NEW COUNTEREXAMPLES FOR SUMS-DIFFERENCES

MARIUS LEMM

(Communicated by Alexander Iosevich)

Abstract. We present new counterexamples, which provide stronger limitations to sums-differences statements than were previously known. The main idea to improve over the original counterexamples by Ruzsa is to consider non-uniform probability measures.

1. Introduction

The sums-differences problem. For \( r \in \mathbb{Q} \cup \{\infty\} \), we define the maps \( \pi_r : \mathbb{R}^2 \to \mathbb{R} \) by
\[
\pi_r(a, b) = a + rb,
\]
with the convention that \( a + \infty b = b \).

Let \( r_1, \ldots, r_n \in \mathbb{Q} \cup \{\infty\} \setminus \{-1\} \) and \( 1 < \alpha \leq 2 \). We say that the statement \( SD(r_1, \ldots, r_n; \alpha) \) holds, if for any number \( N \) and any finite \( G \subset \mathbb{R}^2 \) such that \( \pi_{-1} \) is injective on \( G \) and \( |\pi_{r_j}(G)| \leq N \) for \( j = 1, \ldots, n \), it must be that \( |G| < N^\alpha \). Here, \( |A| \) denotes the cardinality of a set \( A \).

We say that the statement \( SD(\alpha) \) holds, if for any \( \epsilon > 0 \), there exists \( r_1, \ldots, r_n \in \mathbb{Q} \cup \{\infty\} \setminus \{-1\} \) such that \( SD(r_1, \ldots, r_n; \alpha + \epsilon) \).

The sums-differences problem was introduced by Bourgain in [1] as a combinatorial tool to prove lower bounds on the Hausdorff dimension of Kakeya sets in \( \mathbb{R}^d \). Already the trivial statement \( SD(2) \) implies the a priori non-trivial fact that the Hausdorff dimension of any Kakeya set is at least \((d+1)/2\). A proof of \( SD(1) \) would imply the Kakeya conjecture, i.e., that any Kakeya set has Hausdorff dimension \( d \).

The goal of the sums-differences approach to the Kakeya problem is then to prove \( SD(\alpha) \) statements with \( \alpha \) as small as possible.

In [1], Bourgain proved the statement \( SD(0, 1, \infty; 25/13) \). In [2], Katz and Tao showed \( SD(0, 1, \infty; 11/6) \) and \( SD(0, 1, 2, \infty; 7/4) \). In [3], they improved to \( SD(\alpha) \) with \( \alpha \approx 1.67513 \) using iteration. Well over ten years later, these are still the best known values of \( \alpha \).

Our results will go in the opposite direction. We say \( \neg SD(r_1, \ldots, r_n; \alpha) \), if there exists a counterexample, i.e., an explicit choice of \( G \) such that \( \pi_{-1} \) is injective on \( G \) and such that
\[
(1) \quad \alpha = \frac{\log |G|}{\max_j \{\log |\pi_{r_j}(G)|\}}.
\]

In this paper, we present new counterexamples that prove \( \neg SD(0, 1, \infty; \alpha) \) as well as \( \neg SD(0, 1, 2, \infty; \alpha) \) for considerably larger values of \( \alpha \) than previously known.

Received by the editors April 19, 2014.
2010 Mathematics Subject Classification. Primary 42B99; Secondary 11B75.

©2015 Marius Lemm
Entropy formulation of sums-differences. We will state our counterexamples in an equivalent formulation of the problem, in which the logarithm of cardinality in (1) is replaced by entropy; see [2]. The entropy viewpoint is instrumental to our construction of counterexamples. It is due to Ruzsa, but was not published by him and is therefore not as well known as it could be. We discuss it here in some detail.

Let $I$ be a finite set. We denote by $\mathcal{M}(I)$ the set of probability measures on $I$. Given $P \in \mathcal{M}(I)$, we define its *entropy* $H(P)$ by

$$H(P) = -\sum_{i \in I} p_i \log p_i.$$ 

Let $J$ be another finite set. Given a map $f : I \to J$, the *push-forward measure* $fP$ is defined by

$$fP(j) = P(f^{-1}(j))$$

for all $j \in J$.

**Proposition 1.1** (Entropy formulation, Ruzsa). Let $r_1, \ldots, r_n \in \mathbb{Q} \cup \{\infty\} \setminus \{-1\}$.

The following are equivalent:

(i) $\neg SD(r_1, \ldots, r_n; \alpha)$,

(ii) there exists a finite set $G \subset \mathbb{R}^2$ such that $\pi_{-1}$ is injective on $G$ and $P \in \mathcal{M}(G)$ such that

$$\frac{H(P)}{\max_j \{H(\pi_{r_j}P)\}} \geq \alpha.$$ 

Proof. (ii)$\Rightarrow$(i): We will use without proof the fact that the sums-differences problem is independent of the choice of underlying vector space, i.e., instead of $G \subset \mathbb{R}^2$ one can equivalently consider $G \subset V^2$ for any vector space $V$. The reason for this is that one can re-formulate sums-differences as a purely graph-theoretical problem; see [2].

Suppose we are given a finite set $G \subset \mathbb{R}^2$ such that $\pi_{-1}$ is injective on $G$ and $P \in \mathcal{M}(G)$ such that (2) holds. For every $\epsilon > 0$, we will construct an explicit $G' \subset (\mathbb{R}^M)^2$ for some large $M$ such that $\pi_{-1}$ is injective on $G'$ and such that

$$\alpha' := \frac{\log |G'|}{\max_j \{\log |\pi_{r_j}(G')|\}} > \alpha - \epsilon.$$ 

Taking $\epsilon \to 0$ then proves $\neg SD(r_1, \ldots, r_n; \alpha)$.

The basic idea of our construction is that we can approximate any $P$ by a multinomial distribution that arises from appropriately binning uniform measure on a large underlying set.

Let $\delta > 0$. For all $g \in G$, we can find a rational number $q_g$ such that $|q_g - P(g)| < \delta$. We may arrange that $\sum_g q_g = 1$. Let $M$ denote the largest denominator appearing in the collection $\{q_g\}_g$ after maximal reduction. Let $k_g$ denote the positive integer $q_g M$. We define $G' \subset (\mathbb{R}^M)^2$ by

$$G' = \left\{ \left( \left( g_1(1), \ldots, g_M(1) \right), \left( g_1(2), \ldots, g_M(2) \right) \right) \in (\mathbb{R}^M)^2 : g_i = (g_i(1), g_i(2)) \in G, \forall i \land |\{i : g_i = g\}| = k_g, \forall g \in G \right\},$$

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use
and observe that

$$|G'| = \frac{M!}{\prod_{g \in G} k_g!}.$$ 

It is easy to check that

$$\pi_{r_j}(G') = \left\{(\nu_1, \ldots, \nu_M) \in \mathbb{R}^M : \nu_i \in \pi_{r_j}(G), \forall i \land |\{i : \nu_i = \nu\}| = \sum_{g \in \pi_{r_j}^{-1}(\nu)} k_g, \forall \nu \in \pi_{r_j}(G) \right\},$$

and so

$$|\pi_{r_j}(G')| = \frac{M!}{\prod_{\nu \in \pi_{r_j}(G)} \left(\sum_{g \in \pi_{r_j}^{-1}(\nu)} k_g\right)!}.$$ 

In particular, $|\pi_{-1}(G)| = |G|$ implies $|\pi_{-1}(G')| = |G'|$. We now have everything to compute

$$\alpha' = \frac{\log |G'|}{\log \{\log |\pi_{r_j}(G')|\}} = \frac{\log(M!) - \sum_{g \in G} \log(k_g!)}{\max_j \left\{\log(M!) - \sum_{\nu \in \pi_{r_j}(G)} \log \left(\left(\sum_{g \in \pi_{r_j}^{-1}(\nu)} k_g\right)\right)\right\}}.$$ 

The key fact that (asymptotically) relates combinatorics to entropy is Stirling’s formula: $\log(N!) = N \log(N/e) + O(\log N)$. Introducing $\psi(x) = -x \log x$, we obtain

$$\alpha' = \frac{-\sum_{g \in G} \psi \left(\frac{k_g}{M}\right)}{\max_j \left\{\sum_{\nu \in \pi_{r_j}(G)} \psi \left(\sum_{g \in \pi_{r_j}^{-1}(\nu)} \frac{k_g}{M}\right)\right\}} + o(1).$$ 

Since $k_g/M = q_g$ can be made arbitrarily close to $P(g)$, $\alpha'$ follows.

(i)$\implies$(ii): This direction is easy: Take $P$ to be a uniform measure on the finite set $\tilde{G} \subset \mathbb{R}^2$ provided by $\sim SD(r_1, \ldots, r_n; \alpha)$. Then, $H(P) = \log(|G|)$. By Jensen’s inequality, $H(\pi_{r_j} P) \leq \log(|\pi_{r_j}|)$ and so

$$\frac{H(P)}{\max_j \{H(\pi_{r_j} P)\}} \geq \frac{\log(|G|)}{\max_j \{\log(|\pi_{r_j}|)\}} \leq \alpha.'$$

\[\square\]

Ruzsa’s counterexample. The following classical construction is due to Ruzsa. It yields $\sim SD(0, 1, \infty; \log(27)/\log(27/4))$ and was the best known counterexample in that case so far. Let

$$G = \left\{(0, 1), (1, 0), (1, 1)\right\}$$

and note that $|\pi_{-1}(G)| = |G| = 3$. Let $P$ be a uniform probability measure on $G$, i.e., $P$ assigns probability $1/3$ to each element of $G$. Then, an easy computation shows

$$\frac{H(P)}{\max_j \{H(\pi_{r_j} P)\}} = \frac{\log(27)}{\log(27/4)}.$$ 

By Proposition 1.1 this implies $\sim SD(0, 1, \infty; \log(27)/\log(27/4)).$
2. Results

To motivate our first result, let us compare Ruzsa’s $\frac{\log(27)}{\log(27/4)} \approx 1.726$ with $11/6 \approx 1.833$, the smallest value of $\alpha$ for which $SD(0, 1, \infty; \alpha)$ is known to hold $[3]$. There is a gap of size $\approx 0.1$ between these two values. Since improvements over Ruzsa’s counterexample were elusive, it was believed that $SD(0, 1, \infty; \alpha)$ could hold for all $\alpha > \frac{\log(27)}{\log(27/4)}$.

Theorem 2.1. There exists $\alpha > 1.77898$, such that $\neg SD(0, 1, \infty, \alpha)$.

This manages to close about half of the 0.1 gap. The value of 1.77898 is obtained by numerical non-linear maximization, which is notorious for getting stuck in local extrema. Thus, it is not clear that this value is best possible.

We also have

Theorem 2.2. There exists $\alpha > 1.61226$, such that $\neg SD(0, 1, 2, \infty, \alpha)$.

The number 1.61226 is to be compared with 7/4, the smallest value of $\alpha$ for which $SD(0, 1, 2, \infty; \alpha)$ is known to hold $[3]$.

The main idea. To explain our approach, it is instructive to consider a simple modification of Ruzsa’s construction that already yields $\neg SD(0, 1, \infty, \alpha)$ with an explicit $\alpha$ satisfying $\alpha \approx 1.773$. We will see that choosing a (particular) non-uniform $P$ is what enables us to improve over Ruzsa’s original counterexample, which featured uniform measure. Let

$$G = \left\{ (0, 1), (1, 0), (1, 1), (2, 0) \right\}$$

and note that $|\pi^{-1}(G)| = |G| = 4$. According to Proposition 1.1, we can consider any probability measure $P = (p_1, p_2, p_3, 1 - p_1 - p_2 - p_3)$ on $G$.

Introducing the functions

$$\psi(x) = -x \log x, \quad \phi(x) = \psi(x) + \psi(1 - x)$$

the entropies can be written as

$$H(P) = \psi(p_1) + \psi(p_2) + \psi(p_3) + \psi(1 - p_1 - p_2 - p_3),$$

$$H(\pi_0 P) = \psi(p_2 + p_3) + \psi(p_1) + \psi(1 - p_1 - p_2 - p_3),$$

$$H(\pi_1 P) = \phi(p_1 + p_2),$$

$$H(\pi_\infty P) = \phi(p_1 + p_3).$$

We aim to find the values of $p_1, p_2, p_3$ that maximize

$$\alpha(P) = \min_{j=0,1,\infty} \frac{H(P)}{H(\pi_j P)}.$$

The minimum renders this non-differentiable and prevents it from being a calculus problem. From symmetry and convexity considerations, it is sensible to set

$$H(\pi_0 P) = H(\pi_1 P) = H(\pi_\infty P).$$

Elementary computation then yields

$$p_3 = p_2, \quad p_2 = 1/2 - p_1, \quad \log(2) = \psi(1 - 2p_1) + 2\psi(p_1)$$
which uniquely determine $p_1, p_2, p_3$ and thus $\alpha$. The numerical values are $p_1 \approx .1135$, $p_2 = p_3 \approx .3865$ and $\alpha \approx 1.773$.

**Proofs.** We now give the counterexamples that prove Theorems 2.1 and 2.2.

**Proof of Theorem 2.1** We consider

$$G = \left\{ \left( 0, 1 \right), \left( 1, 1 \right), \left( 1, 0 \right), \left( 2, 0 \right), \left( 2, -1 \right), \left( 3, -1 \right), \left( 3, -2 \right) \right\}.$$  

Note that $|\pi^{-1}(G)| = |G|$. If we denote $P = (p_1, \ldots, p_7)$, we can set $p_7 = p_1, p_6 = p_2, p_5 = p_3$ to ensure that $H(\pi_0 P) = H(\pi_\infty P)$. By numerical maximization of $H(P)$

$$\max\{H(\pi_0 P), H(\pi_1 P)\},$$

we find that the choice $p_1 \approx .00024983, p_2 \approx .028156, p_3 \approx .22425$ together with Proposition 1.1 imply Theorem 2.1. \hfill \Box

**Remark 2.3.** It is noteworthy that, when one adds the points $(4, -2), (4, -3)$ to $G$ and sets $p_i = p_{i-1}$ for all $i$, one does not obtain a better value of $\alpha$, at least on the level of numerics.

**Proof of Theorem 2.2** We consider

$$G = \left\{ \left( 0, 1 \right), \left( 1, 0 \right), \left( 2, -1 \right), \left( 1, \frac{1}{2} \right) \right\}.$$  

Note that $|\pi^{-1}(G)| = |G|$. Setting $p_1 = p_2 = p_3 = p_4 = \ldots = p$ ensures

$$H(\pi_1 P) = H(\pi_\infty P), \quad H(\pi_0 P) = H(\pi_2 P).$$

Furthermore, we suppose that $H(\pi_1 P) = H(\pi_0 P)$ or equivalently

$$2\psi(2p)) + \psi(1 - 4p) = \psi(1 - 2p) + 2\psi(p)$$

with $\psi$ as in (4). This has a unique non-zero solution which satisfies $p \approx .21798$. By Proposition 1.1, Theorem 2.2 follows. \hfill \Box

**Acknowledgement**

The author wishes to thank Nets Katz for encouragement and advice.

**References**


Department of Mathematics MC 253-37, California Institute of Technology, Pasadena, California 91125

E-mail address: mlemm@caltech.edu