(X_n > 0) \to \min\{1, t\}.$$

□

The next corollary proves the lower bound on $(\mathbb{E}|S_n + T_n|)^{1/n}$ which, together with Theorem 26, completes the proof of Theorem 24.

Corollary 30. *Let α and β be fractional sets, suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively, and let $\gamma = \alpha + \beta$. Then*

$$\liminf_{n\to\infty} (\mathbb{E}|S_n + T_n|)^{1/n} \geq \|\gamma\|.$$

Proof. Since α and β have finite support, so does γ. Let $S = \mathrm{supp}(\gamma) = \{s_1, \ldots, s_N\}$. By Lemma 21, there exist non-negative numbers $y_1, \ldots, y_N$ summing to 1 with

$$\|\gamma\| = 2^{H(y_1,\ldots,y_N)} \min\left\{1, \prod_{i=1}^{N} \gamma(s_i)^{y_i}\right\}.$$

For each n, choose integers $z_{1,n} \ldots, z_{N,n}$ summing to n, and with $z_i/n \to y_i$ for each $1 \leq i \leq N$. Let $V_n \in \mathbb{Z}^n$ be the set of vectors with exactly $z_{i,n}$ coordinates equal to s_i, for each $1 \leq i \leq N$. Then, for each $v \in V_n$, Corollary 29 shows that

$$\lim_{n\to\infty} \mathbb{P}(v \in S_n + T_n)^{1/n} = \min\left\{1, \prod_{i=1}^{N} \gamma(s_i)^{y_i}\right\}.$$

It is well known that, abbreviating $z_{i,n}$ to z_i,

$$\lim_{n\to\infty} |V_n|^{1/n} = \lim_{n\to\infty} \binom{n}{z_1, z_2, \ldots, z_N}^{1/n} = 2^{H(y_1,\ldots,y_N)}.$$

Consequently,

$$\begin{aligned}\liminf_{n\to\infty}(\mathbb{E}|S_n+T_n|)^{1/n} &\geq \liminf_{n\to\infty}(\mathbb{E}|(S_n+T_n)\cap V_n|)^{1/n}\\ &= \liminf_{n\to\infty}(|V_n|\cdot\mathbb{P}(v\in S_n+T_n|v\in V_n))^{1/n}\\ &= \lim_{n\to\infty}|V_n|^{1/n}\cdot\lim_{n\to\infty}\mathbb{P}(v\in S_n+T_n|v\in V_n)^{1/n}\\ &= 2^{H(y_1,y_2,\ldots,y_N)}\min\left\{1,\prod_{i=1}^{N}\gamma(s_i)^{y_i}\right\}\\ &= \|\gamma\|.\end{aligned}$$

□

With Theorem 24 proved, we turn to Theorem 25.

Lemma 31. *Let α and β be fractional sets, and suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively, and let $\gamma = \alpha + \beta$. Suppose that γ is strictly spartan, in the sense that*

$$\sum_{n\in\mathrm{supp}(\gamma)}\gamma(n)\log\gamma(n) < 0.$$

Then

$$\mathbb{E}(|S_n||T_n|) = \mathbb{E}|S_n|\cdot\mathbb{E}|T_n| = \|\alpha\|^n\|\beta\|^n = \|\gamma\|^n$$

and

$$\mathbb{E}(|S_n||T_n| - |S_n+T_n|) = o(\|\gamma\|^n).$$

Proof. The first part of the conclusion follows from Lemmas 22 and 23. For the second part, for $v = (v_1,\ldots,v_n)\in\mathbb{Z}^n$, write

$$X_v = \mathbb{E}(\mathrm{Mult}_{S_n+T_n}(v)).$$

Since X_v is a sum of independent Bernoulli random variables, Lemma 27 shows that

$$\mathbb{E}(X_v) - \mathbb{P}(X_v > 0) \leq \mathbb{E}(X_v)^2.$$

Since the left hand side is also at most $\mathbb{E}(X_v)$, it follows that

$$\mathbb{E}(X_v) - \mathbb{P}(X_v > 0) \leq \mathbb{E}(X_v)^p \text{ for all } 1\leq p\leq 2.$$

Therefore, for all $1\leq p\leq 2$,

$$\begin{aligned}\mathbb{E}(|S_n||T_n| - |S_n+T_n|) &= \sum_v(\mathbb{E}(X_v) - \mathbb{P}(X_v>0)) \leq \sum_v\mathbb{E}(X_v)^p\\ &= \sum_{v_1,v_2,\ldots,v_n}\gamma(v_1)^p\ldots\gamma(v_n)^p = \left(\sum_v\gamma(v)^p\right)^n.\end{aligned}$$

Now γ is strictly spartan, so the function $f(p) = \sum_v\gamma(v)^p$ is strictly decreasing on the interval $[0,1+\epsilon]$, for some $\epsilon>0$. Consequently, for that ϵ, we have $\sum_v\gamma(v)^{1+\epsilon} < \|\gamma\|$. Thus $\mathbb{E}(|S_n||T_n| - |S_n+T_n|) = o(\|\gamma\|^n)$ as $n\to\infty$. □

Theorem 25 follows from Lemma 31 and Markov's inequality.

4.3 From two sets to one: the rainbow connection

In this section we will prove Theorems 4 and 5. Let α be a fractional set, let k be a nonzero integer, and let $\gamma := \alpha + k \cdot \alpha$ denote the fractional dilate defined by $\gamma(n) = \sum_{i+kj=n} \alpha(i)\alpha(j)$.

First we prove two easy lemmas.

Lemma 32. *Let α be a fractional set, and suppose that $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n. Then*

$$\mathrm{Var}|S_n| \leq \|\alpha\|^n.$$

Proof. $|S_n|$ is the sum of independent Bernoulli random variables X_i with $\mathbb{P}(X_i = 1) =: p_i$. We have

$$\mathrm{Var}|S_n| = \sum_{i \in S} \mathrm{Var}X_i = \sum_{i \in S} p_i(1-p_i) \leq \sum_{i \in S} p_i = \mathbb{E}|S_n| = \|\alpha\|^n,$$

where the last equality is Lemma 23. □

Lemma 33. *Let α be a fractional set with $\|\alpha\| > 1$, and let $\gamma := \alpha + k \cdot \alpha$ for a fixed nonzero integer k. Then $\|\alpha\| \leq \|\gamma\|$.*

Proof. Let S_n be drawn from α^n. Then $|S_n|$ can be written as the sum of independent Bernoulli random variables, and so $(\mathbb{E}|S_n|)^{1/n} = \|\alpha\| > 1$ for all n by Lemma 23. Thus, by Lemma 28, we have

$$\lim_{n\to\infty} \Pr(|S_n| > 0)^{1/n} = 1.$$

Now let T_n be drawn independently from α^n. By Corollary 30, we have

$$\|\gamma\| = \lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot T_n|)^{1/n}.$$

But $|S_n + k \cdot T_n| \geq |T_n|$ whenever S_n is non-empty, so

$$|S_n + k \cdot T_n| \geq |T_n| \cdot \mathbb{1}_{|S_n|>0}.$$

Since $|S_n|$ and $|T_n|$ are independent, it follows that

$$\|\gamma\| = \lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot T_n|)^{1/n} \geq \lim_{n\to\infty} (\mathbb{E}|T_n| \cdot \mathbb{P}(|S_n| > 0))^{1/n} = \|\alpha\|.$$

□

We will prove Theorem 4 by comparing the sizes of $S_n + k \cdot S_n$ and $S_n + k \cdot T_n$, where S_n and T_n are drawn independently from α^n. For α and γ fixed, with supports A and Γ respectively, we say that a vector $v \in \mathbb{Z}^n$ is *rainbow* if its components include at least one copy of each element of Γ. Finally, let R_n denote the set of rainbow vectors in $\mathbb{Z}^n$.

The cases $k \neq 1$ and $k = 1$ require separate analyses. We treat the case $k \neq 1$ first.

Theorem 34. *Fix a fractional set α with $\|\alpha\| > 1$ and a positive integer n, and let S_n and T_n be drawn independently from α^n. If $k \neq 1$, and v is a rainbow vector for $\gamma = \alpha + k \cdot \alpha$, then*

$$\mathbb{P}(v \in S_n + k \cdot S_n) = \mathbb{P}(v \in S_n + k \cdot T_n)$$

and so

$$\mathbb{E}|(S_n + k \cdot S_n) \cap R_n| = \mathbb{E}|(S_n + k \cdot T_n) \cap R_n|.$$

Proof. Recall that $A = \mathrm{supp}(\alpha)$. For a fixed rainbow vector $v \in \mathbb{Z}^n$, write

$$S = \{x \in \mathbb{Z}^n : x \in A^n, v - kx \in A^n\} = \{x \in \mathbb{Z}^n : \mathbb{P}(x \in S_n, v - kx \in S_n) > 0\}.$$

Since A is finite, so is S.

We claim that there exist distinct $a, b \in A$ such that the expression $a + kb$ is unique, i.e., $a + kb$ cannot be expressed in any other way $a' + kb'$, where $a', b' \in A$. Indeed, if $k < 0$, let $a = \max A$ and $b = \min A$. If $a', b' \in A$, then $a \geq a'$ and $b \leq b'$, so $a + kb \geq a' + kb'$, with equality only if $a = a'$ and $b = b'$. Similarly, if $k > 1$, we can take $b = \max A$ and $a = \max(A \setminus \{b\})$. If $a', b' \in A$ with $a' + kb' = a + kb$ but with $a' \neq a$ and $b' \neq b$, we must have $b' < b$, whence $b' \leq a$ and also $a' \leq b$, so that

$$a' + kb' \leq b + ka < b + ka + (k-1)(b-a) = a + kb,$$

a contradiction.

Now, since v is a rainbow vector, there exists i with $v_i = a + kb$. It follows that for all $x \in S$, $x_i = a$ and $(v - kx)_i = b \neq a$, so that $v - kx \notin S$ and $x \neq v - kx$. Consequently, the events $x \in S_n$ and $v - kx \in S_n$ are independent, and hence

$$\mathbb{P}(x \in S_n, v - kx \in S_n) = \mathbb{P}(x \in S_n)\mathbb{P}(v - kx \in S_n).$$

Furthermore, since the sets $\{x, v - kx\}$ for all $x \in S$ are disjoint, we have by independence

$$\begin{aligned}
\mathbb{P}(v \in S_n + S_n) &= 1 - \prod_{x \in S}(1 - \mathbb{P}(x \in S_n, v - kx \in S_n)) \\
&= 1 - \prod_{x \in S}(1 - \mathbb{P}(x \in S_n)\mathbb{P}(v - kx \in S_n)) \\
&= 1 - \prod_{x \in S}(1 - \mathbb{P}(x \in S_n)\mathbb{P}(v - kx \in T_n)) \\
&= 1 - \prod_{x \in S}(1 - \mathbb{P}(x \in S_n, v - kx \in T_n)) \\
&= \mathbb{P}(v \in S_n + T_n).
\end{aligned}$$

The statement about expectations follows by summing over all $v \in R_n$. □

For $k = 1$, $a + kb = b + ka$, so $S_n + S_n$ will be usually be a lot smaller than $S_n + T_n$. Thus we need to modify our strategy. Order the elements of $\mathbb{Z}^n$ lexicographically, so that, for $v, v' \in \mathbb{Z}^n$, if v and v' first differ in the ith coordinate, we set $v < v'$ if $v_i < v'_i$. Then, for subsets $U, V \subseteq \mathbb{Z}^n$, we define

$$U +^< V = \{u + v \,:\, u \in U, v \in V, u < v\}.$$

Theorem 35. *Fix a fractional set α with $\|\alpha\| > 1$ and a positive integer n, and let S_n and T_n be drawn independently from α^n. If v is a rainbow vector for $\gamma = \alpha + \alpha$, then*

$$\mathbb{P}(v \in S_n + S_n) = \mathbb{P}(v \in S_n +^< T_n)$$

and so

$$\mathbb{E}|(S_n + S_n) \cap R_n| = \mathbb{E}|(S_n +^< T_n) \cap R_n|.$$

Proof. First we argue that, since v is rainbow, $v/2 \notin A^n = (\mathrm{supp}(\alpha))^n$. For let a and b be the two largest elements of A. Then $c = a + b \in \Gamma = \mathrm{supp}(\gamma)$, so, since v is a rainbow vector, there exists i such that $v_i = c$. But, by choice of a and b, $(v/2)_i = c/2 = (a+b)/2 \notin A$, so $v/2 \notin A^n$.

Next, as before, we write

$$S = \{x \in \mathbb{Z}^n : x \in A^n, v - x \in A^n\} = \{x \in \mathbb{Z}^n : \mathbb{P}(x \in S_n, v - x \in S_n) > 0\}.$$

As before, S is a finite set. From the above argument, there is no x for which $x = v - x$. Furthermore, the sets $\{x, v - x\}$ are all disjoint. Therefore

$$\begin{aligned}
\mathbb{P}(v \in S_n + S_n) &= 1 - \prod_{\substack{x \in S \\ x < v - x}} (1 - \mathbb{P}(x \in S_n, v - x \in S_n)) \\
&= 1 - \prod_{\substack{x \in S \\ x < v - x}} (1 - \mathbb{P}(x \in S_n)\mathbb{P}(v - x \in S_n)) \\
&= 1 - \prod_{\substack{x \in S \\ x < v - x}} (1 - \mathbb{P}(x \in S_n)\mathbb{P}(v - x \in T_n)) \\
&= 1 - \prod_{\substack{x \in S \\ x < v - x}} (1 - \mathbb{P}(x \in S_n, v - x \in T_n)) \\
&= \mathbb{P}(v \in S_n +^{<} T_n).
\end{aligned}$$

As in the proof of Theorem 34, the result about expectations follows by summing over $v \in R_n$. □

Theorems 34 and 35 give us a good bound on $\mathbb{E}|S_n + k \cdot S_n|$ since, usually, most of the elements of $S_n + k \cdot T_n$ are in fact rainbow. Recall that $(\mathbb{E}|S_n + k \cdot T_n|)^{1/n} \to \|\alpha + k \cdot \alpha\| = \|\gamma\|$ as $n \to \infty$.

Theorem 36. *Let α be a fractional set with $\|\alpha\| > 1$, and let $\gamma := \alpha + k \cdot \alpha$ for a fixed nonzero integer k. For $n \geq 1$, let S_n and T_n be drawn independently from α^n. Then there exists an $\epsilon > 0$ such that $\mathbb{E}|(S_n + k \cdot T_n) \setminus R_n| = o((\|\gamma\| - \epsilon)^n)$ as $n \to \infty$.*

Proof. As above, write $\Gamma = \mathrm{supp}(\gamma)$. Let $p \in [0, 1]$ be such that $\|\gamma\| = \sum_{z \in \Gamma} \gamma(z)^p$, and let $\delta = \min_{z \in \Gamma} \gamma(z)$. For $z \in \Gamma$, let

$$Q_z = \{v \in S_n + k \cdot T_n : v_i \neq z \text{ for all } i\}.$$

From the argument in the proof of Theorem 26, we have, for all $0 \leq q \leq 1$,

$$\mathbb{E}|Q_z| \leq \left(\sum_{w \neq z} \gamma(w)^q \right)^n.$$

In particular, taking $q = p$,

$$\mathbb{E}|Q_z| \leq \left(\sum_{w \neq z} \gamma(w)^p \right)^n = (\|\gamma\| - \delta^p)^n,$$

and so

$$\mathbb{E}|(S_n + k \cdot T_n) \setminus R_n| \leq |\Gamma|(\|\gamma\| - \delta^p)^n = o((\|\gamma\| - \epsilon)^n,$$

for any $\epsilon < \delta^p$. □

Theorem 37. *Let α be a fractional set with $\|\alpha\| > 1$, and let $\gamma := \alpha + k \cdot \alpha$ for a fixed nonzero integer k. For $n \geq 1$, let S_n be drawn from α^n. Then*

$$\mathbb{E}|S_n + k \cdot S_n| \leq 2\|\gamma\|^n.$$

Proof. Write

$$S_n \hat{+} k \cdot S_n = \{a + kb : a, b \in S_n, a \neq b\}.$$

Then

$$S_n + k \cdot S_n = (S_n \hat{+} k \cdot S_n) \cup ((k+1) \cdot S_n)$$

and so

$$|S_n + k \cdot S_n| \leq |S_n \hat{+} k \cdot S_n| + |S_n|.$$

The argument in the proof of Theorem 26 shows that

$$\mathbb{E}|S_n \hat{+} k \cdot S_n| \leq \|\gamma\|^n,$$

and Lemmas 23 and 33 show that $\mathbb{E}|S_n| = \|\alpha\|^n \leq \|\gamma\|^n$, so that

$$\mathbb{E}|S_n + k \cdot S_n| \leq 2\|\gamma\|^n,$$

as required. □

Proof of Theorem 4. Let α be a fractional set with $\|\alpha\| > 1$, and suppose $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n. We have $\mathbb{E}|S_n| = \|\alpha\|^n$ and $\mathrm{Var}|S_n| \leq \|\alpha\|^n$ from Lemmas 23 and 32 respectively. It remains to show that

$$\lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot S_n|)^{1/n} = \|\alpha + k \cdot \alpha\|.$$

Let $\gamma := \alpha + k \cdot \alpha$. From Theorem 37 we have, for all nonzero k,

$$\limsup_{n\to\infty} \mathbb{E}|S_n + k \cdot S_n|^{1/n} \leq \|\gamma\|.$$

Now, if $k \neq 1$, Theorem 34 gives

$$\begin{aligned}
\mathbb{E}|S_n + k \cdot S_n| &\geq \mathbb{E}|(S_n + k \cdot S_n) \cap R_n| \\
&= \mathbb{E}|(S_n + k \cdot T_n) \cap R_n| \\
&= \mathbb{E}|S_n + k \cdot T_n| - \mathbb{E}|(S_n + k \cdot T_n) \setminus R_n|.
\end{aligned}$$

By Theorem 24, we have $\mathbb{E}|S_n + k \cdot T_n|^{1/n} \to \|\gamma\|$, and Theorem 36 gives us an $\epsilon > 0$ such that $\mathbb{E}|(S_n + k \cdot T_n) \setminus R_n| = o((\|\gamma\| - \epsilon)^n)$. Consequently, we have

$$\liminf_{n\to\infty} \mathbb{E}|S_n + k \cdot S_n|^{1/n} \geq \|\gamma\|$$

and hence $\mathbb{E}|S_n + k \cdot S_n|^{1/n} \to \|\gamma\|$, as required.

When $k = 1$, Theorem 35 gives

$$\begin{aligned}
\mathbb{E}|S_n + S_n| &\geq \mathbb{E}|(S_n + S_n) \cap R_n| \\
&= \mathbb{E}|(S_n +^{<} T_n) \cap R_n| \\
&= \mathbb{E}|S_n +^{<} T_n| - \mathbb{E}|(S_n +^{<} T_n) \setminus R_n| \\
&= \tfrac{1}{2}\mathbb{E}|S_n \hat{+} T_n| - \mathbb{E}|(S_n +^{<} T_n) \setminus R_n| \\
&\geq \tfrac{1}{2}(\mathbb{E}|S_n + T_n| - \mathbb{E}|S_n|) - \mathbb{E}|(S_n +^{<} T_n) \setminus R_n| \\
&= \tfrac{1}{2}(\mathbb{E}|S_n + T_n| - \|\alpha\|^n) - \mathbb{E}|(S_n +^{<} T_n) \setminus R_n|.
\end{aligned}$$

Now, if $\|\gamma\| = \|\alpha\|$, we certainly have $\mathbb{E}|S_n + S_n| \geq \mathbb{E}|S_n| = \|\alpha\|^n = \|\gamma\|^n$, so we may assume $\|\gamma\| > \|\alpha\|$. In this case, Theorems 24 and 36 now yield

$$\liminf_{n\to\infty} \mathbb{E}|S_n + S_n|^{1/n} \geq \|\gamma\|$$

and hence $\mathbb{E}|S_n + S_n|^{1/n} \to \|\gamma\|$, as required.

Corollary 38. *Let α be a fractional set with $\|\alpha\| > 1$, and let $\gamma := \alpha + k \cdot \alpha$ for $k \neq 1$. For $n \geq 1$, let S_n be drawn from α^n. Then, if γ is strictly spartan (i.e., $\sum_{n\in\mathrm{supp}(\gamma)} \gamma(n) \log \gamma(n) < 0$), then*

$$\mathbb{E}\left(|S_n|^2 - |S_n + k \cdot S_n|\right) = o(\mathbb{E}|S_n|^2).$$

Proof. If $\gamma = \alpha + k \cdot \alpha$ is spartan, then $\|\gamma\| = \|\alpha\|^2$. We have

$$\begin{aligned}
\mathbb{E}|S_n + k \cdot S_n| &\geq \mathbb{E}|S_n + k \cdot T_n| + o((\|\gamma\| - \epsilon)^n) \\
&= \mathbb{E}|S_n||T_n| + o(\|\gamma\|^n) + o((\|\gamma\| - \epsilon)^n) \\
&= (\mathbb{E}|S_n|)^2 + o(\|\gamma\|^n) \\
&= \mathbb{E}(|S_n|^2) - \mathrm{Var}|S_n| + o(\|\gamma\|^n) \\
&= \mathbb{E}(|S_n|^2) + o(\|\gamma\|^n),
\end{aligned}$$

where the first line follows from Theorems 34 and 36 (as in the proof of Theorem 4), the second line follows from Lemma 31, and the last line is from Lemma 32. The conclusion follows, since the random variable $|S_n|^2 - |S_n + k \cdot S_n|$ is always nonnegative. □

Corollary 39. *Let α be a fractional set with $\|\alpha\| > 1$, and let $\gamma := \alpha + \alpha$. For $n \geq 1$, let S_n be drawn from α^n. Then, if γ is strictly spartan (i.e., $\sum_{n\in\mathrm{supp}(\gamma)} \gamma(n) \log \gamma(n) < 0$), then*

$$\mathbb{E}\left(\tfrac{1}{2}|S_n|^2 - |S_n + S_n|\right) = o(\mathbb{E}|S_n|^2).$$

Proof. If $\alpha + \alpha$ is spartan, then $\|\gamma\| = \|\alpha\|^2$. We have

$$\begin{aligned}
\mathbb{E}|S_n + S_n| &\geq \tfrac{1}{2}\mathbb{E}|S_n + T_n| + o(\|\gamma\|^n) \\
&= \tfrac{1}{2}\mathbb{E}|S_n||T_n| + o(\|\gamma\|^n) \\
&= \tfrac{1}{2}(\mathbb{E}|S_n|)^2 + o(\|\gamma\|^n) \\
&= \tfrac{1}{2}\mathbb{E}(|S_n|^2) - \tfrac{1}{2}\mathrm{Var}|S_n| + o(\|\gamma\|^n) \\
&= \tfrac{1}{2}\mathbb{E}(|S_n|^2) + o(\|\gamma\|^n),
\end{aligned}$$

where the first line follows from Theorems 35 and 36 (as in the proof of Theorem 4), the second line follows from Lemma 31, and the last line is from Lemma 32. The conclusion follows, since the random variable $\frac{1}{2}|S_n|^2 + \frac{1}{2}|S_n| - |S_n + S_n|$ is always nonnegative, and $\mathbb{E}|S_n| = \|\alpha\|^n = o(\|\gamma\|^n)$. □

Theorem 5 follows from the last two corollaries, Theorem 4, and Markov's inequality, noting that the random variables $|S_n|^2 - |S_n + k \cdot S_n|$ (for $k \neq 1$) and $\frac{1}{2}|S_n|^2 + \frac{1}{2}|S_n| - |S_n + S_n|$ are always nonnegative.

4.4 Ruzsa's method, and Hennecart, Robert and Yudin's construction

In [15], Ruzsa constructs sets by taking a finite set S, and a fixed probability $0 < q < 1$, and selecting subsets of $\mathbb{Z}^n$ by taking each element of S^n independently with probability q^n. In our terminology, this is the same as drawing from α^n, where α is the fractional set $q\mathbb{1}_S$.

Let us suppose that $|S| = M$ and $|S + k \cdot S| = N$, and write

$$S + k \cdot S = \{x_1, \ldots, x_N\}.$$

For $1 \leq i \leq N$, write λ_i for the number of ordered pairs $(s_1, s_2) \in S^2$ such that $x_i = s_1 + ks_2$. We say that λ_i is the *multiplicity* of x_i, and that the multiset $\{\lambda_1, \lambda_2, \ldots, \lambda_N\}$ is the *multiplicity spectrum* of the fractional dilate $S + k \cdot S$. Note that $\sum_{i=1}^N \lambda_i = M^2$. With these definitions, we have

$$(\alpha + k \cdot \alpha)(x) = \begin{cases} 0 & \text{if } x \notin S + k \cdot S, \\ q^2\lambda_i & \text{if } x = x_i. \end{cases}$$

Theorem 20 now specializes to the following.

Theorem 40. *For a finite set $S \subseteq \mathbb{Z}$, and a fixed probability $0 < q < 1$, let $\alpha = q\mathbb{1}_S$. Then, for a nonzero integer k, with M, N, λ_i defined as above, and with $\gamma := \alpha + k \cdot \alpha$, we have*

$$\|\gamma\| = \|\alpha + k \cdot \alpha\| = \begin{cases} (qM)^2 & \text{if } q^2 \leq \prod_i \lambda_i^{-\lambda_i/M^2} \quad (\gamma \text{ is spartan}) \\ N & \text{if } q^2 \geq \prod_i \lambda_i^{-1/N} \quad (\gamma \text{ is opulent}) \\ q^{2p}\sum_i \lambda_i^p & \text{if } q^2 = \prod_i \lambda_i^{-\Lambda(p)} \quad (\gamma \text{ is } p\text{−comfortable}), \end{cases}$$

where

$$\Lambda(p) = \frac{\lambda_i^p}{\sum_1^N \lambda_j^p}.$$

Before proceeding to the Hennecart, Robert and Yudin construction, we first give an easier example, using the set $\{0, 1, 3, 7\}$.

Claim 41. *For all $\epsilon > 0$, there exists a set S with $|S - S| > |S|^{2-\epsilon}$ and $|S + S| < |S|^{1.8983+\epsilon}$.*

Using the proof of Corollary 7 from the introduction, this will follow from the next claim (just as Corollary 7 follows from Theorem 6).

Claim 42. *There exists a fractional set α for which $\|\alpha\| > 1$, $\alpha - \alpha$ is strictly spartan (so that $\|\alpha - \alpha\| = \|\alpha\|^2$), and $\|\alpha + \alpha\| \leq \|\alpha\|^{1.8983}$.*

Proof. Let $S = \{0, 1, 3, 7\}$, and let $\frac{1}{4} < q < 1$ be fixed. Then $S + S = \{0, 2, 6, 14, 1, 3, 7, 4, 8, 10\}$, with corresponding multiplicities $\{1, 1, 1, 1, 2, 2, 2, 2, 2, 2\}$. From Theorem 40, we have

$$\|\alpha + \alpha\| = \begin{cases} (4q)^2 & \text{if } q \leq 2^{-\frac{3}{8}}, \\ 10 & \text{if } q \geq 2^{-\frac{3}{10}}, \\ 2q^{2p}(2 + 3 \cdot 2^p) & \text{if } q = 2^{-\frac{3 \cdot 2^p}{2(2+3\cdot 2^p)}}. \end{cases}$$

On the other hand, we have that $S - S = \{-7, -6, -4, -3, -2, -1, 0, 1, 2, 3, 4, 6, 7\}$, with corresponding multiplicities $\{1, 1, 1, 1, 1, 1, 4, 1, 1, 1, 1, 1, 1\}$, so that

$$\|\alpha - \alpha\| = \begin{cases} (4q)^2 & \text{if } q \leq 2^{-\frac{1}{4}}, \\ 13 & \text{if } q \geq 2^{-\frac{1}{13}}, \\ q^{2p}(12 + 4^p) & \text{if } q = 2^{-\frac{4^p}{12+4^p}}. \end{cases}$$

Note that

$$\tfrac{1}{4} < 2^{-\frac{3}{10}} < 2^{-\frac{1}{4}},$$

so that if we let q be just slightly less than $2^{-\frac{1}{4}}$, $\alpha - \alpha$ will be strictly spartan, and also

$$\|\alpha\| = 4q = 2^{\frac{7}{4}} - \epsilon, \qquad \|\alpha + \alpha\| = 10, \qquad \|\alpha - \alpha\| = (4q)^2 = \left(2^{\frac{7}{4}} - \epsilon\right)^2,$$

so that

$$\|\alpha + \alpha\| < \|\alpha\|^{\frac{4\log 10}{7\log 2} + \epsilon'} < \|\alpha\|^{1.8983},$$

as required. □

Hennecart, Robert and Yudin [3] constructed sets $A_{k,d} \in \mathbb{Z}^{d+1}$ for which $|A_{k,d} - A_{k,d}|$ is much larger than $|A_{k,d} + A_{k,d}|$. Their construction is

$$A_{k,d} = \{(x_1, \ldots, x_{d+1}) : x_1, \ldots, x_{d+1} \geq 0,\ x_1 + \cdots + x_{d+1} = k\}.$$

A standard textbook argument shows that $|A_{k,d}| = \binom{k+d}{d}$. It turns out that the multiplicity spectrum for $A_{k,d} - A_{k,d}$ is particularly easy to describe.

Theorem 43. *The multiplicity spectrum for $A_{k,d} - A_{k,d}$ consists of*

- *one copy of $\binom{k+d}{d}$*
- *$\sum_{i=1}^{\min(t,d)} \binom{d+1}{i}\binom{t-1}{i-1}\binom{t+d-i}{d-i}$ copies of $\binom{k+d-t}{d}$, for $1 \leq t \leq k$.*

Proof. Clearly, the multiplicity of $0 \in A_{k,d} - A_{k,d}$ is $|A_{k,d}| = \binom{k+d}{d}$.

For the other multiplicities, fix $0 \neq w = (w_1, \ldots, w_{d+1}) \in A_{k,d} - A_{k,d}$. Then $w = x - y$, where $x = (x_1, \ldots, x_{d+1})$ and $y = (y_1, \ldots, y_{d+1})$ are nonnegative vectors summing to k. It follows that $\sum_i w_i = 0$.

Next, write w^+ for the vector containing only the positive coordinates of w, so that

$$w^+ = (\max\{w_1, 0\}, \ldots, \max\{w_{d+1}, 0\}),$$

and write w^- for the corresponding vector with the negative coordinates. Then, for all i, we have $\max\{w_i, 0\} \leq x_i$, so that $1 \leq \sum_i (w^+)_i := t \leq k$. If w is any integer vector with $\sum_i w_i = 0$, and x and y are nonnegative vectors such that $w = x - y$, then the vector $z = x - w^+$ is a nonnegative vector with $\sum_i z_i = k - t$. Conversely, for any such z, the vectors $x = w^+ + z$ and $y = z - w^-$ are nonnegative vectors, both summing to k, and satisfying $w = x - y$. Consequently, the multiplicity of w in $A_{k,d} - A_{k,d}$ is just the number of choices for z, i.e., the number of nonnegative $(d+1)$-dimensional vectors summing to $k - t$. This number is $\binom{k-t+d}{d}$.

To calculate the number of integer vectors of length $d+1$, summing to 0, whose positive elements sum to $t > 0$, we classify such vectors according to the number i of their positive elements. This number must be in the range $1 \leq i \leq \min\{t, d\}$. The number of choices for the locations of the i positive elements is $\binom{d+1}{i}$. The number of choices for the i positive numbers summing to t equals the number of choices for i nonnegative numbers summing to $t - i$, which is $\binom{t-1}{i-1}$. Finally, the number of choices for the $d + 1 - i$ nonpositive numbers summing to $-t$ is $\binom{t+d-i}{d-i}$. □

This allows us to prove Theorem 6, namely, that there exists a fractional set α for which $\|\alpha\| > 1$, $\alpha - \alpha$ is strictly spartan, and with $\|\alpha + \alpha\| \leq \|\alpha\|^{1.7354}$.

Proof of Theorem 6. Our α will be $q\mathbb{1}_{A_{k,d}}$, where k and d will be chosen later, and where $0 < q < 1$ is a probability that will be chosen in terms of k and d. For $0 \le t \le k$, let $\lambda_t = \binom{k+d-t}{d}$. Let $\mu_0 = 1$, and, for $t > 0$, let

$$\mu_t = \sum_{i=1}^{t} \binom{d+1}{i}\binom{t-1}{i-1}\binom{t+d-i}{d-i}.$$

Now, from Theorem 43, we know that the nonzero values of $\alpha - \alpha$ consist of μ_t copies of $q^2\lambda_t$, for each $0 \le t \le k$. Write $A = A_{k,d} - A_{k,d}$. Then, from Theorem 20, $\alpha - \alpha$ is strictly spartan when

$$\sum_{x \in A} (\alpha - \alpha)(x) \log_2 (\alpha - \alpha)(x) < 0,$$

or

$$\sum_{t=0}^{k} q^2 \lambda_t \mu_t \log_2 (q^2 \lambda_t) < 0.$$

Rearranging, we need

$$\sum_{t=0}^{k} 2\lambda_t \mu_t \log_2 q < -\sum_{t=0}^{k} \lambda_t \mu_t \log_2 \lambda_t.$$

In summary, for $\alpha - \alpha$ to be strictly spartan, we need $q < 2^{-f(k,d)}$, where

$$f(k,d) = \frac{\sum_{t=0}^{k} \lambda_t \mu_t \log_2(\lambda_t)}{2\sum_{t=0}^{k} \lambda_t \mu_t}.$$

We need to show that we can choose q so that, in addition, $\|\alpha\| = q\binom{k+d}{d} > 1$. For this, we need an upper bound on $f(k,d)$. But $2f(k,d)$ is just a weighted average of the $k+1$ numbers $\log_2 \lambda_t$. Therefore

$$2f(k,d) = \frac{\sum_{t=0}^{k} \mu_t \lambda_t \log_2 \lambda_t}{\sum_{t=0}^{k} \mu_t \lambda_t} \le \max_t \log_2 \lambda_t = \log_2 \lambda_0 = \log_2 \binom{k+d}{d}.$$

Consequently, we have $2^{-f(k,d)} \ge \binom{k+d}{d}^{-1/2}$, so that if we choose q satisfying

$$\binom{k+d}{d}^{-1} < q < \binom{k+d}{d}^{-1/2} \le 2^{-f(k,d)} =: p(k,d)$$

then $\alpha - \alpha$ will be strictly spartan, and we will also have $\|\alpha\| > 1$.

Finally, we turn to $\alpha + \alpha$. We have

$$A_{k,d} + A_{k,d} = \{(x_1, \ldots, x_{d+1}) : x_1, \ldots, x_{d+1} \ge 0,\ x_1 + \cdots + x_{d+1} = 2k\},$$

so $\|\alpha + \alpha\| \le |A_{k,d} + A_{k,d}| = \binom{2k+d}{d}$. Note that we believe $\alpha + \alpha$ is opulent, so we have equality here, but we do not need that for this proof. If we let

$$\beta = \beta(k,d) = \frac{\log \binom{2k+d}{d}}{\log(p(k,d)|A_{k,d}|)},$$

it follows that $\|\alpha + \alpha\| \le \|\alpha\|^\beta$. Computer calculations show that the function $\beta(k,d)$ seems to have a global minimum of $\beta = 1.735383\ldots$ at $d = 14929$ and $k = 987$. □

4.5 MSTD sets and the region $F_{1,-1}$

In this subsection, we collect all the results displayed in Figure 1.

For a finite set $A \subset Z$, with sumset $A+A$ and difference set $A-A$, write

$$|A+A| = |A|^x \quad \text{and} \quad |A-A| = |A|^y.$$

In 1973, Freiman and Pigarev [11] proved

$$|A+A|^{3/4} \le |A-A| \le |A+A|^{4/3} \quad \text{or} \quad \tfrac{3}{4}x \le y \le \tfrac{4}{3}x. \tag{1}$$

Noting that $1 \le x, y \le 2$, this is weaker than the best known bounds, proved by Ruzsa [14, 15]:

$$\left(\frac{|A+A|}{|A|}\right)^{\frac{1}{2}} \le \frac{|A-A|}{|A|} \le \left(\frac{|A+A|}{|A|}\right)^2 \quad \text{or} \quad y \le 2x-1 \quad \text{and} \quad x \le 2y-1. \tag{2}$$

The upper bound comes from taking $B = C = -A$ in Ruzsa's triangle inequality:

$$|A||B-C| \le |A-B||A-C|,$$

and the lower bound comes from taking $B = C = -A$ in Corollary 7.3.6 of [16]:

$$|A||B+C| \le |A+B||A+C|.$$

Together, these results show that the shaded regions in Figure 1 are all infeasible.

Next we turn to MSTD sets; these are sets A satisfying $|A+A| > |A-A|$. The terminology is due to Nathanson, and stands for "more sums than differences". According to Nathanson (see Footnote 1 of [8]), Conway found the first MSTD set in 1967:

$$A = \{0, 2, 3, 4, 7, 11, 12, 14\}.$$

This is the smallest MSTD set, it's unique among sets of size 8 up to scaling and shifting, and it satisfies

$$|A| = 8 \qquad |A-A| = 25 \qquad |A+A| = 26.$$

Various families of MSTD sets are known. The record-breaker, in terms of minimizing both $\frac{y}{x}$ and $\frac{y-1}{x-1}$ (in our notation), is due to Penman and Wells [9]. They construct a family of sets A_t, for $t \ge 1$, with

$$|A_t| = 5t+17 \qquad |A_t - A_t| = 26t+61 \qquad |A_t + A_t| = 32t+63.$$

Both these constructions are also illustrated in Figure 1, with the latter one plotted for real $t \ge 1$.

Finally, we discuss the construction of Hennecart, Robert and Yudin [3]. As already mentioned, their construction is

$$A_{k,d} = \{(x_1, \dots, x_{d+1}) : x_1, \dots, x_{d+1} \ge 0,\ x_1 + \cdots + x_{d+1} = k\},$$

and they show that

$$|A| = \binom{k+d}{d} \qquad |A+A| = \binom{2k+d}{d} \qquad |A-A| = \sum_{t=0}^{\min(d,k)} \binom{d}{t}^2 \binom{k+d-t}{d}.$$

Taking $k = ad$, for $a > 0$, yields the curve shown in Figure 1. Hennecart, Robert and Yudin choose $k = d/2$, so that

$$|A| = \binom{\frac{3d}{2}}{d} \qquad |A+A| = \binom{2d}{d} \qquad |A-A| \geq \max_{0 \leq t \leq \frac{d}{2}} \binom{d}{t}^2 \binom{\frac{3d}{2}-t}{d}.$$

This results in the asymptotics

$$\frac{\log|A+A|}{\log|A|} \to \frac{4\log 2}{3\log 3 - 2\log 2} \approx 1.4520$$

and

$$\frac{\log|A-A|}{\log|A|} \to \frac{4\log(1+\sqrt{2})}{3\log 3 - 2\log 2} \approx 1.8463,$$

leading to the point $(1.4520, 18463)$ plotted in Figure 1.

5 Open Questions

We introduced the concept of a fractional dilate as a more general version of Ruzsa's method from [15]. Ruzsa's method is the specialisation where a fractional dilate has all nonzero values equal. However, we in fact only used this same specialisation to prove Theorem 6. We believe that using a more general fractional dilate supported on the Hennecart, Robert and Yudin sets $A_{k,d}$ could give a better bound than 1.7354. In particular, the best bound one can get from a Ruzsa-style dilate on $A_{2,d}$ is that for $d = 23$, which with a value of

$$q = 5^{-\frac{1}{300}} 2^{-\frac{46}{625}} 12^{-\frac{1129}{15000}}$$

yields a bound of 1.7897. However, if one takes a fractional dilate on $A_{2,22}$ with a value of approximately 0.9951 on the elements of the form $2e_i$, and approximately 0.7617 on the elements of the form $e_i + e_j$, one can instead get a bound of 1.7889.

Our proof of Theorem 6 relies on the fact that if S_n is drawn from α^n, and $\alpha - \alpha$ is spartan, then the size of $S_n - S_n$ is close to its expected value. We believe that this holds without the requirement of spartaneity.

Conjecture 44. *If α is a fractional dilate with $\|\alpha\| > 1$, k is a positive integer, and A_n is drawn from α^n, then*

$$\lim_{n\to\infty} \frac{\log|A_n + k \cdot A_n|}{n} = \log\|\alpha + k \cdot \alpha\|.$$

This would directly imply that various results for the sizes of sums and differences of sets would also hold for fractional dilates. For example, Ruzsa's Triangle Inequality would imply that

$$\|\alpha\|\|\beta - \gamma\| \leq \|\alpha - \beta\|\|\alpha - \gamma\|$$

for fractional dilates α, β, γ.

A weaker conjecture is that the feasible regions for dilates coincide with the feasible regions for fractional dilates.

Conjecture 45. *For any fractional dilate α, any positive integer N, and any $\epsilon > 0$, there exists a finite subset S of the integers such that, for all $|k| \leq N$,*

$$\left| \frac{\log\|\alpha + k \cdot \alpha\|}{\log\|\alpha\|} - \frac{\log|S + k \cdot S|}{\log|S|} \right| < \epsilon.$$

We also ask whether the fractional dilate versions of the open questions from Section 3 are true. For the reader's convenience, we write out these questions in full. Note that Theorem 20 gives a useful way of computing $\|\alpha+\alpha\|$ and $\|\alpha+2\cdot\alpha\|$.

Question 46. *Suppose that $\alpha:\mathbb{Z}\to[0,1]$ is a function with finite support. We write*

$$\|\alpha\| = \sum_i \alpha(i)$$

$$\|\alpha+\alpha\| = \inf_{0\le p\le 1} \sum_i \left(\sum_{j+k=i} \alpha(j)\alpha(k)\right)^p$$

$$\|\alpha+2\cdot\alpha\| = \inf_{0\le p\le 1} \sum_i \left(\sum_{j+2k=i} \alpha(j)\alpha(k)\right)^p.$$

Are each of the following statements true for all such α?

1. $\|\alpha\|\|\alpha+2\cdot\alpha\| \le \|\alpha+\alpha\|^2$
2. $\|\alpha+2\cdot\alpha\| \le \log_3 4\|\alpha+\alpha\|$
3. $\|\alpha+2\cdot\alpha\| \ge \|\alpha+\alpha\|$

Since a subset of the integers is just a fractional dilate of its characteristic function, positive answers to these questions would imply positive answers to the corresponding questions in Section 3. If either Conjecture 44 or Conjecture 45 is true, the questions in the two sections are equivalent. A negative answer to any of these questions would either lead to an extension of the feasible region $F_{1,2}$, or to a better understanding of the above conjectures.

The biggest open question we leave is whether fractional dilates can find a use elsewhere.

References

[1] Lars Becker, Patta Ivanisvili, Dmitry Krachun, and José Madrid, *Discrete Brunn-Minkowski inequality for subsets of the cube*, (2024).

[2] Boris Bukh, *Sums of dilates*, Combin. Probab. Comput. **17** (2008), no. 5, 627–639.

[3] G. Robert F. Hennecart and A. Yudin, *On the number of sums and differences*, Asterisque **258** (1999), 173–178.

[4] Charles M. Goldie and Richard G. E. Pinch, *Communication theory*, London Mathematical Society Student Texts, vol. 20, Cambridge University Press, Cambridge, 1991.

[5] Ben Green, *Waring's problem with restricted digits*, (2023).

[6] Brandon Hanson and Giorgis Petridis, *A question of Bukh on sums of dilates*, Discrete Anal. (2021), Paper No. 13, 21.

[7] Geoffrey Iyer, Oleg Lazarev, Steven J. Miller, and Liyang Zhang, *Finding and counting MSTD sets*, Combinatorial and additive number theory—CANT 2011 and 2012, Springer Proc. Math. Stat., vol. 101, Springer, New York, 2014, pp. 79–98.

[8] Melvyn B. Nathanson, *Problems in additive number theory. I*, Additive combinatorics, CRM Proc. Lecture Notes, vol. 43, Amer. Math. Soc., Providence, RI, 2007, pp. 263–270.

[9] David Penman and Matthew Wells, *On sets with more restricted sums than differences*, Integers **13** (2013), Paper No. A57, 24.

[10] Giorgis Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica **32** (2012), no. 6, 721–733.

[11] V. P. Pigarev and G. A. Freĭman, *The relation between the invariants R and T*, Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (Russian), Kalinin. Gosudarstv. Univ., Moscow, 1973, pp. 172–174.

[12] Helmut Plünnecke, *Eine zahlentheoretische Anwendung der Graphentheorie*, J. Reine Angew. Math. **243** (1970), 171–183.

[13] C. A. Rogers and G. C. Shephard, *The difference body of a convex body*, Arch. Math. (Basel) **8** (1957), 220–233.

[14] I. Z. Ruzsa, *On the cardinality of $A + A$ and $A - A$*, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. II, Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Amsterdam-New York, 1978, pp. 933–938.

[15] ———, *On the number of sums and differences*, Acta Math. Hungar. **59** (1992), no. 3-4, 439–447.

[16] Yufei Zhao, *Graph theory and additive combinatorics—exploring structure and randomness*, Cambridge University Press, Cambridge, 2023.