

Sums of dilates over groups of prime order

David Conlon* Jeck Lim†

Abstract

For p prime, $A \subseteq \mathbb{Z}/p\mathbb{Z}$ and $\lambda \in \mathbb{Z}$, the sum of dilates $A + \lambda \cdot A$ is defined by

$$A + \lambda \cdot A = \{a + \lambda a' : a, a' \in A\}.$$

The basic problem on such sums of dilates asks for the minimum size of $|A + \lambda \cdot A|$ for given λ , A of given density α and p tending to infinity. We investigate this problem for α fixed and λ tending to infinity, proving near-optimal bounds in this case.

1 Introduction

Given subsets A and B of an abelian group G , their sumset $A + B$ is given by

$$A + B = \{a + b : a \in A, b \in B\}.$$

The difference set $A - B$ is defined similarly with subtraction replacing addition.

If $G = \mathbb{Z}$, then it is a simple exercise to show that $|A + B| \geq |A| + |B| - 1$. Indeed, if we order the elements of A as $a_1 < a_2 < \dots < a_s$ and B as $b_1 < b_2 < \dots < b_t$, then $A + B$ contains the elements

$$a_1 + b_1 < a_1 + b_2 < \dots < a_1 + b_t < a_2 + b_1 < \dots < a_s + b_t,$$

so we have at least $|A| + |B| - 1$ distinct elements. If we work instead over $G = \mathbb{Z}/p\mathbb{Z}$ with p prime, the corresponding inequality, known as the Cauchy–Davenport theorem [5, 10], says that

$$|A + B| \geq \min\{|A| + |B| - 1, p\},$$

since one must account for the possibility that the sumset contains all the elements of $\mathbb{Z}/p\mathbb{Z}$. Several proofs of this inequality are known (see, for example, [1]), but, unlike the integer case, none of them is particularly simple.

Our concern in this paper will be with sumsets of a particular type. Given a subset A of an abelian group G and $\lambda \in \mathbb{Z}$, let

$$A + \lambda \cdot A = \{a + \lambda a' : a, a' \in A\}.$$

*Department of Mathematics, Caltech, Pasadena, CA 91125, USA. Email: dconlon@caltech.edu. Research supported by NSF Awards DMS-2054452 and DMS-2348859.

†Department of Mathematics, Caltech, Pasadena, CA 91125, USA. Email: jlim@caltech.edu. Research partially supported by an NUS Overseas Graduate Scholarship.

Such sums of dilates, as they are known, have attracted considerable attention in recent years, with the basic problem asking for an estimate on the minimum size of $|A + \lambda \cdot A|$ given $|A|$. Over the integers, this problem was essentially solved by Bukh [4], who showed that, for any finite set of integers A ,

$$|A + \lambda \cdot A| \geq (|\lambda| + 1)|A| - o(|A|).$$

This result was later tightened by Balogh and Shakan [2], improving the $o(|A|)$ term to a constant C_λ depending only on λ , which is best possible up to the value of C_λ (see also [6, 7, 11, 13, 16] for some earlier work on specific cases and [3, 9, 14, 15, 22] for extensions and variations).

The analogous problem over $\mathbb{Z}/p\mathbb{Z}$ with p prime was first studied in detail by Plagne [17] and by Fiz Pontiveros [12]. For instance, using a rectification argument, which allows one to treat small subsets of $\mathbb{Z}/p\mathbb{Z}$ as though they are sets of integers, the latter showed that for every $\lambda \in \mathbb{Z}$ there exists $\alpha > 0$ such that

$$|A + \lambda \cdot A| \geq (|\lambda| + 1)|A| - C_\lambda$$

for all $|A| \leq \alpha p$. On the other hand, he showed that for every $\lambda \in \mathbb{Z}$ and $\epsilon > 0$ there exists $\delta > 0$ such that, for every sufficiently large prime p , there is a set $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| \geq (\frac{1}{2} - \epsilon)p$ such that $|A + \lambda \cdot A| \leq (1 - \delta)p$. That is, as $|A|$ approaches $p/2$, one cannot do much better than the Cauchy–Davenport theorem, which tells us that $|A + \lambda \cdot A| \geq 2|A| - 1$.

For our purposes, it will be convenient to introduce some terminology. For p prime, $\lambda \in \mathbb{Z}$ and $\alpha \in (0, 1)$, we let

$$\text{ex}(\mathbb{Z}/p\mathbb{Z}, \lambda, \alpha) = \min \{|A + \lambda \cdot A|/p : A \subseteq \mathbb{Z}/p\mathbb{Z}, |A| \geq \alpha p\}$$

and then define $\text{ex}(\lambda, \alpha) = \limsup_p \text{ex}(\mathbb{Z}/p\mathbb{Z}, \lambda, \alpha)$. The problem of asymptotically estimating the minimum size of sums of dilates over $\mathbb{Z}/p\mathbb{Z}$ may then be rephrased as the problem of determining $\text{ex}(\lambda, \alpha)$. This seems very difficult in full generality, though the results of Fiz Pontiveros described above imply that

- $\text{ex}(\lambda, \alpha) = (|\lambda| + 1)\alpha$ for λ fixed and α sufficiently small in terms of λ and
- $\text{ex}(\lambda, \alpha) < 1$ for $\alpha < \frac{1}{2}$.

Here we look at the case where α is fixed and λ is allowed to grow. In rough terms, we wish to understand how small the sum of dilates $A + \lambda \cdot A$ can be if we fix the density α of A and let λ tend to infinity. More precisely, we set $\text{ex}(\alpha) = \limsup_{\lambda \rightarrow \infty} \text{ex}(\lambda, \alpha)$ and investigate the behavior of $\text{ex}(\alpha)$.

By Cauchy–Davenport, if $\alpha \geq \frac{1}{2}$, then $\text{ex}(\alpha) = 1$. Moreover, if $\alpha \leq \frac{1}{2}$, then, again by Cauchy–Davenport, $|A + \lambda \cdot A| \geq 2|A| - 1$, so $\text{ex}(\alpha) \geq 2\alpha$. On the other hand, since $|A + \lambda \cdot A| \leq p$, we always have the trivial upper bound $\text{ex}(\alpha) \leq 1$. Our main result improves these simple bounds significantly, giving a reasonably complete picture of the behavior of $\text{ex}(\alpha)$.

Theorem 1.1. *There exist constants $C, C', c > 0$ such that*

$$e^{C' \log^c(1/\alpha)} \alpha \leq \text{ex}(\alpha) \leq e^{C \sqrt{\log(1/\alpha)}} \alpha$$

for all $\alpha \in (0, \frac{1}{2})$. Moreover, $\text{ex}(\alpha) < 1$ for all $\alpha \in (0, \frac{1}{2})$.

Unlike in the fixed λ case, we cannot improve the trivial upper bound $\text{ex}(\alpha) \leq 1$ by just taking A to be an interval. Instead, what we do is show that $\text{ex}(\alpha)$ is bounded above by a continuous variant defined over the torus $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and then provide an upper bound for that variant. We go straight into the details of this construction, before returning to the lower bound, which makes use of several classical tools from additive combinatorics, in Section 3.

2 The upper bound

Let $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, $n > 1$ be an integer and μ be the Lebesgue measure on $\mathbb{T}^k$ for any positive integer k . Let $\pi_1 : \mathbb{T}^n \rightarrow \mathbb{T}^{n-1}$ be the projection map ignoring the first coordinate and $\pi_n : \mathbb{T}^n \rightarrow \mathbb{T}^{n-1}$ the projection map ignoring the last coordinate. Consider the following problem: given $0 < \alpha < 1$, what is the smallest possible value of $\mu(\pi_1(B) + \pi_n(B))$ over all open sets $B \subseteq \mathbb{T}^n$ with $\mu(B) > \alpha$?

Equivalently, we can ask for the smallest possible value of $\mu(B \times \mathbb{T} + \mathbb{T} \times B)$ over all open sets $B \subseteq \mathbb{T}^n$ with $\mu(B) > \alpha$. In this form, written as a problem about sums of shifts rather than sums of projections, there is a ready analogy with the problem of estimating sums of transcendental dilates, which can also be phrased in terms of sums of shifts and ultimately has bounds of a similar form [8]. This analogy partly motivates the methods we use here for both the upper and lower bounds.

To capture this question more succinctly, we define

$$\text{ex}_T(n, \alpha) = \inf \{ \mu(\pi_1(B) + \pi_n(B)) : B \subseteq \mathbb{T}^n \text{ open, } \mu(B) > \alpha \}$$

and set $\text{ex}_T(\alpha) = \lim_{n \rightarrow \infty} \text{ex}_T(n, \alpha)$. This limit exists since $\text{ex}_T(n, \alpha)$ is decreasing in n . Indeed, if $B \subseteq \mathbb{T}^n$ with $\mu(\pi_1(B) + \pi_n(B)) = \beta$, consider $B' = B \times \mathbb{T} \subseteq \mathbb{T}^{n+1}$. Then $\mu(B') = \mu(B)$ and $\mu(\pi_1(B') + \pi_{n+1}(B')) = \mu(\pi_1(B) \times \mathbb{T} + B) = \mu(\pi_1(B) + \pi_n(B)) = \beta$, so that $\text{ex}_T(n+1, \alpha) \leq \text{ex}_T(n, \alpha)$.

The main result of this section says that $\text{ex}(\alpha) \leq \text{ex}_T(\alpha)$, thereby allowing us to give an upper bound on $\text{ex}(\alpha)$ by instead bounding $\text{ex}_T(\alpha)$. The idea of the proof is to construct an example in $\mathbb{Z}/p\mathbb{Z}$ from one in $\mathbb{T}^n$ by approximating each point of $\mathbb{T}^n$ by a number in $\mathbb{Z}/p\mathbb{Z}$ written in base λ , with each point $(x_1, \dots, x_n) \in \mathbb{T}^n$ roughly corresponding to $\lfloor (x_1 + \frac{x_2}{\lambda} + \dots + \frac{x_n}{\lambda^{n-1}})p \rfloor \in \mathbb{Z}/p\mathbb{Z}$.

Theorem 2.1. $\text{ex}(\alpha) \leq \text{ex}_T(\alpha)$.

Proof. Let $n > 1$ and $B \subseteq \mathbb{T}^n$ be an open set such that $\mu(B) = \alpha' > \alpha$ and $\mu(\pi_1(B) + \pi_n(B)) = \beta$. We will show that $\text{ex}(\alpha) \leq \beta$.

Let $\epsilon > 0$ be arbitrary, λ be a positive integer, $T = \mathbb{Z}/\lambda\mathbb{Z}$ and discretize $\mathbb{T}^n$ into T^n . For $x = (x_1, \dots, x_n) \in T^n$ (with integers $0 \leq x_i < \lambda$ for each i), define $C_x \subseteq \mathbb{T}^n$ to be the cubical box

$$\prod_{i=1}^n \left[\frac{x_i}{\lambda}, \frac{x_i + 1}{\lambda} \right).$$

Let $S = \{x \in T^n \mid C_x \subseteq B\}$ and $B' = \bigcup_{x \in S} C_x \subseteq B$. As $\lambda \rightarrow \infty$, $\mu(B')$ approaches $\mu(B) = \alpha'$ since B is open. Therefore, for λ sufficiently large in terms of ϵ , we have $\mu(B') \geq \alpha' - \epsilon$. For $x \in T^n$, define I_x to be the interval $[y, y + \lambda^{-n})$, where

$$y = \frac{x_1}{\lambda} + \frac{x_2}{\lambda^2} + \dots + \frac{x_n}{\lambda^n}.$$

Set $A = \bigcup_{x \in S} I_x \subseteq \mathbb{T}$. Then $\mu(A) = |S|/\lambda^n = \mu(B') \geq \alpha' - \epsilon$. We claim that

$$\mu(A + \lambda \cdot A) \leq \mu(\pi_1(B') + \pi_n(B')).$$

To see how the theorem follows from this claim, we again discretize $\mathbb{T}$ into $\mathbb{Z}/p\mathbb{Z}$. Set $A' \subseteq \mathbb{Z}/p\mathbb{Z}$ to be $A' = \{0 \leq a < p : [\frac{a}{p}, \frac{a+1}{p}) \subseteq A\}$. By construction, $|A'|/p \leq \mu(A)$. Moreover, since A is a finite union of half-closed intervals, $|A'|/p$ approaches $\mu(A)$ as $p \rightarrow \infty$. Therefore, for p sufficiently large in terms of ϵ , we have $|A'| \geq (\mu(A) - \epsilon)p$. For any $a + \lambda b \in A' + \lambda \cdot A'$ with $a, b \in A'$, we have

$\left[\frac{a}{p}, \frac{a+1}{p}\right) \subseteq A$ and $\frac{b}{p} \in A$. Thus, $\left[\frac{a+\lambda b}{p}, \frac{a+\lambda b+1}{p}\right) \subseteq A + \lambda \cdot A$. Hence, $|A' + \lambda \cdot A'|/p \leq \mu(A + \lambda \cdot A)$. From the claim,

$$\frac{|A' + \lambda \cdot A'|}{p} \leq \mu(A + \lambda \cdot A) \leq \mu(\pi_1(B') + \pi_n(B')) \leq \beta.$$

Since $|A'| \geq (\mu(A) - \epsilon)p \geq (\alpha' - 2\epsilon)p$, taking $\epsilon = \frac{\alpha' - \alpha}{2}$ gives $\text{ex}(\alpha) \leq \beta$, as required.

To prove the claim, let $S' = \pi_1(S) + \pi_n(S) + \{0, 1\}^{n-1}$. Then S' is the set of all $z = (z_1, z_2, \dots, z_{n-1}) \in \mathbb{T}^{n-1}$ with $z_k = a_{k+1} + b_k + \epsilon_k$ for some $a = (a_1, a_2, \dots, a_n), b = (b_1, b_2, \dots, b_n) \in S$ and $\epsilon_k \in \{0, 1\}$ for all k . Since B' is the union of boxes $\bigcup_{x \in S} C_x$, we have that $\pi_1(B') + \pi_n(B')$ is the union of boxes $\bigcup_{x \in S'} C_x$, though now with each $C_x \subseteq \mathbb{T}^{n-1}$. Thus,

$$|S'|/\lambda^{n-1} = \mu(\pi_1(B') + \pi_n(B')).$$

On the other hand, $A + \lambda \cdot A$ consists of all points in $\mathbb{T}$ of the form

$$\frac{b_1 + a_2}{\lambda} + \frac{b_2 + a_3}{\lambda^2} + \dots + \frac{b_{n-1} + a_n}{\lambda^{n-1}} + \frac{b_n}{\lambda^n} + \epsilon,$$

where $a, b \in S$ and $\epsilon \in [0, \lambda^{-n} + \lambda^{-n+1})$. Here, we are viewing a_i and b_i as integers in $[0, \lambda - 1]$, so $b_i + a_{i+1}$ could “overflow”. Nevertheless, each element of $A + \lambda \cdot A$ is of the form

$$\frac{c_1}{\lambda} + \frac{c_2}{\lambda^2} + \dots + \frac{c_{n-1}}{\lambda^{n-1}} + \delta,$$

where $c_i = b_i + a_{i+1} \bmod \lambda$ or $b_i + a_{i+1} + 1 \bmod \lambda$ and $\delta \in [0, \lambda^{-n+1})$. Thus, $A + \lambda \cdot A \subseteq \bigcup_{x \in S'} I_x$, so we have

$$\mu(A + \lambda \cdot A) \leq |S'|/\lambda^{n-1} = \mu(\pi_1(B') + \pi_n(B')),$$

as required. $\square$

We believe that the two functions $\text{ex}(\alpha)$ and $\text{ex}_T(\alpha)$ should in fact be equal, but leave the task of proving that $\text{ex}(\alpha) \geq \text{ex}_T(\alpha)$ as an open problem.

We now give an upper bound for $\text{ex}_T(\alpha)$, and therefore $\text{ex}(\alpha)$, by considering a suitable set $B \subseteq \mathbb{T}^n$.

Theorem 2.2. *For any positive integer d , $\text{ex}_T(\alpha) \leq 2^{d-1}\alpha^{1-1/d}$ for all $\alpha \in (0, 2^{-d})$. In particular, there is a constant $C > 0$ such that $\text{ex}_T(\alpha) \leq e^{C\sqrt{\log(1/\alpha)}}\alpha$ for all $\alpha \in (0, \frac{1}{2})$.*

Proof. If $B = (0, \gamma^{1/d})^d \subseteq \mathbb{T}^d$, then $\mu(B) = \gamma$. Furthermore, $\pi_1(B) = \pi_d(B) = (0, \gamma^{1/d})^{d-1} \subseteq \mathbb{T}^{d-1}$, so we have $\mu(\pi_1(B) + \pi_d(B)) = (2\gamma^{1/d})^{d-1} = 2^{d-1}\gamma^{1-1/d}$. Taking the infimum over all $\gamma > \alpha$ then gives the required upper bound $\text{ex}_T(\alpha) \leq \text{ex}_T(d, \alpha) \leq 2^{d-1}\alpha^{1-1/d}$. To get a general bound independent of d , we simply optimize by setting $d = \sqrt{\log(1/\alpha)}$ and the bound follows. $\square$

Remark. *The constant term 2^{d-1} in Theorem 2.2 is not optimal. For example, for $d = 3$, instead of picking B to be the $\gamma^{1/3} \times \gamma^{1/3} \times \gamma^{1/3}$ box, we could optimize the side lengths of the box by picking B to be $(2\gamma)^{1/3} \times (\gamma/4)^{1/3} \times (2\gamma)^{1/3}$. This yields $\mu(\pi_1(B) + \pi_3(B)) = \frac{9}{2^{4/3}}\gamma^{2/3}$, where we note that $\frac{9}{2^{4/3}} < 2^2$. We made no attempt to optimize these constants for higher values of d , as any improvement would not change the form of the bound $e^{C\sqrt{\log(1/\alpha)}}\alpha$.*

While Theorem 2.2 proves the first upper bound in Theorem 1.1, the following result proves the second upper bound $\text{ex}(\alpha) < 1$.

Theorem 2.3. $\text{ex}_T(\alpha) < 1$ for all $\alpha \in (0, \frac{1}{2})$.

Proof. Let n be sufficiently large and set $B = \{x \in \mathbb{T}^n : x_i > 0 \text{ for all } i, \sum_{i=1}^n x_i < \frac{n}{2} - 1\}$, where x_i is considered an element of $[0, 1)$ for all i . As $n \rightarrow \infty$, $\mu(B) \rightarrow \frac{1}{2}$, since, if $x \in \mathbb{T}^n$ is picked uniformly randomly, $\sum x_i$ is approximately normal with mean $\frac{n}{2}$ and variance $\Theta(n)$. Thus, for sufficiently large n , $\alpha < \mu(B) < \frac{1}{2}$. Fix such an n . Now both $\pi_1(B)$ and $\pi_n(B)$ are contained in the set $C = \{x \in \mathbb{T}^{n-1} : \sum_{i=1}^{n-1} x_i < \frac{n}{2} - 1\}$, so

$$\pi_1(B) + \pi_n(B) \subseteq C + C = \{x \in \mathbb{T}^{n-1} : \sum_{i=1}^{n-1} x_i < n - 2\} \subsetneq \mathbb{T}^{n-1}.$$

Hence, $\mu(\pi_1(B) + \pi_n(B)) < 1$, so that $\text{ex}_T(\alpha) \leq \text{ex}_T(n, \alpha) < 1$. $\square$

3 The lower bound

We now prove the lower bound in Theorem 1.1, which we restate as follows. As prefaced in the previous section, the proof of this result makes use of ideas similar to those used in [20] for studying sums of transcendental dilates.

Theorem 3.1. *There are constants $C', c > 0$ such that $\text{ex}(\alpha) \geq e^{C' \log^c(1/\alpha)} \alpha$ for all $\alpha \in (0, 1/2)$. In particular, one may take $c = \frac{1}{7}$.*

In what follows, as well as the notation $\lambda \cdot B = \{\lambda b : b \in B\}$ for dilates, we will use mB to denote the m -fold sumset

$$mB = \underbrace{B + B + \cdots + B}_{m \text{ times}}.$$

Before proving Theorem 3.1, we require the following result, a variant of the Plünnecke–Ruzsa inequality [18], which states that if A, B are finite subsets of an abelian group with $|A + B| \leq K|A|$, then $|mB - nB| \leq K^{m+n}|A|$. In particular, if $|B + B| \leq K|B|$, then $|mB| \leq K^m|B|$. Our result is a version of this latter inequality allowing for dilates of each term.

Lemma 3.2. *Let B be a finite subset of an abelian group, λ an integer and $K > 0$ such that $|B + \lambda \cdot B| \leq K|B|$. Then, for any positive integer l ,*

$$|B + \lambda \cdot B + \lambda^2 \cdot B + \cdots + \lambda^l \cdot B| \leq K^{7l-6}|B|.$$

Proof. The sum version of Ruzsa’s triangle inequality [19] states that, for any finite subsets X, Y, Z of an abelian group,

$$|X||Y + Z| \leq |X + Y||X + Z|.$$

Taking $X = \lambda \cdot B$, $Y = Z = B$ and noting that $|\lambda \cdot B| = |B|$, we have $|B + B| \leq K^2|B|$. Hence, by the Plünnecke–Ruzsa inequality, $|B + B + B| \leq K^6|B|$. Thus, another application of Ruzsa’s triangle inequality (with $X = B$, $Y = B + B$, $Z = \lambda \cdot B$) yields

$$|B + B + \lambda \cdot B| \leq |B + B + B||B + \lambda \cdot B|/|B| \leq K^7|B|.$$

We prove the lemma by induction on l , noting that the case $l = 1$ follows from the given assumption. Suppose now that we have

$$|B + \lambda \cdot B + \lambda^2 \cdot B + \cdots + \lambda^l \cdot B| \leq K^{7l-6}|B|$$

for some l and we wish to prove it for $l + 1$. Yet another application of Ruzsa's triangle inequality (with $X = \lambda^l \cdot B$, $Y = B + \lambda \cdot B + \cdots + \lambda^{l-1} \cdot B$, $Z = \lambda^l \cdot B + \lambda^{l+1} \cdot B$) yields

$$\begin{aligned} |B + \lambda \cdot B + \cdots + \lambda^{l+1} \cdot B| &\leq |B + \lambda \cdot B + \cdots + \lambda^l \cdot B| |\lambda^l \cdot B + \lambda^l \cdot B + \lambda^{l+1} \cdot B| / |B| \\ &\leq K^{7l-6} |\lambda^l \cdot B + \lambda^l \cdot B + \lambda^{l+1} \cdot B| \\ &= K^{7l-6} |B + B + \lambda \cdot B| \\ &\leq K^{7(l+1)-6} |B|, \end{aligned}$$

as required. $\square$

The other thing that we need for the proof of Theorem 3.1 is Sanders' quantitative version of the Bogolyubov–Ruzsa lemma [21, Theorem 1.1], which states that if A is a finite subset of an abelian group with $|A + A| \leq K|A|$, then $2A - 2A$ contains a proper generalized arithmetic progression P of dimension $d \leq d_0(K) \leq C \log^6 K$ and size at least $C_1(K)|A|$, where C is an absolute constant. Here a generalized arithmetic progression P of dimension d is a set of the form

$$P = \{a + \sum_{i=1}^d n_i v_i : 0 \leq n_i \leq k_i - 1 \text{ for all } i\}$$

and such a generalized arithmetic progression is proper if all of its elements are distinct, that is, if $|P| = k_1 k_2 \cdots k_d$.

Proof of Theorem 3.1. Fix $\alpha \in (0, 1/2)$ and let $K = 2 \operatorname{ex}(\alpha)/\alpha$. Let λ be sufficiently large and p be sufficiently large in terms of λ . Let $A \subseteq \mathbb{Z}/p\mathbb{Z}$, which we may assume has size $|A| = \alpha p$, be such that $|A + \lambda \cdot A| \leq 2 \operatorname{ex}(\alpha)p = K|A|$. By Ruzsa's triangle inequality, we again have $|A + A| \leq K^2|A|$. Hence, by Sanders' quantitative version of the Bogolyubov–Ruzsa lemma, $2A - 2A$ contains a proper generalized arithmetic progression P of dimension $d \leq d_0(K) \leq C \log^6 K$ and size at least $C_1(K)\alpha p$, where C is an absolute constant. By the Plünnecke–Ruzsa inequality, we have $|2A - 2A + 2A - 2A| \leq K^{16}|A|$. By Ruzsa's triangle inequality (with $X = A$, $Y = 2A - 2A + A - 2A$, $Z = \lambda \cdot A$), we have

$$|2A - 2A + A - 2A + \lambda \cdot A| \leq |2A - 2A + 2A - 2A| |A + \lambda \cdot A| / |A| \leq K^{17}|A|.$$

Repeating three more times, each time replacing an appropriate A term with $\lambda \cdot A$, we get

$$|(2A - 2A) + \lambda \cdot (2A - 2A)| \leq K^{20}|A|.$$

By Lemma 3.2 applied to $2A - 2A$, we then have that,

$$|(2A - 2A) + \lambda \cdot (2A - 2A) + \cdots + \lambda^d \cdot (2A - 2A)| \leq K^{140d}|A|.$$

Suppose $P = v_0 + P_0$ for some $v_0 \in \mathbb{Z}/p\mathbb{Z}$ and P_0 a proper Minkowski sum of d arithmetic progressions $\{0, v_i, 2v_i, \dots, (k_i - 1)v_i\}$, $i = 1, \dots, d$, with $|P| = |P_0| = k_1 k_2 \cdots k_d$ and $k_1 \geq k_2 \geq \cdots \geq k_d$. Let $m \leq d$ be the largest integer with $k_m \geq \lambda$. Since $|P_0| \geq \lambda^d$ for sufficiently large

p , we have $m \geq 1$. Let $P' = \sum_{i=1}^m \{0, v_i, 2v_i, \dots, (k_i - 1)v_i\}$. Then this is a proper sum with $|P'| \geq |P_0|/\lambda^{d-m}$. Since $k_1 \geq \dots \geq k_m \geq \lambda$, we have that,

$$P' + \lambda \cdot P' + \lambda^2 \cdot P' + \dots + \lambda^d \cdot P' \supseteq \sum_{i=1}^m \{0, v_i, 2v_i, \dots, \lambda^d(k_i - 1)v_i\} = \lambda^d P'.$$

By repeated application of the Cauchy–Davenport theorem, we have that

$$|\lambda^d P'| \geq \min(\lambda^d |P'| - \lambda^d + 1, p) \geq \min(\lambda^m C_1 \alpha p - \lambda^d + 1, p) = p$$

for λ large enough that $\lambda C_1 \alpha \geq 2$ and p sufficiently large. Thus, $P' + \lambda \cdot P' + \lambda^2 \cdot P' + \dots + \lambda^d \cdot P' = \mathbb{Z}/p\mathbb{Z}$. On the other hand,

$$\begin{aligned} & |P' + \lambda \cdot P' + \lambda^2 \cdot P' + \dots + \lambda^d \cdot P'| \\ & \leq |P + \lambda \cdot P + \lambda^2 \cdot P + \dots + \lambda^d \cdot P| \\ & \leq |(2A - 2A) + \lambda \cdot (2A - 2A) + \lambda^2 \cdot (2A - 2A) + \dots + \lambda^d \cdot (2A - 2A)| \\ & \leq K^{140d} |A| \leq K^{140d_0} |A|. \end{aligned}$$

This implies that $K^{140d_0} \alpha \geq 1$. From $d_0 \leq C \log^6 K$, we obtain $e^{140C \log^7 K} \alpha \geq 1$, which implies that

$$\text{ex}(\alpha) = K\alpha/2 \geq e^{C'(\log \frac{1}{\alpha})^c} \alpha$$

for some absolute constants c and C' , where one may take $c = \frac{1}{7}$. $\square$

If one could show that the Bogolyubov–Ruzsa lemma holds with $d_0(K) \leq C \log K$, which would be best possible, then we could take $c = \frac{1}{2}$, matching our upper bound.

To close, let us mention a variant of the problem we have studied, namely, that of estimating the minimum size of $|A + \dots + A + \lambda \cdot A|$ over all $A \subseteq \mathbb{Z}/p\mathbb{Z}$ of given size. If there are k summands, we can again study the asymptotic behaviour of this minimum by considering

$$\text{ex}(k, \lambda, \alpha) = \limsup_{p \rightarrow \infty} \min \left\{ \underbrace{|A + \dots + A + \lambda \cdot A|}_{k-1 \text{ times}}/p : A \subseteq \mathbb{Z}/p\mathbb{Z}, |A| \geq \alpha p \right\}.$$

As a possible extension of his result that $\text{ex}(\lambda, \alpha) < 1$ for $\alpha < \frac{1}{2}$, Fiz Pontiveros [12, Conjecture 1.3] conjectured that $\text{ex}(k, \lambda, \alpha) < 1$ for $\alpha < \frac{1}{k}$. However, this is easily seen to be false. Indeed, a simple consequence of the proof of Theorem 3.1 is that, provided k is sufficiently large, $|A + \lambda \cdot A| \geq 10|A|$ for all $A \subseteq \mathbb{Z}/p\mathbb{Z}$ with $|A| = \lceil p/(k+1) \rceil$ and all λ sufficiently large in terms of k . But then, by repeated application of the Cauchy–Davenport inequality, $|A + \dots + A + \lambda \cdot A| \geq \min\{(k+8)|A| - (k-2), p\} = p$. In particular, $\text{ex}(k, \lambda, \alpha) = 1$ for $\alpha \geq 1/(k+1)$ and λ sufficiently large in terms of k . This bound on the minimum α such that $\text{ex}(k, \lambda, \alpha) = 1$ for λ sufficiently large in terms of k can certainly be improved, though we have made no serious attempt to do so here. Instead, we leave it as an open problem to give more precise estimates on how this threshold changes with k .

References

- [1] N. Alon, M. B. Nathanson and I. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer. Math. Monthly* **102** (1995), 250–255.
- [2] A. Balog and G. Shakan, On the sum of dilations of a set, *Acta Arith.* **164** (2014), 153–162.
- [3] A. Balog and G. Shakan, Sum of dilates in vector spaces, *North-West. Eur. J. Math.* **1** (2015), 46–54.
- [4] B. Bukh, Sums of dilates, *Combin. Probab. Comput.* **17** (2008), 627–639.
- [5] A. L. Cauchy, Recherches sur les nombres, *J. École Polytech.* **9** (1813), 99–116.
- [6] J. Cilleruelo, Y. O. Hamidoune and O. Serra, On sums of dilates, *Combin. Probab. Comput.* **18** (2009), 871–880.
- [7] J. Cilleruelo, M. Silva and C. Vinuesa, A sumset problem, *J. Comb. Number Theory* **2** (2010), 79–89.
- [8] D. Conlon and J. Lim, Sums of transcendental dilates, *Bull. London Math. Soc.* **55** (2023), 2400–2406.
- [9] D. Conlon and J. Lim, Sums of linear transformations, preprint available at arXiv:2203.09827 [math.CO].
- [10] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.
- [11] S.-S. Du, H.-Q. Cao and Z.-W. Sun, On a sumset problem for integers, *Electron. J. Combin.* **21** (2014), Paper 1.13, 25pp.
- [12] G. Fiz Pontiveros, Sum of dilates in $\mathbb{Z}_p$, *Combin. Probab. Comput.* **22** (2013), 282–293.
- [13] Y. O. Hamidoune and J. Rué, A lower bound for the size of a Minkowski sum of dilates, *Combin. Probab. Comput.* **20** (2011), 249–256.
- [14] M. Huicochea, On the sum of dilates in $\mathbb{R}^d$, *North-West. Eur. J. Math.* **7** (2021), 7–27.
- [15] D. Krachun and F. Petrov, On the size of $A + \lambda A$ for algebraic λ , *Mosc. J. Comb. Number Theory* **12** (2023), 117–126.
- [16] Z. Ljujić, A lower bound for the size of a sum of dilates, *J. Comb. Number Theory* **5** (2013), 31–51.
- [17] A. Plagne, Sums of dilates in groups of prime order, *Combin. Probab. Comput.* **20** (2011), 867–873.
- [18] I. Z. Ruzsa, An application of graph theory to additive number theory, *Sci. Ser. A Math. Sci.* **3** (1989), 97–109.
- [19] I. Z. Ruzsa, Sums of finite sets, in *Number theory* (New York, 1991–1995), 281–293, Springer, New York, 1996.

- [20] T. Sanders, Appendix to “Roth’s theorem on progressions revisited” by J. Bourgain, *J. Anal. Math.* **104** (2008), 193–206.
- [21] T. Sanders, On the Bogolyubov–Ruzsa lemma, *Anal. PDE* **5** (2012), 627–655.
- [22] G. Shakan, Sum of many dilates, *Combin. Probab. Comput.* **25** (2016), 460–469.