Sums of linear transformations

David Conlon* Jeck Lim†

Abstract

We show that if $\mathcal{L}_1$ and $\mathcal{L}_2$ are linear transformations from $\mathbb{Z}^d$ to $\mathbb{Z}^d$ satisfying certain mild conditions, then, for any finite subset A of $\mathbb{Z}^d$,

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d}\right)^d |A| - o(|A|).$$

This result corrects and confirms the two-summand case of a conjecture of Bukh and is best possible up to the lower-order term for many choices of $\mathcal{L}_1$ and $\mathcal{L}_2$. As an application, we prove a lower bound for $|A + \lambda \cdot A|$ when A is a finite set of real numbers and λ is an algebraic number. In particular, when λ is of the form $(p/q)^{1/d}$ for some $p, q, d \in \mathbb{N}$, each taken as small as possible for such a representation, we show that

$$|A + \lambda \cdot A| \geq (p^{1/d} + q^{1/d})^d |A| - o(|A|).$$

This is again best possible up to the lower-order term and extends a recent result of Krachun and Petrov which treated the case $\lambda = \sqrt{2}$.

1 Introduction

For any subset A of a commutative ring R (or, more generally, an R-module M) and any elements $\lambda_1, \dots, \lambda_k$ of R, let

$$\lambda_1 \cdot A + \cdots + \lambda_k \cdot A = \{\lambda_1 a_1 + \cdots + \lambda_k a_k : a_1, \dots, a_k \in A\}.$$

Such sums of dilates have attracted considerable attention in recent years, with the basic problem asking for an estimate on the minimum size of $|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ given $|A|$. Over the integers, this problem was essentially solved by Bukh [6], who showed that if $\lambda_1, \dots, \lambda_k$ are coprime integers, then, for any finite set of integers A,

$$|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq (|\lambda_1| + \cdots + |\lambda_k|)|A| - o(|A|),$$

which is best possible up to the lower-order term. This result was later tightened by Balogh and Shakan [1] when $k = 2$ and then Shakan [28] in the general case, improving the $o(|A|)$ term to a constant depending only on $\lambda_1, \dots, \lambda_k$ (see also [8, 9, 11, 16, 20] for some earlier work on specific cases).

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

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

Our principal concern here will be with generalisations of these results to higher dimensions. One possible direction is to again look at sums of dilates (see, for example, [2, 10, 17, 21, 22, 23]). However, we will be concerned with a generalisation of a different kind, encapsulated in the following conjecture of Bukh. This conjecture first appeared on Bukh's webpage, but has since been reiterated by several other authors [19, 21, 28].

Conjecture 1.1. *Suppose that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ have no common non-trivial invariant subspace and $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq (|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d})^d |A| - o(|A|).$$

The intuition behind this conjecture comes from the Brunn–Minkowski inequality (see, for example, [13]). This classic inequality states that if A and B are two non-empty compact subsets of $\mathbb{R}^d$, then

$$\mu(A+B)^{1/d} \geq \mu(A)^{1/d} + \mu(B)^{1/d},$$

where μ is the Lebesgue measure on $\mathbb{R}^d$. Since $\mu(\mathcal{L}A) = |\det(\mathcal{L})|\mu(A)$ for any $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{R})$ and any measurable subset A of $\mathbb{R}^d$, we may conclude that, for any $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{R})$,

$$\mu(\mathcal{L}_1 A + \mathcal{L}_2 A) \geq (\mu(\mathcal{L}_1 A)^{1/d} + \mu(\mathcal{L}_2 A)^{1/d})^d \geq (|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d})^d \mu(A).$$

Moreover, the analogous statement holds for the sum of more transformations by a simple induction. Conjecture 1.1 is then the statement that, under appropriate technical conditions, a discrete analogue of this result should hold, possibly with some correction term to deal with boundary effects.

The first result towards this conjecture was given by Mudgal [21], who showed that if $\mathcal{L} \in GL_2(\mathbb{R})$ has no real eigenvalues, then $|A + \mathcal{L}A| \geq 4|A| - o(|A|)$ for any finite subset A of $\mathbb{R}^2$. In particular, this confirms Conjecture 1.1 when $k = d = 2$, $\mathcal{L}_1$ is the identity and $|\det(\mathcal{L}_2)| = 1$.[1] Surprisingly, despite this success, it turns out that Bukh's conjecture is not quite correct and both conditions, that $\mathcal{L}_1, \dots, \mathcal{L}_k$ have no common non-trivial invariant subspace and that $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$, need modification.

The first condition, that $\mathcal{L}_1, \dots, \mathcal{L}_k$ have no common non-trivial invariant subspace is clearly necessary, since otherwise, for subsets A of such a common invariant subspace, the problem reduces to one of lower dimension. However, this is not the only case where the problem can reduce to one of lower dimension. For instance, a simple concrete example where this can happen is when $d = k = 2$ and both $\mathcal{L}_1$ and $\mathcal{L}_2$ are anti-clockwise rotations about the origin by $\pi/2$. Indeed, even though $|\det(\mathcal{L}_1)| = |\det(\mathcal{L}_2)| = 1$, so that the conjecture predicts that $|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq 4|A| - o(|A|)$, we only have $|\mathcal{L}_1 A + \mathcal{L}_2 A| = 2|A| - 1$ when $A = \{(0, x) \mid x \in [n]\}$. In order to rule out such examples, we update Bukh's condition as follows.

Definition 1.2. We say that $\mathcal{L}_1, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are *irreducible* if there are no non-trivial subspaces U, V of $\mathbb{Q}^d$ of the same dimension such that $\mathcal{L}_i U \subseteq V$ for all i.

To reiterate the point, this condition is clearly necessary, since otherwise we may restrict A and the $\mathcal{L}_i$ to U, again reducing the problem to one of lower dimension.

[1] There is a caveat here, which is that Mudgal's result, which applies to arbitrary subsets of $\mathbb{R}^2$, requires that $\mathcal{L}$ have no non-trivial invariant subspace over $\mathbb{R}$. Our interpretation of Bukh's conjecture, which concerns subsets of $\mathbb{Z}^d$ (or $\mathbb{Q}^d$), is that there is instead no non-trivial invariant subspace over $\mathbb{Q}$.

Consider now the transformations

$$\mathcal{L}_1 = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathcal{L}_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}.$$

It is easily checked that $\mathcal{L}_1$ and $\mathcal{L}_2$ are irreducible and that $\mathcal{L}_1\mathbb{Z}^2 + \mathcal{L}_2\mathbb{Z}^2 = \mathbb{Z}^2$. However, the set $A = \{(x, 2y) \mid x, y \in [n]\}$ has $|A| = n^2$ and $|\mathcal{L}_1 A + \mathcal{L}_2 A| = (2n-1)^2 \sim 4|A|$, giving another counterexample to Conjecture 1.1, which predicts that $|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq 8|A| - o(|A|)$.

The issue here is that $\mathcal{L}_1$ and $\mathcal{L}_2$ have a "common right factor" with determinant of absolute value > 1. On the other hand, Bukh's condition that $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$ is equivalent to $\mathcal{L}_1, \ldots, \mathcal{L}_k$ not having a "common left factor" with determinant of absolute value > 1. Indeed, if $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = L \subsetneq \mathbb{Z}^d$, then there is some $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ with determinant of absolute value > 1 such that $\mathcal{P}\mathbb{Z}^d \supseteq L$, which implies that $\mathcal{P}^{-1}\mathcal{L}_i\mathbb{Z}^d \subseteq \mathbb{Z}^d$ and so $\mathcal{P}^{-1}\mathcal{L}_i \in \mathrm{Mat}_d(\mathbb{Z})$ for all i. Conversely, if there is some $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ with determinant of absolute value > 1 such that $\mathcal{P}^{-1}\mathcal{L}_i \in \mathrm{Mat}_d(\mathbb{Z})$ for all i, then $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d \subseteq \mathcal{P}\mathbb{Z}^d \subsetneq \mathbb{Z}^d$. Our second condition incorporates and generalises both of these possibilities.

Definition 1.3. We say that $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are *coprime* if there are no $\mathcal{P}, \mathcal{Q} \in \mathrm{GL}_d(\mathbb{Q})$ with $0 < |\det(\mathcal{P})\det(\mathcal{Q})| < 1$ such that

$$\mathcal{P}\mathcal{L}_1\mathcal{Q}, \mathcal{P}\mathcal{L}_2\mathcal{Q}, \ldots, \mathcal{P}\mathcal{L}_k\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z}).$$

In particular, $\mathcal{L}_1\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$.

To see that this condition is also necessary, observe that, for any $A \subset \mathbb{Q}^d$, if we let $A' = \mathcal{Q}^{-1}A$, then $|A'| = |A|$ and $|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| = |\mathcal{P}\mathcal{L}_1\mathcal{Q}A' + \cdots + \mathcal{P}\mathcal{L}_k\mathcal{Q}A'|$. But the transformations $\mathcal{P}\mathcal{L}_i\mathcal{Q}$ have smaller determinants, suggesting that the lower bound should instead be phrased in terms of these determinants.

Taking all these observations into account, we arrive at the following modified version of Bukh's conjecture.

Conjecture 1.4. *Suppose that $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq \Big(|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d}\Big)^d |A| - o(|A|).$$

Our main result is a proof of this modified conjecture for $k = 2$ and any d in the following strong form. We note that this result is best possible up to the lower-order term in certain cases, for instance, when $d = 2$, $\mathcal{L}_1$ is the identity and $\mathcal{L}_2 \in \mathrm{Mat}_2(\mathbb{Z})$ is a dilate of a rotation about the origin through an angle which is not an integer multiple of π.

Theorem 1.5. *Suppose that $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there are constants D, $\sigma > 0$ such that, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq \Big(|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d}\Big)^d |A| - D|A|^{1-\sigma}.$$

The proof of this result has two main steps. First, in Section 2, we use compression methods to prove a certain discrete version of the Brunn–Minkowski inequality. The core of the proof is then

a bootstrapping argument that starts with a trivial bound and repeatedly improves it using our Brunn–Minkowski inequality, ultimately approaching the estimate stated in Theorem 1.5. Because the details of this second step are rather easier to digest when $\mathcal{L}_1$ is the identity map, we will, in Section 3, first prove Theorem 1.5 in this special case. We then prove the full result in Section 4.

As an application of Theorem 1.5, we make progress on a question raised recently by Shakan [28] and by Krachun and Petrov [19], namely, for a fixed real algebraic number λ and a finite subset A of $\mathbb{R}$, how large is $|A + \lambda \cdot A|$ in terms of $|A|$? The analogous question when λ is transcendental has received considerable attention [18, 25, 27], culminating in a result of Sanders [26] saying that $|A + \lambda \cdot A| \geq e^{\log^c |A|}|A|$ for some $c > 0$, which is best possible up to the value of c.

For algebraic λ, there is a general result due to Chen and Fang [7], itself improving an earlier result of Breuillard and Green [5], saying that, for any fixed $\lambda \geq 1$, $|A + \lambda \cdot A| \geq (1 + \lambda - o(1))|A|$ holds for all finite subsets A of $\mathbb{R}$. This is best possible when λ is an integer, but can be quite slack in other cases. For instance, when $\lambda = p/q$ with p and q coprime, then the result of Balog and Shakan [1] that $|p \cdot A + q \cdot A| \geq (p + q)|A| - C_{p,q}$ for all finite subsets A of $\mathbb{Z}$ easily implies that

$$|A + \tfrac{p}{q} \cdot A| \geq (p + q)|A| - C_{p,q}$$

for all finite subsets A of $\mathbb{R}$.

In their paper, Krachun and Petrov [19] studied the case where $\lambda = \sqrt{2}$, showing that

$$|A + \sqrt{2} \cdot A| \geq (1 + \sqrt{2})^2|A| - o(|A|),$$

which is best possible up to the lower-order term, as may be seen by considering the set $A = \{x + y\sqrt{2} : 0 \leq x < M, 0 \leq y < N\}$ with the ratio M/N approaching $\sqrt{2}$. They also formulated a conjecture for a general real algebraic λ. Indeed, if $f(x) \in \mathbb{Z}[x]$ is the minimal polynomial of λ, assumed to have coprime coefficients, and $f(x) = \prod_{i=1}^{d}(a_i x + b_i)$ is a full complex factorisation of f, let $H(\lambda) = \prod_{i=1}^{d}(|a_i| + |b_i|)$. Then the conjecture of Krachun and Petrov, for which they prove the upper bound, is as follows.

Conjecture 1.6 (Krachun–Petrov [19])**.** *For any real algebraic number λ,*

$$\lim_{n\to\infty} \min_{A\subset\mathbb{R},|A|=n} \frac{|A + \lambda \cdot A|}{|A|} = H(\lambda).$$

While we fall short of proving this conjecture, Theorem 1.5 does allow us to prove the following result.

Theorem 1.7. *Suppose that $\lambda \in \mathbb{R}$ is an algebraic number with minimal polynomial $p(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$, where all the a_i are coprime. Then there are constants D, $\sigma > 0$ such that*

$$|A + \lambda \cdot A| \geq (|a_d|^{1/d} + |a_0|^{1/d})^d|A| - D|A|^{1-\sigma}$$

holds for all finite subsets A of $\mathbb{R}$.

In particular, when λ is of the form $(p/q)^{1/d}$ for some $p, q, d \in \mathbb{N}$, each taken as small as possible for such a representation, the minimal polynomial for λ is $f(x) = qx^d - p$, so that there are constants D, $\sigma > 0$ such that

$$|A + \lambda \cdot A| \geq (p^{1/d} + q^{1/d})^d|A| - D|A|^{1-\sigma}.$$

However, it is also easy to see that $H((p/q)^{1/d}) = (p^{1/d} + q^{1/d})^d$, so that we have confirmed the Krachun–Petrov conjecture in this case.

Corollary 1.8. *For any λ of the form $(p/q)^{1/d}$ for some $p, q, d \in \mathbb{N}$, each taken as small as possible for such a representation, there are constants D, $\sigma > 0$ such that*

$$|A + \lambda \cdot A| \geq (p^{1/d} + q^{1/d})^d |A| - D|A|^{1-\sigma}$$

holds for all finite subsets A of $\mathbb{R}$. Moreover, this is best possible up to the lower-order term.

For further details, we refer the reader to Section 5.

2 A discrete Brunn–Minkowski inequality

In this section, we begin our proof of Theorem 1.5 by using compression arguments to establish the following discrete analogue of the Brunn–Minkowski theorem. We refer the reader to [4, 14, 15] for a selection of results in a similar vein.

Lemma 2.1. *Fix a basis $\{b_1, \dots, b_d\}$ of $\mathbb{R}^d$. For each $I \subseteq [d]$, let $p_I : \mathbb{R}^d \to \mathbb{R}^I$ be the projection onto the span of $\{b_i\}_{i \in I}$ along the given basis. Then, for any finite subsets A, B of $\mathbb{R}^d$,*

$$|A + B| \geq (|A|^{1/d} + |B|^{1/d})^d - \sum_{I \subsetneq [d]} |p_I(A + B)|.$$

Proof. By applying a suitable linear transformation, we may assume that the basis is the standard one. Let $p_i = p_{[d]\setminus\{i\}} : \mathbb{R}^d \to \mathbb{R}^{d-1}$ be the linear map that removes the ith coordinate.

We define i-compressions for $i = 1, \dots, d$ as follows. For a set $A \subset \mathbb{R}^d$ and a point $x \in p_i(A)$, let $A_x = p_i^{-1}(x)$. Define the i-compression of A to be the set A' such that $p_i(A') = p_i(A)$ and, for each $x \in p_i(A)$, the ith coordinates of A'_x are $0, 1, \dots, |A_x| - 1$. Note that $|A'| = |A|$, so an i-compression does not alter the size of the set.

Suppose that A' and B' are the i-compressions of A and B. We will now show that $|A' + B'| \leq |A + B|$ and, more generally, that $|p_S(A' + B')| \leq |p_S(A + B)|$ for any $S \subseteq [d]$. If $i \notin S$, then $p_S(A' + B') = p_S(A + B)$. We may therefore assume that $i \in S$. Let $T = S \setminus \{i\}$. For a set C and $x \in p_T(C)$, denote by $(p_S(C))_x$ the set $\{y \in p_S(C) \mid p_T(y) = x\}$. Then, for any $z \in p_T(A' + B') = p_T(A') + p_T(B')$, there is some $x \in p_T(A') = p_T(A)$ and $y \in p_T(B') = p_T(B)$ such that $x + y = z$ and $|(p_S(A' + B'))_z| = |(p_S(A'))_x| + |(p_S(B'))_y| - 1$. Hence,

$$|(p_S(A + B))_z| \geq |(p_S(A))_x| + |(p_S(B))_y| - 1 = |(p_S(A'))_x| + |(p_S(B'))_y| - 1 = |(p_S(A' + B'))_z|.$$

Taking the sum over all z, we have $|p_S(A' + B')| \leq |p_S(A + B)|$, as claimed. We therefore see that if the required inequality holds for the i-compressions of A and B, then it also holds for the original sets.

By repeatedly taking i-compressions for $i = 1, \dots, d$, we may assume that $A, B \subset \mathbb{Z}^d_{\geq 0}$. We will say that A is i-compressed if the i-compression of A is A itself and A is compressed if it is i-compressed for all i. Now, by considering the sum of the coordinates of all the points of A or B, we see that taking the i-compression strictly decreases these sums unless they are already i-compressed. Therefore, by repeatedly taking i-compressions for each i, we may assume that A and B are compressed. This means that for any points $(x_1, \dots, x_d) \in A$ and $(y_1, \dots, y_d)$ such that $0 \leq y_i \leq x_i$ for all i, $(y_1, \dots, y_d) \in A$ and similarly for B.

For a point $x = (x_1, \dots, x_d) \in \mathbb{Z}^d$, let C_x be the closed cube $\prod_{i=1}^d [x_i - 1, x_i]$. Define $A^* = \bigcup_{x \in A} C_x$, a compact set with $\mu(A^*) = |A|$, and define B^* similarly. Then, by the Brunn–Minkowski inequality, we have

$$\mu(A^* + B^*) \geq (|A|^{1/d} + |B|^{1/d})^d.$$

We can write $A^* + B^*$ as the union of closed cubes

$$A^* + B^* = \bigcup_{x \in A + B + \{0,-1\}^d} C_x.$$

Since A and B are compressed, so is $A + B$. Using this fact, we can rewrite $A^* + B^*$ as a union of closed sets with disjoint interiors in the following way. For $S \subseteq [d]$, let P_S be the set of points in $\mathbb{Z}^d$ such that $p_S(P_S) = p_S(A + B)$ and the coordinates outside of S are all -1. Notice that the P_S are pairwise disjoint for each $S \subseteq [d]$ and $P_S \subseteq A + B + \{0, -1\}^d$. Furthermore, for each $x \in A + B + \{0, -1\}^d$, let S be the set of coordinates of x which are not -1. Then $x \in P_S$, so that

$$A^* + B^* = \bigcup_{S \subseteq [d]} \bigcup_{x \in P_S} C_x.$$

In particular, $\mu(A^* + B^*) = \sum_{S \subseteq [d]} |P_S| = \sum_{S \subseteq [d]} |p_S(A + B)|$. Hence, since $p_{[d]}(A + B) = A + B$, we have

$$\mu(A^* + B^*) = |A + B| + \sum_{I \subsetneq [d]} |p_I(A + B)|$$

and the lemma follows. □

Our aim now is to apply this discrete Brunn–Minkowski inequality to prove an estimate that will play an important role in the bootstrap arguments of the next two sections. For this, we will need several additional ingredients, beginning with the following classical theorem of Freiman [12] (see also [3]) on subsets of small doubling in torsion-free abelian groups. Given such a group G, a proper progression P of dimension s and size L is a set of the form

$$P = \{v_0 + u_1 v_1 + \cdots + u_s v_s \mid 0 \leq u_i < L_i \text{ for } 1 \leq i \leq s\},$$

where $L_1 L_2 \cdots L_s = L$, $v_0, v_1, \dots, v_s$ are elements of G and all of the sums arising in the definition of P are distinct.

Theorem 2.2. *For any $K > 0$, there exist constants C_1 and C_2 such that if A is a subset of a torsion-free abelian group G with $|A + A| \leq K|A|$, then A is contained in a proper progression of dimension $s \leq C_1$ and size $L \leq C_2|A|$.*

We also need the following result of Plünnecke–Ruzsa type [19, Lemma 3.1].

Lemma 2.3. *Let G be an abelian group. If sets $A, B \subseteq G$ with $|A| = |B|$ are such that $C := A + B$ satisfies $|C| \leq K|A|$ for some $K > 0$, then $|C + C| \leq K^6|C|$.*

Finally, we need the following technical lemma, saying that if $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ has no non-trivial invariant subspace over $\mathbb{Q}$ and A is a finite subset of $\mathbb{Z}^d$ with $|A + \mathcal{L}A| \leq K|A|$, then A cannot be concentrated on an affine subspace.

Lemma 2.4. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ with no non-trivial invariant subspace over $\mathbb{Q}$ and let $A \subset \mathbb{Z}^d$ be such that $|A| = n$ and $|A+\mathcal{L}A| \leq Kn$ for some $K > 0$. If U is a vector subspace of $\mathbb{Q}^d$ of dimension $k < d$, then every translate of U contains at most $(Kn)^{1-2^{-k}}$ points of A.*

Proof. The fact that $\mathcal{L}$ has no non-trivial invariant subspace implies that $\mathcal{L}$ is invertible (over $\mathbb{Q}$). We prove the lemma by induction on k. For $k = 1$, let U_1 be a 1-dimensional subspace. Then, since $\mathcal{L}$ is invertible, $\mathcal{L}U_1$ is a line. Furthermore, the line $\mathcal{L}U_1$ is not parallel to U_1, since U_1 is not an invariant subspace of $\mathcal{L}$. Thus, for any translate $U_1 + u$ of U_1, $|(U_1 + u) \cap A|^2 = |((U_1 + u) \cap A) + \mathcal{L}((U_1 + u) \cap A)| \leq Kn$, so $|(U_1 + u) \cap A| \leq (Kn)^{1/2}$. This proves the base case of our induction.

For $1 < k < d$, let U_k be a subspace of dimension k. Then $\mathcal{L}U_k \neq U_k$ since $\mathcal{L}$ has no non-trivial invariant subspace, so $V = \mathcal{L}U_k \cap U_k$ is a subspace of dimension strictly smaller than k. Let $U_k + u$ be a translate of U_k with $|(U_k + u) \cap A| = m$. Suppose r translates of V are required to cover $(U_k + u) \cap A$. Note that for any collection of translates V' of V, the affine subspaces $V' + \mathcal{L}(U_k + u)$ are translates of $\mathcal{L}U_k$ and are disjoint. Thus, $Kn \geq |((U_k + u) \cap A) + \mathcal{L}((U_k + u) \cap A)| \geq mr$. On the other hand, each translate of V intersects A in at most $(Kn)^{1-2^{1-k}}$ points by the induction hypothesis. Thus, $m \leq r(Kn)^{1-2^{1-k}}$. Using $mr \leq Kn$, it follows that $m^2 \leq (Kn)^{2-2^{1-k}}$, so $m \leq (Kn)^{1-2^{-k}}$, as desired. □

We now come to our application of Lemma 2.1.

Lemma 2.5. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ with no non-trivial invariant subspace over $\mathbb{Q}$ and let $A \subset \mathbb{Z}^d$ be such that $|A + \mathcal{L}A| \leq K|A|$ for some $K > 0$. Then there are constants $D, \sigma > 0$ depending only on d and K such that, for any $B_1 \subseteq A$, $B_2 \subseteq \mathcal{L}A$,*

$$|B_1 + B_2| \geq \left(|B_1|^{1/d} + |B_2|^{1/d}\right)^d - D|A|^{1-\sigma}.$$

Proof. Let $n = |A|$. By Lemma 2.3, $|A + \mathcal{L}A + A + \mathcal{L}A| \leq K^6|A + \mathcal{L}A| \leq K_1 n$, where $K_1 = K^7$. We also claim that

$$|A + \mathcal{L}A + \mathcal{L}(A + \mathcal{L}A)| \leq K_2 n,$$

where $K_2 = K_1^2$. To see this, first note that $|A + \mathcal{L}A + \mathcal{L}A| \leq |A + \mathcal{L}A + A + \mathcal{L}A| \leq K_1 n$ and $|\mathcal{L}A + \mathcal{L}A + \mathcal{L}^2 A| = |A + A + \mathcal{L}A| \leq |A + \mathcal{L}A + A + \mathcal{L}A| \leq K_1 n$. By applying the sum version of Ruzsa's triangle inequality [24], which states that

$$|A_1||A_2 + A_3| \leq |A_1 + A_2||A_1 + A_3|$$

for any finite subsets A_1, A_2, A_3 of an abelian group, to the sets $A_1 = \mathcal{L}A, A_2 = A + \mathcal{L}A, A_3 = \mathcal{L}A + \mathcal{L}^2 A$, we have

$$n|A + \mathcal{L}A + \mathcal{L}A + \mathcal{L}^2 A| \leq |A + \mathcal{L}A + \mathcal{L}A||\mathcal{L}A + \mathcal{L}A + \mathcal{L}^2 A| \leq K_1^2 n^2.$$

Thus, $|A + \mathcal{L}A + \mathcal{L}(A + \mathcal{L}A)| \leq K_1^2 n$, as claimed.

Since $|A+\mathcal{L}A+A+\mathcal{L}A| \leq K_1 n$, we can apply Theorem 2.2 to conclude that $A+\mathcal{L}A$ is contained in a proper progression

$$P = \{v_0 + u_1 v_1 + \cdots + u_s v_s \mid 0 \leq u_i < L_i \text{ for } 1 \leq i \leq s\},$$

where $s \leq K_3$, $L_1 \geq L_2 \geq \cdots \geq L_s$ and $L_1 L_2 \cdots L_s \leq K_4 n$ for some K_3, K_4 depending only on K. Note that P cannot be contained in a hyperplane, since otherwise it would contradict Lemma 2.4.

Let $i_1 = 1$ and, for $j = 2, \ldots, d$, set i_j to be the smallest number such that v_{i_j} does not lie in the span of $v_{i_1}, \ldots, v_{i_{j-1}}$. Then $v_{i_1}, \ldots, v_{i_d}$ forms a basis of $\mathbb{R}^d$. By applying Lemma 2.1 with this basis, we get that

$$\begin{aligned} |B_1 + B_2| &\geq \left(|B_1|^{1/d} + |B_2|^{1/d}\right)^d - \sum_{I \subsetneq [d]} |p_I(B_1 + B_2)| \\ &\geq \left(|B_1|^{1/d} + |B_2|^{1/d}\right)^d - 2^d(|p_1(B_1 + B_2)| + \cdots + |p_d(B_1 + B_2)|), \end{aligned}$$

where $p_j = p_{[d]\setminus\{j\}}$, the projection along the basis element v_{i_j}. Hence, it suffices to show that there is some $\sigma > 0$ such that $|p_j(A + \mathcal{L}A)| = O(n^{1-\sigma})$ for all j.

Note that $|p_j(A + \mathcal{L}A)| \leq L_1 \cdots L_s / L_{i_j} \leq K_4 n / L_{i_j}$. Let H be the span of $v_1, v_2, \ldots, v_{i_j - 1}$, which is a proper subspace. Using the claim that $|A + \mathcal{L}A + \mathcal{L}(A + \mathcal{L}A)| \leq K_2 n$, we can apply Lemma 2.4 with A replaced by $A + \mathcal{L}A$ to conclude that each translate of H contains at most $(K_2 n)^{1-2^{1-d}}$ points of $A + \mathcal{L}A$. But P is covered by $L_{i_j} L_{i_j+1} \cdots L_s$ translates of H. Hence,

$$L_{i_j} L_{i_j+1} \cdots L_s \geq n/(K_2 n)^{1-2^{1-d}} = K_5 n^{2^{1-d}},$$

where $K_5 = K_2^{2^{1-d}-1}$. Since $L_{i_j} \geq L_{i_j+1} \geq \cdots \geq L_s$, we have

$$L_{i_j} \geq K_5^{1/s} n^{2^{1-d}/s} \geq K_6 n^{2^{1-d}/K_3},$$

where $K_6 = K_5^{1/K_3}$. Thus,

$$|p_j(A + \mathcal{L}A)| \leq K_4 n / L_{i_j} \leq \frac{K_4}{K_6} n^{1-2^{1-d}/K_3}.$$

The result therefore follows by taking $\sigma = 2^{1-d}/K_3$ and $D = 2^d d K_4 / K_6$. □

3 Bounding $A + \mathcal{L}A$

As promised, we will first prove our main result in the special case where one of the transformations is the identity. Like the general case, we will do this by proving a bootstrapping lemma which allows us to successively obtain better and better bounds, approaching the optimal one. We start with a weaker version of this bootstrapping lemma.

Both here and in what follows, we will make extensive use of the fact that if $\mathcal{L}$ is not singular, then $\mathcal{L}\mathbb{Z}^d$ has index $k = |\det \mathcal{L}|$ in $\mathbb{Z}^d$. Indeed, this can be seen by considering the Smith normal form $\mathcal{L} = SDT$, where $S, T \in \mathrm{Mat}_d(\mathbb{Z})$ are invertible over $\mathbb{Z}$ and $D \in \mathrm{Mat}_d(\mathbb{Z})$ is diagonal. Then the index satisfies

$$[\mathbb{Z}^d : \mathcal{L}\mathbb{Z}^d] = [S^{-1}\mathbb{Z}^d : DT\mathbb{Z}^d] = [\mathbb{Z}^d : D\mathbb{Z}^d] = |\det D| = |\det \mathcal{L}|.$$

Lemma 3.1. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ have no non-trivial invariant subspace over $\mathbb{Q}$ and $k = |\det \mathcal{L}|$. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d and k such that the following holds. Suppose that there are $0 < \alpha < (1 + k^{1/d})^d$ and $D_1 > 0$ such that*

$$|A + \mathcal{L}A| \geq ((1 + k^{1/d})^d - \alpha)|A| - D_1 |A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$. Let $I_1, \dots, I_k$ be the cosets of $\mathcal{L}\mathbb{Z}^d$ in $\mathbb{Z}^d$ and let $A_i = A \cap I_i$ for $i = 1, \dots, k$. If there is some j for which $0 < |A_j| \leq |A|/k$, then

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A| - (D + (k-1)D_1)|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$.

Proof. Assume that $|A + \mathcal{L}A| \leq (1 + k^{1/d})^d |A|$. Let D and $\sigma_1 = \sigma$ be the constants obtained from applying Lemma 2.5 with $K = (1 + k^{1/d})^d$. Then, for each i, we have

$$|A_i + \mathcal{L}A| \geq \left(|A_i|^{1/d} + |A|^{1/d}\right)^d - D|A|^{1-\sigma_1}.$$

Since $\mathcal{L}A \subset \mathcal{L}\mathbb{Z}^d$, we have $(A + \mathcal{L}A) \cap I_i = A_i + \mathcal{L}A$. Hence, we can write $A + \mathcal{L}A$ as the disjoint union

$$A + \mathcal{L}A = (A_1 + \mathcal{L}A) \cup \cdots \cup (A_k + \mathcal{L}A).$$

Suppose, without loss of generality, that $0 < |A_1| \leq |A|/k$. We shall bound $|A_1 + \mathcal{L}A|$ by the estimate above and the rest by

$$\begin{aligned} |A_i + \mathcal{L}A| &\geq |A_i + \mathcal{L}A_i| \geq ((1 + k^{1/d})^d - \alpha)|A_i| - D_1|A_i|^{1-\sigma_1} \\ &\geq ((1 + k^{1/d})^d - \alpha)|A_i| - D_1|A|^{1-\sigma_1} \end{aligned}$$

for $i = 2, \dots, k$. Combining these estimates, we have

$$\begin{aligned} |A + \mathcal{L}A| &\geq |A_1 + \mathcal{L}A| + |A_2 + \mathcal{L}A| + \ldots + |A_1 + \mathcal{L}A| \\ &\geq \left(|A_1|^{1/d} + |A|^{1/d}\right)^d + ((1 + k^{1/d})^d - \alpha)\sum_{i=2}^{k} |A_i| - (D + (k-1)D_1)|A|^{1-\sigma_1} \\ &= \left(|A_1|^{1/d} + |A|^{1/d}\right)^d + ((1 + k^{1/d})^d - \alpha)(|A| - |A_1|) - (D + (k-1)D_1)|A|^{1-\sigma_1}. \end{aligned}$$

This last expression is concave in terms of $|A_1|$, which can be seen by expanding the binomial term and noting that each term in the binomial sum is concave. Hence, it is minimised when $|A_1| = 0$ or $|A_1| = |A|/k$.

In the first case, where the minimum is when $|A_1| = 0$, we have

$$|A + \mathcal{L}A| \geq (((1 + k^{1/d})^d - (\alpha - 1))|A| - (D + (k-1)D_1)|A|^{1-\sigma_1}.$$

In the second case, where the minimum is when $|A_1| = |A|/k$, we have

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \frac{k-1}{k}\alpha\right)|A| - (D + (k-1)D_1)|A|^{1-\sigma_1}.$$

In either case, we have

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A| - (D + (k-1)D_1)|A|^{1-\sigma_1},$$

as required. □

This lemma shows that bootstrapping works if each of the k cosets A_i of A are non-empty. To show that a similar result holds in general, we split each of the cosets A_i into smaller cosets A_{ij}. There are then three cases: if A is contained in some smaller sublattice, then we can rescale A, which will contradict a certain minimality assumption; if $A + \mathcal{L}A$ contains cosets that are distinct from all the $A_{ij} + \mathcal{L}A_{ij}$, then this additional coset boosts the bound; and, finally, if any of the A_i splits into k non-empty cosets, we can again apply the lemma above. The following lemma will allow us to show that one of these three cases must hold.

Lemma 3.2. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ be a linear transformation that is invertible over $\mathbb{Q}$. Let X be a subset of the finite abelian group $G = \mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d$ containing 0 and let H be the subgroup $\mathcal{L}\mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d$ of G. Notice that $\mathcal{L}$ naturally induces a map $G \to G$. Then at least one of the following holds:*

1. *$X + H$ does not generate G;*
2. *$X + \mathcal{L}X \supsetneq X$ (note that $X + \mathcal{L}X \supseteq X$ always holds);*
3. *$H \subseteq X$.*

Proof. Suppose all 3 do not hold. Let $L = \{v \in G \mid \mathcal{L}v \in X\}$. Since $0 \in X$, we have $H \subseteq L$. For any $v \in L$ and $a \in X$, we have $\mathcal{L}v + \mathcal{L}a \in X + \mathcal{L}X = X$, so $v + a \in L$. Since $H + X$ generates G, for any $b \in G$, there are $h \in H$ and $a_1, \ldots, a_k \in X$ for some k such that $b = h + a_1 + \cdots + a_k$. If $h + a_1 + \cdots + a_i \in L$ for some i, then $(h + a_1 + \cdots + a_i) + a_{i+1} \in L$, so, by the fact that $h \in L$ and a simple induction, we have that $b = h + a_1 + \cdots + a_k \in L$. Thus, $L = G$, which implies that $H \subseteq X$, a contradiction. □

We are now ready for our main bootstrapping lemma.

Lemma 3.3. *Let d and k be positive integers. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d and k such that the following holds. Suppose that there are $0 < \alpha < (1+k^{1/d})^d$ and $D_1 > 0$ such that*

$$|A + \mathcal{L}A| \geq ((1 + k^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$ and all $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ with no non-trivial invariant subspace over $\mathbb{Q}$ and $k = |\det \mathcal{L}|$. Then

$$|A + \mathcal{L}A| \geq \left((1 + k^{1/d})^d - \max\left(\alpha - \frac{1}{k^2}, \frac{k^2 - 1}{k^2}\alpha\right)\right)|A| - (D + k^2 D_1)|A|^{1-\sigma_1}$$

holds for all such A and $\mathcal{L}$.

Proof. Take σ_1, D as in Lemma 3.1. By translating A, we may assume that $0 \in A$. We may also assume that $|A+\mathcal{L}A| \leq (1+k^{1/d})^d|A|$, so that, by Lemma 2.4, A does not lie on a hyperplane. Let $\langle A \rangle$ denote the $\mathbb{Z}$-span of A, which is a d-dimensional sublattice of $\mathbb{Z}^d$. Suppose the lemma does not hold and pick a counterexample $(A, \mathcal{L})$ such that $\langle A \rangle$ has minimum index in $\mathbb{Z}^d$.

Let $0 = v_1, v_2, \ldots, v_k$ be coset representatives of $\mathcal{L}\mathbb{Z}^d$ over $\mathbb{Z}^d$. For $i, j = 1, \ldots, k$, let $A_i = A \cap (v_i + \mathcal{L}\mathbb{Z}^d)$ and $A_{ij} = A \cap (v_i + \mathcal{L}v_j + \mathcal{L}^2\mathbb{Z}^d)$. Then the A_{ij} partition A_i and the A_i partition A. If there is some i for which $0 < |A_i| \leq |A|/k$, then we are done by Lemma 3.1. Hence, we may assume that either $A_i = \emptyset$ or $|A_i| > |A|/k$ for every i. If there is some i, j such that $A_i \neq \emptyset$ and $0 < |A_{ij}| \leq |A_i|/k$, then let $A' = \mathcal{L}^{-1}(A_i - v_i) = \mathcal{L}^{-1}(A - v_i) \cap \mathbb{Z}^d \subseteq \mathbb{Z}^d$. For each $l = 1, \ldots, k$,

let $A'_l = \mathcal{L}^{-1}(A_{il} - v_i) = \mathcal{L}^{-1}(A - v_i) \cap (v_l + \mathcal{L}\mathbb{Z}^d)$. Thus, $A'_l = A' \cap (v_l + \mathcal{L}\mathbb{Z}^d)$. Hence, applying Lemma 3.1 with A and A_j replaced by A' and A'_j, we have

$$\begin{aligned}|A_i + \mathcal{L}A_i| &= |A' + \mathcal{L}A'| \\ &\geq \left((1+k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A_i| - (D + (k-1)D_1)|A_i|^{1-\sigma_1}.\end{aligned}$$

Using the fact that $|A + \mathcal{L}A| \geq \sum_{l=1}^{k} |A_l + \mathcal{L}A_l|$, we have

$$\begin{aligned}|A + \mathcal{L}A| &\geq \sum_{l\neq i} |A_l + \mathcal{L}A_l| + |A_i + \mathcal{L}A_i| \\ &\geq \left((1+k^{1/d})^d - \alpha\right)\sum_{l\neq i}|A_l| - (k-1)D_1|A|^{1-\sigma_1} \\ &\quad + \left((1+k^{1/d})^d - \max\left(\alpha - 1, \frac{k-1}{k}\alpha\right)\right)|A_i| - (D + (k-1)D_1)|A|^{1-\sigma_1} \\ &= \left((1+k^{1/d})^d - \alpha\right)|A| + \min\left(1, \frac{\alpha}{k}\right)|A_i| - (D + 2(k-1)D_1)|A|^{1-\sigma_1} \\ &\geq \left((1+k^{1/d})^d - \alpha\right)|A| + \min\left(\frac{1}{k}, \frac{\alpha}{k^2}\right)|A| - (D + 2(k-1)D_1)|A|^{1-\sigma_1} \\ &\geq \left((1+k^{1/d})^d - \max\left(\alpha - \frac{1}{k}, \frac{k^2-1}{k^2}\alpha\right)\right)|A| - (D + k^2D_1)|A|^{1-\sigma_1}.\end{aligned}$$

Hence, we may assume that, for all i, j, either $A_{ij} = \emptyset$ or $|A_{ij}| > |A_i|/k > |A|/k^2$.

Let X be the image of A in $G = \mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d$ and let $H = \mathcal{L}\mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d \subseteq G$. Applying Lemma 3.2 to X, we have the following 3 cases:

Case 1: $X + H$ does not generate G

Let $E \subset \mathbb{Z}^d$ be the lattice that is the preimage of the subgroup of G generated by $X + H$ with respect to the quotient map $q : \mathbb{Z}^d \to \mathbb{Z}^d/\mathcal{L}^2\mathbb{Z}^d = G$. In other words, $E = \langle A\rangle + \mathcal{L}\mathbb{Z}^d$. Since A does not lie on a hyperplane, E is d-dimensional and, since $X + H$ does not generate G, $E \neq \mathbb{Z}^d$. Consider a linear transformation $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ such that $\mathcal{P}\mathbb{Z}^d = E$, so that $|\det \mathcal{P}| > 1$. Then

$$|A + \mathcal{L}A| = |\mathcal{P}\mathcal{P}^{-1}A + \mathcal{P}\mathcal{P}^{-1}\mathcal{L}\mathcal{P}\mathcal{P}^{-1}A| = |\mathcal{P}^{-1}A + (\mathcal{P}^{-1}\mathcal{L}\mathcal{P})(\mathcal{P}^{-1}A)|.$$

Since $\mathcal{L}E \subset \mathcal{L}\mathbb{Z}^d = q^{-1}(H) \subseteq E$, we have

$$\mathcal{P}^{-1}\mathcal{L}\mathcal{P}\mathbb{Z}^d = \mathcal{P}^{-1}\mathcal{L}E \subset \mathcal{P}^{-1}E = \mathbb{Z}^d,$$

so that $\mathcal{P}^{-1}\mathcal{L}\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ and $|\det \mathcal{P}^{-1}\mathcal{L}\mathcal{P}| = |\det \mathcal{P}|^{-1}|\det \mathcal{L}||\det \mathcal{P}| = k$. Now replace A by $\mathcal{P}^{-1}A \subset \mathbb{Z}^d$ and $\mathcal{L}$ by $\mathcal{P}^{-1}\mathcal{L}\mathcal{P}$. But then the index of $\langle \mathcal{P}^{-1}A\rangle$ is

$$[\mathbb{Z}^d : \langle \mathcal{P}^{-1}A\rangle] = [\mathcal{P}\mathbb{Z}^d : \langle A\rangle] = [\mathbb{Z}^d : \langle A\rangle]/[\mathbb{Z}^d : \mathcal{P}\mathbb{Z}^d] = |\det \mathcal{P}|^{-1}[\mathbb{Z}^d : \langle A\rangle].$$

Thus, $\langle \mathcal{P}^{-1}A\rangle$ has strictly smaller index than $\langle A\rangle$, so the pair $(\mathcal{P}^{-1}A, \mathcal{P}^{-1}\mathcal{L}\mathcal{P})$ contradicts the minimality of the pair $(A, \mathcal{L})$.

Case 2: $X + \mathcal{L}X \supsetneq X$
This case is saying that $A + \mathcal{L}A$ intersects strictly more cosets of $\mathcal{L}^2\mathbb{Z}^d$ than A, so we can exploit the extra cosets to obtain a better lower bound. Let $I = \{(i,j) \in [k]^2 \mid A_{ij} \neq \emptyset\}$. Suppose $(i,j),(i',j') \in I$ are distinct pairs. We claim that $A_{ij} + \mathcal{L}A_{ij}$ and $A_{i'j'} + \mathcal{L}A_{i'j'}$ belong to different cosets of $\mathcal{L}^2\mathbb{Z}^d$. Indeed, suppose they belong to the same coset. $A_{ij} + \mathcal{L}A_{ij}$ belongs to the coset $v_i + \mathcal{L}v_j + \mathcal{L}v_i + \mathcal{L}^2\mathbb{Z}^d$, while $A_{i'j'} + \mathcal{L}A_{i'j'} \subset v_{i'} + \mathcal{L}v_{j'} + \mathcal{L}v_{i'} + \mathcal{L}^2\mathbb{Z}^d$. So if they belong to the same coset, we must have $i = i'$ and $j = j'$. Now, since $A + \mathcal{L}A$ intersects more than $|I|$ cosets, there are $(i_1,j_1),(i_2,j_2) \in I$ such that $A_{i_1j_1} + \mathcal{L}A_{i_2j_2}$ belongs to a coset different from $A_{ij} + \mathcal{L}A_{ij}$ for all $(i,j) \in I$. Hence, we have

$$\begin{aligned}
|A + \mathcal{L}A| &\geq \sum_{(i,j)\in I} |A_{ij} + \mathcal{L}A_{ij}| + |A_{i_1j_1} + \mathcal{L}A_{i_2j_2}| \\
&\geq ((1+k^{1/d})^d - \alpha)|A| - k^2 D_1 |A|^{1-\sigma_1} + |A_{i_1j_1}| \\
&\geq ((1+k^{1/d})^d - \alpha)|A| - k^2 D_1 |A|^{1-\sigma_1} + \frac{1}{k^2}|A| \\
&= ((1+k^{1/d})^d - (\alpha - 1/k^2))|A| - k^2 D_1 |A|^{1-\sigma_1}.
\end{aligned}$$

Case 3: $H \subseteq X$
In this case, $A_{1j} \neq \emptyset$ for $j = 1,\ldots,k$. But, since the A_{1j} partition A_1, there is then some j for which $|A_{1j}| \leq |A_1|/k$, contradicting our assumption. This completes the proof of the lemma. □

It is now a simple matter to complete the proof of Theorem 1.5 in the special case where $\mathcal{L}_1$ is the identity.

Theorem 3.4. *Let $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ be a linear transformation with no non-trivial invariant subspace over $\mathbb{Q}$ and $k = |\det \mathcal{L}|$. Then there are $D_2, \sigma_2 > 0$ depending only on d and k such that*

$$|A + \mathcal{L}A| \geq (1+k^{1/d})^d |A| - D_2 |A|^{1-\sigma_2}$$

for all finite $A \subset \mathbb{Z}^d$.

Proof. Let $\sigma_1, D > 0$ be as in Lemma 3.3. Using the trivial base case $|A + \mathcal{L}A| \geq |A|$ and repeatedly applying Lemma 3.3, we can find some $0 < \epsilon < 1$ and $D_2' > D$ such that

$$|A + \mathcal{L}A| \geq ((1+k^{1/d})^d - \epsilon)|A| - D_2' |A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$.

Applying Lemma 3.3 m more times, we have

$$|A + \mathcal{L}A| \geq \left((1+k^{1/d})^d - \left(\frac{k^2-1}{k^2}\right)^m \epsilon\right)|A| - (k^2+1)^m D_2' |A|^{1-\sigma_1}.$$

Taking $m = \frac{\sigma_1 \log |A|}{2\log(k^2+1)}$ (and ignoring integer rounding issues), we have

$$(k^2+1)^m D_2' |A|^{1-\sigma_1} = D_2' |A|^{1-\sigma_1/2}$$

and

$$\left(\frac{k^2-1}{k^2}\right)^m \epsilon|A| = \epsilon|A|^{1+\frac{\sigma_1(\log(k^2-1)-\log k^2)}{2\log(k^2+1)}}.$$

Now, taking $\sigma_2 = \min\left(\frac{\sigma_1}{2}, \frac{\sigma_1(\log k^2 - \log(k^2-1))}{2\log(k^2+1)}\right)$, we get

$$|A+\mathcal{L}A| \geq (1+k^{1/d})^d|A| - D_2|A|^{1-\sigma_2},$$

where $D_2 = \epsilon + D_2'$. □

4 Bounding $\mathcal{L}_1 A + \mathcal{L}_2 A$

In this section, we prove our main result, our lower bound on $|\mathcal{L}_1 A + \mathcal{L}_2 A|$ when $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Note that we may assume that both $\mathcal{L}_1$ and $\mathcal{L}_2$ are invertible over $\mathbb{Q}$. Indeed, if $\mathcal{L}_1$, say, is not invertible, then there is a line L such that $\mathcal{L}_1 L = 0$, so $\mathcal{L}_1, \mathcal{L}_2$ would not be irreducible.

We first note the following elementary fact about abelian groups.

Lemma 4.1. *Let G be an abelian group and H_1, H_2 be subgroups of finite index such that $H_1 + H_2 = G$. Then*

$$[G : H_1 \cap H_2] = [G : H_1][G : H_2].$$

Proof. By the isomorphism theorems, we have that

$$H_1/(H_1 \cap H_2) \equiv (H_1 + H_2)/H_2$$

$$G/H_1 \equiv (G/(H_1 \cap H_2))/(H_1/(H_1 \cap H_2)).$$

Hence, $[H_1 : H_1 \cap H_2] = [G : H_2]$ and $[G : H_1 \cap H_2] = [G : H_1][H_1 : H_1 \cap H_2] = [G : H_1][G : H_2]$. □

For the proof, we will need to introduce a number of additional linear transformations associated with $\mathcal{L}_1$ and $\mathcal{L}_2$. Indeed, let $p = |\det \mathcal{L}_1|$ and $q = |\det \mathcal{L}_2|$. Since $\mathcal{L}_1, \mathcal{L}_2$ are coprime, we know that $\mathcal{L}_1\mathbb{Z}^d + \mathcal{L}_2\mathbb{Z}^d = \mathbb{Z}^d$. Thus, by Lemma 4.1 with $G = \mathbb{Z}^d$, $H_1 = \mathcal{L}_1\mathbb{Z}^d$ and $H_2 = \mathcal{L}_2\mathbb{Z}^d$, we have

$$[\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d] = [\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d][\mathbb{Z}^d : \mathcal{L}_2\mathbb{Z}^d] = pq.$$

Hence,

$$[\mathcal{L}_1\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d] = q, \quad [\mathcal{L}_2\mathbb{Z}^d : \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d] = p$$

and so

$$[\mathbb{Z}^d : \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d] = q, \quad [\mathbb{Z}^d : \mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d] = p.$$

We now let $\mathcal{P}_1, \mathcal{P}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be linear transformations such that $\mathcal{P}_1\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d$ and $\mathcal{P}_2\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$, noting that $|\det \mathcal{P}_1| = p$ and $|\det \mathcal{P}_2| = q$.

As in the $A + \mathcal{L}A$ case, we begin the proof proper with a weak bootstrapping lemma.

Lemma 4.2. *Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be irreducible, coprime linear transformations with $|\det \mathcal{L}_1| = p$ and $|\det \mathcal{L}_2| = q$. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d, p and q such that the following holds. Suppose that there are $0 < \alpha < (p^{1/d} + q^{1/d})^d$ and $D_1 > 0$ such that*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$. Let $I_1, \dots, I_p$ be the cosets of $\mathcal{P}_1\mathbb{Z}^d$ in $\mathbb{Z}^d$ and $I^1, \dots, I^q$ the cosets of $\mathcal{P}_2\mathbb{Z}^d$ and let $A_i = A \cap I_i$, $A^j = A \cap I^j$ and $A_i^j = A \cap I_i \cap I^j$. If either

1. *$A_i, A^j \neq \emptyset$ for all $1 \leq i \leq p, 1 \leq j \leq q$ or*
2. *there are some i, j such that $A_i, A^j \neq \emptyset$ and $|A_i^j| \leq c|A|$, where $c = \frac{1}{2p(p^{1/d}+q^{1/d})^{2d}}$,*

then

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$.

Proof. Since $\mathcal{L}_1, \mathcal{L}_2$ are irreducible, $\mathcal{L}_1^{-1}\mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Q})$ has no non-trivial invariant subspace over $\mathbb{Q}$. We may also assume that $|\mathcal{L}_1 A + \mathcal{L}_2 A| \leq (p^{1/d} + q^{1/d})^d |A|$, so that, by Lemma 2.5 with $\mathcal{L} = \mathcal{L}_1^{-1}\mathcal{L}_2$, there are $\sigma_1, D > 0$ such that, for any $B_1, B_2 \subseteq A$,

$$|\mathcal{L}_1 B_1 + \mathcal{L}_2 B_2| = |B_1 + \mathcal{L} B_2| \geq (|B_1|^{1/d} + |B_2|^{1/d})^d - D|A|^{1-\sigma_1}.$$

We claim that there is a choice of i and j such that $A_i, A^j \neq \emptyset$ and

$$(|A_i|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \geq \alpha c|A|.$$

Suppose first that $A_i, A^j \neq \emptyset$ for all i, j. Pick i and j such that $|A_i^j|$ is minimal. If $|A_i^j| \leq c|A|$, then we may pass to the second case. Otherwise, $|A_i^j| > c|A|$. Since, for any i', j', we have $|A_{i'}^j| \geq |A_i^j|$ and $|A_i^{j'}| \geq |A_i^j|$, we see that $|A^j| \geq p|A_i^j|$ and $|A_i| \geq q|A_i^j|$. Hence,

$$(|A_i|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \geq \alpha|A_i^j| \geq \alpha c|A|.$$

Suppose now that there are i, j such that $A_i, A^j \neq \emptyset$ and $|A_i^j| \leq c|A|$. If there is some i' such that $|A_{i'}^j| > (p^{1/d} + q^{1/d})^d c|A|$, then

$$\begin{aligned}(|A_i|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| &\geq |A_{i'}^j| - ((p^{1/d} + q^{1/d})^d - \alpha)|A_i^j| \\ &\geq (p^{1/d} + q^{1/d})^d c|A| - ((p^{1/d} + q^{1/d})^d - \alpha)c|A| \\ &= \alpha c|A|.\end{aligned}$$

Otherwise, we may assume that $|A_{i'}^j| \leq (p^{1/d} + q^{1/d})^d c|A|$ for all i'. Since $\sum_i |A_i| = |A|$, there is some i' such that $|A_{i'}| \geq |A|/p$. Thus,

$$\begin{aligned}(|A_{i'}|^{1/d} + |A^j|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_{i'}^j| &\geq |A_{i'}| - ((p^{1/d} + q^{1/d})^d - \alpha)|A_{i'}^j| \\ &\geq \frac{1}{p}|A| - ((p^{1/d} + q^{1/d})^d - \alpha)(p^{1/d} + q^{1/d})^d c|A| \\ &\geq \frac{1}{2p}|A| > \alpha c|A|.\end{aligned}$$

This proves the claim. From here on, without loss of generality, we will assume that $A_1, A^1 \neq \emptyset$ and

$$(|A_1|^{1/d} + |A^1|^{1/d})^d - ((p^{1/d} + q^{1/d})^d - \alpha)|A_1^1| \geq \alpha c|A|.$$

We will now show that the sets $\mathcal{L}_1 A + \mathcal{L}_2 A_i$ belong to different cosets of $\mathcal{L}_1\mathbb{Z}^d$ for $i = 1, \dots, p$ and so are disjoint. Note that $\mathcal{L}_2\mathcal{P}_1\mathbb{Z}^d \subseteq \mathcal{L}_1\mathbb{Z}^d$, so the sets do indeed belong to cosets of $\mathcal{L}_1\mathbb{Z}^d$. If, for some i, i', the corresponding sets belong to the same coset, then $\mathcal{L}_2 I_i - \mathcal{L}_2 I_{i'} \subseteq \mathcal{L}_1\mathbb{Z}^d$, so $I_i - I_{i'} \subseteq \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d$. But this means that I_i and $I_{i'}$ are the same coset of $\mathcal{P}_1\mathbb{Z}^d$. Hence, $\mathcal{L}_1 A + \mathcal{L}_2 A$ can be partitioned into the sets $\mathcal{L}_1 A + \mathcal{L}_2 A_i$ for $i = 1, \dots, p$. Similarly, the sets $\mathcal{L}_1 A^j + \mathcal{L}_2 A_1$ belong to disjoint cosets of $\mathcal{L}_2\mathbb{Z}^d$, so $\mathcal{L}_1 A + \mathcal{L}_2 A_1$ can be partitioned into the sets $\mathcal{L}_1 A^j + \mathcal{L}_2 A_1$ for $j = 1, 2, \dots, q$.

Note now that, by our choice of σ_1 and D, we have

$$|\mathcal{L}_1 A^1 + \mathcal{L}_2 A_1| \geq (|A^1|^{1/d} + |A_1|^{1/d})^d - D|A|^{1-\sigma_1}.$$

Thus, using our earlier claim, we have

$$\begin{aligned}
|\mathcal{L}_1 A + \mathcal{L}_2 A| &= \sum_{i=2}^{p} |\mathcal{L}_1 A + \mathcal{L}_2 A_i| + \sum_{j=2}^{q} |\mathcal{L}_1 A^j + \mathcal{L}_2 A_1| + |\mathcal{L}_1 A^1 + \mathcal{L}_2 A_1| \\
&\geq \sum_{i=2}^{p} |\mathcal{L}_1 A_i + \mathcal{L}_2 A_i| + \sum_{j=2}^{q} |\mathcal{L}_1 A_1^j + \mathcal{L}_2 A_1^j| + |\mathcal{L}_1 A^1 + \mathcal{L}_2 A_1| \\
&\geq ((p^{1/d} + q^{1/d})^d - \alpha)(|A| - |A_1^1|) - (p+q)D_1|A|^{1-\sigma_1} \\
&\quad + (|A^1|^{1/d} + |A_1|^{1/d})^d - D|A|^{1-\sigma_1} \\
&\geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| + \alpha c|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1} \\
&= ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1},
\end{aligned}$$

as required. □

We now introduce some further notation. Indeed, let $\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$ be a linear transformation such that

$$\mathcal{P}\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d = \mathcal{P}_1\mathbb{Z}^d \cap \mathcal{P}_2\mathbb{Z}^d.$$

Then, by Lemma 4.1,

$$\begin{aligned}
|\det \mathcal{P}| &= [\mathbb{Z}^d : \mathcal{P}\mathbb{Z}^d] = [\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d][\mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d \cap \mathcal{P}_2\mathbb{Z}^d] \\
&= [\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d][\mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d][\mathcal{P}_1\mathbb{Z}^d + \mathcal{P}_2\mathbb{Z}^d : \mathcal{P}_2\mathbb{Z}^d] \\
&\leq [\mathbb{Z}^d : \mathcal{P}_1\mathbb{Z}^d][\mathbb{Z}^d : \mathcal{P}_2\mathbb{Z}^d] = |\det \mathcal{P}_1||\det \mathcal{P}_2| = pq.
\end{aligned}$$

Moreover, let $\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z})$ be such that

$$\mathcal{Q}\mathbb{Z}^d = \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d,$$

so that, as above, $|\det \mathcal{Q}| = |\det \mathcal{L}_1||\det \mathcal{L}_2| = pq$.

Note that $\mathcal{L}_1\mathcal{P}\mathbb{Z}^d, \mathcal{L}_2\mathcal{P}\mathbb{Z}^d \subseteq \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d = \mathcal{Q}\mathbb{Z}^d$, so $\mathcal{Q}^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d, \mathcal{Q}^{-1}\mathcal{L}_2\mathcal{P}\mathbb{Z}^d \subseteq \mathbb{Z}^d$, implying that $\mathcal{Q}^{-1}\mathcal{L}_1\mathcal{P}, \mathcal{Q}^{-1}\mathcal{L}_2\mathcal{P} \in \mathrm{Mat}_d(\mathbb{Z})$. Therefore, since $\mathcal{L}_1, \mathcal{L}_2$ are coprime,

$$|\det \mathcal{Q}^{-1}\mathcal{P}| \geq 1.$$

But $|\det \mathcal{Q}| = pq$ and $|\det \mathcal{P}| \leq pq$, so we must have $|\det \mathcal{P}| = pq$.

Finally, we let L_1 be the lattice $\mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ and $L_2 = \mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathcal{P}\mathbb{Z}^d$. The next lemma will be important in the proof of Lemma 4.4 below, which, like Lemma 3.2 in the last section, says that any set A falls into one of three categories, each helpful for our bootstrap.

Lemma 4.3. *The linear maps $\mathcal{L}_1, \mathcal{L}_2$ induce homomorphisms*

$$\phi_1, \phi_2 : \mathbb{Z}^d/L_1 \to \mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$$

of finite abelian groups. Furthermore, $\phi_1 + \phi_2$ is an isomorphism.

Proof. If $x \in L_1$, then $\mathcal{L}_1 x \in \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ and $\mathcal{L}_2 x \in \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so ϕ_1 and ϕ_2 are well-defined group homomorphisms. If we now let $\phi : \mathbb{Z}^d \to \mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ be the map induced by $\mathcal{L}_1 + \mathcal{L}_2$, we wish to show that $\ker \phi = L_1$. We have already seen above that $\ker \phi \supseteq L_1$. For the converse, suppose that $x \in \ker \phi$, so that $\mathcal{L}_1 x + \mathcal{L}_2 x = \mathcal{L}_1\mathcal{P}y$ for some $y \in \mathbb{Z}^d$. This implies that

$$x = \mathcal{P}y - \mathcal{L}_1^{-1}\mathcal{L}_2 x,$$

$$x = \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}y - \mathcal{L}_2^{-1}\mathcal{L}_1 x.$$

Since $\mathcal{P}y \in \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$, the first equation implies that $x \in \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$. From the second equation, we have $x \in \mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d$, so that $x \in \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathbb{Z}^d = \mathcal{P}\mathbb{Z}^d$. It then follows from applying the second equation again that $x \in \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so that $x \in \mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = L_1$, as required. □

Since $\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ has index $|\det \mathcal{L}_1\mathcal{P}| = p^2q$ and $\phi_1 + \phi_2$ is an isomorphism, the lemma implies that L_1 also has index p^2q. Similarly, L_2 has index pq^2.

Lemma 4.4. *Let X be a subset of $G = \mathbb{Z}^d/L_1$ containing 0 and define ϕ_1, ϕ_2 as in the previous lemma. Then at least one of the following holds:*

1. *X does not generate G;*
2. *$|\phi_1(X) + \phi_2(X)| > |X|$;*
3. *$\mathcal{P}\mathbb{Z}^d/L_1 \subseteq X$.*

Proof. Suppose all 3 do not hold. Let $\phi = \phi_1 + \phi_2$, which is an isomorphism by Lemma 4.3. Note that $\phi(X) \subseteq \phi_1(X) + \phi_2(X)$, so $|\phi_1(X) + \phi_2(X)| \geq |X|$ always holds. By assumption, we must have $\phi_1(X) + \phi_2(X) = \phi(X)$. Hence, for any $x, y \in X$, we have $\phi^{-1}\phi_1(x) + \phi^{-1}\phi_2(y) \in X$. In particular, since $0 \in X$, we have $\phi^{-1}\phi_1(x), \phi^{-1}\phi_2(x) \in X$.

We claim that $\phi^{-1}\phi_2(G) = \mathcal{P}_2\mathbb{Z}^d/L_1$ and $\phi^{-1}\phi_1(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{P}\mathbb{Z}^d/L_1$. For the first claim, note that $\phi_2(G) = \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so it suffices to show that $\phi(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. Note that, for any $x \in \mathcal{P}_2\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{L}_1^{-1}\mathcal{L}_2\mathbb{Z}^d$, we have $\mathcal{L}_1 x, \mathcal{L}_2 x \in \mathcal{L}_2\mathbb{Z}^d$, so that $\phi(\mathcal{P}_2\mathbb{Z}^d/L_1) \subseteq \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. Since $\mathcal{P}_2\mathbb{Z}^d$ and $\mathcal{L}_2\mathbb{Z}^d$ have index q and L_1 and $\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ have index p^2q, we have $|\mathcal{P}_2\mathbb{Z}^d/L_1| = |\mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d| = p^2$. Since ϕ is an isomorphism, we must then have $\phi(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{L}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$.

For the second claim, note that $\phi_1(\mathcal{P}_2\mathbb{Z}^d/L_1) = \mathcal{L}_1\mathcal{P}_2\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so it suffices to show that $\phi(\mathcal{P}\mathbb{Z}^d/L_1) = (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. If $x \in \mathcal{P}\mathbb{Z}^d$, then $\mathcal{L}_1 x, \mathcal{L}_2 x \in \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d$, so we have the inclusion $\phi(\mathcal{P}\mathbb{Z}^d/L_1) \subseteq (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$. By again counting sizes, we have $|\mathcal{P}\mathbb{Z}^d/L_1| = |(\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d| = p$, so $\phi(\mathcal{P}\mathbb{Z}^d/L_1) = (\mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d)/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, proving our claim.

Let $X' = X \cap \mathcal{P}_2\mathbb{Z}^d/L_1$. Since $\phi^{-1}\phi_2(X) \subseteq X'$ and X generates G, we have that X' generates $\mathcal{P}_2\mathbb{Z}^d/L_1$. Moreover, $\phi^{-1}\phi_1(X') \subseteq X$ and generates $\mathcal{P}\mathbb{Z}^d/L_1$. Note that, for any $x \in \mathcal{P}\mathbb{Z}^d/L_1$, $\phi_1(x) = 0$, so $\phi^{-1}\phi_2(x) = x$. This implies that, for any $x \in X \cap \mathcal{P}\mathbb{Z}^d/L_1$ and $y \in X'$, we have $\phi^{-1}\phi_1(y) + x = \phi^{-1}\phi_1(y) + \phi^{-1}\phi_2(x) \in X \cap \mathcal{P}\mathbb{Z}^d/L_1$. But $\phi^{-1}\phi_1(X')$ generates $\mathcal{P}\mathbb{Z}^d/L_1$ and $0 \in X \cap \mathcal{P}\mathbb{Z}^d/L_1$. Hence, by a simple induction, it follows that $X \cap \mathcal{P}\mathbb{Z}^d/L_1 = \mathcal{P}\mathbb{Z}^d/L_1$, contradicting our third assumption. □

We now come to our main bootstrapping lemma.

Lemma 4.5. *Let d, p and q be positive integers. Then there are constants $\sigma_1 > 0$ and $D > 0$ depending only on d, p and q such that the following holds. Suppose that there are $0 < \alpha < (p^{1/d} + q^{1/d})^d$ and $D_1 > 0$ such that*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - \alpha)|A| - D_1|A|^{1-\sigma_1}$$

holds for all finite $A \subset \mathbb{Z}^d$ and all irreducible, coprime linear transformations $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ with $|\det \mathcal{L}_1| = p$ and $|\det \mathcal{L}_2| = q$. Then

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq ((p^{1/d} + q^{1/d})^d - (1 - c^2)\alpha)|A| - (4p^2q^2D_1 + D)|A|^{1-\sigma_1}$$

holds for all such $A \subset \mathbb{Z}^d$ and $\mathcal{L}_1, \mathcal{L}_2$, where $c = \frac{1}{2\max(p,q)(p^{1/d}+q^{1/d})^{2d}}$.

Proof. Take σ_1, D as in Lemma 4.2. By translating A, we may assume that $0 \in A$. We may also assume that $|\mathcal{L}_1 A + \mathcal{L}_2 A| \leq (p^{1/d} + q^{1/d})^d |A|$, so that, by Lemma 2.4, A cannot lie on a hyperplane. Suppose now that A is a counterexample to the lemma with $[\mathbb{Z}^d : \langle A \rangle]$ minimal. Let A' be the image of A in $\mathbb{Z}^d/L_1$. By Lemma 4.4, one of the following possibilities holds:

1. A' does not generate $\mathbb{Z}^d/L_1$;
2. $|\phi_1(A') + \phi_2(A')| > |A'|$;
3. $\mathcal{P}\mathbb{Z}^d/L_1 \subseteq A'$.

We consider each case separately.

Case 1: (1) holds, but not (2)

The fact that (1) holds means that $\langle A \rangle + L_1 \neq \mathbb{Z}^d$, so it must be a strictly smaller sublattice of $\mathbb{Z}^d$ of some index $k > 1$. Let $\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $\mathcal{Q}\mathbb{Z}^d = \langle A \rangle + L_1$, so that $|\det \mathcal{Q}| = k$. Since (2) does not hold, we have $\phi_1(A') + \phi_2(A') = \phi(A')$, so $\langle \phi_1(A') + \phi_2(A') \rangle = \phi(\langle A' \rangle)$. Since ϕ is an isomorphism and $\langle A' \rangle$ is a subgroup of $\mathbb{Z}/L_1$ of index k, $\phi(\langle A' \rangle)$ is a subgroup of $\mathbb{Z}^d/\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ of index k. Thus, $\langle \mathcal{L}_1 A + \mathcal{L}_2 A \rangle + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ is a sublattice of $\mathbb{Z}^d$ of index k.

Let $\mathcal{Q}' \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $\mathcal{Q}'\mathbb{Z}^d = \langle \mathcal{L}_1 A + \mathcal{L}_2 A \rangle + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, so that $|\det \mathcal{Q}'| = k$. Notice that

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| = |\mathcal{Q}'^{-1}\mathcal{L}_1\mathcal{Q}(\mathcal{Q}^{-1}A) + \mathcal{Q}'^{-1}\mathcal{L}_2\mathcal{Q}(\mathcal{Q}^{-1}A)|,$$

so we may replace the triple $(\mathcal{L}_1, \mathcal{L}_2, A)$ with $(\mathcal{Q}'^{-1}\mathcal{L}_1\mathcal{Q}, \mathcal{Q}'^{-1}\mathcal{L}_2\mathcal{Q}, \mathcal{Q}^{-1}A)$. It is easy to see that $\mathcal{Q}'^{-1}\mathcal{L}_1\mathcal{Q}, \mathcal{Q}'^{-1}\mathcal{L}_2\mathcal{Q}$ are still irreducible and coprime and $\mathcal{Q}^{-1}A \subset \mathbb{Z}^d$. However, this contradicts the minimality of $[\mathbb{Z}^d : \langle A \rangle]$, since $[\mathbb{Z}^d : \langle \mathcal{Q}^{-1}A \rangle] = [\mathbb{Z}^d : \langle A \rangle]/k$.

Case 2: (2) holds

Let $I_1, \dots, I_{pq}$ be the cosets of $\mathcal{P}\mathbb{Z}^d$ with $0 \in I_1$ and let $A_i = A \cap I_i$ for $i = 1, \dots, pq$. Note that the cosets I_i are the intersections of the cosets of $\mathcal{P}_1\mathbb{Z}^d$ and the cosets of $\mathcal{P}_2\mathbb{Z}^d$. If $0 < |A_i| \le c|A|$ for some i, then condition 2 of Lemma 4.2 implies that

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \ge ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A| - ((p+q)D_1 + D)|A|^{1-\sigma_1}.$$

We may therefore assume that $|A_i| > c|A|$ whenever $A_i \ne \emptyset$. Let $I_{i,k}$ be the cosets of $\mathcal{P}\mathbb{Z}^d \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$ in I_i for $k = 1, \dots, p$, where $0 \in I_{1,1}$, and let $A_{i,k} = A \cap I_{i,k} = A_i \cap I_{i,k}$.

Suppose that $|A_{i,k}| > c^2|A|$ whenever $A_{i,k} \ne \emptyset$. By (2), $|\phi_1(A') + \phi_2(A')| > |A'| = |\phi(A')|$. Hence, since $\phi(A') \subseteq \phi_1(A') + \phi_2(A')$, there are $a_1, a_2 \in A$ such that

$$\mathcal{L}_1 a_1 + \mathcal{L}_2 a_2 \notin (\mathcal{L}_1 + \mathcal{L}_2)a + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d$$

for all $a \in A$. Take i_1, k_1, i_2, k_2 such that $a_1 \in A_{i_1,k_1}, a_2 \in A_{i_2,k_2}$, so they are both non-empty. Then

$$\mathcal{L}_1 A_{i_1,k_1} + \mathcal{L}_2 A_{i_2,k_2} \subset \mathcal{L}_1 a_1 + \mathcal{L}_2 a_2 + \mathcal{L}_1\mathcal{P}\mathbb{Z}^d,$$

which is disjoint from any of the $\mathcal{L}_1 A_{i,k} + \mathcal{L}_2 A_{i,k}$. Therefore,

$$\begin{aligned}
|\mathcal{L}_1 A + \mathcal{L}_2 A| &\ge \sum_{i=1}^{pq}\sum_{k=1}^{p} |\mathcal{L}_1 A_{i,k} + \mathcal{L}_2 A_{i,k}| + |\mathcal{L}_1 A_{i_1,k_1} + \mathcal{L}_2 A_{i_2,k_2}| \\
&\ge ((p^{1/d} + q^{1/d})^d - \alpha)|A| - p^2 q D_1 |A|^{1-\sigma_1} + |A_{i_1,k_1}| \\
&\ge ((p^{1/d} + q^{1/d})^d - (1-c^2)\alpha)|A| - p^2 q D_1 |A|^{1-\sigma_1}.
\end{aligned}$$

Otherwise, by translating if necessary, we may assume that $|A_{1,1}| \le c^2|A| \le c|A_1|$ and $0 \in A_{1,1}$. Let $\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $\mathcal{Q}\mathbb{Z}^d = \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d$, so that $|\det \mathcal{Q}| = pq$. Set $\mathcal{M}_i = \mathcal{Q}^{-1}\mathcal{L}_i\mathcal{P}$. Since $\mathcal{L}_i\mathcal{P}\mathbb{Z}^d \subseteq \mathcal{L}_1\mathbb{Z}^d \cap \mathcal{L}_2\mathbb{Z}^d = \mathcal{Q}\mathbb{Z}^d$, we have $\mathcal{M}_i\mathbb{Z}^d \subseteq \mathbb{Z}^d$ for $i = 1, 2$, so $\mathcal{M}_i \in \mathrm{Mat}_d(\mathbb{Z})$. Moreover, $\mathcal{M}_1, \mathcal{M}_2$ are irreducible and coprime, with determinants of absolute value p and q, respectively.

If we let $B = \mathcal{P}^{-1}A_1 \subset \mathbb{Z}^d$, our aim now is to apply Lemma 4.2 to the sum $\mathcal{M}_1 B + \mathcal{M}_2 B$. Indeed, if we replace $\mathcal{P}_1, \mathcal{P}_2$ in that lemma by $\mathcal{P}_1', \mathcal{P}_2'$ chosen so that $\mathcal{P}_1'\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$ and $\mathcal{P}_2'\mathbb{Z}^d = \mathbb{Z}^d \cap \mathcal{M}_1^{-1}\mathcal{M}_2\mathbb{Z}^d$, the set A_1 by $B_1 = \mathcal{P}^{-1}A_{1,1}$, which, since $A_{1,1} = A_1 \cap \mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d$, satisfies $B_1 = B \cap \mathcal{P}^{-1}\mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d = B \cap \mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$, and A_1^1 by an appropriate non-empty subset $B_1^1 \subseteq B_1$ (which is possible since B_1 contains 0), then we have $0 < |B_1^1| \le |B_1| \le c|B|$, so condition 2 of Lemma 4.2 holds. Hence, by that lemma,

$$|\mathcal{M}_1 B + \mathcal{M}_2 B| \ge ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|B| - ((p+q)D_1 + D)|B|^{1-\sigma_1}.$$

This implies that

$$\begin{aligned}
|\mathcal{L}_1 A_1 + \mathcal{L}_2 A_1| &= |\mathcal{Q}^{-1}\mathcal{L}_1\mathcal{P}(\mathcal{P}^{-1}A_1) + \mathcal{Q}^{-1}\mathcal{L}_2\mathcal{P}(\mathcal{P}^{-1}A_1)| \\
&= |\mathcal{M}_1 B + \mathcal{M}_2 B| \\
&\ge ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|B| - ((p+q)D_1 + D)|B|^{1-\sigma_1} \\
&\ge ((p^{1/d} + q^{1/d})^d - (1-c)\alpha)|A_1| - ((p+q)D_1 + D)|A|^{1-\sigma_1}.
\end{aligned}$$

Thus,

$$\begin{aligned}|\mathcal{L}_1A+\mathcal{L}_2A| &\geq \sum_{i=2}^{pq}|\mathcal{L}_1A_i+\mathcal{L}_2A_i|+|\mathcal{L}_1A_1+\mathcal{L}_2A_1|\\ &\geq ((p^{1/d}+q^{1/d})^d-\alpha)(|A|-|A_1|)-pqD_1|A|^{1-\sigma_1}\\ &\quad +((p^{1/d}+q^{1/d})^d-(1-c)\alpha)|A_1|-((p+q)D_1+D)|A|^{1-\sigma_1}\\ &\geq ((p^{1/d}+q^{1/d})^d-\alpha)|A|+c\alpha|A_1|-((p+q+pq)D_1+D)|A|^{1-\sigma_1}\\ &\geq ((p^{1/d}+q^{1/d})^d-\alpha)|A|+c^2\alpha|A|-((p+q+pq)D_1+D)|A|^{1-\sigma_1}\\ &\geq ((p^{1/d}+q^{1/d})^d-(1-c^2)\alpha)|A|-(4p^2q^2D_1+D)|A|^{1-\sigma_1}.\end{aligned}$$

Case 3: (3) holds

Let A'' be the image of A in $\mathbb{Z}^d/L_2$. If we apply Lemma 4.4 to A'', but with the roles of $\mathcal{L}_1,\mathcal{L}_2$ swapped, we arrive at three similar cases. If either of the first two occurs, then we are again done as above. Otherwise, the third case holds, i.e., $\mathcal{P}\mathbb{Z}^d/L_2\subseteq A''$. Define $A_1,\mathcal{M}_1,\mathcal{M}_2,B$ as in Case 2 and partition B into $B_1\cup\cdots\cup B_p$, where the B_i belong to different cosets of $\mathbb{Z}^d\cap\mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$, and into $B^1\cup\cdots\cup B^q$, where the B^j belong to different cosets of $\mathbb{Z}^d\cap\mathcal{M}_1^{-1}\mathcal{M}_2\mathbb{Z}^d$.

Since $\mathcal{P}\mathbb{Z}^d/L_1\subseteq A'$, we have $\mathcal{P}\mathbb{Z}^d\subseteq A+L_1$ and so $\mathcal{P}\mathbb{Z}^d\subseteq A_1+L_1$, since $A_1=A\cap\mathcal{P}\mathbb{Z}^d$. Thus, $\mathbb{Z}^d=\mathcal{P}^{-1}A_1+\mathcal{P}^{-1}L_1$, which means that $B=\mathcal{P}^{-1}A_1$ intersects every coset of $\mathcal{P}^{-1}L_1=\mathbb{Z}^d\cap\mathcal{P}^{-1}\mathcal{L}_2^{-1}\mathcal{L}_1\mathcal{P}\mathbb{Z}^d=\mathbb{Z}^d\cap\mathcal{M}_2^{-1}\mathcal{M}_1\mathbb{Z}^d$, so all the B_i are non-empty. Similarly, all of the B^j are non-empty. Thus, condition 1 of Lemma 4.2 holds, so that

$$|\mathcal{M}_1B+\mathcal{M}_2B|\geq((p^{1/d}+q^{1/d})^d-(1-c)\alpha)|B|-((p+q)D_1+D)|B|^{1-\sigma_1}.$$

The same calculation as in Case 2 then shows that

$$|\mathcal{L}_1A+\mathcal{L}_2A|\geq((p^{1/d}+q^{1/d})^d-(1-c^2)\alpha)|A|-(4p^2q^2D_1+D)|A|^{1-\sigma_1},$$

as required. □

Theorem 4.6. *Let $\mathcal{L}_1,\mathcal{L}_2\in\mathrm{Mat}_d(\mathbb{Z})$ be irreducible, coprime linear transformations with $|\det\mathcal{L}_1|=p$ and $|\det\mathcal{L}_2|=q$. Then there are constants $\sigma_2>0$ and $D_2>0$ depending only on d, p and q such that*

$$|\mathcal{L}_1A+\mathcal{L}_2A|\geq(p^{1/d}+q^{1/d})^d|A|-D_2|A|^{1-\sigma_2}$$

for all finite $A\subset\mathbb{Z}^d$.

Proof. This follows from Lemma 4.5 just as Theorem 3.4 follows from Lemma 3.3. □

5 The size of $A+\lambda\cdot A$ for algebraic λ

In this section, we prove Theorem 1.7, our lower bound on $|A+\lambda\cdot A|$ for algebraic $\lambda\in\mathbb{R}$. Though our estimate applies for all finite $A\subset\mathbb{R}$, the following simple lemma of Krachun and Petrov [19, Lemma 2.1] allows us to restrict attention to sets $A\subset\mathbb{Q}[\lambda]$.

Lemma 5.1. *Suppose that $\lambda\in\mathbb{C}$ and A is a finite set of complex numbers. Then there exists a finite set $B\subset\mathbb{Q}[\lambda]$ such that $|B|=|A|$ and $|B+\lambda\cdot B|\leq|A+\lambda\cdot A|$.*

Suppose now that λ has minimal polynomial $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \in \mathbb{Q}[x]$. If we view $\mathbb{Q}[\lambda]$ as a d-dimensional $\mathbb{Q}$-vector space with basis $1, \lambda, \lambda^2, \ldots, \lambda^{d-1}$, then multiplication by λ is given by the linear transformation

$$\mathcal{L} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix} \in \mathrm{GL}_d(\mathbb{Q}).$$

Thus, the problem reduces to that of bounding $|A + \mathcal{L}A|$ for $A \subset \mathbb{Q}^d$. Let b be the smallest positive integer such that $ba_i \in \mathbb{Z}$ for all $i = 0, 1, \ldots, d-1$. Then, if we let

$$\mathcal{L}_1 = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & b \end{pmatrix}, \quad \mathcal{L}_2 = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -ba_0 \\ 1 & 0 & 0 & \cdots & 0 & -ba_1 \\ 0 & 1 & 0 & \cdots & 0 & -ba_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -ba_{d-1} \end{pmatrix} \in \mathrm{Mat}_d(\mathbb{Z}),$$

we see that $|A + \mathcal{L}A| = |\mathcal{L}_1(\mathcal{L}_1^{-1}A) + \mathcal{L}_2(\mathcal{L}_1^{-1}A)|$. Setting $B = \mathcal{L}_1^{-1}A$, the problem becomes that of bounding $|\mathcal{L}_1 B + \mathcal{L}_2 B|$ for $B \subset \mathbb{Q}^d$. By scaling, we may even assume that $B \subset \mathbb{Z}^d$. Therefore, in order to apply Theorem 4.6, we only need to verify that $\mathcal{L}_1, \mathcal{L}_2$ are irreducible and coprime. For this, we now derive general conditions for irreducibility and coprimeness. We first look at irreducibility.

Theorem 5.2. *$P, Q \in \mathrm{Mat}_d(\mathbb{Q})$ are irreducible if and only if they are invertible and the characteristic polynomial of $P^{-1}Q$ is irreducible over $\mathbb{Q}$.*

Proof. Suppose P, Q are irreducible. If P, say, is not invertible, then there is a one-dimensional subspace $U \subset \mathbb{Q}^d$ such that $PU = 0$. But then both PU and QU lie in the subspace QU of dimension at most 1, contradicting irreducibility.

Note that P, Q are irreducible iff $R = P^{-1}Q$ has no non-trivial invariant subspace over $\mathbb{Q}$. Let $p(x) \in \mathbb{Q}[x]$ be the characteristic polynomial of $P^{-1}Q$. If $P^{-1}Q$ has a non-trivial invariant subspace U, then restricting to U gives a linear transformation $R|_U : U \to U$. But the characteristic polynomial of $R|_U$ divides p, so p is reducible.

Conversely, suppose that $p = fg$ is reducible, with $\deg f, \deg g < d$. Then at least one of $f(R), g(R)$ is not invertible, since $0 = p(R) = f(R)g(R)$. Without loss of generality, assume that $f(R)$ is not invertible, so there is some $v \in \mathbb{Q}^d - \{0\}$ such that $f(R)v = 0$. If f has degree $e < d$, then $R^e v$ lies in the space $U = \langle v, Rv, \ldots, R^{e-1}v \rangle$. Thus, U is a non-trivial invariant subspace. □

For our coprimeness condition, we need the following lemma.

Lemma 5.3. *Let $P \in \mathrm{Mat}_d(\mathbb{Q})$ and $Q \in \mathrm{Mat}_d(\mathbb{Z})$ be such that $QP \in \mathrm{Mat}_d(\mathbb{Z})$. For $1 \le k \le d$, let m be a $k \times k$ minor of P, i.e., the determinant of a $k \times k$ submatrix. Then $m \det(Q) \in \mathbb{Z}$.*

Proof. Let m be the $k \times k$ minor corresponding to rows $S \subseteq [d]$ and columns $T \subseteq [d]$. Construct a matrix $R \in \mathrm{Mat}_d(\mathbb{Q})$ as follows: the T columns of R are just the T columns of P; the $S \times T^c$ submatrix of R is all zeroes; and the $S^c \times T^c$ submatrix of R is the identity matrix. Then $\det R = \pm m$, so that $\det(QR) = \pm m \det Q$. But the T columns of QR are the T columns of QP, which has all integer entries, and each of the other columns of QR is a column of Q, which also has integer entries. Thus, $QR \in \mathrm{Mat}_d(\mathbb{Z})$, so that $m \det Q = \pm \det(QR) \in \mathbb{Z}$. □

Theorem 5.4. *Suppose that $P, Q \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and $p(x) \in \mathbb{Q}[x]$ is the characteristic polynomial of $P^{-1}Q$. Then P, Q are coprime if and only if $c = |\det P|$ is the smallest positive integer such that $cp \in \mathbb{Z}[x]$.*

Proof. Let c' be the smallest positive integer such that $c'p \in \mathbb{Z}[x]$. Let $R, S \in \mathrm{GL}_d(\mathbb{Q})$ be such that $RPS, RQS \in \mathrm{Mat}_d(\mathbb{Z})$. Let $M = (RPS)^{-1}RQS = S^{-1}P^{-1}QS \in \mathrm{Mat}_d(\mathbb{Q})$. Then the characteristic polynomial of M is again p. By Lemma 5.3 with M and RPS as P and Q, if m is any $k \times k$ minor of M, then $m \det(RPS) \in \mathbb{Z}$. Suppose $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$. By looking at the expansion of $p(x) = \det(xI - M)$, we see that a_{d-k} can be written as a $\mathbb{Z}$-linear combination of $k \times k$ minors of M. Thus, $a_{d-k} \det(RPS) \in \mathbb{Z}$ for all k, so $c' \mid \det(RPS) = \pm c \det(RS)$. In particular, if we take both R and S to be the identity matrix, then $c' \mid c$.

Suppose now that $c' = |\det P|$. Then this implies that $|\det(RS)| \geq 1$, so P, Q are indeed coprime. Conversely, suppose that P, Q are coprime. Consider the rational canonical form of $P^{-1}Q$, which is a block diagonal matrix similar to $P^{-1}Q$ where each block looks like

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{k-1} \end{pmatrix}.$$

The characteristic polynomial of such a block is $x^k + c_{k-1}x^{k-1} + \cdots + c_0$ and the characteristic polynomial p of $P^{-1}Q$ is the product of the characteristic polynomials of its blocks. But, by Theorem 5.2, $p(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ is irreducible, so the rational canonical form of $P^{-1}Q$ consists of a single block. That is, there is some $S \in \mathrm{GL}_d(\mathbb{Q})$ such that

$$S^{-1}P^{-1}QS = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{d-1} \end{pmatrix}.$$

Let D be the diagonal matrix with entries $(1, 1, \ldots, 1, c')$. Then D and $DS^{-1}P^{-1}QS$ are integer matrices. Now set $R = DS^{-1}P^{-1}$, so that $RPS, RQS \in \mathrm{Mat}_d(\mathbb{Z})$. By coprimeness, $|\det R \det S| \geq 1$. But this implies that $c'/c \geq 1$, so $c \leq c'$. However, from before, we have $c' \mid c$, so that $c = c'$, as required. □

Using Theorems 5.2 and 5.4, it is now a simple matter to verify that $\mathcal{L}_1, \mathcal{L}_2$ are irreducible and coprime. Thus, by Theorem 4.6, we have that if $\lambda \in \mathbb{R}$ is an algebraic number with minimal polynomial $p(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x]$, where all the a_i are coprime, then there are $D, \sigma > 0$ such that

$$|A + \lambda \cdot A| \geq (|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d})^d |A| - D|A|^{1-\sigma}$$

holds for all finite $A \subset \mathbb{Q}[\lambda]$. But, taking the rescaling of the characteristic polynomial into account, $|\det(\mathcal{L}_1)| = |a_d|$ and $|\det(\mathcal{L}_2)| = |a_0|$, completing the proof of Theorem 1.7. Though we have not stressed the point before, it is worth noting that the same proof also goes through for $A \subset \mathbb{C}$ and $\lambda \in \mathbb{C}$.

6 Concluding remarks

Better bounds. Although Theorem 1.5 can be tight, we suspect that there is a stronger general bound. In analogy with the algebraic number setting, given $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Q})$ with minimal polynomial $f(x) \in \mathbb{Z}[x]$, which we assume to have coprime coefficients, suppose that $f(x) = \prod_{i=1}^d (a_i x + b_i)$ is a full complex factorisation of f and let $H(\mathcal{L}) = \prod_{i=1}^d (|a_i| + |b_i|)$. Our conjecture, a variant of a recent conjecture of Krachun and Petrov [19, Conjecture 2] that was itself inspired by a continuous analogue [19, Theorem 2], is then as follows.

Conjecture 6.1. *Let $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ be irreducible. Then, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq H(\mathcal{L}_1^{-1}\mathcal{L}_2)|A| - o(|A|).$$

Note that the coprimeness condition is unnecessary here, since if we were to replace $\mathcal{L}_1, \mathcal{L}_2$ with $\mathcal{P}\mathcal{L}_1\mathcal{Q}, \mathcal{P}\mathcal{L}_2\mathcal{Q}$ to make them coprime, then

$$H((\mathcal{P}\mathcal{L}_1\mathcal{Q})^{-1}(\mathcal{P}\mathcal{L}_2\mathcal{Q})) = H(\mathcal{Q}^{-1}\mathcal{L}_1^{-1}\mathcal{L}_2\mathcal{Q}) = H(\mathcal{L}_1^{-1}\mathcal{L}_2).$$

Moreover, Conjecture 6.1 implies our Theorem 1.5, since if $\mathcal{L}_1, \mathcal{L}_2$ are coprime, then, by Theorem 5.4, the minimal polynomial of $\mathcal{L}_1^{-1}\mathcal{L}_2$ over $\mathbb{Z}$ is $c_d x^d + c_{d-1}x^{d-1} + \cdots + c_0$, where $|c_d| = |\det(\mathcal{L}_1)|$ and $|c_0| = |c_d||\det(\mathcal{L}_1^{-1}\mathcal{L}_2)| = |\det(\mathcal{L}_2)|$. Therefore, by Hölder's inequality,

$$H(\mathcal{L}_1^{-1}\mathcal{L}_2) = \prod_{i=1}^d (|a_i| + |b_i|) \geq \left(\prod_{i=1}^d |a_i|^{1/d} + \prod_{i=1}^d |b_i|^{1/d} \right)^d = (|c_d|^{1/d} + |c_0|^{1/d})^d.$$

There should also be a suitable generalisation of Conjecture 6.1 to more than two variables, but, unlike Conjecture 1.4, which itself remains open for three or more variables, it is not at all obvious what this should be.

Lower-order terms. Unlike with sums of dilates (see, for instance, [1, 10, 17, 28]), we cannot in general hope for the error term in Theorem 1.5 to be a constant. Indeed, in two dimensions, if we set $A = \{(x, y) \mid 0 \leq x, y \leq n-1\}$ and $\mathcal{L}$ to be the anti-clockwise rotation about the origin through $\pi/2$, then $|A| = n^2$, but $|A + \mathcal{L}A| = (2n-1)^2 = 4|A| - 4|A|^{1/2} + 1$. That is, the error term in this case is a multiple of $|A|^{1/2}$. Similarly, in d dimensions, there are examples for which the error term is a multiple of $|A|^{1-1/d}$. Following Shakan [28], we conjecture that there are no significantly worse examples.

Conjecture 6.2. *Suppose that $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there is a constant D such that, for any finite subset A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_1 A + \cdots + \mathcal{L}_k A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d} \right)^d |A| - D|A|^{1-1/d}.$$

A proof of this conjecture when $k = 2$ would already constitute a significant improvement on our Theorem 1.5, which gives an error term of the form $D|A|^{1-\sigma}$ for some $\sigma > 0$ which depends not only on d, but also on $|\det(\mathcal{L}_1)|$ and $|\det(\mathcal{L}_2)|$.

Real-valued analogues. Our main result, Theorem 1.5, can be extended to subsets of $\mathbb{R}^d$ as follows.

Theorem 6.3. *Suppose that $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then there are constants D, $\sigma > 0$ such that, for any finite subset A of $\mathbb{R}^d$,*

$$|\mathcal{L}_1 A + \mathcal{L}_2 A| \geq \left(|\det(\mathcal{L}_1)|^{1/d} + |\det(\mathcal{L}_2)|^{1/d} \right)^d |A| - D|A|^{1-\sigma}.$$

To see this, suppose that $A \subset \mathbb{R}^d$ and let $B \subset \mathbb{R}$ be the set consisting of all real numbers that appear as a coordinate of some element of A. For any fixed natural number k, a standard result in additive combinatorics (see, for instance, [29, Lemma 5.25]) allows us to find a set $B' \subset \mathbb{Z}$ which has a Freiman isomorphism of order k with B. We then obtain a set $A' \subset \mathbb{Z}^d$ by replacing each coordinate of each element of A with its image in B'. Provided k is chosen sufficiently large in terms of the coefficients of $\mathcal{L}_1$ and $\mathcal{L}_2$, it is now easy to verify that $|\mathcal{L}_1 A' + \mathcal{L}_2 A'| = |\mathcal{L}_1 A + \mathcal{L}_2 A|$. Therefore, since the conclusion of the theorem is known for all $A' \subset \mathbb{Z}^d$, it is also true for all $A \subset \mathbb{R}^d$.

Our results also allow us to say something about the size of $A + \mathcal{L}A$ when $\mathcal{L}$ has real algebraic entries. In this case, by a process similar to that used in Section 5 to estimate $|A + \lambda \cdot A|$ for algebraic λ and $A \subset \mathbb{R}$, we can convert the problem of estimating $|A + \mathcal{L}A|$ to one of estimating $|\mathcal{L}_1 B + \mathcal{L}_2 B|$ for some integer matrices $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_{d'}(\mathbb{Z})$ and $B \subset \mathbb{Z}^{d'}$. Indeed, a generalisation of Lemma 5.1 allows us to assume that $A \subset \mathbb{Q}[\lambda_1, \lambda_2, \ldots]^d$, where $\lambda_1, \lambda_2, \ldots$ are the entries of $\mathcal{L}$, so that the problem becomes equivalent to estimating $|A' + \mathcal{L}'A'|$ for some $\mathcal{L}' \in \mathrm{Mat}_{d'}(\mathbb{Q})$ and some $A' \subset \mathbb{Q}^{d'}$ with $|A'| = |A|$. Clearing denominators, we can then rephrase this as the problem of estimating $|\mathcal{L}_1 B + \mathcal{L}_2 B|$ for some $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_{d'}(\mathbb{Z})$ and some $B \subset \mathbb{Z}^{d'}$ with $|B| = |A|$. Finally, if $\mathcal{L}_1, \mathcal{L}_2$ are not irreducible or coprime, we can make them irreducible by restricting to a subspace and coprime by replacing them with a suitable $\mathcal{P}\mathcal{L}_1\mathcal{Q}, \mathcal{P}\mathcal{L}_2\mathcal{Q}$.

References

[1] A. Balog and G. Shakan, On the sum of dilations of a set, *Acta Arith.* **164** (2014), 153–162.

[2] A. Balog and G. Shakan, Sum of dilates in vector spaces, *North-West. Eur. J. Math.* **1** (2015), 46–54.

[3] Y. Bilu, Structure of sets with small sumset, *Astérisque* **258** (1999), 77–108.

[4] B. Bollobás and I. B. Leader, Sums in the grid, *Discrete Math.* **162** (1996), 31–48.

[5] E. Breuillard and B. Green, Contractions and expansion, *Eur. J. Combin.* **34** (2013), 1293–1296.

[6] B. Bukh, Sums of dilates, *Combin. Probab. Comput.* **17** (2008), 627–639.

[7] Y.-G. Chen and J.-H. Fang, Sums of dilates in the real numbers, *Acta Arith.* **182** (2018), 231–241.

[8] J. Cilleruelo, Y. O. Hamidoune and O. Serra, On sums of dilates, *Combin. Probab. Comput.* **18** (2009), 871–880.

[9] J. Cilleruelo, M. Silva and C. Vinuesa, A sumset problem, *J. Comb. Number Theory* **2** (2010), 79–89.

[10] D. Conlon and J. Lim, Difference sets in $\mathbb{R}^d$, preprint available at arXiv:2110.09053 [math.CO].

[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, 25 pp.

[12] G. A. Freiman, **Foundations of a structural theory of set addition**, Translations of Mathematical Monographs, Vol. 37, American Mathematical Society, Providence, R.I., 1973.

[13] R. J. Gardner, The Brunn–Minkowski inequality, *Bull. Amer. Math. Soc.* **39** (2002), 355–405.

[14] R. J. Gardner and P. Gronchi, A Brunn–Minkowski inequality for the integer lattice, *Trans. Amer. Math. Soc.* **353** (2001), 3995–4024.

[15] B. Green and T. Tao, Compressions, convex geometry and the Freiman–Bilu theorem, *Q. J. Math.* **57** (2006), 495–504.

[16] 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.

[17] M. Huicochea, On the sum of dilates in $\mathbb{R}^d$, *North-West. Eur. J. Math.* **7** (2021), 7–27.

[18] S. Konyagin and I. Łaba, Distance sets of well-distributed planar sets for polygonal norms, *Israel J. Math.* **152** (2006), 157–179.

[19] D. Krachun and F. Petrov, On the size of $A + \lambda A$ for algebraic λ, preprint available at arXiv:2010.00119 [math.CO].

[20] Z. Ljujić, A lower bound for the size of a sum of dilates, *J. Comb. Number Theory* **5** (2013), 31–51.

[21] A. Mudgal, Sums of linear transformations in higher dimensions, *Q. J. Math.* **70** (2019), 965–984.

[22] A. Mudgal, Difference sets in higher dimensions, *Math. Proc. Cambridge Philos. Soc.* **171** (2021), 467–480.

[23] A. Mudgal, New lower bounds for cardinalities of higher dimensional difference sets and sumsets, preprint available at arXiv:2110.11300 [math.CO].

[24] I. Z. Ruzsa, Sums of finite sets, in Number theory (New York, 1991–1995), 281–293, Springer, New York, 1996.

[25] T. Sanders, Appendix to "Roth's theorem on progressions revisited" by J. Bourgain, *J. Anal. Math.* **104** (2008), 193–206.

[26] T. Sanders, On the Bogolyubov–Ruzsa lemma, *Anal. PDE* **5** (2012), 627–655.

[27] T. Schoen, Near optimal bounds in Freiman's theorem, *Duke Math. J.* **158** (2011), 1–12.

[28] G. Shakan, Sum of many dilates, *Combin. Probab. Comput.* **25** (2016), 460–469.

[29] T. Tao and V. Vu, **Additive combinatorics**, Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge, 2006.