Sums, Differences and Dilates

Jonathan Cutler Luke Pebody Amites Sarkar

May 15, 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 [5] 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 [12], 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 [2] 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 [13].

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 [12] 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 [2] 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 [10]. 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 [6] 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

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

for an appropriate choice of integers λ_i.

Another line of investigation was opened by Bukh [1] in 2008. Given a set of integers A and an integer k, define the *dilate set* $A + k \cdot A$ by

$$A + k \cdot A = \{a_1 + ka_2 : a_1, a_2 \in A\}.$$

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 not the same set as $A + A + A$, 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 $\lambda_1, \ldots, \lambda_k$), 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* [9] (see also [7]) 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 [5], 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 [8] and Ruzsa [11] in the 1970s (and indeed Conway in the 1960s).

Our starting point is a 1992 paper of Ruzsa [12]. 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 [12], 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.

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 $(i_1, i_2, \dots, i_n)$ is selected is $\alpha(i_1)\alpha(i_2)\dots\alpha(i_n)$. 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.

Theorem 4. *Let α be a fractional set with $\|\alpha\| \geq 1$, 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

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

Theorem 5. *Let α be a fractional set with $\|\alpha\| \geq 1$, and suppose $S_n \subseteq \mathbb{Z}^n$ is drawn from α^n. If $\alpha + k \cdot \alpha$ is spartan, so that*

$$\|\alpha + k \cdot \alpha\| = \|\alpha\|^2$$

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 6, we apply these theorems to a construction of Hennecart, Robert and Yudin [2], 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 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 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

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

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

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

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

In the other direction, it follows from results of Freiman and Pigarev [8] and Ruzsa [11] that $(x, 2)$ is not attainable for any $x < 3/2$. All these results are illustrated in Figure 1.

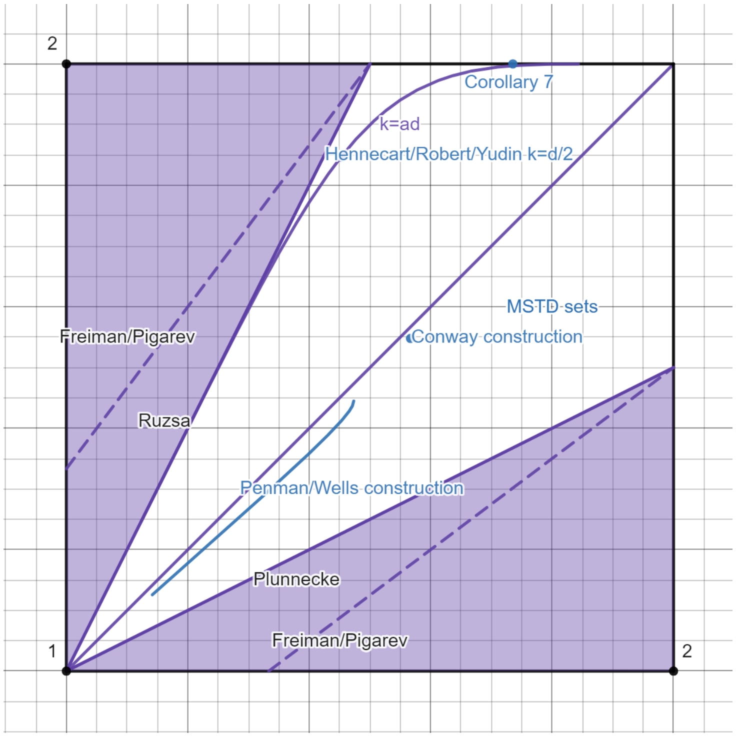

Figure 1: The feasible region $F_{1,-1}$

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 $|A| \le |A + k \cdot A| \le |A|^2$ 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 $D = \{(x,x) : 1 \le x \le 2\}$.*

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 $A := A_N = \{1, 2, \ldots, N\}$ 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 $B = \{1, b, b^2, \ldots, b^N\}$. 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 Construction for $F_{1,2}$

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

If set A is the union of sets $A_1, \ldots, A_n$, then it is clear that

$$\begin{array}{rcccl} \max_{1 \leq i \leq n} |A_i| & \leq & |A| & \leq & \sum_{1 \leq i \leq n} |A_i| \\ \max_{1 \leq i \leq j \leq n} |A_i + A_j| & \leq & |A + A| & \leq & \sum_{1 \leq i \leq j \leq n} |A_i + A_j|, \quad \text{and} \\ \max_{1 \leq i,j \leq n} |A_i + 2 \cdot A_j| & \leq & |A + 2 \cdot A| & \leq & \sum_{1 \leq i,j \leq n} |A_i + 2 \cdot A_j|. \end{array}$$

Now, we are ready to describe the hypercube + interval construction. To this end, let

$$H_n = \left\{ \sum_{i=0}^{n-1} a_i 4^i : \forall i,\ a_i \in \{0, 1\} \right\} \quad \text{and} \quad I_k = \left[0, \frac{4^k - 1}{3} \right) \cap \mathbb{Z}.$$

So, H_n denotes the set of all natural numbers with a base 4 representation being of length at most n and containing only 0s and 1s, making up the hypercube portion of our construction. Of course, I_k is simply an interval of integers. We begin by giving bounds on the sizes of various sumsets related to H_n and I_k.

Theorem 9. *For $n \geq k > \frac{n+1}{2}$, the sizes of various sets, sumsets, and dilates are as follows:*

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

Proof. We leave to the interested reader the job of calculating the sizes of $|I_k + I_k|$, $|H_n + 2 \cdot I_k|$, $|I_k + 2 \cdot H_n|$, and $|I_k + 2 \cdot I_k|$. [1]

Since there are two choices for each a_i where $0 \leq i \leq n-1$, we have that $|H_n| = 2^n$. Also, since $(4^k-1)/3$ is an integer, we know that $|I_k| = (4^k-1)/3$. Further, since $k \geq \frac{n+2}{2}$, we have $4^k \geq 2^{n+2} > 1 + 3 \times 2^n$ and so $(4^k-1)/3 > 2^n$.

Note that $H_n + H_n = \left\{\sum_{i=0}^{n-1} a_i 4^i : \forall i,\ a_i \in \{0,1,2\}\right\}$. In other words, elements of $H_n + H_n$ are natural numbers whose base 4 representation is of length at most n and contains only 0s, 1s, and 2s. Thus, $|H_n + H_n| = 3^n$. Similarly $H_n + 2 \cdot H_n$ are natural numbers whose base 4 representation is of length at most n and contains only 0s, 1s, 2s and 3s, which is $[0, 4^n)$. Further, since the maximum element of H_n is at least as large as the maximum element of I_k it is clear that all of $H_n + 2 \cdot I_k$, $I_k + 2 \cdot H_n$ and $I_k + 2 \cdot I_k$ are subsets of $[0, 4^n)$ and therefore of size at most 4^n.

For $H_n + I_k$, note that H_n is the sum of the sets $\{0,1\}, \{0,4\}, \{0,4^2\}, \ldots, \{0, 4^{n-1}\}$. Now if $p \geq q$ are positive integers, then the sum of the integer interval $[0,p)$ with the set $\{0,q\}$ is the integer interval $[0, p+q)$. Thus,

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

Further 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, so $H_n + I_k$ consists of 2^{n-k} intervals of length $2\left(\frac{4^k-1}{3}\right)$ and contains $I_k + I_k$. □

Let $A_{n,k} = H_n \cup I_k$. Then, using Theorem 9, we can show the following.

Corollary 10. *Let α be any real number in the open region $(\frac{1}{2}, 1)$. Then as $n \to \infty$,*

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

[1] They are $2\frac{4^k-1}{3} - 1$, $2^{n+1-k}(2 \times 4^{k-1} - 1)$ twice, and $4^k - 3$ respectively.

Proof. Note that if k is a fixed constant and $a_{n,i}$ for $1 \le i \le k$ and $1 \le n$ are positive integers and c_i for $1 \le i \le k$ are real numbers such that $\lim_{n\to\infty} \log a_{n,i}/n = c_i$ for all i, and integers b_n satisfy that $\max_i a_{n,k} \le b_n \le \sum_i a_{n,k}$, then

$$\lim_{n\to\infty} \frac{\log b_n}{n} \to \max\{c_1, \ldots, c_n\}.$$

Let us write $k = \lfloor \alpha n \rfloor$. For the first part of the Corollary, we note that by Theorem 9, we have

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

Since we know that $I_k \subseteq A_{n,k}$ and $|A_{n,k}| \le |H_n| + |I_k|$, it follows that $\lim_{n\to\infty} \log|A_{n,k}|/n = \alpha \log 4$.

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

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

and

$$\begin{aligned}\lim_{n\to\infty} \frac{\log|H_n + I_k|}{n} &= (1-\alpha)\log 2 + \alpha \log 4 \\ &= \frac{1+\alpha}{2}\log 4 > \lim_{n\to\infty} \frac{\log|I_k + I_k|}{n}.\end{aligned}$$

Since we know that $H_n + H_n$ and $H_n + I_k$ are both subsets of $A_{n,k} + A_{n,k}$ and that $|A_{n,k} + A_{n,k}| \le |H_n + H_n| + |H_n + I_k| + |I_k + I_k|$, it follows that $\lim_{n\to\infty} \log|A_{n,k} + A_{n,k}|/n = \max(\log 3, \frac{1+\alpha}{2}\log 4)$.

Finally, for the dilates, we have

$$\begin{aligned}\lim_{n\to\infty} \frac{\log|H_n + 2\cdot H_n|}{n} &= \log 4 \\ &> \max\left\{\lim_{n\to\infty} \frac{\log|H_n + 2\cdot I_k|}{n}, \lim_{n\to\infty} \frac{\log|I_k + 2\cdot H_n|}{n}, \lim_{n\to\infty} \frac{\log|I_k + 2\cdot I_k|}{n}.\right\}\end{aligned}$$

Thus $\log|A_{n,k} + 2\cdot A_{n,k}|/n \to \log 4$. □

The upper limit in the second interval above is $\log 3$ when α is below $2\frac{\log 3}{\log 4} - 1$, and $\frac{1+\alpha}{2}\log 4$ above it. As mentioned above, this gives a partial converse to Theorem 2.

Corollary 11. *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. Let $\frac{1}{2} \le \alpha \le 2\frac{\log 3}{\log 4} - 1$. Then Corollary 10 shows that

$$\frac{\log|A_{n,\lfloor\alpha n\rfloor} + 2\cdot A_{n,\lfloor\alpha n\rfloor}| - \log|A_{n,\lfloor\alpha n\rfloor}|}{\log|A_{n,\lfloor\alpha n\rfloor} + A_{n,\lfloor\alpha n\rfloor}| - \log|A_{n,\lfloor\alpha n\rfloor}|} \to \frac{\log 4 - \alpha\log 4}{\frac{1+\alpha}{2}\log 4 - \alpha \log 4} = \frac{1-\alpha}{\frac{1-\alpha}{2}} = 2.$$

□

We now use Corollary 10 to show that we have feasible points in $F_{1,2}$. Let the function $f : [1,2] \to [1,2]$ be defined by

$$f(x) = \begin{cases} \frac{1}{2}(\beta+1) & \text{if } 1 \le x \le \frac{\log 4}{\log(9/4)}, \\ (\log_4 3)x & \text{if } \frac{\log 4}{\log(9/4)} \le x \le 2. \end{cases}$$

Corollary 12. *For all* $1 < \beta < 2$, $(f(\beta), \beta) \in F_{1,2}$.

Proof. Let $\alpha = 1/\beta$, 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 gives the existence of sets where

$$\begin{aligned} \log |A_{n,\lfloor \alpha n \rfloor}|/n &\to \alpha \log 4, \\ \log |A_{n,\lfloor \alpha n \rfloor} + A_{n,\lfloor \alpha n \rfloor}|/n &\to \alpha \log 4 f(\beta), \quad \text{and} \\ \log |A_{n,\lfloor \alpha n \rfloor} + 2 \cdot A_{n,\lfloor \alpha n \rfloor}|/n &\to \log 4 = \alpha \log 4\beta. \end{aligned}$$

So

$$\begin{aligned} \log |A_{n,\lfloor \alpha n \rfloor} + A_{n,\lfloor \alpha n \rfloor}|/ \log |A_{n,\lfloor \alpha n \rfloor}| &\to f(\beta) \quad \text{and} \\ \log |A_{n,\lfloor \alpha n \rfloor} + 2 \cdot A_{n,\lfloor \alpha n \rfloor}|/ \log |A_{n,\lfloor \alpha n \rfloor}| &\to \beta. \end{aligned}$$

□

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

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

Proof. Corollary 7.3.6 of [13], which is an easy conseqeunce of Plünnecke's inequality, states that for any three sets A, B, C,

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

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

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

□

So, we know that if $\log |A + 2 \cdot A|/ \log |A| \leq t$, then $\log |A + A|/ \log |A| \leq 2t - 1$. This means that anything below the line $y = 1 + x/2$ is not in the feasible region $F_{1,2}$.

Also, note that the two results of Hanson and Petridis (Theorems 2 and 3) give two upper bounds on $F_{1,2}$, namely the lines $y = 2.95x - 1.95$ and $y = 4t/3$. The first follows from the fact that if $|A + A| = |A|^t$, then by Theorem 2, we have $|A + 2 \cdot A| \leq |A|^{2.95t-1.95}$. The second follows similarly. We put all of these results together into Figure 2.

Corollary 12 shows that lines OD and DC are feasible, while Theorem 8 shows that the line OE is feasible and hence that the entire quadrilateral $ODCE$ is feasible.

For infeasibility, the two results of Hanson and Petridis (Theorems 2 and 3) show that nothing can be feasible to the left of the line OA and above the line AB respectively. Specifically, if $|A + A| = |A|^t$, Theorem 2 implies that $|A + 2 \cdot A| \leq |A|^{2.95t-1.95}$ and Theorem 3 implies that $|A + 2 \cdot A| \leq |A|^{4t/3}$.

We leave as open questions whether any of the sides of the quadrilateral $ODCE$ (other than CE, for which we have a proof but there is not enough space to give it here) are actually hard bounds on feasibility. Specifically, we ask the following:

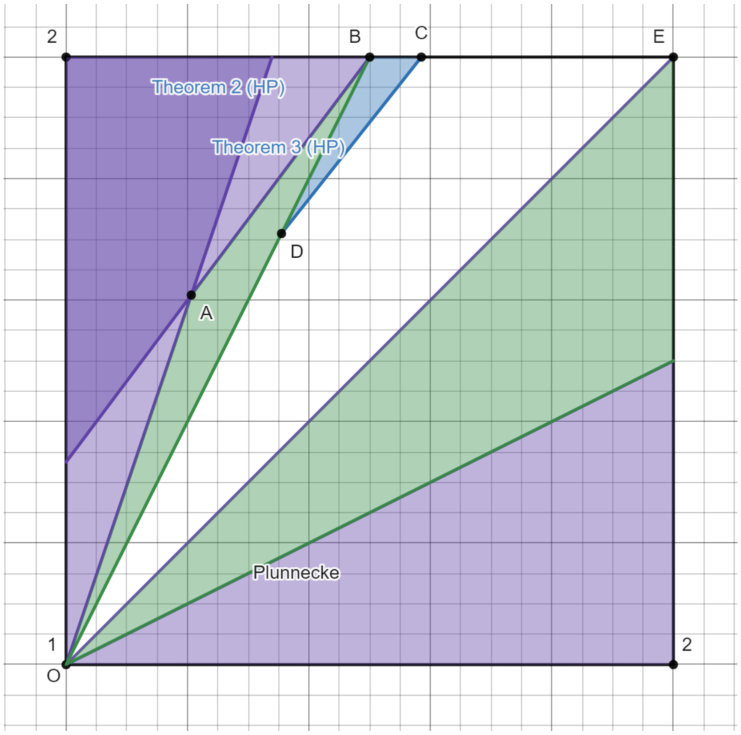

Figure 2: The feasible region $F_{1,2}$

Question 14. *Is it true that nothing to the left of the line ODB is in $F_{1,2}$. In other words, if $|A+A| = |A|^t$, is $|A+2\cdot A| \le |A|^{1+2t}$? In yet more other words, is it true that for all A, $|A||A+2\cdot A| \le |A+A||A+A|$.*

Question 15. *Is it true that nothing above the line DC is in $F_{1,2}$. In other words, is it true that $\frac{\log|A+2\cdot A|}{\log|A+A|} \le \frac{\log 4}{\log 3}$ for all sets A? In yet more other words, is it true for all n that if $|A+A| \le 3^n$, then $|A+2\cdot A| \le 4^n$?*

Question 16. *Is it true that nothing below the line OE is in $F_{1,2}$. In other words, are there no sets A with $|A+A| > |A+2\cdot A|$?*

We coin the term *MST2D sets* (or *more sums than 2-dilates sets*) for counterexamples to Question 16. One of the first places you might think to find such a set is a Sidon set (that is, a set for which $|A+A|$ is as large as it can be). 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 $|A+2\cdot A| > |A+A|$.*

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 i.i.d. drawn from any distribution on a finite set S, then $\Pr(X_1 = X_2) \ge 1/|S|$. Thus if A_1, A_2, A_3, A_4 are i.i.d. drawn from the uniform (or indeed any) distribution on A, then $|A+2\cdot A| \ge 1/\Pr(A_1 + 2\cdot A_2 = A_3 + 2\cdot A_4)$. Now since A is a Sidon set,

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

Thus $\Pr(A_1 + 2 \cdot A_2 = A_3 + 2 \cdot A_4) = \Pr(A_1 - A_3 = 2(A_4 - A_2)) = 1/n^2 + K/n^4$, 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 (as $0 \in A$ and $gcd(A) = 1$), so $A - A$ contains at least $2(n-1)$ odd elements, so $K \leq n^2 - 3n + 2$.

Thus

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

□

Similarly, one of the first things you might think to look for a counterexample to Question 15 is a "2-Sidon" set (i.e., one where $|A + 2 \cdot A|$ is as large as it can be). An easy way to construct such sets is a subset of the hypercube $\{0,1\}^n$. But it follows from Theorem 2.3 of [4] that such sets in fact satisfy the condition of Question 15.

Lemma 18. *[4] Suppose A and B are subsets of the hypercube $\{0,1\}^n$. Then*

$$|A + 2 \cdot B| = |A||B| \leq |A + B|^{\frac{\log 4}{\log 3}}.$$

This lemma has an interesting history, going back to the 1970s. Details are in Appendix B of [4].

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 19. *A fractional dilate γ with support $S = \mathrm{supp}(\gamma)$ is*

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

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 $\|\gamma\| = \inf_{0 \leq p \leq 1} f(p)$. 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

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

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

Suppose next that

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

Then we must have $f'(p) \geq 0$ 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 $y_1, \ldots, y_n$ summing to 1, the entropy function $H(y_1, \ldots, y_n)$ is defined to be

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

Gibbs' inequality (see for instance [3]) states that

$$H(y_1, \ldots, y_n) \leq -\sum y_i \log_2 z_i$$

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

Lemma 20. *Suppose γ is a fractional dilate with support $S = \{s_1, \ldots, s_n\}$. Then*

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

Proof. First we observe that, for real x and $0 \leq p \leq 1$, we have $\min\{0, x\} \leq px$, 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
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 19. 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.

Lemma 21. *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 22. *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 23. *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*

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

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. If $\gamma = \alpha + k \cdot \beta$ is strictly spartan, in the sense that*

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

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 23. 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 23, it is enough to prove the theorem for $k = 1$. In the rest of this subsection, we will make this simplification.

Theorem 25. *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 26. *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 27. *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 26 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

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

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 27 to calculate the asymptotic behaviour of the probability that a randomly chosen vector lies in $S_n + T_n$.

Corollary 28. *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 25,

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

so $\mathbb{E}(X_n)^{1/n} \to t$. Applying Lemma 27, 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 25, completes the proof of Theorem 23.

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 $\gamma = \alpha + \beta$. 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 20, 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 28 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 23 proved, we turn to Theorem 24.

Lemma 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 $\gamma = \alpha + \beta$. Suppose that γ is strictly spartan, in the sense that*

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

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 21 and 22. For the second part, for $v = (v_1,\ldots,v_n)\in\mathbb{Z}^n$, write

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

X_v is a sum of independent Bernoulli random variables, so Lemma 26 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 24 follows from Lemma 30 and Markov's inequality.

4.3 The rainbow connection

Let α be a fractional set and let p be a non-zero integer. Let $\gamma := \alpha + p \cdot \alpha$ denote the fractional dilate defined by $\gamma(n) = \sum_{i+pj=n} \alpha(i)\alpha(j)$. In this section we will show that if S_n is a random set drawn from α^n then $\lim_{n\to\infty}(\mathbb{E}|S_n + p \cdot S_n|)^{1/n}$ is $\max(\|\alpha\|, \|\gamma\|)$.

First let us deal with the easy case.

Lemma 31. *If* $\|\alpha\| \leq 1$ *then* $\lim_{n\to\infty}(\mathbb{E}|S_n + p \cdot S_n|)^{1/n} = \|\alpha\|$. *On the other hand, if* $\|\alpha\| > 1$, *then* $\|\gamma\| \geq \|\alpha\|$.

Proof. Clearly $\mathbb{E}|S_n + p \cdot S_n| \geq \mathbb{E}|S_n| = \|\alpha\|^n$. Further,

$$\mathbb{E}|S_n + p \cdot S_n| \leq \mathbb{E}|S_n|^2 = (\mathbb{E}|S_n|)^2 + \mathrm{Var}|S_n| \leq (\mathbb{E}|S_n|)^2 + \mathbb{E}|S_n| = \|\alpha\|^{2n} + \|\alpha\|^n.$$

Thus if $\|\alpha\| \leq 1$ then $\lim_{n\to\infty}(\mathbb{E}|S_n + p \cdot S_n|)^{1/n} = \|\alpha\|$.

If $\|\alpha\| > 1$, let S_n be drawn from α^n. Then $|S_n|$ can be written as the sum of independent Bernoulli random variables and $\lim_{n\to\infty}(\mathbb{E}|S_n|)^{1/n} = \|\alpha\| > 1$. Thus by Lemma 27, we have $\lim_{n\to\infty} \Pr(|S_n| > 0)^{1/n} = 1$. Let T_n be independently drawn from α^n. By Corollary 29, $\|\gamma\| = \lim_{n\to\infty}(\mathbb{E}|S_n + p \cdot T_n|)^{1/n}$, but $|S_n + p \cdot T_n| \geq |T_n|$ whenever S_n is non-empty, so $|S_n + p \cdot T_n| \geq |T_n|\mathbb{1}_{|S_n|>0}$. Since $|S_n|$ and $|T_n|$ are independent, it follows that $\mathbb{E}|S_n + p \cdot T_n| \geq \mathbb{E}|T_n| \Pr(|S_n| > 0)$, whence

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

□

In the $\|\alpha\| > 1$ case we will prove that $\lim_{n\to\infty}(\mathbb{E}|S_n + p \cdot S_n|)^{1/n} = \|\gamma\|$ by comparing the size of $S_n + p \cdot S_n$ with $S_n + p \cdot T_n$ where T_n is a random set drawn from α^n independently from S_n. Let us say that a vector $v \in \mathbb{Z}^n$ is *rainbow* if it has at least one copy of each coefficient from the support $\{x_1, \ldots, x_k\}$ of γ, and let R_n denote the set of rainbow vectors in $\mathbb{Z}^n$.

Theorem 32. *If* $p \neq 1$ *and* v *is a rainbow vector, then* $\Pr(v \in S_n + p \cdot S_n) = \Pr(v \in S_n + p \cdot T_n)$. *Hence* $\mathbb{E}|(S_n + p \cdot S_n) \cap R_n| = \mathbb{E}|(S_n + p \cdot T_n) \cap R_n|$.

Proof. There are a finite number of x such that $\Pr(x \in S_n, v - px \in S_n) > 0$. Let us denote the set of all such x by S.

We claim that there exist distinct a, b in the support of α such that $a + pb$ cannot be expressed in any other way as $a' + pb'$ where a' and b' are in the support of α. Indeed if $p < 0$, let a and b be the largest and smallest elements, respectively, of the support of α. If a' and b' are any elements of the support of α, then $a \geq a'$ and $b \leq b'$, so $a + pb \geq a' + pb'$ with equality only if $a = a'$ and $b = b'$. Similarly, if $p > 1$, we can take a and b to be the second-largest and largest elements, respectively, of the support of α. If a' and b' are any elements of the support of α with $a' + pb' = a + pb$ but with $a' \neq a$ and $b' \neq b$, it must follow that $b' < b$ (as b is the largest element), whence $b' \leq a$ and hence $a' + pb' \leq b + pa < b + pa + (p-1)(b-a) = a + kb$, forming a contradiction.

Now since v is a rainbow vector, it contains a coordinate equal to $a + kb$, say $v_i = a + kb$. Then it follows that for all $x \in S$, $x_i = a$ and $(v - px)_i = b$, and therefore for all $x \in S$, $v - px \notin S$ (as $a \neq b$). In particular, for each $x \in S$, it is the case that $x \neq v - px$ and so the events $x \in S_n$ and $v - px \in S_n$ are independent, and hence $\Pr(x \in S_n, v - px \in S_n) = \Pr(x \in S_n)\Pr(v - px \in S_n)$. Furthermore, since the sets $\{x, v - px\}$ for all $x \in S$ are disjoint, these events are all independent, so

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

Since $\mathbb{E}|(S_n + p \cdot S_n) \cap R_n|$ is the sum of $\Pr(v \in S_n + p \cdot S_n)$ over all rainbow v, the equality of expectations follows. □

This gives us a good bound on the size of $\mathbb{E}|S_n + p \cdot S_n|$ because it usually happens that all but exponentially few of the elements of $S_n + p \cdot T_n$ are rainbow.

Theorem 33. *There exists an $\epsilon > 0$ such that $\mathbb{E}|(S_n + p \cdot T_n) \setminus R_n| = o((\|\gamma\| - \epsilon)^n)$.*

Proof. Let $p \in [0, 1]$ be such that $\|\gamma\| = \sum_{z:\gamma(z)\neq 0} \gamma(z)^p$, and let $\alpha = \min\{\gamma(z) : \gamma(z) \neq 0\}$.

Let z be any value with $\gamma(z) \neq 0$. By a similar argument to Theorem 25, for all $0 \leq q \leq 1$, the expected number of elements of $S_n + p \cdot T_n$ with no coefficient equal to z is at most $(\sum_{w \neq z} \gamma(w)^q)^n$. In particular, taking $q = p$, it is at most $(\|\gamma\| - \alpha^p)^n$.

If there are N elements of the support of γ, we have $\mathbb{E}|(S_n + p \cdot T_n) \setminus R_n|$ is at most $N(\|\gamma\| - \alpha^p)^n$, which is $o((\|\gamma\| - \epsilon)^n$ for any $\epsilon < \alpha^p$. □

Corollary 34. *If $\|\alpha\| > 1$ and $p \neq 1$, then $\lim_{n\to\infty} \mathbb{E}|S_n + p \cdot S_n|^{1/n} = \|\alpha + p \cdot \alpha\|$. Furthermore, if $\alpha + p \cdot \alpha$ is spartan, $\mathbb{E}|S_n|^2 - |S_n + p \cdot S_n| = o(\mathbb{E}|S_n|^2)$.*

Proof. By Theorem 25, $\mathbb{E}|S_n + p \cdot S_n| \leq \|\alpha + p \cdot \alpha\|^n$. Further, by Theorem 32,

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

By Corollary 29, we have $\lim_{n\to\infty} \mathbb{E}|S_n + p \cdot T_n|^{1/n} \to \|\alpha + p \cdot \alpha\|$. By Theorem 33, there is an $\epsilon > 0$ such that $\mathbb{E}|(S_n + p \cdot T_n) \setminus R_n| = o((\|\alpha + p \cdot \alpha\| - \epsilon)^n)$. So, it follows that $\liminf_{n\to\infty} \mathbb{E}|S_n + p \cdot S_n|^{1/n} \geq \|\alpha + p \cdot \alpha\|$ and hence $\lim_{n\to\infty} \mathbb{E}|S_n + p \cdot S_n|^{1/n} = \|\alpha + p \cdot \alpha\|$.

If $\alpha + p \cdot \alpha$ is spartan, then $\mathbb{E}|S_n|^2 - |S_n + p \cdot S_n|$ can be expressed as:

$$\begin{aligned}\mathbb{E}|S_n|^2 - |S_n + p \cdot S_n| &= \mathbb{E}|S_n|^2 - (\mathbb{E}|S_n|)^2 && (2)\\ &+ (\mathbb{E}|S_n|)^2 - \mathbb{E}|S_n||T_n| && (3)\\ &+ \mathbb{E}|S_n||T_n| - |S_n + p \cdot T_n| && (4)\\ &+ \mathbb{E}|(S_n + p \cdot T_n) \setminus R_n| && (5)\\ &+ \mathbb{E}|(S_n + p \cdot T_n) \cap R_n| - \mathbb{E}|(S_n + p \cdot S_n) \cap R_n| && (6)\\ &- \mathbb{E}|(S_n + p \cdot S_n) \setminus R_n|. && (7)\end{aligned}$$

The first line is $\mathrm{Var}|S_n|$ which (since S_n is the sum of independent Bernoulli variables) is at most $\mathbb{E}|S_n| = o(\mathbb{E}|S_n|^2)$. The second is clearly 0. The third is $o(\mathbb{E}|S_n|^2)$ by Corollary **??**, the fourth and sixth by Theorem 33 and the fifth is zero by Theorem 32. □

For sets A and B of integers, we define $A +^{<} B = \{x + y : x \in A, y \in B, x < y\}$.

Theorem 35. *If v is a rainbow vector, the probabilities that $v \in S_n + S_n$ and $v \in S_n +^{<} T_n$ are the same and hence $\mathbb{E}|(S_n + S_n) \cap R_n| = \mathbb{E}|(S_n +^{<} T_n) \cap R_n|$.*

Proof. Similar to Theorem 32, the expectation follows directly from the probability. Also, since v is rainbow, $v/2$ is not in the support of α. There are a finite number of x such that $\Pr(x \in S_n, v - x \in S_n) > 0$. Let us denote the set of all such x by S.

Thus

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

□

Corollary 36. *If $\|\alpha\| > 1$, then $\lim_{n\to\infty} \mathbb{E}|S_n + S_n|^{1/n} = \|\alpha + \alpha\|$. Furthermore, if $\alpha + \alpha$ is spartan, $\mathbb{E}\left(\frac{|S_n|^2}{2} - |S_n + S_n|\right) = o(\mathbb{E}|S_n|^2)$*

Proof. By Theorem 25, $\mathbb{E}|S_n + S_n| \le \|\alpha + \alpha\|^n$. Further, by Theorem 35,

$$\begin{aligned}
\mathbb{E}|S_n + S_n| &\ge \mathbb{E}|(S_n + S_n) \cap R_n| \\
&= \mathbb{E}|(S_n +^{<} T_n) \cap R_n| \\
&= \mathbb{E}|S_n +^{<} T_n| - \mathbb{E}|(S_n +^{<} T_n) \setminus R_n|.
\end{aligned}$$

Now $S_n + T_n = (S_n +^{<} T_n) \cup (T_n +^{<} S_n)$ and these two sets have the same distribution, so $\mathbb{E}|S_n +^{<} T_n| \ge \frac{1}{2}\mathbb{E}|S_n + T_n|$. Thus by Corollary 29 and Theorem 33, $\lim_{n\to\infty} \mathbb{E}|S_n + S_n|^{1/n} = \|\alpha + \alpha\|$.

Furthermore, if $\alpha + \alpha$ is spartan, then

$$\begin{aligned}
\mathbb{E}|S_n + S_n| &= \mathbb{E}|(S_n + S_n) \cup R_n| + \mathbb{E}|(S_n + S_n) \setminus R_n| \\
&= \mathbb{E}|(S_n +^{<} T_n) \cup R_n| + o(\|\alpha\|^{2n}) \\
&= \mathbb{E}|(S_n +^{<} T_n)| + o(\|\alpha\|^{2n}) \\
&\ge \frac{1}{2}\mathbb{E}|S_n + T_n| + o(\|\alpha\|^{2n}) \\
&= \frac{1}{2}\mathbb{E}|S_n|\mathbb{E}|T_n| + o(\|\alpha\|^{2n}) \\
&= \frac{1}{2}\mathbb{E}|S_n|\mathbb{E}|S_n| + o(\|\alpha\|^{2n}) \\
&= \frac{1}{2}\mathbb{E}|S_n|^2 + \frac{1}{2}\mathrm{Var}|S_n| + o(\|\alpha\|^{2n}) = \frac{1}{2}\mathbb{E}|S_n|^2 + o(\|\alpha\|^{2n}).
\end{aligned}$$

Since clearly $|S_n + S_n| \le \frac{1}{2}(|S_n|^2 + |S_n|)$ it follows that $\mathbb{E}|S_n + S_n| \le \frac{1}{2}\mathbb{E}|S_n|^2 + o(\|\alpha\|^{2n})$, so we are done. □

4.4 Ruzsa's Method and Hennecart, Robert and Yudin's Construction

In [12], Ruzsa constructs sets by taking a fixed probability $0 < q < 1$ and a finite set S 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 dilate equal to $q\mathbb{1}_S$.

Let us suppose that there are M elements of S and N elements of $S + k \cdot S$. Let us label the elements of $S + k \cdot S$ as $\{x_1, \ldots, x_N\}$. For $1 \leq i \leq N$, let us write λ_i for the number of ways of writing x_i as $s_1 + ks_2$ where $s_1, s_2 \in S$. We say λ_i is the *multiplicity* of x_i and say the unordered set $\{\lambda_1, \lambda_2, \ldots, \lambda_N\}$ is the *multiplicity spectrum* of $S + k \cdot S$. Note that $\sum_{i=1}^N \lambda_i = M^2$. It is clear that

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

Then we can rewrite the results of Theorem 19 as

$$\|\alpha + k \cdot \alpha\| = \begin{cases} (qM)^2 & \text{if } q^2 < 1/\left(\prod_i \lambda_i\right)^\Lambda, \\ N & \text{if } q^2 > 1/\prod_i \lambda_i^{1/N}, \\ q^{2p} \sum_i \lambda_i^p & \text{if } q^2 = 1/\left(\prod_i \lambda_i\right)^\Lambda, \end{cases}$$

where $\Lambda = \frac{\lambda_i^p}{\sum_j \lambda_j^p}$.

Before proceeding into the Hennecart, Robert, and Yudin construction, we first give an easier example of the addition and subtraction of the set $\{0, 1, 3\}$.

Claim 37. *For all $\epsilon > 0$, there exists a set S with $|S - S| > |S|^{2-\epsilon}$ and $|S + S| < |S|^{1.9364+\epsilon}$.*

Proof. Let $S = \{0, 1, 3\}$ and let $\frac{1}{3} < q < 1$ be some fixed probability, and let S_n be a random subset of S^n chosen by choosing each element of S with probability q^n.

Then $S + S = \{0, 2, 6, 1, 3, 4\}$ with corresponding multiplicities $\{1, 1, 1, 2, 2, 2\}$. As such, the limit of $\mathbb{E}|S_n + S_n|^{1/n}$ as $n \to \infty$ is

$$\|\alpha + \alpha\| = \begin{cases} (3q)^2 & \text{if } q < \frac{1}{2}^{\frac{1}{3}}, \\ 6 & \text{if } q > \frac{1}{2}^{\frac{1}{4}}, \\ 3q^{2p}(1 + 2^p) & \text{if } q = \frac{1}{2}^{\frac{2^p}{2(1+2^p)}}. \end{cases}$$

On the other hand, we have that $S - S = \{-3, -2, -1, 0, 1, 2, 3\}$ with corresponding multiplicities $\{1, 1, 1, 3, 1, 1, 1\}$, and so the limit of $\mathbb{E}|S_n - S_n|^{1/n}$ as $n \to \infty$ is

$$\|\alpha - \alpha\| = \begin{cases} (3q)^2 & \text{if } q < \frac{1}{3}^{\frac{1}{6}}, \\ 7 & \text{if } q > \frac{1}{3}^{\frac{1}{14}}, \\ q^{2p}(6 + 3^p) & \text{if } q = \frac{1}{3}^{\frac{3^p}{2(6+3^p)}}. \end{cases}$$

Now $3^4 = 81 > 64 = 2^6$ so it follows that $\frac{1}{2}^{\frac{1}{4}} > \frac{1}{3}^{\frac{1}{6}}$. Thus if we take q just below $\frac{1}{2}^{\frac{1}{4}}$, it will follow that $\|\alpha + \alpha\| = 6$ and $\|\alpha - \alpha\| = (3q)^2$. Furthermore, since $\alpha - \alpha$ will be spartan, it will actually follow that $\mathbb{E}|S_n|^2 - |S_n - S_n| = o((3q)^{2n})$. So, we get a set S_n for which $|S_n|$ is very close to $(3q)^n$, the difference set $|S_n - S_n|$ is very close to $(3q)^{2n}$, and $|S_n + S_n|$ is at most 6^n. Thus, for any $\epsilon > 0$, we find a set S with $|S - S| > |S|^{2-\epsilon}$ and $|S + S| < |S|^{\frac{\log 6}{\log 3q}+\epsilon}$, where q can be chosen arbitrarily close to $\frac{1}{2}^{\frac{1}{4}}$, so $\frac{\log 6}{\log 3q}$ can be less than 1.93647. □

Hennecart, Robert and Yudin [2] gave a construction of sets $A_{k,d} \in \mathbb{Z}^d$ for which $|A_{k,d} - A_{k,d}|$ was a lot bigger than $|A_{k,d} + A_{k,d}|$. Their construction was

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

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

Theorem 38. *The multiplicity spectrum for subtraction on $A_{k,d}$ consists of one copy of $\binom{k+d}{d}$ and $\sum_{i=1}^{\min(t,d)} \binom{d+1}{i}\binom{t-1}{i-1}\binom{t+d-i}{d-i}$ copies of $\binom{k+d-t}{d}$ for $1 \leq t \leq k$.*

Proof. Let $w = (w_1, \ldots, w_{d+1})$ be an element of $A_{k,d} - A_{k,d}$. Then w can be written as $w = x - y$ where $x = (x_1, \ldots, x_{d+1})$ and $y = (y_1, \ldots, y_{d+1})$ are non-negative vectors summing to k. It follows that $\sum_i w_i = 0$.

Now write w^+ as the vector containing only the positive coordinates of w, so

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

and write w^- for the corresponding vector for the negative coordinates. Then for all i, we have $\max\{w_i, 0\} \leq x_i$, so $\sum_i (w^+)_i \leq k$. If w is any integer vector with $\sum_i w_i = 0$ it is clear for nonnegative vectors x, y that $w = x - y$ if and only if there is a non-negative vector z such that $x = w^+ + z$ and $y = z - w^-$. Thus the number of ways that w can be written as an element of $A_{k,d} - A_{k,d}$ is the number of nonnegative $(d+1)$-dimensional vectors summing to $k - \sum_i (w^+)_i$ which is $\binom{k - \sum_i (w^+)_i + d}{d}$.

To calculate the number of $(d+1)$-length integer vectors summing to 0 such that the positive elements sum to $k > 0$, we split according to the number i of positive elements (which must be in the range $1 \leq i \leq \min\{k, d\}$). The number of choices of the locations of those i positive elements is $\binom{d+1}{i}$, the number of i positive numbers adding to k is $\binom{k-1}{i-1}$, and the number of $d + 1 - i$ nonnegative numbers adding to k is $\binom{k+d-i}{d-i}$. □

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

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

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

Then from Theorem 38, we know that the non-zero values of $\alpha - \alpha$ consist of μ_t copies of $q^2\lambda_t$ for each $0 \leq t \leq k$. Then $\alpha - \alpha$ is spartan, by definition, when

$$0 > \sum_{\substack{x \in \mathbb{Z}^{d+1} \\ (\alpha - \alpha)(x) \neq 0}} (\alpha - \alpha)(x) \log_2 (\alpha - \alpha)(x),$$

or

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

which is equivalent to

$$-\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t) > \sum_{t=0}^{k} \mu_t \lambda_t \log_2(q^2),$$

or

$$-\frac{\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t)}{2\sum_{t=0}^{k} \mu_t \lambda_t} > \log_2(q),$$

which gives

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

So, let $p = 2^{-\frac{\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t)}{2\sum_{t=0}^{k} \mu_t \lambda_t}}$ and we have that $\alpha - \alpha$ is spartan for all $p > q$.

Now $\|\alpha + \alpha\| \leq |A_{k,d} + A_{k,d}| = \binom{2k+d}{d}$. 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 $\beta = \log(\binom{2k+d}{d}) / \log(p|S|)$, it follows that $\|\alpha + \alpha\| \leq \|\alpha\|^{\beta}$. If we think of β as a function of d and k, then it seems to have a global minimum of $\beta = 1.735383\ldots$ at $d = 14929$ and $k = 987$. □

This was in the introduction, and still needs to be incorporated into this section:

Let α be the fractional set with properties as in Theorem 4, and let S_n be drawn from α^n.

Pick ϵ' in the range $(0, \epsilon)$. We will show that the probabilities of the events $|S_n| < 0.5\|\alpha\|^n$, $|S_n| > 1.5\|\alpha\|^n$, $|S_n - S_n| < 0.15\|\alpha\|^{2n}$ and $|S_n + S_n| > 0.5\|\alpha\|^{(1.7354+\epsilon')n}$ all vanish as $n \to \infty$ from which we will show that S_n satisfies the required conditions for A with probability tending to 1.

$|S_n|$ is the sum of independent Bernoulli variables $(X_i : i \in S)$. Let each variable X_i have probability p_i of being 1. Then

$$\mathrm{Var}|S_n| = \sum_{i \in S} \mathrm{Var} X_i = \sum_{i \in S} p_i - p_i^2 \leq \sum_{i \in S} p_i = \mathbb{E}|S_n|.$$

We know that $\mathbb{E}|S_n|$ is precisely $\|\alpha\|^n$, so the variance is at most $\|\alpha\|^n$, so by Cauchy's Inequality:

$$\begin{aligned}\Pr(||S_n| - \|\alpha\|^n| > 0.5\|\alpha\|^n) &= \Pr(||S_n| - \mathbb{E}|S_n||^2 > 0.25\|\alpha\|^{2n}) \\ &\leq \mathrm{Var}|S_n| / 0.25\|\alpha\|^{2n} \\ &\leq 4/\|\alpha\|^n.\end{aligned}$$

Thus both the events $|S_n| < 0.5\|\alpha\|^n$ and $|S_n| > 1.5\|\alpha\|^n$ have probabilities that vanish.

Since $\alpha - \alpha$ is spartan, Theorem 4 states that $\mathbb{E}|S_n|^2 - |S_n - S_n|$ is $o(\|\alpha\|^{2n})$. Since $|S_n - S_n|$ is always at most as large as $|S_n|^2$, it follows that the probability that $|S_n|^2 - |S_n - S_n| > 0.1\|\alpha\|^{2n}$ tends to 0. Further, since $|S_n| > 0.5\|\alpha\|^n$ with probability tending to 1, it follows that $|S_n - S_n| > |S_n|^2 - 0.1\|\alpha\|^{2n} > 0.15\|\alpha\|^{2n}$ with probability tending to 1.

Choose ϵ'' in the range $(0, \epsilon')$. Theorem 4 states that $\lim_{n\to\infty}(\mathbb{E}|S_n + S_n|)^{1/n} \to \|\alpha + \alpha\| \leq \|\alpha\|^{1.7354}$, so for all sufficiently large n, $\mathbb{E}|S_n + S_n| < \|\alpha\|^{(1.7354+\epsilon'')n}$, so by Cauchy's inequality, the probability that $|S_n + S_n| > \alpha^{(1.7534+\epsilon')n}$ is at most $\|\alpha\|^{(\epsilon''-\epsilon')n}$ which vanishes.

So, for all sufficiently large n, with probability at least a half, $0.5\|\alpha\|^n < |S_n| < 1.5\|\alpha\|^n$, $0.15\|\alpha\|^{2n} < |S_n - S_n|$ and $|S_n + S_n| < 0.5\|\alpha\|^{(1.7354+\epsilon')n}$. Since, for all sufficiently large n, $0.15\|\alpha\|^{2n} \geq (1.5\|\alpha\|^n)^{2-\epsilon}$ and $\|\alpha\|^{(1.7354+\epsilon')n} \leq (0.5\|\alpha\|^n)^{1.7354+\epsilon}$, it follows that for all sufficiently large n, with probability at least a half, S_n satisfies the conditions of this corollary.

5 Open Questions

We introduced the concept of a fractional dilate as a more general version of Ruzsa's method from [12], Ruzsa's method being the specialisation where a fractional dilate has all non-0 values being equal. However, we in fact only used this same specialisation to prove Theorem 6. We believe that using a more general fractional dilate defined on the Hennecart, Robert and Yudin sets $A_{k,d}$ could give a better bound than 1.7354. In particular, the best bound you can get from a Ruzsa-style dilate on $A_{2,d}$ is that for $d = 23$, which with a value of $q = \frac{1}{5}^{\frac{1}{300}} \frac{1}{2}^{\frac{46}{625}} \frac{1}{12}^{\frac{1129}{15000}}$ gives a bound of 1.7897, whereas if you take 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 $e_i + e_j$ you 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 quite clumped around the expected value. We believe this will be true without the requirement of spartaneity.

Conjecture 39. *If α is a fractional dilate with $\|\alpha\| > 1$ and 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 sizes of sums and differences of sets 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 we make is that the feasible regions for dilates are the same as the feasible regions for fractional dilates.

Conjecture 40. *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. Since we know that many readers just jump straight to the open questions section to see if there will be anything interesting for them to work on, we write out these questions in full, noting that Theorem 19 gives a useful way of computing $\|\alpha + \alpha\|$ and $\|\alpha + 2 \cdot \alpha\|$.

Question 41. *Suppose that $\alpha : \mathbb{Z} \to [0, 1]$ is a function with finite sum. We write*

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

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

1. $\|\alpha\|\|\alpha + 2 \cdot \alpha\| \leq \|\alpha + \alpha\|^2$

2. $\|\alpha + 2 \cdot \alpha\| \leq \log_3 4 \|\alpha + \alpha\|$

3. $\|\alpha + 2 \cdot \alpha\| \geq \|\alpha + \alpha\|$

Since a subset of the integers is equivalent to the 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 39 or Conjecture 40 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 a better understanding of the above conjectures.

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

References

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

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

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

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

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

[6] 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.

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

[8] 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.

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

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

[11] 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.

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

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