Sums, Differences, and Dilates

Jonathan Cutler Luke Pebody Amites Sarkar

February 27, 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 $|A + 2 \cdot A| \leq K^{2.95}|A|$. At a presentation of this result, Petridis stated that the highest known value for $\frac{\log(|A+2\cdot A|/|A|)}{\log(|A+A|/|A|)}$ (bounded above by 2.95) was $\frac{\log 4}{\log 3}$. We show 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 [10], and generalise it to give continuous analogues of the sizes of sumsets, differences 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 [11]. Given a number $x \in Z$ the *multiplicity* of x in $A + A$ (and correspondingly in $A - A$) are defined by

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

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 [10] 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*

$$|A + A| \le n^{2-c} \qquad \textit{and} \qquad |A - A| \ge n^2 - n^{2-c},$$

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

$$|B - B| \le n^{2-c}, \qquad \textit{and} \qquad |B + B| \ge \frac{n^2}{2} - n^{2-c}.$$

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 [2]. 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 [5] for a recent survey).

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*

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

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. We define the *multiplicity* of x in $A + k \cdot A$ to be

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

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 $|A + A| \le K|A|$, for some fixed constant K (known as the *doubling constant*). For such a set A, *Plünnecke's inequality* [8] (see also [7]) shows that

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

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 $|A + A| \le K|A|$, then*

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

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 $|A + A| \le K|A|$, then*

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

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. This is proved 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 upper bounds in Theorems 2 and 3 of Hanson and Petridis. Specifically, this construction shows that graph (x,y) 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 exist positive constants K and sets 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 [4] and Ruzsa [9] in the 1970s (and indeed Conway in the 60s). We analyse and generalise Ruzsa's method from [10], 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. Define a *fractional dilate* γ to be a map $\gamma : \mathbb{Z} \to \mathbb{R}^+ \cup \{0\}$ with a finite support. We denote the *size of a fractional dilate* to be

$$\|\gamma\| = \inf_{0<p<1} \sum_{n\in\mathbb{Z}} \gamma(n)^p.$$

We define a *fractional set* to be a fractional dilate α for which $\alpha(n) \leq 1$ for all $n \in Z$. Note that the formula for the size of a fractional set simplifies to $\|\alpha\| = \sum_{n\in\mathbb{Z}} \alpha(n)$.

Given fractional sets α, β and an integer k, let $\alpha + k\cdot\beta$ denote the fractional dilate defined by

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

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 $\alpha(i_1)\alpha(i_2)\ldots\alpha(i_n)$.

We can identify an actual subset S of $\mathbb{Z}$ with the fractional set $\mathbb{1}_S$ and then for any sets S, T, $|S+k\cdot T|$ can easily be seen to be equal to $\|\mathbb{1}_S + k\cdot\mathbb{1}_T\|$.

We describe a fractional dilate γ as being *spartan* if $\sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \gamma(n)\log\gamma(n) < 0$, *opulent* if $\sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \log\gamma(n) > 0$ and *comfortable* if neither of these holds. In the case that γ is comfortable, there will be a unique $p \in [0,1]$ with $\sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \gamma(n)^p \log\gamma(n) = 0$. If we wish to emphasise, we will say that γ is p-comfortable.

We will show this alternate characterisation of the size of a fractional dilate.

Theorem 4. *The size of a fractional dilate γ is*

$$\begin{cases} \sum_{n\in\mathbb{Z}} \gamma(n) \text{ if } \gamma \text{ is spartan,} \\ |\{n : n \in \mathbb{Z}, \gamma(n) \neq 0\}| \text{ if } \gamma \text{ is opulent,} \\ \sum_{n\in\mathbb{Z}} \gamma(n)^p \text{ if } \gamma \text{ is } p\text{-comfortable.} \end{cases}$$

In Section 4 and Section 5, we prove the following.

Theorem 5. *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*

$$\lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot T_n|)^{1/n} \to \|\alpha + k \cdot \beta\|$$
$$\lim_{n\to\infty} (\mathbb{E}|S_n + k \cdot S_n|)^{1/n} \to \begin{cases} \|\alpha + k \cdot \alpha\| \text{ if } \|\alpha\| \geq 1 \\ \|\alpha\| \text{ otherwise.} \end{cases}$$

Furthermore, if $\alpha + k \cdot \beta$ is spartan then

$$\mathbb{E}|S_n||T_n| - |S_n + k \cdot T_n| = o(\|\alpha + k \cdot \beta\|^n)$$

and similarly if $\alpha + k \cdot \alpha$ is spartan then

$$\mathbb{E}|S_n|^2 - |S_n + k \cdot S_n| = o(\|\alpha + k \cdot \alpha\|^n) \text{ if } k \neq 1$$
$$\mathbb{E}\frac{|S_n|^2}{2} - |S_n + k \cdot S_n| = o(\|\alpha + k \cdot \alpha\|^n) \text{ if } k = 1$$

In Section 6, we apply this method to the 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 spartan, and with $\|\alpha + \alpha\| \leq \|\alpha\|^{1.7354}$.*

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 5, 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 5 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 5 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. $\square$

In the other direction, it follows from results of Freiman and Pigarev [4] and Ruzsa [9] that $(x, 2)$ is not attainable for any $x < 3/2$. All these results are illustrated in Figure 1.

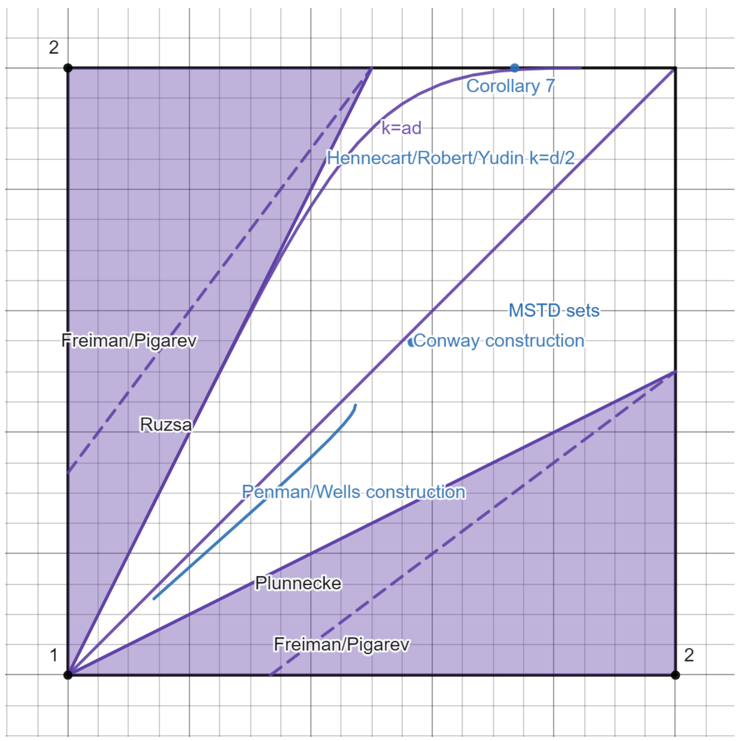

Figure 1: The feasible region $F_{1,-1}$

Finally, in Section 7, 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

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

And so,

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

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

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

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 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 $|I_k + I_k|$, $|H_n + 2 \cdot I_k|$, $|I_k + 2 \cdot H_n|$, $|I_k + 2 \cdot I_k|$ (spoiler warning: 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.)

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 $k \geq \frac{n+2}{2}$, $4^k \geq 2^{n+2} > 1 + 3 \times 2^n$, 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 $\{0, 1\}$, $\{0, 4\}$ all the way up to $\{0, 4^{n-1}\}$. 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

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

Further the set $\{0, 4^k\} + \ldots + \{0, 4^{n-1}\}$ consists of multiples of 4^k, which are all further than $2\frac{4^k-1}{3}$ apart, so $H_n + I_k$ consists of 2^{n-k} intervals of length $2\frac{4^k-1}{3}$ and contains $I_k + I_k$. $\square$

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 $n \to \infty$,*

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

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 $\lim_{n\to\infty} \log a_{n,i}/n \to c_i$ 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)

$$\begin{aligned}
&\lim_{n\to\infty} \frac{\log |H_n + H_n|}{n} = \log 3, \quad \text{and} \\
&\lim_{n\to\infty} \frac{\log |H_n + I_k|}{n} = (1-\alpha)\log 2 + \alpha \log 4 = \frac{1+\alpha}{2} \log 4 > \lim_{n\to\infty} \frac{\log |I_k + I_k|}{n}.
\end{aligned}$$

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

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

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 this corollary 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

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

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 given by Plünnecke's inequality [8].

Theorem 13 (Plünnecke 1970)**.** *Let U and V be finite subsets of $\mathbb{Z}$ and let $X \subseteq U$ such that*

$$\rho := \frac{|X+V|}{|X|} \le \frac{|X'+V|}{|X'|}$$

for all nonempty subsets $\emptyset \neq X' \subseteq X$. Then, for any set W, we have

$$|X+V+W| \le \frac{|X+V||X+W|}{|X|}.$$

This gives a simple upper bound on $|A+A|$ in terms of $|A+2\cdot A|$.

Corollary 14. *For all sets A, $|A+A| \le \frac{|A+2\cdot A|^2}{|A|}$.*

Proof. Let $1 \le t \le 2$ be such that $|A+2\cdot A| = |A|^t$. Suppose that $S \subseteq A$ minimises $\frac{|S+2\cdot A|}{|S|}$. Then

$$\rho := \frac{|S+2\cdot A|}{|S|} \le \frac{|A+2\cdot A|}{|A|} \le \frac{|A|^t}{|A|} = |A|^{t-1}.$$

Further, we note that

$$|A+A| = |2\cdot A + 2\cdot A| \le |S+2\cdot A+2\cdot A| \le \frac{|S+2\cdot A|^2}{|S|} = \rho^2 |S| \le \rho^2 |A|,$$

where the second inequality is Plünnecke's inequality. Thus, we have

$$|A+A| = |2\cdot A+2\cdot A| \le \rho^2|A| \le (|A|^{t-1})^2|A| = \frac{|A+2\cdot A|^2}{|A|}.$$

□

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 $|A + 2 \cdot A| \leq |A|^{4t/3}$.

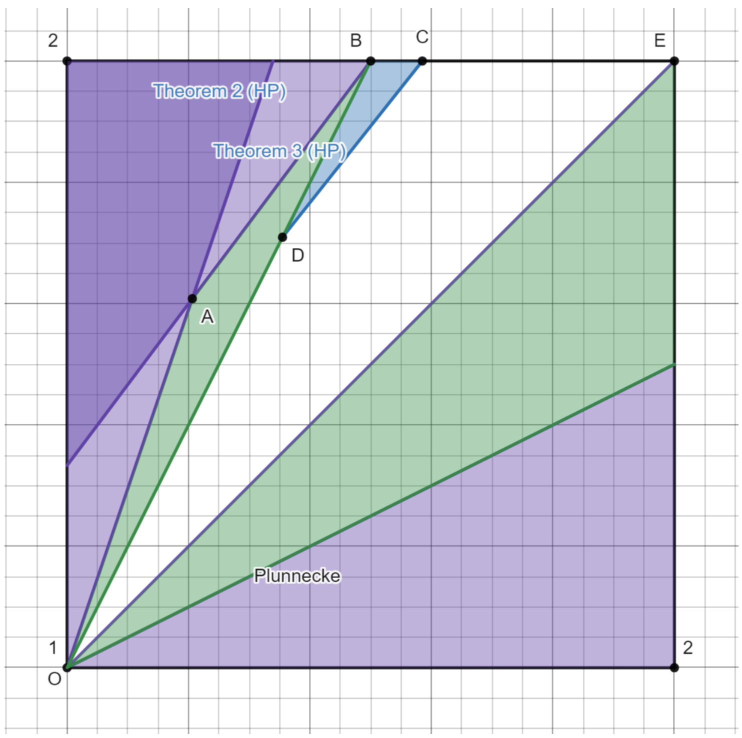

Figure 2: The feasible region $F_{1,2}$

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:

Question 15. *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 $|A + 2 \cdot A| \leq |A|^{1+2t}$? In yet more other words, is it true that for all A, $|A||A + 2 \cdot A| \leq |A + A||A + A|$.*

Question 16. *Is it true that nothing above the line DC is in $F_{1,2}$. In other words, is it true that $\frac{\log |A+2 \cdot A|}{\log |A+A|} \leq \frac{\log 4}{\log 3}$ for all sets A? In yet more other words, is it true for all n that if $|A + A| \leq 3^n$, then $|A + 2 \cdot A| \leq 4^n$?*

Question 17. *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 17. 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 18. *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 $\Pr(X_1 = X_2) \geq 1/|S|$.

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 $|A+2\cdot A| \geq 1/\Pr(A_1 + 2\cdot A_2 = A_3 + 2\cdot A_4)$. 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 $n^2 - n$ 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 16 is a "2-Sidon" set (ie 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 $\{0,1\}^n$. We can show that such sets in fact satisfy the condition of Question 16

Lemma 19. *Suppose A, B are subsets of the Hypercube $\{0,1\}^n$, then*

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

Proof. Define a function $f : \mathbb{N}^2 \to \mathbb{N}$ iteratively by: $f(i,j) = ij$ if $i \leq 1$ or $j \leq 1$ and otherwise $f(i,j) = \min(f(i_1,j_1) + f(i_2,j_2) + \max(f(i_1,j_2), f(i_2,j_1)) : i_1 + i_2 = i, j_1 + j_2 = j)$.

We claim that for any finite subsets A, B of the Hypercube, $|A+B| \geq f(|A|,|B|)$. This is clearly true if $|A| \leq 1$ or $|B| \leq 1$. Otherwise, assume the result is true for all smaller $|A|+|B|$. There is some coordinate i for which not every element of A is identical. Then if $A_0 = \{x : x \in A | x_i = 0\}$ and we define A_1, B_0 and B_1 correspondingly, it is clear that

$$\begin{aligned}
|A+B| &= |\{x : x \in A+B | x_i = 0\}| + |\{x : x \in A+B | x_i = 1\}| + |\{x : x \in A+B | x_i = 2\}| \\
&= |A_0 + B_0| + |(A_0 + B_1) \cup (A_1 + B_0)| + |A_1 + B_1| \\
&\geq |A_0 + B_0| + |A_1 + B_1| + \max(|A_0 + B_1|, |A_1 + B_0|) \\
&\geq f(|A_0|, |B_0|) + f(|A_1|, |B_1|) + \max(f(|A_0|, |B_1|), f(|A_1|, |B_0|)) \\
&\geq f(|A|, |B|),
\end{aligned}$$

where the last two inequalities are the inductive hypothesis and the definition of f respectively.

We claim also that $f(i,j) \geq (ij)^\beta$ where $\beta = \frac{\log 3}{\log 4}$ for all i, j. This is clearly true if $i \leq 1$ or $j \leq 1$ and to prove by induction we need to show that

$$((i_1 + i_2)(j_1 + j_2))^\beta \leq (i_1 j_1)^\beta + (i_2 j_2)^\beta + \max((i_1 j_2)^\beta, (i_2 j_1)^\beta)$$

for all non-negative integers i_1, i_2, j_1, j_2.

To that end, note that for $t > 1$, $(t^{2\beta} - 1)/(t-1)$ is the average value of $(2\beta - 1)x^{2\beta - 1}$ over the range $x \in [1, t]$. Since $0 < 2\beta - 1 < 1$, this is a concave function and hence this average value is greater than $(2\beta - 1)((1+t)/2)^{2\beta - 1}$. Further, since $(2\beta - 1) > 2^{2\beta - 1}$, this is larger than $(1+t)^{2\beta - 1}$.

So it follows that for all $t > 1$

$$\begin{aligned}
(t^{2\beta} - 1)/(t-1) &> (1+t)^{2\beta - 1} \\
(t^{2\beta} - 1) &> (t-1)(1+t)^{2\beta - 1} \\
(t^{\beta - 1} - t^{-\beta - 1}) &> (t-1)(1+t)^{2\beta - 1}/t^{\beta + 1} \\
&= \frac{(t-1)(1+t)}{t^2} \frac{(1+t)^{2\beta - 2}}{t^{\beta - 1}} \\
&= (1 - 1/t^2)(t + 1/t + 2)^{\beta - 1}
\end{aligned}$$

It then follows for all $r \geq 1$, since $r + 1/r \geq 2$, that $(t^{\beta - 1} - t^{-\beta - 1}) > (1 - 1/t^2)(t + 1/t + r + 1/r)^{\beta - 1}$ for all $t > 1$, and hence that the function $g(t, r) = t^\beta + t^{-\beta} + r^\beta - (t + 1/t + r + 1/r)^\beta$ is increasing in the range $t \geq 1$ and therefore that $g(t, r) \geq g(1, r) = 2 + r^\beta - (2 + r + 1/r)^\beta$.

Now $\beta < 1$, so for all $r > 1$

$$\begin{aligned}
(1 + 1/r)^{2\beta - 2} &< 1 \\
(1 + 1/r)^{2\beta - 1} &< 1 + 1/r \\
(1 + 1/r)^{2\beta - 1}(1 - 1/r) &< 1 \\
((1 + 1/r)^2)^{\beta - 1}(1 - 1/r^2) &< 1 \\
(2 + r + 1/r)^{\beta - 1}(1 - 1/r^2) &< r^{\beta - 1} \\
0 &< \beta r^{\beta - 1} - (1 - 1/r)^2(2 + r + 1/r)^\beta.
\end{aligned}$$

It follows that $g(1, r)$ is increasing in r, so for all $r \geq 1, t \geq 1$, $g(t, r) \geq g(1, r) = 3 - 4^\beta = 0$. Thus for all $t \geq 1$, $r \geq 1$, $t^\beta + t^{-\beta} + r^\beta \geq (t + 1/t + r + 1/r)^\beta$. By replacing t with $1/t$ if necessary, we see this inequality is true for $t > 0$, $r \geq 1$.

Now if we let $t = \frac{i_1 j_1}{\sqrt{i_1 i_2 j_1 j_2}}$ and $r = \frac{\max(i_1 j_2, i_2 j_1)}{\sqrt{i_1 i_2 j_1 j_2}}$, we get $(i_1 j_1)^\beta + (i_2 j_2)^\beta + \max(i_1 j_2, i_2 j_1)^\beta \geq ((i_1 + i_2)(j_1 + j_2))^\beta$ as was required. $\square$

4 Fractional Dilates

We remind the reader of the definition of fractional dilates and their size - a fractional dilate γ is a map $\gamma : \mathbb{Z} \to \mathbb{R}^+ \cup \{0\}$ with a finite support. We denote the *size of a fractional dilate* to be

$$\|\gamma\| = \inf_{0<p<1} \sum_{n\in\mathbb{Z}} \gamma(n)^p.$$

We describe a fractional dilate γ as being *spartan* if $\sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \gamma(n)\log\gamma(n) < 0$, *opulent* if $\sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \log\gamma(n) > 0$ and *comfortable* if neither of these holds. In the case that γ is comfortable, there will be a unique $p \in [0,1]$ with $\sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \gamma(n)^p \log\gamma(n) = 0$. If we wish to emphasise, we will say that γ is p-comfortable. We will first prove Theorem 4 giving an alternate characterisation of $\|\gamma\|$.

Proof of Theorem 4. For a fixed γ with support S, define a function $f : [0,1] \to \mathbb{R}$ by $f(p) = \sum_{n\in S} \gamma(n)^p$. It is clear that f is doubly differentiable and that $f''(p) = \sum_{n\in S}(\log\gamma(n))^2\gamma(n)^p > 0$.

Now if γ is spartan, then $f'(1) = \sum_{n\in S} \gamma(n)\log\gamma(n) < 0$. It follows that $f'(p) < 0$ for all $0 < p < 1$ and hence $\|\gamma\| = \inf_{0<p<1} f(p) = f(1) = \sum_{n\in\mathbb{Z}} \gamma(n)$.

If γ is opulent, then $f'(0) = \sum_{n\in S} \log\gamma(n) > 0$. It follows that $f'(p) > 0$ for all $0 < p < 1$ and hence $\|\gamma\| = \inf_{0<p<1} f(p) = f(1) = |S|$.

Otherwise, $f'(0) < 0 < f'(1)$ and hence there is a unique p for which $0 = f'(p) = \sum_{n\in\mathbb{Z}:\gamma(n)\neq 0} \gamma(n)^p \log\gamma(n)$ and hence for which γ is p-comfortable. Then for this value of p, $\|\gamma\| = f(p) = \sum_{n\in\mathbb{Z}} \gamma(n)^p$. $\square$

We will give yet another alternate characterisation of $\|\gamma\|$, if γ has finite support. Recall that the entropy function $H(y_1,\ldots,y_n)$ for positive numbers $y_1,\ldots,y_n$ summing to 1 is defined to be

$$H(y_1,\ldots,y_n) = -(y_1\log_2 y_1 + \ldots y_n \log_2 y_n).$$

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

$$\|\gamma\| = \max_{y_1+\ldots+y_n=1} 2^{H(y_1,\ldots,y_n)} \min(1, \gamma(s_1)^{y_1}\ldots\gamma(s_n)^{y_n})$$

Proof. It is clear that for real x and $0 \le p \le 1$, that $\min(0,x) \le px$ and further that equality happens exactly when:

1. $p = 0$ and $x \ge 0$

2. $p = 1$ and $x \le 0$

3. $0 < p < 1$ and $x = 0$.

Gibbs Inequality[**GibbsInequality**] states that

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

for any sequence of non-negative z_i summing to 1 with equality only if $y_i = z_i$ for all i.

For now fix $0 \le p \le 1$ and let $z_i = \frac{\gamma(s_i)^p}{\sum_i \gamma(s_i)^p}$. Clearly $\sum z_i = 1$.

Then for all non-negative sequences y_i with $y_1 + \ldots + y_n = 1$

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

with the second inequality being Gibbs Inequality.

Raising 2 to both sides shows that

$$2^{H(y_1,\ldots,y_n)} \min(1, \gamma(s_i)^{y_1} \ldots \gamma(s_n)^{y_n}) \le \sum_i \gamma(s_i)^p$$

for all $y_1, \ldots, y_n$ and all $0 \le p \le 1$. Equality here only happens if equality happens in both the inequalities above, which is if $\min(0, \sum_i y_i \log_2 \gamma(s_i)) = \sum_i p y_i \log_2 \gamma(s_i)$ and if $y_i = z_i$ for all i.

To put it another way, $\max_{y_1+\ldots+y_n=1} 2^{H(y_1,\ldots,y_n)} \min(1, \gamma(s_1)^{y_1} \ldots \gamma(s_n)^{y_n})$ is bounded above by $\sum_i \gamma(s_i)^p$ with equality only if $\sum_i p z_i \log_2 \gamma(s_i) = \min(0, \sum_i z_i \log_2 \gamma(s_i))$ where $z_i = \frac{\gamma(s_i)^p}{\sum_i \gamma(s_i)^p}$, which is equivalent to the requirement that

$$p \sum_i \gamma(s_i)^p \log \gamma(s_i) = \min(0, \sum_i \gamma(s_i)^p \log \gamma(s_i)).$$

As discussed above, equality happens exactly when

1. $p = 0$ and $0 < \sum_i \log \gamma(s_i)$, which is the requirement for γ to be opulent
2. $p = 1$ and $0 > \sum_i \gamma(s_i) \log \gamma(s_i)$, which is the requirement for γ to be spartan
3. $0 < p < 1$ and $\sum_i \gamma(s_i)^p \log \gamma(s_i) = 0$, which is the requirement that γ to be p-comfortable.

Putting this all together, we see that

$$\max_{y_1+\ldots+y_n=1} 2^{H(y_1,\ldots,y_n)} \min(1, \gamma(s_1)^{y_1} \ldots \gamma(s_n)^{y_n} = \begin{cases} \sum_{n\in\mathbb{Z}} \gamma(n) \text{ if } \gamma \text{ is spartan,} \\ |\{n : n \in \mathbb{Z}, \gamma(n) \neq 0\}| \text{ if } \gamma \text{ is opulent,} \\ \sum_{n\in\mathbb{Z}} \gamma(n)^p \text{ if } \gamma \text{ is } p\text{-comfortable.} \end{cases}$$

Comparing with Theorem 4, it is clear that this is equal to $\|\gamma\|$. □

A *fractional set* is a fractional dilate α for which $\alpha(n) \le 1$ for all $n \in Z$. It is clear that for $0 < p < 1$, $\alpha(n)^p \ge \alpha(n)$ for all $n \in \mathbb{Z}$ for a fractional set α, and hence $\|\alpha\| = \sum_{n\in\mathbb{Z}} \alpha(n)$. (It also follows trivially from Theorem 4 since fractional sets are clearly spartan.) 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 $\alpha(i_1)\alpha(i_2)\ldots\alpha(i_n)$.

In this section we will consider two fractional sets α and β and let $S_n, T_n \subseteq \mathbb{Z}^n$ be independently drawn from α^n and β^n respectively, and will show that $\lim_{n\to\infty}(\mathbb{E}|S_n + T_n|)^{1/n} = \|\alpha + \beta\|$ where $\alpha + \beta$ denotes the fractional dilate defined by $(\alpha+\beta)(n) = \sum_{i+j=n} \alpha(i)\beta(j)$. We will henceforth denote $\alpha + \beta$ by γ. Further if γ is spartan (in which case $\|\gamma\| = \|\alpha\|\|\beta\|$), we prove that $|S_n + T_n|$

is highly likely to be very close to this bound. In the next section we consider sums and dilates of a set with itself.

When proving that $\|\gamma\|$ is a lower bound for the limit, we will need the following technical lemma.

Lemma 21. *Let us suppose that $(X_n)_{n=1}^{\infty}$ is a collection of random variables, each of which can be written as the sum of independent Bernoulli random variables and suppose that $\lim_{n\to\infty}(\mathbb{E}X_n)^{1/n}$ exists and is equal to t. Then $\lim_{n\to\infty}\Pr(X_n > 0)^{1/n}$ also exists and is equal to $\min(1,t)$.*

Proof. We claim that if X is a random variable which can be written as the sum of independent Bernoulli random variables then $\mathbb{E}X - \frac{(\mathbb{E}X)^2}{2} \leq \Pr(X > 0)$. Indeed, write $X = \sum_{i\in S} Z_i$ where each i is Bernoulli, then

$$(\mathbb{E}X)^2 = \sum_{i\in S}\sum_{j\in S} E(Z_iZ_j) \geq 2\sum_{i\in S, j\in S, i>j} E(Z_iZ_j) = 2E(\binom{X}{2}),$$

so $\mathbb{E}X - \frac{(\mathbb{E}X)^2}{2} \leq \mathbb{E}(X - \binom{X}{2}) \leq \mathbb{E}\mathbb{1}_{X>0} = \Pr(X = 0)$, the last inequality being because $n - \binom{n}{2} \leq \mathbb{1}_{n>0}$ for all n.

Now if $t < 1$, then since $\mathbb{E}X_n - \Pr(X_n > 0) \leq (\mathbb{E}X_n)^2/2$, it follows that

$$\limsup_{n\to\infty}(\mathbb{E}X_n - \Pr(X_n > 0))^{1/n} \leq \limsup_{n\to\infty}(\frac{(\mathbb{E}X_n)^2}{2})^{1/n} = t^2$$

and hence $\Pr X_n > 0$ is the difference between $\mathbb{E}X_n$ (which is asymptotically t^n) and $\mathbb{E}X_n - \Pr X_n$ (which is asymptotically t^{2n}). Since $t < 1$, it follows that $(\Pr X_n)^{1/n} \to t$.

Given any $u < 1$, we can find a collection of random variables Y_n satisfying the conditions of the Lemma and with $\lim(\mathbb{E}Y_n)^{1/n} = u$ and $\Pr(X_n > 0) > \Pr(Y_n > 0)$ (simply reduce the probabilities of the underlying independent Bernoulli random variables being 1 until we get the required expectation). Then $u = \lim_{n\to\infty}\Pr(Y_n > 0)^{1/n} < \liminf_{n\to\infty}\Pr(X_n > 0)^{1/n}$. Since this is true for all $u < 1$, $\lim_{n\to\infty}\Pr(X_n > 0)^{1/n} = 1$. $\square$

Let us first prove the upper bound of the two-set part of Theorem 5. Recall that the multiplicity $\mathrm{Mult}_{A+k\cdot B}(x)$ is defined to be the number of ways of writing $x = y + kz$ where $y \in A$ and $z \in B$.

Theorem 22. *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 $\gamma = \alpha + \beta$. 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 $x \in X^n$, the probability that $x \in S_n + T_n$ is the probability that $\mathrm{Mult}_{S_n+T_n}(x) > 0$, which is bounded above by $\min(1, \mathbb{E}\,\mathrm{Mult}_{S_n+T_n}(x))$ and hence by $(\mathbb{E}\,\mathrm{Mult}_{S_n+T_n}(x))^p$ for all $0 \leq p \leq 1$.

Now if the coefficients of x are $x = (x_1, \ldots, x_k) \in x^n$, the expected value of the multiplicity of x in $S_n + T_n$ is

$$\begin{aligned}\mathbb{E}\,\mathrm{Mult}_{S_n+T_n}(x) &= \Sigma_{z_1+y_1=x_1,\ldots,z_n+y_n=x_n}\alpha(z_1)\ldots\alpha(z_n)\beta(y_1)\ldots\beta(y_n)\\ &= (\Sigma_{z_1+y_1=x_1}\alpha(z_1)\beta(y_1))\ldots(\Sigma_{z_n+y_n=x_n}\alpha(z_n)\beta(y_n))\\ &= \gamma(x_1)\gamma(x_2)\ldots\gamma(x_n).\end{aligned}$$

It follows that the expected size of $S_n + T_n$ is at most

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

for all $0 \leq p \leq 1$.

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

As a step towards the equivalent lower bound, we will use Lemma 21 to calculate the asymptotic behaviour of the probability of vectors lying in $S_n + T_n$.

Corollary 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 and let $\gamma = \alpha + \beta$. Suppose also that $x_1, \ldots, x_N$ are integers, that $y_1, \ldots, y_N$ are non-negative numbers summing to 1 and that for each n we have non-negative integers $z_{1,n}, \ldots, z_{N,n}$ summing to n such that for each i, $\lim_{n\to\infty} z_{i,n}/n = y_i$. Let $t = \gamma(x_1)^{y_1} \ldots \gamma(x_N)^{y_N}$.*

Suppose finally that for each n, v_n is an n-dimensional vector such that $z_{i,n}$ of the coordinates are equal to x_i. Then

$$lim_{n\to\infty} \Pr(v_n \in A_n + B_n)^{1/n} = \min(1, t).$$

Proof. Let vector $X_n = \mathrm{Mult}_{A_n+B_x}(v_n)$. As in the proof of Theorem 19,

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

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

Furthermore X_n can be written as $\sum_{z \in \mathbb{Z}^n} \mathbb{1}_{z \in A_n, v_n - z \in B_n}$, which are independent Bernoulli random variables. The result therefore follows from applying Lemma 21 to the random variables X_n. □

Corollary 24. *Let α and β be fractional sets with finite support, and suppose $S_n, T_n \subseteq \mathbb{Z}^n$ are drawn from α^n and β^n respectively and let $\gamma = \alpha + \beta$.*

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

Proof. By Lemma 20, if $S = \{s_1, \ldots, s_N\}$ is the support of γ, there exist non-negative numbers $y_1, \ldots, y_N$ summing to 1 with

$$\|\gamma\| = 2^{H(y_1,\ldots,y_N)} \min(1, \gamma(s_1)^{y_1} \ldots \gamma(s_N)^{y_N}).$$

Then we can choose integers $z_1 + \ldots + z_N = n$ with $z_i/n \to y_i$ for each $1 \leq i \leq N$. There are $\binom{n}{z_1, z_2, \ldots, z_N}$ n-dimensional vectors with z_k of each coordinate i_k and they all have the same probability p_n of being in $A_n + B_n$, and by Lemma 23, $p_n^{1/n} \to \min(1, c_{i_1}^{y_1} \ldots c_{i_N}^{y_N})$.

It is well known that $\binom{n}{z_1, z_2, \ldots, z_N}^{1/n} \to 2^{H(y_1,\ldots,y_n)}$.

It follows that

$$\begin{aligned}\liminf_{n\to\infty} \mathbb{E}|A_n+B_n|^{1/n} &\geq \lim_{n\to\infty}(\binom{n}{z_1, z_2, \ldots, z_N} p_n)^{1/n} \\ &= 2^{H(y_1, y_2, \ldots, y_n)} \min(1, \gamma(i_1)^{y_1} \ldots \gamma(i_n)^{y_N}) \\ &= \|\gamma\|.\end{aligned}$$

By Theorem 22, it follows that the limit of $\mathbb{E}|A_n+B_n|^{1/n}$ exists and is equal to $\|\gamma\|$. □

Corollary 25. *Let α and β be fractional sets with finite support, 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 spartan (so $\|\gamma\| = \|\alpha\|\|\beta\|$.)*

Then $\mathbb{E}|S_n||T_n| - |S_n+T_n| = o(|S_n||T_n|)$, so the probability that $|S_n+T_n|$ is at least $0.99\|\gamma\|^n$ tends to 1 as n tends to infinity.

Proof. As in the Proof of Lemma 21, we claim that if X is a random variable which can be written as the sum of independent Bernoulli random variables then $\mathbb{E}X - \frac{(\mathbb{E}X)^2}{2} \leq \Pr(X>0)$. In particular, for all v, $\mathrm{Mult}_{S_n+T_n}(v)$ can be written in such a fashion, so

$$\mathbb{E}\mathrm{Mult}_{S_n+T_n}(v) - \Pr(\mathrm{Mult}_{S_n+T_n}(v)>0) \leq (\mathbb{E}\mathrm{Mult}_{S_n+T_n}(v))^2/2 \leq (\mathbb{E}\mathrm{Mult}_{S_n+T_n}(v))^2.$$

Since it is clear that the left hand side is also at most $\mathbb{E}\mathrm{Mult}_{S_n+T_n}(v)$, it follows that

$$\mathbb{E}\mathrm{Mult}_{S_n+T_n}(v) - \Pr(\mathrm{Mult}_{S_n+T_n}(v)>0) \leq (\mathbb{E}\mathrm{Mult}_{S_n+T_n}(v))^p \text{ for all } 1 \leq p \leq 2.$$

Then $\mathbb{E}|S_n||T_n| - |S_n+T_n|$ is the sum over all v of the expected value of $\mathbb{E}\ \mathrm{Mult}_{S_n+T_n}(v) - \Pr(\mathrm{Mult}_{S_n+T_n}(v)>0)$, which is at most the sum over all v of $\mathbb{E}(\mathrm{Mult}_{S_n+T_n}(v))^p$ for all $1 \leq p \leq 2$. If v is $(v_1, \ldots, v_n)$ then $\mathbb{E}(\mathrm{Mult}_{S_n+T_n}(v)) = \gamma(v_1)\ldots\gamma(v_n)$.

It follows that

$$\mathbb{E}|S_n||T_n| - |S_n+T_n| \leq \sum_{v_1, v_2, \ldots, v_n} \gamma(v_1)^p \ldots \gamma(v_n)^p = (\sum_v \gamma(v)^p)^n$$

for all $1 \leq p \leq 2$.

Since γ is spartan, the function $p \to \sum_v \gamma(v)^p$ is decreasing for all $p \leq 1$ and beyond, so for all $\epsilon > 0$, $\sum_v \gamma(v)^{1+\epsilon} < \|\gamma\|$. Thus there exists ϵ such that $\mathbb{E}|S_n||T_n| - |S_n+T_n| \leq (\|\gamma\|-\epsilon)^n$ for all n. □

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

Let S_n be drawn from α^n. $|S_n|$ 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 21, $\lim_{n\to\infty}\Pr(|S_n| > 0)^{1/n} = 1$.

Let T_n be independently drawn from α^n. By Corollary 24, $\|\gamma\| = \lim_{n\to\infty}(\mathbb{E}|S_n + p\cdot T_n|)^{1/n}$, 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 $\{x_1, \dots, x_k\}$ of γ, and let R_n denote the set of rainbow vectors in $\mathbb{Z}^n$.

Theorem 27. *If $p \neq 1$ and v is a rainbow vector, the probabilities that $v \in S_n + p\cdot S_n$ and $v \in S_n + p\cdot T_n$ are the same. 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 $x \in S$, $x \neq v - px$ 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 28. *There exists an $\epsilon > 0$ such that the expected size of* $\mathbb{E}|(S_n+p\cdot T_n)\setminus R_n| = o((\|\gamma\|-\epsilon)^n)$.

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 22, 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, $\mathbb{E}|(S_n+p\cdot T_n)\setminus R_n|$ is therefore at most $N(\|\gamma\|-\alpha^p)^n$, which is $o((\|\gamma\| - \epsilon)^n$ for any $\epsilon < \alpha^p$. □

Corollary 29. *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 22, $\mathbb{E}|S_n + p \cdot S_n| \leq \|\alpha + p \cdot \alpha\|^n$.

Further, by Theorem 27,

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

By Corollary 24, $\lim_{n\to\infty} \mathbb{E}|S_n+p\cdot T_n|^{1/n} \to \|\alpha+p\cdot\alpha\|$ and by Theorem 28, $\mathbb{E}|(S_n+p\cdot T_n)\setminus R_n| = o((\|\alpha + p \cdot \alpha\| - \epsilon)^n)$, 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 $\lim_{n\to\infty} \mathbb{E}|S_n + p \cdot S_n|^{1/n} = \|\alpha + p \cdot \alpha\|$.

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

$$\begin{aligned}\mathbb{E}|S_n|^2 - |S_n + p \cdot S_n| &= \mathbb{E}|S_n|^2 - (\mathbb{E}|S_n|)^2 && (1)\\ &+ (\mathbb{E}|S_n|)^2 - \mathbb{E}|S_n||T_n| && (2)\\ &+ \mathbb{E}|S_n||T_n| - |S_n + p \cdot T_n| && (3)\\ &+ \mathbb{E}|(S_n + p \cdot T_n) \setminus R_n| && (4)\\ &+ \mathbb{E}|(S_n + p \cdot T_n) \cap R_n| - \mathbb{E}|(S_n + p \cdot S_n) \cap R_n| && (5)\\ &- \mathbb{E}|(S_n + p \cdot S_n) \setminus R_n|. && (6)\end{aligned}$$

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 25, the fourth and sixth by Theorem 28 and the fifth is zero by Theorem 27. □

Theorem 30. *If v is a rainbow vector, the probabilities that $v \in S_n + \cdot S_n$ 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 27, 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

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

$\square$

Corollary 31. *If* $\|\alpha\| > 1$*, then* $\lim_{n\to\infty} \mathbb{E}|S_n+S_n|^{1/n} = \|\alpha+\alpha\|$*. Furthermore, if* $\alpha+\alpha$ *is spartan,* $\mathbb{E}\frac{|S_n|^2}{2} - |S_n+S_n| = o(\mathbb{E}|S_n|^2)$

Proof. By Theorem 22, $\mathbb{E}|S_n + S_n| \le \|\alpha+\alpha\|^n$.

Further, by Theorem 30,

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

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 24 and Theorem 28, $\lim_{n\to\infty}\mathbb{E}|S_n+S_n|^{1/n} = \|\alpha+\alpha\|$.

Furthermore,

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

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. $\square$

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

In [10], 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 $\{x_1,\dots,x_N\}$. For $1 \le i \le N$, 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 $\{\lambda_1,\lambda_2,\dots,\lambda_N\}$ 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 4 as

$$\|\alpha + k\cdot\alpha\| = \begin{cases} (qM)^2 \text{ if } q^2 < 1/\prod_i \lambda_i^{\frac{\lambda_i}{\sum_j \lambda_j}}, \\ N \text{ if } q^2 > 1/\prod_i \lambda_i^{1/N}, \\ q^{2p}\sum_i \lambda_i^p \text{ if } q^2 = 1/\prod_i \lambda_i^{\frac{\lambda_i^p}{\sum_j \lambda_j^p}}. \end{cases}$$

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 32. *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 $S - S = \{-3, -2, -1, 0, 1, 2, 3\}$ 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 $(3q)^n$, $|S_n - S_n|$ is very close to $(3q)^{2n}$ and $|S_n + S_n|$ is at most 6^n.

Thus, for any ϵ 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. $\square$

In a 1999 paper [3], Hennecart, Robert and Yudin 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

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

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

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 clearly 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, $\max(w_i, 0) \leq x_i$, so $\sum_i (w^+)_i \leq k$.

Now if w is any integer vector with $\sum_i w_i = 0$ it is clear for non-negative 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 non-negative $d+1$-dimensional vectors summing to $k - \sum_i (w^+)_i$ which is $\binom{k - \sum_i (w^+)_i + d}{d}$.

Now 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 $d+1-i$ non-negative numbers adding to k is $\binom{k+d-i}{d-i}$. $\square$

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 $\mu_0 = 1$ and for $t > 0$,

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

Then from Theorem 33, we know that the non-0 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

$$\begin{aligned}
0 &> \sum_{x \in \mathbb{Z}^{d+1} : \alpha - \alpha(x) \neq 0} \alpha - \alpha(x) \log_2 \alpha - \alpha(x) \\
0 &> \sum_{t=0}^{k} \mu_t q^2 \lambda_t \log_2(q^2 \lambda_t) \\
-\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t) &> \sum_{t=0}^{k} \mu_t \lambda_t \log_2(q^2) \\
-\frac{\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t)}{2 \sum_{t=0}^{k} \mu_t \lambda_t} &> \log_2(q) \\
2^{-\frac{\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t)}{2 \sum_{t=0}^{k} \mu_t \lambda_t}} &> q.
\end{aligned}$$

So let $p = 2^{-\frac{\sum_{t=0}^{k} \mu_t \lambda_t \log_2(\lambda_t)}{2 \sum_{t=0}^{k} \mu_t \lambda_t}}$. $\alpha - \alpha$ 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.

So if we let $\beta = \log(\binom{2k+d}{d})/\log(p|S|)$, it follows that $\|\alpha+\alpha\| \leq \|\alpha\|^{\beta}$.

β as a function of d and k seems to have a global minimum of $\alpha = 1.735383\ldots$ at $d = 14929$ and $k = 987$. □

7 Open Questions

We introduced the concept of a fractional dilate as a more general version of Ruzsa's method from [10], 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 34. *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 Rusza'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 35. *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 $|k| \leq N$,*

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

We also ask whether the fractional dilate versions of the open questions from Section 3 are true. Since we know that many readers 1just 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 4 gives a useful way of computing $\|\alpha+\alpha\|$ and $\|\alpha + 2\cdot\alpha\|$.

Question 36. *Suppose that $\alpha : \mathbb{Z} \to [0,1]$ is a function with finite sum. We write*

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

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

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

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 34 or Conjecture 35 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] B. Bukh. "Sums of dilates". In: *Combinatorics, Probability and Computing* 17 (2008), pp. 627–639.

[2] Rogers C and G. Shephard. "The diference body of a convex body". In: *Arch. Math.* 8 (1957), pp. 220–233.

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

[4] G. Freiman and V. Pigarev. "The relation between the invariants R and T". In: *Number-theoretic studies in the Markov spectrum and in the structural theory of set addition (Russian)* (1973), pp. 172–174.

[5] S. Miller G. Iyer O. Lazarev and L. Zhang. "Finding and counting MSTD sets". In: *Combinatorial and Additive Number Theory, Springer Proceedings in Mathematics and Statistics* 101 (2014), pp. 79–98.

[6] B. Hanson and G. Petridis. "A question of Bukh on sums of dilates". In: *Discrete Analysis* (2021).

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

[8] H. Plúnnecke. "Eine zahlentheoretische anwendung der graphentheorie". In: *J. Reine Angew. Math.* 243 ().

[9] I. Ruzsa. "On the cardinality of $A + A$ and $A - A$". In: *Combinatorics: Colloq. Math. Soc. János Bolyai* 18 (1976), pp. 933–938.

[10] I. Ruzsa. "On the number of sums and differences". In: *Acta. Math. Hung.* 59 (1992), pp. 439–447.

[11] Y. Zhao. *Graph Theory and Additive Combinatorics - Exploring Structure and Randomness.* Cambridge University Press, 2023.