Sums of algebraic dilates

David Conlon* Jeck Lim†

Abstract

We show that if $\lambda_1, \dots, \lambda_k$ are algebraic numbers, then

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

for all finite subsets A of $\mathbb{C}$, where $H(\lambda_1, \dots, \lambda_k)$ is an explicit constant that is best possible. The proof combines several ingredients, including a lower bound estimate on the measure of sums of linear transformations of compact sets in $\mathbb{R}^d$, a variant of Freiman's theorem tuned specifically to sums of dilates and the analysis of what we call lattice density, which succinctly captures how a subset of $\mathbb{Z}^d$ is arranged relative to a given flag of lattices. As an application, we revisit the study of sums of linear transformations of finite sets, in particular proving an asymptotically best possible lower bound for sums of two linear transformations.

1 Introduction

For any subset A of $\mathbb{C}$ and $\lambda_1, \dots, \lambda_k \in \mathbb{C}$, the sum of dilates $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ is given by

$$A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A := \{a_0 + \lambda_1 a_1 + \cdots + \lambda_k a_k : a_0, a_1, \dots, a_k \in A\}.$$

Our concern in this paper will be with estimating the minimum size of $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ in terms of $|A|$. For $\lambda_1, \dots, \lambda_k \in \mathbb{Q}$, this problem was essentially solved by Bukh [4], from whose results it follows that if $\lambda_i = p_i/q$ for q as small as possible for such a common denominator, then

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq (|p_1| + \cdots + |p_k| + |q|)|A| - o(|A|)$$

for all finite subsets A of $\mathbb{C}$, which is best possible up to the lower-order term. This result was later sharpened by Balog and Shakan [1] when $k = 1$ and then Shakan [18] in the general case, improving the $o(|A|)$ term to a constant depending only on $\lambda_1, \dots, \lambda_k$.

When at least one of the λ_i is transcendental, it was shown by Konyagin and Łaba [11] that

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| = \omega(|A|).$$

The problem of giving more precise lower bounds for $|A+\lambda \cdot A|$ when λ is transcendental was studied in some depth by Sanders [15, 16] and Schoen [17], with progress tied to advances in quantitative

*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.

estimates for Freiman's theorem on sets of small doubling. Using quite different techniques, Conlon and Lim [6] recently resolved this problem, showing that there is a constant c such that

$$|A + \lambda \cdot A| \geq e^{c\sqrt{\log |A|}}|A|,$$

which, by a construction of Konyagin and Łaba, is best possible up to the value of c.

Our focus here will be on the complementary case, where each of $\lambda_1, \dots, \lambda_k$ is algebraic. Early results in this direction were proved by Breuillard and Green [2] and Chen and Fang [5], with the latter showing that, for any fixed $\lambda \geq 1$, $|A + \lambda \cdot A| \geq (1 + \lambda)|A| - o(|A|)$ for all finite subsets A of $\mathbb{R}$. The problem of giving more precise lower bounds for $|A + \lambda \cdot A|$ when λ is algebraic was raised explicitly by Shakan [18] and by Krachun and Petrov [12], with the latter authors conducting the first systematic study and making the first concrete conjectures.

To state their conjecture, suppose that $f(x) \in \mathbb{Z}[x]$ 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. If we set $H(\lambda) := \prod_{i=1}^{d}(|a_i| + |b_i|)$, the conjecture of Krachun and Petrov [12] is then as follows.

Conjecture 1.1. *For any algebraic number λ,*

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

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

Krachun and Petrov [12] gave some evidence for their conjecture by proving it in the special case where $\lambda = \sqrt{2}$. Subsequently, as a consequence of their work [7] on a conjecture of Bukh regarding sums of linear transformations, Conlon and Lim verified the conjecture for all λ of the form $(p/q)^{1/d}$ with $p, q, d \in \mathbb{N}$. Assuming all of p, q and d are as small as possible for such a representation, their result, which includes that of Krachun and Petrov, says that

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

for all finite subsets A of $\mathbb{C}$. Their results also imply a general lower bound for sums of algebraic dilates, though this bound only matches the conjectured one in some special cases.

More recently, Krachun and Petrov [13] have revisited the problem, proving their conjecture in full whenever λ is an algebraic integer. This is somewhat incomparable to the result of Conlon and Lim, since $(p/q)^{1/d}$, when written in lowest terms, is only an algebraic integer when $q = 1$. Here we again revisit the problem, proving Conjecture 1.1 in full for all algebraic numbers. Our method also extends to longer sums of algebraic dilates, so we will state our results in that level of generality.

To state the result, given algebraic numbers $\lambda_1, \dots, \lambda_k$, recall that if the field extension $K := \mathbb{Q}(\lambda_1, \dots, \lambda_k)$ of $\mathbb{Q}$ is of degree $d = \deg(K/\mathbb{Q})$, then there are exactly d different complex embeddings $\sigma_1, \dots, \sigma_d : K \to \mathbb{C}$. We also need to define the *denominator ideal* (see, for example, [19]), which is the ideal in the ring of integers $\mathcal{O}_K$ given by

$$\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K} := \{x \in \mathcal{O}_K \mid x\lambda_l \in \mathcal{O}_K \text{ for } l = 1, \dots, k\}.$$

The key quantity $H(\lambda_1, \dots, \lambda_k)$ that plays the role of $H(\lambda)$ for sums of many algebraic dilates is then

$$H(\lambda_1, \dots, \lambda_k) := N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}) \prod_{i=1}^{d}(1 + |\sigma_i(\lambda_1)| + |\sigma_i(\lambda_2)| + \cdots + |\sigma_i(\lambda_k)|),$$

where $N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K})$ is the ideal norm of $\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$, equal to $[\mathcal{O}_K : \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}]$. To see that this indeed generalises $H(\lambda)$, observe that we can write the minimal polynomial $f(x) \in \mathbb{Z}[x]$ of λ as $f(x) = D(x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_d)$ for some integer D and $\lambda_1,\dots,\lambda_d$ the conjugates of λ. Then $H(\lambda) = |D|(1+|\lambda_1|)\cdots(1+|\lambda_d|)$ and it can be shown that $|D| = N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda;K})$. With this definition in place, our main result, which is best possible up to the behaviour of the lower-order term, is as follows.

Theorem 1.2. *For any algebraic numbers $\lambda_1,\dots,\lambda_k$,*

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

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

In practice, we will view the problem of estimating sums of algebraic dilates as one about estimating sums of linear transformations. More precisely, if we consider the number field $K = Q(\lambda_1,\dots,\lambda_k)$ as a vector space over $\mathbb{Q}$, that is, as $\mathbb{Q}^d$ with $d = \deg(K/\mathbb{Q})$, then multiplication by λ_i becomes a linear map $\mathcal{M}_i$ from $\mathbb{Q}^d$ to itself, so the problem of giving a lower bound for $|A+\lambda_1\cdot A+\cdots+\lambda_k\cdot A|$ for $A \subset \mathbb{R}$ becomes equivalent to the analogous problem for $|A+\mathcal{M}_1A+\cdots+\mathcal{M}_kA|$ for $A \subset \mathbb{Q}^d$. A further reduction (see Section 2 for details) then recasts the problem in terms of estimating $|\mathcal{L}_0A + \mathcal{L}_1A + \cdots + \mathcal{L}_kA|$ for $\mathcal{L}_0,\mathcal{L}_1,\dots,\mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ and $A \subset \mathbb{Z}^d$.

Such sums of linear transformations have been studied before [3, 7, 14], with much of the motivation coming from a conjecture of Bukh asking whether a discrete Brunn–Minkowski-type inequality holds for sums of linear transformations. A corrected version of his original conjecture, first stated in [7], is as follows.

Conjecture 1.3. *Suppose that $\mathcal{L}_0,\dots,\mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then*

$$|\mathcal{L}_0A + \cdots + \mathcal{L}_kA| \geq \left(|\det(\mathcal{L}_0)|^{1/d} + \cdots + |\det(\mathcal{L}_k)|^{1/d}\right)^d |A| - o(|A|)$$

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

The conditions on $\mathcal{L}_0,\dots,\mathcal{L}_k$, that they be irreducible and coprime, are necessary, with irreducibility guaranteeing that the problem does not reduce to one of lower dimension and coprimeness that it cannot be restated in terms of matrices with smaller determinants. The formal definitions are as follows, though we refer the reader to [7] for a more complete discussion and some illustrative examples.

Definition 1.4. We say that $\mathcal{L}_0,\dots,\mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are *irreducible* if there are no non-trivial subspaces U, V of $\mathbb{Q}^d$ of the same dimension such that $\mathcal{L}_iU \subseteq V$ for all i.

Definition 1.5. We say that $\mathcal{L}_0,\dots,\mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ 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

$$\mathcal{P}\mathcal{L}_0\mathcal{Q}, \mathcal{P}\mathcal{L}_1\mathcal{Q}, \dots, \mathcal{P}\mathcal{L}_k\mathcal{Q} \in \mathrm{Mat}_d(\mathbb{Z}).$$

In particular, $\mathcal{L}_0\mathbb{Z}^d + \cdots + \mathcal{L}_k\mathbb{Z}^d = \mathbb{Z}^d$.

For $k = 1$, Conjecture 1.3 was fully resolved in [7] and the lower bound for $|A + \lambda \cdot A|$ when λ is of the form $(p/q)^{1/d}$ followed as a corollary. Here we work in the opposite direction, showing

that our main result, Theorem 1.2, on sums of algebraic dilates implies a lower bound for sums of certain linear transformations. To state this result requires some further definitions, the first of which is an additional condition beyond irreducibility and coprimeness that a collection of linear transformations must satisfy for our methods to apply.

Definition 1.6. We say that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Q})$ are *pre-commuting* if there is some $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ such that $\mathcal{P}\mathcal{L}_0, \dots, \mathcal{P}\mathcal{L}_k$ pairwise commute.

Suppose now that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are non-zero, pre-commuting, irreducible and coprime. Let G be the polynomial

$$G(x_0, \dots, x_k) := \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k).$$

If $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ is such that $\mathcal{P}\mathcal{L}_0, \dots, \mathcal{P}\mathcal{L}_k$ are pairwise commuting, then, by a folklore result, these matrices are simultaneously upper-triangularisable over $\mathbb{C}$, so G factorises into linear terms

$$G(x_0, \dots, x_k) = \prod_{i=1}^{d} (a_{0i}x_0 + \cdots + a_{ki}x_k).$$

We may then define $H(\mathcal{L}_0, \dots, \mathcal{L}_k)$ to be the quantity

$$H(\mathcal{L}_0, \dots, \mathcal{L}_k) := \prod_{i=1}^{d} (|a_{0i}| + \cdots + |a_{ki}|).$$

With this definition in place, our main result about sums of linear transformations, which is again best possible up to the lower-order term, is as follows.

Theorem 1.7. *Suppose that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are pre-commuting, irreducible and coprime. Then*

$$|\mathcal{L}_0A + \cdots + \mathcal{L}_kA| \geq H(\mathcal{L}_0, \dots, \mathcal{L}_k)|A| - o(|A|)$$

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

The first step in establishing our results is to prove a continuous analogue of this statement, a sharpening of the estimate coming from the Brunn–Minkowski inequality standing in the same relation to our results as that inequality does to Conjecture 1.3. For $k = 1$, such a continuous result was proved by Krachun and Petrov [12]. We extend it here to sums of several pre-commuting linear transformations. Our main contribution, Theorem 1.2, whose proof occupies the bulk of this paper, says that a discrete version of this continuous estimate holds for sums of pre-commuting linear transformations corresponding to sums of algebraic dilates. The proof of Theorem 1.7 then involves showing that this seemingly special case really encapsulates all pre-commuting families.

Before moving on to a more in-depth discussion of our proof and what is novel about it, we note that for $k = 1$ the condition that the matrices $\mathcal{L}_0$ and $\mathcal{L}_1$ be pre-commuting is always true, since the irreducibility condition implies that $\mathcal{L}_0$ and $\mathcal{L}_1$ are invertible, so we may take $\mathcal{P} = \mathcal{L}_0^{-1}$. As such, we have the following corollary of Theorem 1.7, resolving another conjecture of Krachun and Petrov [12] (see also [7]) and, unlike the $k = 1$ case of Conjecture 1.3 verified in [7], best possible up to the lower-order term for all $\mathcal{L}_0$ and $\mathcal{L}_1$.

Corollary 1.8. *Suppose that $\mathcal{L}_0, \mathcal{L}_1 \in \mathrm{Mat}_d(\mathbb{Z})$ are irreducible and coprime. Then*

$$|\mathcal{L}_0A + \mathcal{L}_1A| \geq H(\mathcal{L}_0, \mathcal{L}_1)|A| - o(|A|)$$

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

1.1 A sketch of the proof

Our overall strategy is similar to that used by Krachun and Petrov [13] to treat the case of algebraic integers. After rephrasing the problem in terms of sums of linear transformations, their approach can be summarised as having the following three steps:

1. Establishing a continuous version of the required estimate.
2. Reducing to the case where A is a dense subset of a box.
3. Representing the discrete set A by a continuous set $\overline{A}$.

The idea is that Step 2 guarantees that the $\overline{A}$ obtained in Step 3 is well-behaved. One can then apply the continuous variant from Step 1 to $\overline{A}$ and the required result in the discrete world follows. However, despite having the same general outline, our proof is significantly more complex. We now discuss each step in turn, though we refer the reader to the relevant sections for more details and precise definitions.

Step 1 is the part which is most similar to that of Krachun and Petrov. After lifting the problem to one about sums of certain pre-commuting linear transformations, we prove a tight lower bound for the continuous analogue of this problem by partitioning the underlying space into eigenspaces and then symmetrising our set along these eigenspaces.

For their Step 2, Krachun and Petrov make use of Freiman's theorem on sets of small doubling, one version of which says that any finite set of reals A with $|A+A| \leq C|A|$ is contained in a small generalised arithmetic progression (or GAP, for brevity). For our result, we need to prove a novel variant of Freiman's theorem for sets A with a small sum of dilates, that is, with

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C|A|.$$

It is not hard to show that any such A also has small doubling, so, by the usual version of Freiman's theorem, it must be contained in a small GAP. However, a GAP does not necessarily have a small sum of dilates. Our variant of Freiman's theorem, stated below, says instead that A is contained in what we call an $\mathcal{O}_K$-GAP, which shares with A the property that it has a small sum of dilates.

Theorem 1.9. *For every $C > 0$ and $p \in \mathbb{N}$, there are constants n and F such that for any $A \subset K$ satisfying*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C|A|,$$

there exists a p-proper $\mathcal{O}_K$-GAP $P \subset K$ containing A of dimension at most n and size at most $F|A|$.

To prove this result, we first need to extend several results in additive geometry, a term we borrow from Tao and Vu [20, Chapter 3], to the ring of integers $\mathcal{O}_K$. Once the theorem is in place, we can map A to a dense subset of the box $[0, N)^d$ via a Freiman isomorphism of the surrounding $\mathcal{O}_K$-GAP, reducing the problem, as promised, to the case of a dense set.

Step 3 is the main and most difficult step. To say something about it, we first describe the method used by Krachun and Petrov [13] to estimate $|A + \lambda \cdot A|$ when λ is an algebraic integer. As indicated earlier, they viewed this problem in terms of estimating the size of $|A + \mathcal{L}A|$ where A is a dense subset of the box $[N]^d$ and $\mathcal{L} \in \mathrm{Mat}_d(\mathbb{Z})$ is a linear transformation corresponding to multiplication by λ and we will discuss it in these terms here.

A naive way of representing A by a continuous set $\overline{A}$ is to divide the box $[N]^d$ into small cubes and set $\overline{A} \subset \mathbb{R}^d$ to be the union of the cubes which intersect A. However, this is not a good representation, since the volume of $\overline{A}$ can be very different from $|A|$. Indeed, if A consists of all the points in $[N]^d$ with even coordinates, its representation $\overline{A}$ would be the same as if A contained all the points of $[N]^d$.

Krachun and Petrov's solution is to introduce a new dimension to encode the "local density" of A at a point x, which is, roughly speaking, the relative density of A within a small box containing x. More precisely, their continuous representation is a (compact) set $\overline{A} \subset \mathbb{R}^{d+1}$, which can be seen as having a base in $\mathbb{R}^d$ resembling A, as described in the naive way above, and fibres in $\mathbb{R}$, with the fibre at the point $x \in \mathbb{R}^d$ being the interval $[0, r]$, where r is the local density of A at x. In particular, the volume of $\overline{A}$ matches the size $|A|$. The key to their approach is the following simple observation.

Observation 1.10. *The local density of $B = A + \mathcal{L}A$ at $x + \mathcal{L}y$ is at least the local density of A at x.*

If $\overline{B}$ is the continuous representation of B, then this observation is equivalent to saying that $\overline{B}$ contains $\overline{A} + \mathcal{L}'(\overline{A})$, where $\mathcal{L}' : \mathbb{R}^{d+1} \to \mathbb{R}^{d+1}$ is given by $\mathcal{L}'(x, y) = (\mathcal{L}x, 0)$ for $x \in \mathbb{R}^d$ and $y \in \mathbb{R}$. Therefore, $\mathrm{Vol}(\overline{B}) \geq \mathrm{Vol}(\overline{A} + \mathcal{L}'(\overline{A}))$. One can then apply the continuous version of sums of dilates to obtain a tight lower bound for $\mathrm{Vol}(\overline{A} + \mathcal{L}'(\overline{A}))$ in terms of $\mathrm{Vol}(\overline{A})$ and translate the result back to the discrete world using the fact that $\mathrm{Vol}(\overline{A}) = |A|$.

The problem with extending this approach to general algebraic λ is that Observation 1.10 is too weak. Indeed, if λ is not integral, estimating $|A + \lambda \cdot A|$ is equivalent to estimating $|\mathcal{L}_1 A + \mathcal{L}_2 A|$ for some $\mathcal{L}_1, \mathcal{L}_2 \in \mathrm{Mat}_d(\mathbb{Z})$ and A a dense subset of $[N]^d$. The analogue of the observation in this situation is that the local density of $\mathcal{L}_1 A + \mathcal{L}_2 A$ at $\mathcal{L}_1 x + \mathcal{L}_2 y$ is at least $\frac{1}{|\det \mathcal{L}_1|}$ times the local density of A at x. However, this is not tight, since if A contains all the lattice points in some convex region, then the local density of A is 1 uniformly and, by coprimeness, we also expect the local density of $\mathcal{L}_1 A + \mathcal{L}_2 A$ to be 1 uniformly. But the observation only guarantees that the local density of $\mathcal{L}_1 A + \mathcal{L}_2 A$ is at least $\frac{1}{|\det \mathcal{L}_1|}$, which is less than 1 if λ is not integral.

Since the local structure of $\mathcal{L}_1 A + \mathcal{L}_2 A$ at $\mathcal{L}_1 x + \mathcal{L}_2 y$ depends on the local structure of A at x and y, which can look completely different, we need to consider asymmetric sums $\mathcal{L}_1 A_1 + \mathcal{L}_2 A_2$. As an example, consider the periodic sets $A_1, A_2 \subset \mathbb{Z}$ given by $A_1 = \{0, 3\} + 6\mathbb{Z}$ and $A_2 = \{0, 4\} + 6\mathbb{Z}$ and the sums $2 \cdot A_1 + 3 \cdot A_2$ and $2 \cdot A_2 + 3 \cdot A_1$ (for technical reasons we work with periodic sets when defining our notion of local density). Both A_1, A_2 have density $1/3$, whereas $2 \cdot A_1 + 3 \cdot A_2 = 6\mathbb{Z}$ has density $1/6$ and $2 \cdot A_2 + 3 \cdot A_1 = \{0, 2, 3, 5\} + 6\mathbb{Z}$ has density $2/3$. Notice that although $2 \cdot A_1 + 3 \cdot A_2$ is less dense than A_1 and A_2, the swapped sum $2 \cdot A_2 + 3 \cdot A_1$ is more dense. In fact, this observation holds more generally.

Observation 1.11. *Suppose A_1 has local density σ_1 at x and A_2 has local density σ_2 at y. If $\mathcal{L}_1 A_1 + \mathcal{L}_2 A_2$ has local density η at $\mathcal{L}_1 x + \mathcal{L}_2 y$ and $\mathcal{L}_1 A_2 + \mathcal{L}_2 A_1$ has local density η' at $\mathcal{L}_1 y + \mathcal{L}_2 x$, then $\eta\eta' \geq \sigma_1 \sigma_2$.*

This somewhat resolves the previous issue: although $B = \mathcal{L}_1 A + \mathcal{L}_2 A$ can be locally less dense than A in some places, it must be more dense in others. To justify this observation, consider the sets A_1, A_2 as before. Draw the elements of $\mathbb{Z}/6\mathbb{Z}$ as a 2×3 grid according to their residues modulo 2 and 3 and scale the grid to be a square of side length 1. Denote by $\mathrm{LD}(A_1)$ the union of the cells representing the residues modulo 6 contained in A_1 and similarly for $\mathrm{LD}(A_2)$ (see Figure 1). Note

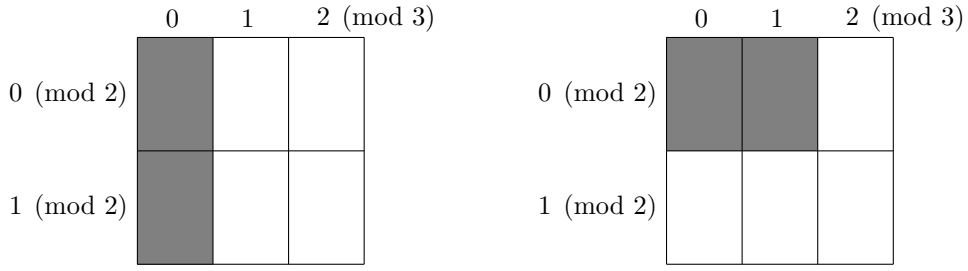

Figure 1: The shaded regions are $\mathrm{LD}(A_1)$ and $\mathrm{LD}(A_2)$.

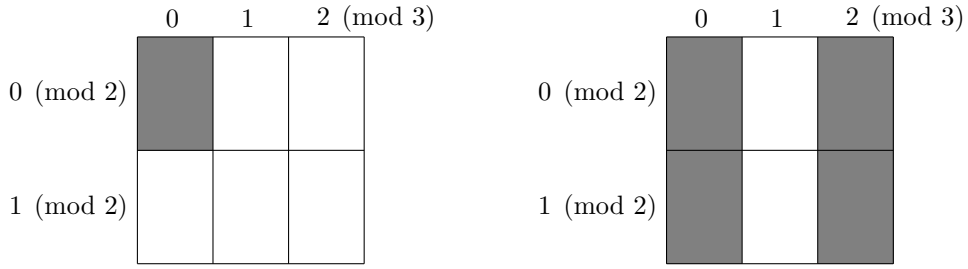

Figure 2: The shaded regions are $\mathrm{LD}(2 \cdot A_1 + 3 \cdot A_2)$ and $\mathrm{LD}(2 \cdot A_2 + 3 \cdot A_1)$.

that the density of A_i is equal to the volume of $\mathrm{LD}(A_i)$. Then do the same for $2 \cdot A_1 + 3 \cdot A_2$ and $2 \cdot A_2 + 3 \cdot A_1$ (see Figure 2).

Writing π_1 and π_2 for the projections onto the mod 3 and mod 2 axes, respectively, we see that $\mathrm{LD}(2 \cdot A_1 + 3 \cdot A_2)$ is a $\pi_1(\mathrm{LD}(A_1)) \times \pi_2(\mathrm{LD}(A_2))$ rectangle, while, if we allow a permutation of the columns, $\mathrm{LD}(2 \cdot A_2 + 3 \cdot A_1)$ is a $\pi_1(\mathrm{LD}(A_2)) \times \pi_2(\mathrm{LD}(A_1))$ rectangle. This justifies Observation 1.11, that $\mathrm{Vol}(\mathrm{LD}(2 \cdot A_1 + 3 \cdot A_2)) \cdot \mathrm{Vol}(\mathrm{LD}(2 \cdot A_2 + 3 \cdot A_1)) \geq \mathrm{Vol}(\mathrm{LD}(A_1)) \cdot \mathrm{Vol}(\mathrm{LD}(A_2))$, in this case. We also note that $|\pi_1(\mathrm{LD}(A_i))|$ is preserved under $\mathcal{L}_1 = 2\times$, while $|\pi_2(\mathrm{LD}(A_i))|$ is preserved under $\mathcal{L}_2 = 3\times$.

The set $\mathrm{LD}(A)$, which records how A is arranged relative to certain lattices, is roughly what we call the "lattice density". More precisely, for a (periodic) set $A \subseteq \mathbb{Z}^d$ and a flag of lattices $\mathcal{F} = \{L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k\}$, the lattice density $\mathrm{LD}(A; \mathcal{F})$ is a compact downset in $[0,1]^{k+1}$ which encodes information about the density of A relative to the lattices L_l. Our continuous representation $\overline{A}$ is then a compact subset of $\mathbb{R}^{d+k+1}$ with a base in $\mathbb{R}^d$ resembling A and fibres in $\mathbb{R}^{k+1}$ equal to the local lattice density at each point of A.

Once again, estimating $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ is equivalent to estimating $|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A|$ for some $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$. The key now, proved through a refinement argument, is that one can find two flags $\mathcal{F}, \mathcal{G}$ such that $\pi_{i+1}(\mathrm{LD}(\mathcal{L}_i A; \mathcal{G})) \approx \pi_{i+1}(\mathrm{LD}(A; \mathcal{F}))$ for each $i = 0, \ldots, k$. In turn, this allows us to show that if $A_0, \ldots, A_k \subset A$ are (periodic) sets, then $\mathrm{LD}(\mathcal{L}_0 A_0 + \cdots + \mathcal{L}_k A_k; \mathcal{G})$ roughly contains the cuboid with side lengths

$$|\pi_1(\mathrm{LD}(A_0; \mathcal{F}))|, \ldots, |\pi_{k+1}(\mathrm{LD}(A_k; \mathcal{F}))|.$$

By making appropriate choices of $A_0, \ldots, A_k \subset A$ locally, this implies that if $B = \mathcal{L}_0 A + \cdots + \mathcal{L}_k A$, then $\overline{B} \subset \mathbb{R}^{d+k+1}$ contains the sumset $\mathcal{L}_0' \overline{A} + \cdots + \mathcal{L}_k' \overline{A}$, where $\mathcal{L}_i' : \mathbb{R}^{d+k+1} \to \mathbb{R}^{d+k+1}$ is given by

$\mathcal{L}_i'(x,y) = (\mathcal{L}_i x, \pi_{i+1}(y))$ for $x \in \mathbb{R}^d$ and $y \in \mathbb{R}^{k+1}$. In line with the application of Observation 1.10 in the algebraic integer case, we can then apply our continuous estimate to $\mathcal{L}_0'\overline{A} + \cdots + \mathcal{L}_k'\overline{A}$, which in turn yields the desired result in the discrete case.

1.2 Notation

Throughout the paper, we will use the following notation:

- $\lambda_0, \lambda_1, \ldots, \lambda_k$ are algebraic numbers with $\lambda_0 = 1$.
- $K := \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$ is the number field generated by $\lambda_1, \ldots, \lambda_k$.
- The degree of K over $\mathbb{Q}$ is $d := \deg(K/\mathbb{Q})$, so $K \cong \mathbb{Q}^d$.
- The ring of integers over K is denoted by $\mathcal{O}_K$, so $\mathcal{O}_K \cong \mathbb{Z}^d$.
- We write $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} = \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^d$ and $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C} \cong \mathbb{C}^d$.
- We will generally use i to index $1, \ldots, d$, j to index $1, \ldots, n$ and l to index $1, \ldots, k$ (possibly starting at 0). However, this is not strict and the usage can depend on context.

1.3 Organisation of the paper

The remainder of the paper is laid out as follows. We begin, in Section 2, by formally describing how to rephrase the problem of estimating sums of algebraic dilates in terms of estimating sums of linear transformations, in particular observing that the linear transformations corresponding to taking various algebraic dilates are simultaneously diagonalisable. In Section 3, we prove the continuous analogue of our estimate, extending a result of Krachun and Petrov to sums of arbitrarily many simultaneously diagonalisable linear transformations of compact sets. It is also here, in Section 3.1, that we show that Theorem 1.2 is best possible. We extend several results from additive geometry, including Minkowski's second theorem and John's theorem, to rings of integers in Section 4, culminating in our Freiman-type structure theorem for small sums of dilates. We then use this result in Section 5 to reduce the proof of Theorem 1.2 to the special case where A is a dense subset of a box. In Section 6, we introduce lattice densities and prove some of their basic properties, while in Section 7 we introduce two key families of flags of lattices and establish some relations between lattice densities taken relative to these flags. Using these results, we conclude the proof of Theorem 1.2 in Section 8 by verifying it in the dense case. In Section 9, we discuss the general problem of estimating sums of pre-commuting linear transformations, showing how it reduces to Theorem 1.2. Finally, in Section 10, we point towards some further possible research directions.

1.4 Acknowledgements

The authors thank Deepesh Singhal for helpful discussions on the algebraic number theory aspects of the paper. We would also like to note that this work was supported by NSF grant DMS-1928930 while the authors were in residence at the Simons–Laufer Mathematical Sciences Institute in Berkeley, California during the Spring 2025 semester on Extremal Combinatorics.

2 Mapping to $\mathbb{Z}^d$

In this section, we show how the problem of estimating sums of algebraic dilates can be recast in terms of estimating sums of linear transformations. Our first lemma, generalising [13, Lemma 3.1], will allow us to assume that A is a subset of K.

Lemma 2.1. *Suppose that $\lambda_1, \dots, \lambda_k \in \mathbb{C}$ and $A \subset \mathbb{C}$ is finite. Then there exists a finite set $B \subset K = \mathbb{Q}(\lambda_1, \dots, \lambda_k)$ such that $|B| = |A|$ and $|B + \lambda_1 \cdot B + \cdots + \lambda_k \cdot B| \leq |A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$.*

Proof. Let L be the field extension of K generated by A. Pick any K-linear map $f : L \to K$ which is injective on A. Such a map exists since A is finite. Set $B = f(A)$. Then $|B| = |A|$ and, for any $a_0, \dots, a_k \in A$,

$$f(a_0 + \lambda_1 a_1 + \cdots + \lambda_k a_k) = f(a_0) + \lambda_1 f(a_1) + \cdots + \lambda_k f(a_k).$$

Hence, $|B + \lambda_1 \cdot B + \cdots + \lambda_k \cdot B| = |f(A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A)| \leq |A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$. □

In light of this result, we will henceforth assume that $A \subset K$. For any $a \in K$, there exists a positive integer n such that $na \in \mathcal{O}_K$. In fact, this is true for any fractional ideal $\mathcal{I} \subseteq \mathcal{O}_K$ – for any $a \in K$, there exists a positive integer n such that $na \in \mathcal{I}$. Thus, since A is finite, by rescaling A to $n \cdot A$ for an appropriately large n, we may assume that $A \subset \mathcal{I}$ if we wish to without any loss of generality.

To pass to linear transformations, we fix a $\mathbb{Z}$-basis $e_1 = 1, e_2, \dots, e_d$ of $\mathcal{O}_K$ and let $\Phi : \mathcal{O}_K \to \mathbb{Z}^d$ be the isomorphism mapping the e_i to the standard basis of $\mathbb{Z}^d$. This map extends linearly to an isomorphism $\Phi : K \to \mathbb{Q}^d$. Under this isomorphism, multiplication by λ_l corresponds to the linear map $\mathcal{M}_l \in \mathrm{Mat}_d(\mathbb{Q})$ defined by

$$\mathcal{M}_l(x) = \Phi(\lambda_l \cdot \Phi^{-1}(x)).$$

The problem of estimating $|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|$ for $A \subset K$ is then equivalent to estimating $|A + \mathcal{M}_1 A + \cdots + \mathcal{M}_k A|$ for $A \subset \mathbb{Q}^d$.

One further step allows us to convert the problem into one about sums of linear transformations with *integer* entries. Recall, from the introduction, that the denominator ideal of $\lambda_1, \dots, \lambda_k$ is the non-zero ideal $\mathfrak{D} = \mathcal{O}_K \cap \lambda_1^{-1}\mathcal{O}_K \cap \cdots \cap \lambda_k^{-1}\mathcal{O}_K$ with the property that $\lambda_l \mathfrak{D} \subseteq \mathcal{O}_K$ for all $l = 0, \dots, k$. If we fix an isomorphism $\Phi' : \mathfrak{D} \to \mathbb{Z}^d$, then multiplication of the elements of $\mathfrak{D}$ by λ_l corresponds to the linear map $\mathcal{L}_l : \mathbb{Z}^d \to \mathbb{Z}^d$ defined by

$$\mathcal{L}_l(x) = \Phi(\lambda_l \cdot \Phi'^{-1}(x)).$$

By rescaling, we may assume that $A \subset \mathfrak{D}$, so that Theorem 1.2 becomes equivalent to the following result, whose proof will now be our principal goal.

Theorem 2.2. *For all finite subsets A of $\mathbb{Z}^d$,*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\lambda_1, \dots, \lambda_k)|A| - o(|A|).$$

The next lemma determines all the (simultaneous) eigenvalues of the λ_l, when they are viewed as $\mathbb{Q}$-linear maps on K. In the statement and proof, we will use the fact that there are exactly d different complex embeddings (that is, injective field homomorphisms) of K in $\mathbb{C}$, which we denote by $\sigma_1, \dots, \sigma_d$ with σ_1 the identity.

Lemma 2.3. *Viewing $K \cong \mathbb{Q}^d$, multiplication by λ_l induces a $\mathbb{Q}$-linear map $\mathcal{M}_l : \mathbb{Q}^d \to \mathbb{Q}^d$. Then the maps $\mathcal{M}_0, \ldots, \mathcal{M}_k$ are simultaneously diagonalisable over $\mathbb{C}$ into the diagonal matrices $\mathcal{D}_0, \ldots, \mathcal{D}_k$, where $\mathcal{D}_l$ has diagonal entries $(\sigma_1(\lambda_l), \ldots, \sigma_d(\lambda_l))$ for $l = 0, \ldots, k$.*

Proof. Let $K_{\mathbb{C}} = K \otimes_{\mathbb{Q}} \mathbb{C}$ and define $\sigma : K_{\mathbb{C}} \to \mathbb{C}^d$ to be the $\mathbb{C}$-linear map defined by $\sigma(\alpha \otimes c) = (c\sigma_1(\alpha), \ldots, c\sigma_d(\alpha))$. We claim that σ is an isomorphism. Indeed, let $\alpha \in K$ be a generator of K, i.e., $K = \mathbb{Q}(\alpha)$. Then $(1, \alpha, \ldots, \alpha^{d-1})$ is a $\mathbb{Q}$-basis for K and $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ are all distinct. Under this basis, which is also a basis for $K_{\mathbb{C}}$, σ is represented by the matrix

$$\begin{pmatrix} 1 & \sigma_1(\alpha) & \sigma_1(\alpha)^2 & \cdots & \sigma_1(\alpha)^{d-1} \\ 1 & \sigma_2(\alpha) & \sigma_2(\alpha)^2 & \cdots & \sigma_2(\alpha)^{d-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_d(\alpha) & \sigma_d(\alpha)^2 & \cdots & \sigma_d(\alpha)^{d-1} \end{pmatrix},$$

which is non-singular, since it is a Vandemonde matrix. Let $e_1, \ldots, e_d \in \mathbb{C}^d$ be the standard basis of $\mathbb{C}^d$ and $v_i = \sigma^{-1}(e_i)$. Then $v_1, \ldots, v_d$ form a basis for $K_{\mathbb{C}}$. We claim that, in this basis, $\mathcal{M}_l$ diagonalises into the desired form. It suffices to check that $\mathcal{M}_l(v_i) = \sigma_i(\lambda_l)v_i$.

Let $x_1, \ldots, x_d \in K$ be a $\mathbb{Q}$-basis for K. Then v_i can be written in the form $v_i = x_1 \otimes c_{i1} + \cdots + x_k \otimes c_{ik}$ for some $c_{il} \in \mathbb{C}$, so that $\sigma(v_i) = e_i$ says that

$$\sum_{l=1}^{k} c_{il}\sigma_j(x_l) = \delta_{ij}.$$

But then

$$\begin{aligned} \sigma_j(\mathcal{M}_l(v_i)) &= \sigma_j\left(\mathcal{M}_l\left(\sum_{m=1}^{k} x_m \otimes c_{im}\right)\right) = \sigma_j\left(\sum_{m=1}^{k} (\lambda_l x_m) \otimes c_{im}\right) \\ &= \sum_{m=1}^{k} c_{im}\sigma_j(\lambda_l x_m) = \sigma_j(\lambda_l)\sum_{m=1}^{k} c_{im}\sigma_j(x_m) \\ &= \sigma_j(\lambda_l)\delta_{ij} = \sigma_i(\lambda_l)\delta_{ij}. \end{aligned}$$

It follows that $\mathcal{M}_l(v_i) = \sigma_i(\lambda_l)v_i$, as required. □

3 The continuous version

We now come to the first part of our argument, which is to extend an estimate of Krachun and Petrov [13, Theorem 2] on sums of linear transformations of compact sets to more than two variables. We will need to assume that the linear transformations are simultaneously diagonalisable. But, as we have seen in Lemma 2.3 above, this is exactly the situation we are concerned with.

Throughout this section, we will fix an identification $K_{\mathbb{R}} \cong \mathbb{R}^d$ and take μ to be the Lebesgue measure on $\mathbb{R}^d$ and, hence, on $K_{\mathbb{R}}$. Our main result may then be stated as follows.

Theorem 3.1. *Suppose $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{R})$ are simultaneously diagonalisable over $\mathbb{C}$ into the diagonal matrices $\mathcal{D}_1, \ldots, \mathcal{D}_k$, where $\mathcal{D}_l = \mathrm{diag}(\lambda_{l1}, \ldots, \lambda_{ld})$ with each $\lambda_{li} \in \mathbb{C}$. Then, for any compact $A \subset \mathbb{R}^d$,*

$$\mu(\mathcal{L}_1 A + \mathcal{L}_2 A + \cdots + \mathcal{L}_k A) \geq \left(\prod_{i=1}^{d}\sum_{l=1}^{k} |\lambda_{li}|\right)\mu(A).$$

Moreover, equality holds for some A with $\mu(A) > 0$.

Proof. Let $\Lambda = \{(\lambda_{1i}, \lambda_{2i}, \ldots, \lambda_{ki})\}_{i=1}^{d}$. Since complex conjugation preserves each $\mathcal{L}_l$, it permutes the elements of Λ. Thus, we can split Λ into two parts Λ_1 and Λ_2, where $\Lambda_1 \subset \mathbb{R}^k$ consists of those tuples fixed by conjugation and Λ_2 consists of conjugate pairs of tuples. Then we may decompose $\mathbb{R}^d$ into the eigenspaces

$$\mathbb{R}^d = \bigoplus_{\lambda \in \Lambda_1} E_\lambda \oplus \bigoplus_{(\lambda, \overline{\lambda}) \in \Lambda_2} E_{\lambda, \overline{\lambda}},$$

where each E_λ is 1-dimensional and each $E_{\lambda,\overline{\lambda}}$ is 2-dimensional. For $\lambda = (\lambda_1, \ldots, \lambda_k) \in \Lambda_1$, each $\mathcal{L}_l$ acts on E_λ by λ_l. For $(\lambda, \overline{\lambda}) \in \Lambda_2$, each $\mathcal{L}_l$ acts on $E_{\lambda,\overline{\lambda}}$ by $|\lambda_l| R_{\arg(\lambda_l)}$, where R_θ is the rotation map on $\mathbb{R}^2$ by θ.

We prove the theorem in the following more general form. Suppose we have a decomposition

$$\mathbb{R}^d = \bigoplus_{j=1}^{n} E_j,$$

where $\dim E_j = d_j$ and $\mathcal{L}_l$ acts on E_j by $r_{lj} P_{lj}$, where $r_{lj} \geq 0$ and P_{lj} is an orthogonal matrix acting on E_j. In other words, for any vector $v \in \mathbb{R}^d$, if we decompose it into $v = v_1 + \cdots + v_n$ with $v_j \in E_j$ for all $1 \leq j \leq n$, then $\mathcal{L}_l v = r_{l1} P_{l1} v_1 + \cdots + r_{ln} P_{ln} v_n$. We will show that

$$\mu(\mathcal{L}_1 A + \mathcal{L}_2 A + \cdots + \mathcal{L}_k A) \geq \left(\prod_{j=1}^{n} \left(\sum_{l=1}^{k} r_{lj} \right)^{d_j} \right) \mu(A).$$

We perform Steiner symmetrisation, a continuous analogue of compression introduced by Steiner in his classical work on the isoperimetric problem, along each of the eigenspaces E_j as follows. Write $\mathbb{R}^d = E_j \oplus E$, where E is the direct sum of the remaining spaces. Let $\pi_1 : \mathbb{R}^d \to E_j$ and $\pi_2 : \mathbb{R}^d \to E$ be the projections onto E_j and E, respectively. For a compact $A \subset \mathbb{R}^d$ and $x \in E$, write $A_x := \pi_1(\pi_2^{-1}(x)) \subset E_j$ for the fibre of A at x. Then $\mu(A) = \int_x \mu(A_x) d\mu(x)$. The *Steiner symmetrisation* of A along E_j is the set $S_j(A) \subset \mathbb{R}^d$ with the same support as A on E and such that, for each $x \in \pi_2(A)$, $S_j(A)_x$ is the closed ball centered at 0 with the same volume as A_x.

Claim 3.2. *The Steiner symmetrisation has the following properties:*

1. $\mu(S_j(A)) = \mu(A)$.
2. $S_j(A)$ *is invariant under any orthogonal transformation of* E_j.
3. $S_j(\mathcal{L}_l A) \supseteq \mathcal{L}_l(S_j(A))$ *for all* l.
4. $S_j(A)$ *is compact.*
5. *If* B *is compact, then* $S_j(A + B) \supseteq S_j(A) + S_j(B)$.
6. *If* $F \in \mathrm{GL}(E)$ *and* $F' \in \mathrm{GL}_d(\mathbb{R})$ *is given by* $I_{E_j} \oplus F$ *and* $F'(A) = A$, *then* $F'(S_j(A)) = S_j(A)$.

Proof. 1. This is true since $\mu(S_j(A)_x) = \mu(A_x)$ for all $x \in E$.

2. This is true since $S_j(A)_x$ is a ball for all $x \in E$.

3. Let $x \in \pi_2(A)$ and $B = S_j(A)_x$, a ball. Then $\mathcal{L}_l(S_j(A)) = \bigcup_{x\in\pi_2(A)} \mathcal{L}_l|_{E_j}(B) \oplus \mathcal{L}_l x$. Note that $\mathcal{L}_l|_{E_j}(B)$ is also a ball of volume $\mu(\mathcal{L}_l|_{E_j}(A_x)) \le \mu((\mathcal{L}_l A)_{\mathcal{L}_l x})$. Thus, $\mathcal{L}_l|_{E_j}(B) \oplus \mathcal{L}_l x \subseteq S_j(\mathcal{L}_l A)$ and the result follows.

4. Since A is bounded, so is $S_j(A)$. To show that $S_j(A)$ is closed, it is sufficient to show that for any sequence $x_1, x_2, \ldots \in E$ converging to $x \in E$, we have $\mu(A_x) \ge \limsup_n \mu(A_{x_n})$. Since A is closed, $A_x \supseteq \limsup_i A_{x_i}$, so it suffices to show that $\mu(\limsup_i A_{x_i}) \ge \limsup_i \mu(A_{x_i})$. But this is true since the A_{x_i} are uniformly bounded.

5. For $x \in \pi_2(A)$ and $y \in \pi_2(B)$, let r, r' be the radii of the balls $S_j(A)_x$ and $S_j(B)_y$, with volumes V, V'. Then $(S_j(A) + S_j(B))_{x+y}$ is a ball of radius $r + r'$, maximised over all x, y with the same fixed sum. But, by the Brunn–Minkowski inequality,

$$\begin{aligned}\mu(S_j(A+B)_{x+y}) &\ge \mu(S_j(A)_x + S_j(B)_y)\\ &\ge (\mu(S_j(A)_x)^{1/d_j} + \mu(S_j(B)_y)^{1/d_j})^{d_j}\\ &= (V^{1/d_j} + V'^{1/d_j})^{d_j}\\ &= \mu((S_j(A) + S_j(B))_{x+y}).\end{aligned}$$

   Thus, $S_j(A+B)_{x+y} \supseteq (S_j(A) + S_j(B))_{x+y}$ and the result follows.

6. Let $x \in E$. Since $F'(A) = A$, we have $A_{F(x)} = A_x$. Therefore, $S_j(A)_{F(x)} = S_j(A)_x$, so we have $F'(S_j(A)) = S_j(A)$. □

Perform Steiner symmetrisation on A successively along $E_1, \ldots, E_n$ to obtain, by Claim 3.2(4), the compact set $B = S_1(S_2(\cdots S_n(A)\cdots))$. By Claim 3.2(1), (5) and (3),

$$\begin{aligned}\mu(\mathcal{L}_1 A + \cdots + \mathcal{L}_k A) &= \mu(S_j(\mathcal{L}_1 A + \cdots + \mathcal{L}_k A))\\ &\ge \mu(S_j(\mathcal{L}_1 A) + \cdots + S_j(\mathcal{L}_k A))\\ &\ge \mu(\mathcal{L}_1(S_j(A)) + \cdots + \mathcal{L}_k(S_j(A))).\end{aligned}$$

Iterating, we see that $\mu(\mathcal{L}_1 A + \cdots + \mathcal{L}_k A) \ge \mu(\mathcal{L}_1 B + \cdots + \mathcal{L}_k B)$, where we also have $\mu(B) = \mu(A)$.

Let $\mathcal{L}'_l$ be the linear map that just scales by r_{lj} on each E_j, i.e., $\mathcal{L}'_l(v_1 + \cdots + v_n) = r_{l1}v_1 + \cdots + r_{ln}v_n$ for any $v_j \in E_j$. By repeated applications of Claim 3.2(2) and (6), we may check that B is rotationally invariant on each E_j, so we have $\mathcal{L}'_l B = \mathcal{L}_l B$. Thus,

$$\begin{aligned}\mu(\mathcal{L}_1 B + \cdots + \mathcal{L}_k B) &= \mu(\mathcal{L}'_1 B + \cdots + \mathcal{L}'_k B)\\ &\ge \mu((\mathcal{L}'_1 + \cdots + \mathcal{L}'_k)(B))\\ &= |\det(\mathcal{L}'_1 + \cdots + \mathcal{L}'_k)|\mu(B)\\ &= \left(\prod_{j=1}^{l}\left(\sum_{l=1}^{k} r_{lj}\right)^{d_j}\right)\mu(B).\end{aligned}$$

Finally, to see that equality may hold, observe that we can take A to be the product of the unit balls in each E_j. □

In particular, this yields the smallest possible value of $\mu(A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A)$ in terms of $\mu(A)$. To see this, let $\mathcal{M}_l \in \mathrm{Mat}_d(\mathbb{Q})$ be the matrix representing multiplication by λ_l for $l = 0, \ldots, k$,

as defined in Section 2. Then, by Lemma 2.3, the $\mathcal{M}_l$ are simultaneously diagonalisable into the diagonal matrices $\mathcal{D}_l$ with entries $(\sigma_1(\lambda_l), \dots, \sigma_d(\lambda_l))$, where $\sigma_1, \dots, \sigma_d$ are all the complex embeddings of K. By Theorem 3.1, we therefore have

$$\begin{aligned}\mu(A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A) &= \mu(\mathcal{M}_0 A + \cdots + \mathcal{M}_k A) \\ &\geq \left(\prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \right) \mu(A).\end{aligned}$$

Comparing this to our main result, Theorem 1.2, we see that the discrete version differs from the continuous one only in the factor $N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K})$, which is a measure of the non-integrality of $\lambda_1, \dots, \lambda_k$. We say more below.

3.1 Lower bound construction

In this short subsection, we give a lower bound construction for the discrete case, showing that the constant $H(\lambda_1, \dots, \lambda_k)$ in Theorem 1.2 is best possible. In brief, the construction is a discretised version of the equality case in Theorem 3.1.

Proposition 3.3. *Let $\lambda_1, \dots, \lambda_k \in K = \mathbb{Q}[\lambda_1, \dots, \lambda_k]$ be algebraic numbers. Then there exist arbitrarily large $A \subset \mathbb{C}$ such that*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq H(\lambda_1, \dots, \lambda_k)|A| + O(|A|^{\frac{d-1}{d}}),$$

where $d = \deg(K/\mathbb{Q})$.

Proof. Let $\sigma_1, \dots, \sigma_d : K \to \mathbb{C}$ be the complex embeddings of K and set $\mathfrak{D} = \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$. Viewing multiplication by λ_l as a $\mathbb{Q}$-linear map $\mathcal{M}_l : K \to K$ for each l, take $A' \subset K_{\mathbb{R}}$ satisfying the equality case in Theorem 3.1 with $\mu(A') = 1$. Then $\mu(A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A') = \left(\prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \right) \mu(A')$.

Let n be an arbitrarily large positive integer and let $A = nA' \cap \mathfrak{D}$, so that

$$|A| = \mu(nA')/\operatorname{Vol}(K_{\mathbb{R}}/\mathfrak{D}) + O(n^{d-1}) = n^d/\operatorname{Vol}(K_{\mathbb{R}}/\mathfrak{D}) + O(n^{d-1}).$$

On the other hand, for each l, $\lambda_l \cdot A \subset \lambda_l \cdot \mathfrak{D} \subseteq \mathcal{O}_K$, so we have

$$A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A \subseteq n(A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A') \cap \mathcal{O}_K.$$

Therefore,

$$\begin{aligned}|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| &\leq \mu(n(A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'))/\operatorname{Vol}(K_{\mathbb{R}}/\mathcal{O}_K) + O(n^{d-1}) \\ &= n^d \left(\prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \right) / \operatorname{Vol}(K_{\mathbb{R}}/\mathcal{O}_K) + O(n^{d-1}).\end{aligned}$$

Since $\operatorname{Vol}(K_{\mathbb{R}}/\mathfrak{D})/\operatorname{Vol}(K_{\mathbb{R}}/\mathcal{O}_K) = [\mathcal{O}_K : \mathfrak{D}] = N_{K/\mathbb{Q}}(\mathfrak{D})$, we obtain that

$$\begin{aligned}|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| &\leq N_{K/\mathbb{Q}}(\mathfrak{D}) \left(\prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \right) |A| + O(n^{d-1}) \\ &= H(\lambda_1, \dots, \lambda_k)|A| + O(|A|^{\frac{d-1}{d}}).\end{aligned}$$

□

4 Algebraic additive geometry

In this section, we extend several results from additive geometry to rings of integers, culminating in the version of Freiman's theorem for sums of dilates mentioned in the introduction. Along the way, we prove several results that may be of independent interest, including versions of Minkowski's second theorem and John's theorem for lattices over rings of integers.

4.1 A norm on $\mathcal{O}_K$ and $K_{\mathbb{R}}$

In this subsection, we define a norm on $\mathcal{O}_K$ and $K_{\mathbb{R}}$ and note some of its basic properties (this is not to be confused with the field norm $N_{K/\mathbb{Q}}(\cdot)$ on K, which we also use). Recall from Section 2 that we have an isomorphism $\Phi : \mathcal{O}_K \to \mathbb{Z}^d$ given by sending a basis $e_1, \dots, e_d$ of $\mathcal{O}_K$ to the standard basis. By pulling back Φ, the ∞-norm on $\mathbb{Z}^d$ defines a norm $\|\cdot\|$ on $\mathcal{O}_K$, namely, for $l_1, \dots, l_d \in \mathbb{Z}$,

$$\|l_1 e_1 + \cdots + l_d e_d\| := \max_i |l_i|.$$

The open ball $B(L)$ of radius $L > 0$ under this norm is then given by

$$B(L) := \{l_1 e_1 + \cdots + l_d e_d \in \mathcal{O}_K \mid |l_i| < L \text{ for all } i\}.$$

$\|\cdot\|$ extends linearly and continuously to a norm on $K_{\mathbb{R}}$, which we also denote by $\|\cdot\|$. The open ball $B_{\mathbb{R}}(R)$ of radius $R > 0$ in $K_{\mathbb{R}}$ is then

$$B_{\mathbb{R}}(R) := \{e_1 \otimes r_1 + \cdots + e_d \otimes r_d \in K_{\mathbb{R}} \mid |r_i| < R \text{ for all } i\}.$$

The following lemma may be seen as defining some constants associated to the norm $\|\cdot\|$.

Lemma 4.1. *There exist constants $C_1, C_2, C_3 \in \mathbb{N}$ such that the following hold:*

1. *For all $x, y \in K_{\mathbb{R}}$, $\|xy\| \le C_1 \|x\| \|y\|$.*
2. *For all $l = 0, \dots, k$, $C_2 \lambda_l \in \mathcal{O}_K$.*
3. *For all $l = 0, \dots, k$ and $x \in \mathcal{O}_K$, $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$.*

Proof. 1. Let $M > 0$ be the maximum of $\|e_i e_j\|$ over all pairs $i, j \in [d]$. Now, for any $x = e_1 \otimes x_1 + \cdots + e_d \otimes x_d$ and $y = e_1 \otimes y_1 + \cdots + e_d \otimes y_d$ with $x_i, y_i \in \mathbb{R}$, we have $|x_i| \le \|x\|$ and $|y_i| \le \|y\|$. Therefore,

$$\|xy\| = \|\sum_{i,j} e_i e_j \otimes x_i y_i\| \le \sum_{i,j} \|e_i e_j \otimes x_i y_i\| = \sum_{i,j} \|e_i e_j\| |x_i y_i| \le d^2 M \|x\| \|y\|,$$

so we may pick $C_1 = d^2 M$.

2. Since $\mathcal{O}_K$ is of full rank, for any $\lambda \in K$, there is some integer $C > 0$ such that $C\lambda \in \mathcal{O}_K$. Thus, we may pick C_2 to be the lowest common multiple of the C's corresponding to each λ_l.

3. Pick an integer C_3 such that $C_3 > C_1 C_2 \max_l \|\lambda_l\|$. Then we have $C_2 \lambda_l x \in \mathcal{O}_K$ and $\|C_2 \lambda_l x\| \le C_1 C_2 \|\lambda_l\| \|x\| < C_3 \|x\|$. Therefore, $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$. □

Throughout the rest of this section, we will use the constants C_1, C_2, C_3 as given by this lemma.

4.2 An algebraic Minkowski's second theorem

In this subsection, we prove a variant of Minkowski's second theorem for lattices over rings of integers. Before we state this result, let us recall the original theorem of Minkowski. We first need a definition, noting that here a *convex body* is assumed to be convex, open, non-empty and bounded.

Definition 4.2. Let $\Gamma \subset \mathbb{R}^n$ be a lattice of rank m and $B \subset \mathbb{R}^n$ a convex body containing 0. We define the *successive minima* $\ell_j = \ell_j(B, \Gamma)$ of B with respect to Γ by

$$\ell_j := \inf \{\ell > 0 \mid \ell \cdot B \text{ contains } j \text{ linearly independent elements of } \Gamma\}$$

for each $1 \leq j \leq m$. Note that $0 < \ell_1 \leq \cdots \leq \ell_m < \infty$.

Minkowski's second theorem (see, for example, [20, Theorem 3.30]) is then as follows.

Theorem 4.3 (Minkowski's second theorem)**.** *Let $\Gamma \subset \mathbb{R}^n$ be a lattice of full rank and let B be a centrally symmetric convex body in $\mathbb{R}^n$ with successive minima $0 < \ell_1 \leq \cdots \leq \ell_n$. Then there exist n linearly independent vectors $v_1, \ldots, v_n \in \Gamma$ with the following properties:*

- *for each $1 \leq j \leq n$, v_j lies in the boundary of $\ell_j \cdot B$, but $\ell_j \cdot B$ itself does not contain any vectors in Γ outside the span of $v_1, \ldots, v_{j-1}$;*
- *the octahedron with vertices $\pm v_j$ for $1 \leq j \leq n$ contains no elements of Γ in its interior other than the origin;*
- *one has*

$$\frac{2^n[\Gamma : \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}]}{n!} \leq \frac{\ell_1 \cdots \ell_n \operatorname{Vol}(B)}{\operatorname{Vol}(\mathbb{R}^n/\Gamma)} \leq 2^n.$$

To state our variant of this theorem, we need to first clarify what we mean by a lattice over a ring of integers.

Definition 4.4. An *$\mathcal{O}_K$-lattice* is a lattice Γ in $K^n \cong \mathbb{Q}^{dn}$ that is closed under multiplication by $\mathcal{O}_K$. That is, for any $v \in \Gamma$ and $a \in \mathcal{O}_K$, $av \in \Gamma$. Equivalently, Γ is a discrete $\mathcal{O}_K$-submodule of K^n. Observe that $\mathbb{Q} \cdot \Gamma = K \cdot \Gamma$ is a K-subspace of K^n. The *$\mathcal{O}_K$-rank* of Γ is the dimension m of this subspace. Note that, when viewed as an ordinary lattice, the rank of Γ is md.

For the next definition, we recall, from Section 2, that we view $\mathcal{O}_K$ as having a fixed $\mathbb{Z}$-basis $e_1, \ldots, e_d$.

Definition 4.5. For a real number $r \geq 1$, a subset $B \subseteq K_{\mathbb{R}}^n$ is said to be *r-thick* if $e_i \cdot B \subseteq r \cdot B$ for all $i \in [d]$.

For example, by Lemma 4.1, $\|e_i x\| \leq C_1 \|e_i\| \|x\| = C_1 \|x\|$ for all $x \in K_{\mathbb{R}}$, so that $B_{\mathbb{R}}(L)$ is C_1-thick for any $L > 0$.

We now redefine successive minima, but with respect to $\mathcal{O}_K$-lattices.

Definition 4.6. Let Γ be an $\mathcal{O}_K$-lattice of $\mathcal{O}_K$-rank m and B a convex body in $K_{\mathbb{R}}^n$ containing 0. We define the *successive minima* $\ell_j = \ell_j(B, \Gamma)$ of B with respect to Γ by

$$\ell_j := \inf \{\ell > 0 \mid \ell \cdot B \text{ contains } j \ K\text{-linearly independent elements of } \Gamma\}$$

for each $1 \leq j \leq m$. Note that we again have $0 < \ell_1 \leq \cdots \leq \ell_m < \infty$, since Γ has $\mathcal{O}_K$-rank m and so contains m K-linearly independent elements of K^n.

We may now state and prove our version of Minkowski's second theorem for $\mathcal{O}_K$-lattices.

Lemma 4.7. *Let $r \geq 1$ be a real number, let $\Gamma \subset K^n$ be an $\mathcal{O}_K$-lattice of full rank and let B be an r-thick centrally symmetric convex body in $K^n_{\mathbb{R}}$ with successive minima $0 < \ell_1 \leq \cdots \leq \ell_n$. Then there exist n K-linearly independent vectors $v_1, \ldots, v_n \in \Gamma$ with the following properties:*

- *for each $1 \leq j \leq n$, v_j lies in the boundary of $\ell_j \cdot B$, but $\ell_j \cdot B$ does not contain any vectors in Γ outside the K-span of $v_1, \ldots, v_{j-1}$;*
- *the octahedron with vertices $\pm \frac{1}{r} e_i v_j$ for $i \in [d], j \in [n]$ contains no elements of Γ in its interior other than the origin;*
- *if Γ' is the $\mathcal{O}_K$-lattice generated by $v_1, \ldots, v_n$, then*

$$\frac{(2/r)^{nd}[\Gamma : \Gamma']}{(nd)!} \leq \frac{(\ell_1 \cdots \ell_n)^d \operatorname{Vol}(B)}{\operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma)} \leq 2^{nd}. \tag{1}$$

We note that here the volume of a set $B \subset K^n_{\mathbb{R}}$ is defined by fixing some isomorphism $K^n_{\mathbb{R}} \cong \mathbb{R}^{nd}$ and using the standard Lebesgue measure on $\mathbb{R}^{nd}$. Crucially, the statement of the lemma does not depend on the particular identification $K^n_{\mathbb{R}} \cong \mathbb{R}^{nd}$, since any two volume forms differ by a scalar.

Proof of Lemma 4.7. The proof is essentially identical to that of the original theorem given in [20, Theorem 3.30], though some care is required to differentiate between the $\mathbb{Q}$-span and K-span.

By the definition of ℓ_1, we may find $v_1 \in \Gamma$ on the boundary of $\ell_1 \cdot B$, where $\ell_1 \cdot B$ does not contain any non-zero elements of Γ. By the definition of λ_2, we may then find $v_2 \in \Gamma$ on the boundary of $\ell_2 \cdot B$ which is K-linearly independent of v_1, where $\ell_2 \cdot B$ contains no elements of Γ outside the K-span of v_1. Continuing, we have a K-basis $v_1, \ldots, v_n$ such that v_j is on the boundary of $\ell_j \cdot B$, where $\ell_j \cdot B$ does not contain any element of Γ outside the K-span of $v_1, \ldots, v_{j-1}$, as required by the first property.

Since $v_1, \ldots, v_n$ are K-linearly independent, the vectors $e_i v_j$ are $\mathbb{Q}$-linearly independent. Therefore, the octahedron S with vertices $\pm \frac{1}{r} e_i v_j$ is non-degenerate and spans K^n over $\mathbb{Q}$. Suppose the interior of S contains a non-zero point $v \in \Gamma$. Let m be the smallest positive integer such that v lies in the K-span of $v_1, \ldots, v_m$. Then v does not lie in the K-span of $v_1, \ldots, v_{m-1}$. Since $\ell_m \cdot \overline{B}$ contains $v_1, \ldots, v_m$ and B is r-thick, $r\ell_m \cdot \overline{B}$ contains $e_i v_j$ for all $i \in [d]$ and $j \leq m$. Therefore, $\ell_m \cdot \overline{B}$ contains $\pm \frac{1}{r} e_i v_j$ for all $i \in [d]$ and $j \leq m$, so its interior $\ell_m \cdot B$ contains v. But this contradicts the definition of ℓ_m, since $\ell_m \cdot B$ cannot contain any vector outside the K-span of $v_1, \ldots, v_{m-1}$, including v. Hence, the interior of S contains no vector in Γ, verifying the second property.

Since $e_i v_j \in r\ell_j \cdot \overline{B}$, we have that $\overline{B}$ contains the vectors $\frac{1}{r\ell_j} e_i v_j$ and, hence, the octahedron S' with vertices $\pm \frac{1}{r\ell_j} e_i v_j$ for $i \in [d]$, $j \in [n]$. The volume of the simplex with vertices 0 and $e_i v_j$ for all $i \in [d]$, $j \in [n]$ is $\frac{1}{(nd)!} \operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma')$. Since S' is the union of 2^{nd} scaled copies of this simplex, the volume of S' is

$$\operatorname{Vol}(S') = \frac{1}{r^{nd} \ell_1^d \cdots \ell_n^d} \frac{2^{nd}}{(nd)!} \operatorname{Vol}(K^n_{\mathbb{R}}/\Gamma').$$

Therefore, since $\overline{B}$ contains S', we have

$$\begin{aligned}\operatorname{Vol}(B) \geq \operatorname{Vol}(S') &= \frac{1}{r^{nd}\ell_1^d \cdots \ell_n^d} \frac{2^{nd}}{(nd)!} \operatorname{Vol}(K_{\mathbb{R}}^n/\Gamma') \\ &= \left(\frac{(2/r)^n}{\ell_1 \cdots \ell_n}\right)^d \frac{[\Gamma : \Gamma']}{(nd)!} \operatorname{Vol}(K_{\mathbb{R}}^n/\Gamma),\end{aligned}$$

establishing the lower bound in (1).

For the upper bound, we require the following lemma.

Lemma 4.8 (Squeezing lemma [20, Lemma 3.31])**.** *Let S be a centrally symmetric convex body in $\mathbb{R}^n$, A be an open subset of S, V be an m-dimensional subspace of $\mathbb{R}^n$ and $0 < \theta \leq 1$. Then there exists an open subset A' of S such that $\operatorname{Vol}(A') = \theta^m \operatorname{Vol}(A)$ and $(A' - A') \cap V \subseteq \theta \cdot (A - A) \cap V$.*

Let V_j be the $\mathbb{R}$-span of the K-span of $v_1, \ldots, v_j$, so that V_j is a jd-dimensional real subspace of $K_{\mathbb{R}}^n$. We apply the squeezing lemma iteratively, starting with $A_0 := \frac{\ell_n}{2} \cdot B$, to create open sets $A_1, \ldots, A_{n-1} \subseteq A_0$ such that

$$\operatorname{Vol}(A_j) = \left(\frac{\ell_j}{\ell_{j+1}}\right)^{jd} \operatorname{Vol}(A_{j-1})$$

and

$$(A_j - A_j) \cap V_j \subseteq \frac{\ell_j}{\ell_{j+1}} \cdot (A_{j-1} - A_{j-1}) \cap V_j$$

for $j = 1, \ldots, n-1$. Then $\operatorname{Vol}(A_{n-1}) = (\ell_1 \cdots \ell_n 2^{-n})^d \operatorname{Vol}(B)$ and one can show by induction that

$$(A_{n-1} - A_{n-1}) \cap V_j \subseteq \frac{\ell_j}{\ell_n} \cdot (A_{j-1} - A_{j-1}) \cap V_j.$$

On the other hand, $A_{j-1} \subseteq A_0 = \frac{\ell_n}{2} \cdot B$ and B is centrally symmetric, so $A_{j-1} - A_{j-1} \subseteq \ell_n \cdot B$. It follows that

$$(A_{n-1} - A_{n-1}) \cap V_j \subseteq \lambda_j \cdot B \cap V_j$$

for $j = 1, \ldots, n$. By the definition of successive minima, $\lambda_j \cdot B \cap V_j$ does not contain any point in Γ except for those in V_{j-1}. This implies that $A_{n-1} - A_{n-1}$ does not contain any point in Γ other than the origin. If $\operatorname{Vol}(A_{n-1}) > \operatorname{Vol}(K_{\mathbb{R}}^n/\Gamma)$, then, by Blichfeldt's principle, one can find a translate $A_{n-1} + t$ of A_{n-1} containing two distinct points of Γ. Thus, $A_{n-1} - A_{n-1}$ contains a non-zero point of Γ, a contradiction. Therefore, we have $\operatorname{Vol}(A_{n-1}) \leq \operatorname{Vol}(K_{\mathbb{R}}^n/\Gamma)$. Hence, we have

$$(\ell_1 \cdots \ell_n 2^{-n})^d \operatorname{Vol}(B) \leq \operatorname{Vol}(K_{\mathbb{R}}^n/\Gamma),$$

giving the upper bound in (1). □

4.3 $\mathcal{O}_K$-GAPs and an algebraic John's theorem

Recall that a *generalised arithmetic progression (or GAP)* $P \subset \mathbb{Z}^d$ is a set of the form

$$P = \{v_0 + l_1 v_1 + \cdots + l_n v_n \mid 0 \leq l_j < L_j \text{ for all } j\}$$

for some $v_0, \dots, v_n \in \mathbb{Z}^d$ and $L_1, \dots, L_n \in \mathbb{N}$. The *dimension* of P is n. We say that P is *proper* if all elements on the RHS are distinct and k-proper if

$$\{l_1 v_1 + \cdots + l_n v_n \mid 0 \le l_j < kL_j \text{ for all } j\}$$

has all elements distinct.

Our object of study for the remainder of this section is the following algebraic analogue of a GAP, which we call an $\mathcal{O}_K$-GAP.

Definition 4.9. An *$\mathcal{O}_K$-GAP* is a set $P \subset K$ of the form

$$P = \{v_0 + l_1 v_1 + \cdots + l_n v_n \mid l_j \in B(L_j) \text{ for all } j\} \tag{2}$$

for some $v_0, \dots, v_n \in K$ and $L_1, \dots, L_n \in \mathbb{N}$. The *dimension* of P is n. For $p \in \mathbb{N}$, define

$$p \star P := \{pv_0 + l_1 v_1 + \cdots + l_n v_n \mid l_j \in B(pL_j) \text{ for all } j\}. \tag{3}$$

We say that P is *proper* if all the elements on the RHS of (2) are distinct and *p-proper* if all the elements on the RHS of (3) are distinct. Note that $p \star P$ is similar, but, because $B(L_j)$ is an *open* ball, not exactly equal, to the p-fold sumset pP.

The classical John's theorem (see [10] or [20, Theorem 3.13]) says that any centrally symmetric convex body A in $\mathbb{R}^n$ can be approximated by an open centrally symmetric ellipsoid E in the sense that $E \subseteq A \subseteq \sqrt{n} \cdot E$. A discrete version of this result, due to Tao and Vu [21], says that the intersection of a centrally symmetric convex body with a lattice in $\mathbb{R}^n$ can be approximated by a GAP. Here we prove the following algebraic analogue of this result.

Lemma 4.10. *For any real number $r \ge 1$, there are integer constants $D_1, D_2 > 0$ such that the following holds. Let $\Gamma \subseteq K^n$ be an $\mathcal{O}_K$-lattice of full rank and $B \subset K^n_{\mathbb{R}}$ be an r-thick convex centrally symmetric body. Then there exist $v_1, \dots, v_n \in K$ and positive integers $L_1, \dots, L_n$ such that the $\mathcal{O}_K$-GAPs given by*

$$P_1 := \{l_1 v_1 + \cdots + l_n v_n \mid l_j \in B(L_j) \text{ for all } j\},$$
$$P_2 := \{l_1 v_1 + \cdots + l_n v_n \mid l_j \in B(D_1 L_j) \text{ for all } j\}$$

satisfy

$$P_1 \subseteq B \cap \Gamma \subseteq \frac{1}{D_2} \cdot P_2. \tag{4}$$

Unlike for the discrete John's theorem for ordinary lattices, the constant D_2 is necessary here. Indeed, if K has non-trivial ideal class group, then, for $\Gamma \subset \mathcal{O}_K$ a non-principal ideal, we cannot hope for a one-dimensional $\mathcal{O}_K$-GAP to span the same lattice as Γ, since any such $\mathcal{O}_K$-GAP is generated by a single element.

Proof of Lemma 4.10. Applying John's theorem to $B \subset K^n_{\mathbb{R}} \cong \mathbb{R}^{dn}$, we obtain an open centrally symmetric ellipsoid $E \subset K^n_{\mathbb{R}}$ such that $E \subseteq B \subseteq \sqrt{dn} \cdot E$. For any $x \in E$ and $i \in [d]$, $e_i x \in e_i \cdot B \subseteq r \cdot B \subseteq r\sqrt{dn} \cdot E$, so E is r_1-thick with $r_1 := r\sqrt{dn}$. Consider the norm $\|\cdot\|_E$ on $K^n_{\mathbb{R}}$ whose unit ball is E, that is,

$$\|x\|_E := \inf\{\ell > 0 \mid x \in \ell \cdot E\}.$$

Since E is r_1-thick, for any $\ell > 0$ and $x \in K_{\mathbb{R}}^n$, $x \in \ell \cdot E$ implies that $e_i x \in r_1 \ell \cdot E$. Therefore, for any $x \in K_{\mathbb{R}}^n$,

$$\|e_i x\|_E \leq r_1 \|x\|_E . \tag{5}$$

Since $|a_i| \leq \|l\|$ for any $l = a_1 e_1 + \cdots + a_d e_d \in \mathcal{O}_K$, we also have, for any $x \in K_{\mathbb{R}}^n$, that

$$\|lx\|_E \leq \sum_{i=1}^{d} \|a_i e_i x\|_E \leq d r_1 \|l\| \|x\|_E . \tag{6}$$

Let $v_1, \ldots, v_n \in K$ be as in Lemma 4.7, when applied to the centrally symmetric convex body E. For each j, let

$$L_j := \left\lceil \frac{1}{n d r_1 \|v_j\|_E} \right\rceil .$$

Then, for any $l_j \in B(L_j)$, $\|l_j\| < \frac{1}{n d r_1 \|v_j\|_E}$. Thus, by (6),

$$\|l_j v_j\|_E \leq d r_1 \|l_j\| \|v_j\|_E < \frac{1}{n}.$$

Therefore, if $l_j \in B(L_j)$ for all j,

$$\|l_1 v_1 + \cdots + l_n v_n\|_E \leq \sum_{j=1}^{n} \|l_j v_j\|_E < 1.$$

In other words, $P_1 \subseteq E \cap \Gamma \subseteq B \cap \Gamma$, giving the first inclusion in (4).

Let $\Gamma' \subseteq \Gamma$ be the $\mathcal{O}_K$-span of $v_1, \ldots, v_n$. Then, from Lemma 4.7, $[\Gamma : \Gamma'] \leq D := \lfloor r^{nd}(nd)! \rfloor$. As a finite abelian group, Γ/Γ' has order at most D, so every element has order dividing $D!$. Therefore, $D! \cdot \Gamma \subseteq \Gamma'$ or, equivalently, $\Gamma \subseteq \frac{1}{D!}\Gamma'$.

Since E is a centrally symmetric ellipsoid, the norm $\|\cdot\|_E$ arises from an inner product on $K_{\mathbb{R}}^n$. Define a volume form on $K_{\mathbb{R}}^n$ based on this inner product. Then $\mathrm{Vol}(E) = V_{nd}$, the volume of the unit ball in $\mathbb{R}^{nd}$. For $u_1, \ldots, u_{nd} \in K_{\mathbb{R}}^n$, write $u_1 \wedge \cdots \wedge u_{nd}$ for the parallelotope in $K_{\mathbb{R}}^n$ spanned by $u_1, \ldots u_{nd}$. Then $\mathrm{Vol}(u_1 \wedge \cdots \wedge u_{nd}) \leq \|u_1\|_E \cdots \|u_{nd}\|_E$.

Let the successive minima of E with respect to Γ be $\ell_1, \ldots, \ell_n$, so we have $\|v_j\|_E = \ell_j$. Let $x \in B \cap \Gamma \subseteq \sqrt{dn} \cdot E$, so that $\|x\|_E \leq \sqrt{dn}$. Since $x \in \Gamma \subseteq \frac{1}{D!}\Gamma'$, we can find unique integers l_{ij} for $i = 1, \ldots, d$ and $j = 1, \ldots, n$ such that

$$x = \frac{1}{D!}(l_{11} e_1 v_1 + \cdots + l_{dn} e_d v_n).$$

Using Cramer's rule, we can solve for $|l_{ij}|$. This gives

$$\begin{aligned}
|l_{ij}| &= D!\frac{\mathrm{Vol}(e_1v_1 \wedge \cdots \wedge x \wedge \cdots \wedge e_dv_n)}{\mathrm{Vol}(e_1v_1 \wedge \cdots \wedge e_dv_n)} && \text{here } x \text{ is in place of } e_iv_j \\
&= D!\frac{\mathrm{Vol}(e_1v_1 \wedge \cdots \wedge x \wedge \cdots \wedge e_dv_n)}{\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')} \\
&\leq D!\frac{\|x\|_E \prod_{(i',j')\neq(i,j)} \|e_{i'}v_{j'}\|_E}{\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')} \\
&\leq D!\frac{r_1^{nd-1}\|x\|_E \prod_{(i',j')\neq(i,j)} \|v_{j'}\|_E}{\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')} && \text{by (5)} \\
&= D!r_1^{nd-1}\frac{(\ell_1\cdots\ell_n)^d\|x\|_E}{\ell_j\,\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma')}.
\end{aligned}$$

From Lemma 4.7, we have

$$\mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma') \geq \mathrm{Vol}(K_{\mathbb{R}}^n/\Gamma) \geq \left(\frac{\ell_1\cdots\ell_n}{2^n}\right)^d \mathrm{Vol}(E) = \left(\frac{\ell_1\cdots\ell_n}{2^n}\right)^d V_{nd}.$$

Therefore, using that $\|x\|_E \leq \sqrt{dn}$ and $L_j \geq \frac{1}{ndr_1\|v_j\|_E}$, we have

$$|l_{ij}| \leq \frac{D!r_1^{nd-1}2^{nd}\|x\|_E}{\ell_j V_{nd}} < \frac{D!r_1^{nd}2^{nd+1}nd\sqrt{nd}}{V_{nd}}L_j.$$

We obtain the second inclusion in (4) by setting $D_2 = D!$ and $D_1 = \left\lceil D!r_1^{nd}2^{nd+1}nd\sqrt{nd}/V_{nd}\right\rceil$. □

We now come to a key lemma, for which we need our algebraic version of John's lemma, saying that if P is an $\mathcal{O}_K$-GAP that is not p-proper, then there is an $\mathcal{O}_K$-GAP of smaller dimension which contains and is not too much larger than P.

Lemma 4.11. *If P is an $\mathcal{O}_K$-GAP of dimension n that is not p-proper, then there is an $\mathcal{O}_K$-GAP Q of dimension $n-1$ containing P with $|Q| \ll_{n,p} |P|$.*

Proof. Assume that P is centered and of the form

$$P = \{l_1v_1 + \cdots + l_nv_n \mid l_j \in B(L_j)\}$$

with $L_j > 1$ for all j. Since P is not p-proper, there exist $l_j, l_j' \in B(pL_j)$ for all j such that $l_j \neq l_j'$ for some j and

$$l_1v_1 + \cdots + l_nv_n = l_1'v_1 + \cdots + l_n'v_n.$$

Setting $a_j = l_j - l_j' \in B(2pL_j)$, we have that the a_j are not all 0 and $a_1v_1 + \cdots + a_nv_n = 0$. We may assume without loss of generality that $a_n \neq 0$. Then we have the relation

$$v_n = -\frac{a_1v_1}{a_n} - \cdots - \frac{a_{n-1}v_{n-1}}{a_n}. \tag{7}$$

Let $w = (-\frac{a_1}{a_n}, \ldots, -\frac{a_{n-1}}{a_n}) \in K^{n-1}$. Let $\Gamma := \mathcal{O}_K^{n-1} + \mathcal{O}_K \cdot w \subset K^{n-1}$. Then Γ is a discrete lattice which is invariant under multiplication by $\mathcal{O}_K$ and so is an $\mathcal{O}_K$-lattice. Γ is also of full rank, since it contains $\mathcal{O}_K^{n-1}$. Consider the homomorphism $f : \Gamma \to K$ given by

$$f((x_1, \ldots, x_{n-1}) + x_n w) := x_1 v_1 + \cdots + x_n v_n.$$

Then f is well-defined because of the relation (7). Note also that f is $\mathcal{O}_K$-linear, that is, f is linear and $f(ax) = af(x)$ for any $a \in \mathcal{O}_K, x \in \Gamma$. We may also extend f $\mathcal{O}_K$-linearly to a K-linear map $f : K^{n-1} \to K$.

Let $B_0 \subset K_{\mathbb{R}}^{n-1}$ be the convex centrally symmetric body

$$B_0 := \left\{(x_1, \ldots, x_{n-1}) \in K_{\mathbb{R}}^{n-1} \;\middle|\; x_i \in B_{\mathbb{R}}(L_i)\right\}.$$

Let $B = B_0 + B_{\mathbb{R}}(L_n) \cdot w$, which is also a convex centrally symmetric body. Since B_0 and $B_{\mathbb{R}}(L_n) \cdot w$ are C_1-thick, so is B. Indeed, if $x \in B_0$ and $y \in B_{\mathbb{R}}(L_n) \cdot w$, then $e_i \cdot (x + y) = e_i \cdot x + e_i \cdot y \in C_1 \cdot B_0 + C_1 \cdot (B_{\mathbb{R}}(L_n) \cdot w) = C_1 \cdot (B_0 + B_{\mathbb{R}}(L_n) \cdot w)$.

Claim 4.12. *One has the inclusions*

$$P \subseteq f(B \cap \Gamma) \subseteq (2pC_1 + 1) \star P.$$

Proof. For the first inclusion, let $v = l_1 v_1 + \cdots + l_n v_n \in P$ with $l_j \in B(L_j)$. Then $v = f((l_1, \ldots, l_{n-1}) + l_n w)$ with $\|l_j\| < L_j$, so that $(l_1, \ldots, l_{n-1}) + l_n w \in B \cap \Gamma$.

For the second inclusion, let $(l_1, \ldots, l_{n-1}) + l_n w \in B \cap \Gamma$ with $l_j \in \mathcal{O}_K$. Since $(l_1, \ldots, l_{n-1}) + l_n w \in B$, there exist $x_1, \ldots, x_n \in K_{\mathbb{R}}$ with $\|x_j\| < L_j$ such that $(l_1, \ldots, l_{n-1}) + l_n w = (x_1, \ldots, x_{n-1}) + x_n w$. In other words, $l_j - \frac{a_j l_n}{a_n} = x_j - \frac{a_j x_n}{a_n}$ for $j = 1, \ldots, n-1$. Let $z = \frac{l_n - x_n}{a_n} \in K_{\mathbb{R}}$, so we have

$$l_j - x_j = a_j z \tag{8}$$

for all $j = 1, \ldots, n$. Let $x \in \mathcal{O}_K$ be the closest element to z according to the metric $\|\cdot\|$. Recall that this is the ∞-norm, so we have $\|x - z\| \leq 1$. Let $l'_j = l_j - a_j x \in \mathcal{O}_K$. Then $l_1 v_1 + \cdots + l_n v_n = l'_1 v_1 + \cdots + l'_n v_n$, so we have $f((l_1, \ldots, l_{n-1}) + l_n w) = l'_1 v_1 + \cdots + l'_n v_n$. It suffices to show that $\|l'_j\| < (2pC_1 + 1)L_j$ for all j. But we have

$$\begin{aligned}
\|l'_j\| &= \|l_j - a_j x\| \\
&\leq \|l_j - a_j x - x_j\| + \|x_j\| \\
&< \|a_j(z - x)\| + L_j && \text{by (8)} \\
&\leq C_1 \|a_j\| \|z - x\| + L_j && \text{by Lemma 4.1} \\
&\leq (2pC_1 + 1)L_j,
\end{aligned}$$

as required. □

By Lemma 4.10, we can find constants $D_1, D_2 = O_n(1)$ and $\mathcal{O}_K$-GAPs P_1, P_2 of dimension $n-1$ such that $P_2 = D_1 \star P_1$ and $P_1 \subseteq B \cap \Gamma \subseteq \frac{1}{D_2} \cdot P_2$. In particular, P_2 can be covered by D_1^{n-1} translates of P_1.

Applying the homomorphism f, we obtain

$$f(P_1) \subseteq f(B \cap \Gamma) \subseteq \frac{1}{D_2} f(P_2).$$

Since f is $\mathcal{O}_K$-linear, $f(P_1)$ and $f(P_2)$ are also $\mathcal{O}_K$-GAPs of dimension $n-1$. Setting $Q = \frac{1}{D_2} f(P_2)$, which is again an $\mathcal{O}_K$-GAP of dimension $n-1$, we have, by the claim above, that $P \subseteq f(B \cap \tilde{\Gamma}) \subseteq Q$, so it suffices to show that Q is small. Since P_2 can be covered by $D_1^{n-1} = O_n(1)$-many translates of P_1, $f(P_2)$ can also be covered by $O_n(1)$-many translates of $f(P_1)$. But then

$$|f(P_2)| \ll_n |f(P_1)| \leq |f(B \cap \Gamma)| \leq |(2pC_1 + 1) \star P| \ll_{n,p} |P|,$$

as required. □

4.4 Freiman's theorem for sums of dilates

One version of Freiman's fundamental theorem on sets of small doubling is as follows.

Theorem 4.13 (Freiman [8])**.** *For every $C > 0$, there are constants n and F such that for any $A \subset \mathbb{Z}^d$ satisfying $|A + A| \leq C|A|$, there exists a proper GAP $P \subset \mathbb{Z}^d$ containing A of dimension at most n and size at most $F|A|$.*

We have now built up sufficient background to prove the promised Freiman-type structure theorem for sets with small sums of dilates, which we restate for the reader's convenience.

Theorem 4.14. *For every $C > 0$ and $p \in \mathbb{N}$, there are constants n and F such that for any $A \subset K$ satisfying*

$$|A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C|A|,$$

there exists a p-proper $\mathcal{O}_K$-GAP $P \subset K$ containing A of dimension at most n and size at most $F|A|$.

Recall, from Lemma 4.1, that we have constants $C_2, C_3 \in \mathbb{N}$ with the property that $\lambda_l x \in \frac{1}{C_2} \cdot B(C_3 \|x\|)$ for all $l = 0, \ldots, k$ and $x \in \mathcal{O}_K$. Thus, if P is an $\mathcal{O}_K$-GAP, then $\lambda_l \cdot P$ lies in a translate of $\frac{1}{C_2} \cdot (C_3 \star P)$. Indeed, if $x = v_0 + l_1 v_1 + \cdots + l_m v_m \in P$, then $\lambda_l x = \lambda_l v_0 + (\lambda_l l_1) v_1 + \cdots + (\lambda_l l_m) v_m$ with $\lambda_l l_i \in \frac{1}{C_2} B(C_3 \|l_i\|)$. Therefore,

$$\begin{aligned} |P + \lambda_1 \cdot P + \cdots + \lambda_k \cdot P| &\leq |(k+1)C_3 \star P| \\ &\leq ((k+1)C_3)^{nd} |P|. \end{aligned}$$

In other words, P has a small sum of dilates. That is, Theorem 4.14 embeds a set A with a small sum of dilates into another, more structured set which, unlike an ordinary GAP, also has a small set of dilates. We now proceed to the proof of this statement.

Proof of Theorem 4.14. By translating, we may assume that $0 \in A$. By the Ruzsa triangle inequality,

$$|A + A||\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq |A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A|^2 \leq C^2 |A|^2.$$

Using the trivial bound $|\lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \geq |A|$, we obtain $|A + A| \leq C^2 |A|$. By the Plünnecke–Ruzsa inequality, $|A + A + A| \leq C^6 |A|$. By the Ruzsa triangle inequality again,

$$|(A + A) + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A||A| \leq |A + A + A||A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C^7 |A|^2,$$

so $|(A + A) + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A| \leq C^7 |A|$. Similar repeated applications of the triangle inequality gives $|(A + A) + \lambda_1 \cdot (A + A) + \cdots + \lambda_k \cdot (A + A)| \leq C^{7+6k} |A|$. Thus, $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ has

small doubling constant. Therefore, by Freiman's theorem, $A + \lambda_1 \cdot A + \cdots + \lambda_k \cdot A$ is contained in a proper GAP

$$P_0 = \{l_1 v_1 + \cdots + l_{n_0} v_{n_0} \mid -L_i < l_i < L_i\}$$

of dimension n_0 with $|P_0| \ll |A|$. Note that since $0 \in A \subseteq P_0$, we are free to assume that P_0 is centered.

Now let P_1 be the $\mathcal{O}_K$-GAP given by

$$P_1 = \{l_1 v_1 + \cdots + l_{n_0} v_{n_0} \mid l_i \in B(L_i)\}.$$

Then P_1 contains P_0. At first glance, it might seem that the size of P_1 could be as large as $|P_0|^d$. However, we now show that this is not the case.

Claim 4.15. $|P_1| \ll |P_0|$.

Proof. For a subset $X \subseteq K$ and $c > 0$, we say that X is (c, P_0)-*small* if X can be covered by c-many translates of P_0. For brevity, we will simply say that X is P_0-small if c is a bounded constant independent of X, P_0. Thus, if X, Y are P_0-small, so is their sumset $X + Y$. Indeed, if X, Y can be covered by x, y-many translates of P_0, respectively, then $X + Y$ can be covered by xy-many translates of $P_0 + P_0$, which itself can be covered by 2^{n_0}-many translates of P_0.

We shall show that for each $i \in [d], j \in [n_0]$, the set $S_{ij} := \{e_i v_j, 2e_i v_j, \ldots, L_j e_i v_j\}$ is P_0-small. Then we would have proved the claim, since the sets $\{-L_j e_i v_j, \ldots, L_j e_i v_j\}$ are then P_0-small, P_1 is the sum of these sets and there are only a bounded number of them.

Since $\lambda_1, \ldots, \lambda_k$ generate K, there exist (fixed) integers $b, a_1, \ldots, a_k$ with $b > 0$ such that $be_i = a_1\lambda_1 + \cdots + a_k\lambda_k$. It will suffice to show that the set $S := \{be_i v_j, 2be_i v_j, \ldots, L_j be_i v_j\}$ is P_0-small, since S_{ij} can be covered by b translates of it. But then it suffices to show that $S'_l := \{a_l\lambda_l v_j, 2a_l\lambda_l v_j, \ldots, L_j a_l \lambda_l v_j\}$ is P_0-small for each l, since S is contained in $S'_1 + \cdots + S'_k$. But then, finally, it suffices to show that $S_l := \{\lambda_l v_j, 2\lambda_l v_j, \ldots, L_j \lambda_l v_j\}$ is P_0-small for each l, since S'_l is covered by $|a_l|$-many translates of S_l.

Suppose $|P_0 + P_0| < c|A|$, where $c = O(1)$ is a positive integer. Let s be an arbitrary positive integer with $s < L_j/c$. Consider the sets

$$A, A + sv_j, A + 2sv_j, \ldots, A + csv_j.$$

All these sets have size $|A|$ and are contained in $P_0 + P_0$. But $|P_0 + P_0| < c|A|$, so two of these sets intersect, say $(A + msv_j) \cap (A + m'sv_j) \neq \emptyset$ for $0 \leq m < m' \leq c$. Thus, $(m' - m)sv_j \in A - A$. Therefore, $c!s\lambda_l v_j \in c!(\lambda_l \cdot A) - c!(\lambda_l \cdot A) \subseteq c!P_0 - c!P_0$. Since $1 \leq s < L_j/c$ was arbitrary, we have that the set

$$\{c!\lambda_l v_j, 2c!\lambda_l v_j, \ldots, \lfloor L_j/c \rfloor\, c!\lambda_l v_j\} \subseteq c!P_0 - c!P_0$$

is P_0-small. Thus, the set $T := \{c!\lambda_l v_j, 2c!\lambda_l v_j, \ldots, L_j c!\lambda_l v_j\}$ is P_0-small. Finally, S_l is P_0-small since it can be covered by $c!$-many translates of T. □

If P_1 is p-proper, then we are done. Otherwise, by Lemma 4.11, we can find an $\mathcal{O}_K$-GAP P_2 of one dimension smaller containing P_1 with $|P_2| \ll |P_1|$. If P_2 is also not p-proper, we invoke Lemma 4.11 again to obtain P_3 and so on. Note that we can only do this at most n_0 times, since any $\mathcal{O}_K$-GAP of dimension 1 is necessarily p-proper. Thus, we will eventually find a p-proper $\mathcal{O}_K$-GAP P containing A of dimension $O(1)$ with $|P| \ll |A|$. □

5 Reduction to a dense subset of the box

With the results of the last section in hand, we are now able to complete the second part of our plan, reducing the proof of our main result, in the form of Theorem 2.2, to the case where A is a dense subset of the box $[0,N)^d$.

Lemma 5.1. *For any $\varepsilon > 0$, there exists N_0 such that if $N \geq N_0$ and $A \subseteq [0,N)^d$ with $|A| \geq \varepsilon N^d$, then*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\lambda_1, \ldots, \lambda_k)|A| - o_\varepsilon(|A|).$$

The proof of Lemma 5.1, which is the heart of this paper, will occupy us for the next few sections. Before moving on to this, we first show that, together with our version of Freiman's theorem for sums of dilates, Lemma 5.1 completes the proof of Theorem 2.2.

Proof of Theorem 2.2 assuming Lemma 5.1. Let $A \subset \mathbb{Z}^d$ be finite and suppose that

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \leq H|A|,$$

where $H = H(\lambda_1, \ldots, \lambda_k)$. Let $\Phi, \Phi', \mathfrak{D}$ be as in Section 2. Setting $A' = \Phi'^{-1}(A) \subseteq \mathfrak{D} \subseteq \mathcal{O}_K$, we have

$$|A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'| \leq H|A'|.$$

Let C_3 be as in Lemma 4.1. By Theorem 4.14, our version of Freiman's theorem for sums of dilates applied with $p = (k+1)C_3$, A' is contained in a $(k+1)C_3$-proper $\mathcal{O}_K$-GAP $P \subset K$ of dimension $n = O(1)$ and size $|P| = O(|A'|)$. Suppose P is of the form

$$\{v_0 + l_1 v_1 + \cdots + l_n v_n \mid l_j \in B(L_j)\}.$$

Then $|P| \sim (\prod_{j=1}^n L_j)^d$, where the notation $A \sim B$ indicates that the quantities A and B are equal up to a constant multiplicative factor depending only on $\lambda_1, \ldots, \lambda_k$. By translating A', we may assume that $v_0 = 0$. By Lemma 4.1, we have $\lambda_l \cdot B(L_j) \subseteq \frac{1}{C_2} \cdot B(C_3 L_j)$ for all j, l. Thus, $\lambda_l \cdot A' \subseteq \lambda_l \cdot P \subseteq \frac{1}{C_2} \cdot (C_3 \star P)$ for all l.

We will now map P to a dense subset of a box via a Freiman isomorphism. Let $v_1^* = 1$ and $v_l^* = 3(k+1)C_3 L_{l-1} v_{l-1}^*$ for $l = 2, \ldots, n$. Let P^* be the $\mathcal{O}_K$-GAP

$$P^* := \{l_1 v_1^* + l_2 v_2^* + \cdots + l_n v_n^* \mid l_j \in B(L_j)\}.$$

Then P^* is $(k+1)C_3$-proper. Indeed, if $l_1 v_1^* + l_2 v_2^* + \cdots + l_n v_n^* = l_1' v_1^* + l_2' v_2^* + \cdots + l_n' v_n^*$ for some $l_j, l_j' \in B((k+1)C_3 L_j)$, then we have

$$(l_1 - l_1')v_1^* + \cdots + (l_n - l_n')v_n^* = 0.$$

Suppose $l_t \neq l_t'$ for some $t \in [n]$. Let t be the largest such index, so we have

$$(l_t' - l_t)v_t^* = (l_1 - l_1')v_1^* + \cdots + (l_{t-1} - l_{t-1}')v_{t-1}^*.$$

However, $\|(l_t' - l_t)v_t^*\| \geq v_t^* = 3(k+1)C_3 L_{t-1} v_{t-1}^*$, whereas

$$\begin{aligned}
\left\|(l_1 - l_1')v_1^* + \cdots + (l_{t-1} - l_{t-1}')v_{t-1}^*\right\| &\leq \|(l_1 - l_1')v_1^*\| + \cdots + \left\|(l_{t-1} - l_{t-1}')v_{t-1}^*\right\| \\
&\leq (\|l_1\| + \|l_1'\|)v_1^* + \cdots + (\|l_{t-1}\| + \left\|l_{t-1}'\right\|)v_{t-1}^* \\
&< 2(k+1)C_3 L_1 v_1^* + \cdots + 2(k+1)C_3 L_{t-1} v_{t-1}^* \\
&\leq 3(k+1)C_3 L_{t-1} v_{t-1}^*,
\end{aligned}$$

a contradiction. This proves that P^* is $(k+1)C_3$-proper.

Consider $\Psi : (k+1)C_3 \star P \to (k+1)C_3 \star P^*$, the natural bijection given by

$$l_1 v_1 + \cdots + l_n v_n \longleftrightarrow l_1 v_1^* + l_2 v_2^* + \cdots + l_n v_n^*.$$

Let $A^* = \Psi(A')$, so that $|A^*| = |A'|$. We claim that for $l = 0, \ldots, k$, we have $\Psi(C_2\lambda_l \cdot A') = C_2\lambda_l \cdot A^*$. Indeed, first observe that the LHS is well-defined, since $\lambda_l \cdot P \subseteq \frac{1}{C_2} \cdot (C_3 \star P)$, so we have $C_2\lambda_l \cdot P \subseteq C_3 \star P$, which is in the domain of Ψ. For any $a = l_1 v_1 + \cdots + l_n v_n \in A'$, set $l'_{jl} = C_2\lambda_l \cdot l_j$, which belongs to $B(C_3 L_j)$ by Lemma 4.1. Then

$$\begin{aligned}\Psi(C_2\lambda_l \cdot a) &= \Psi(l'_{1l} v_1 + \cdots + l'_{nl} v_n) = l'_{1l} v_1^* + \cdots + l'_{nl} v_n^* \\ &= C_2\lambda_l \cdot (l_1 v_1^* + \cdots + l_n v_n^*) = C_2\lambda_l \Psi(a).\end{aligned}$$

This proves the stated claim that $\Psi(C_2\lambda_l \cdot A') = C_2\lambda_l \cdot A^*$.

Since P is $(k+1)C_3$-proper, $C_3 \star P$ is $(k+1)$-proper. Hence, Ψ is a $(k+1)$-Freiman isomorphism on $C_3 \star P$ and, therefore, since $C_3 > C_2$,

$$\begin{aligned}\Psi(C_2 \cdot (A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A')) &= \Psi(C_2\lambda_0 \cdot A' + C_2\lambda_1 \cdot A' + \cdots + C_2\lambda_k \cdot A') \\ &= \Psi(C_2\lambda_0 \cdot A') + \Psi(C_2\lambda_1 \cdot A') + \cdots + \Psi(C_2\lambda_k \cdot A') \\ &= C_2\lambda_0 \cdot A^* + C_2\lambda_1 \cdot A^* + \cdots + C_2\lambda_k \cdot A^* \\ &= C_2 \cdot (A^* + \lambda_1 \cdot A^* + \cdots + \lambda_k \cdot A^*).\end{aligned}$$

It follows that

$$|A^* + \lambda_1 \cdot A^* + \cdots + \lambda_k \cdot A^*| = |A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'|.$$

Note that $P^* \subseteq B(L)$ for some $L \sim \prod_{j=1}^n L_j$. Recall that C_2 is an integer satisyfing $C_2\lambda_l \in \mathcal{O}_K$ for all l. In particular, $C_2 \in \mathfrak{D}$ and, since $P^* \subset \mathcal{O}_K$, $C_2 \cdot P^* \subset \mathfrak{D}$. Since $C_2 \cdot P^* \subseteq B(C_2 L)$, $\Phi'(C_2 \cdot P^*)$ is contained in a box $[-N, N]^d$ with $N \sim L$. But $N^d \sim |P| \sim |A|$ and so $\Phi'(C_2 \cdot A^*)$ is a dense subset of the box $[-N, N]^d$. By Lemma 5.1 (after translating into the box $[0, 2N+1)^d$), we have

$$\begin{aligned}|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| &= |A' + \lambda_1 \cdot A' + \cdots + \lambda_k \cdot A'| \\ &= |A^* + \lambda_1 \cdot A^* + \cdots + \lambda_k \cdot A^*| \\ &= |\mathcal{L}_0(\Phi'(C_2 \cdot A^*)) + \cdots + \mathcal{L}_k(\Phi'(C_2 \cdot A^*))| \\ &\geq H|A^*| - o(|A^*|) \\ &= H|A| - o(|A|),\end{aligned}$$

as required. □

6 Lattice densities

As already mentioned in the introduction, the key to proving Lemma 5.1 is to represent each discrete set A by a continuous set $\overline{A}$, which we call a lattice density, to which we can apply the continuous estimate given by Theorem 3.1. In this section, we introduce these lattice densities and prove some general facts about them. Very roughly, the lattice density of a set $A \subseteq \mathbb{Z}^d$ will encode the density of A with respect to certain lattices.

6.1 Lattice densities for periodic sets

Let L be a lattice of rank d, that is, $L \cong \mathbb{Z}^d$. We say that $A \subseteq L$ is *d-periodic* if its group of translational symmetries has rank d. Let $\mathcal{F} = \{L_1 \subseteq L_2 \subseteq \cdots \subseteq L_k\}$ be a flag of sublattices of L, each of which has rank d. In this section, we will define the *lattice density* of any d-periodic set $A \subseteq L$ with respect to the flag $\mathcal{F}$, denoted by $\mathrm{LD}(A; \mathcal{F})$, which will be a subset of $[0,1]^k$ that is a finite union of closed axis-aligned boxes.

For any affine lattice $M \subseteq L$ of rank d, we write $\rho_M(A)$ for the density of $A \cap M$ in M. Since A is d-periodic, this density is always well-defined. In particular, $0 \leq \rho_M(A) \leq 1$. This already allows us to define the lattice density for $k = 1$. Indeed, if $\mathcal{F} = \{L_1\}$ and $A \cap L_1 \neq \emptyset$, we set $\mathrm{LD}(A; \mathcal{F})$ to be the interval $[0, \rho_{L_1}(A)] \subset \mathbb{R}$, while if $A \cap L_1 = \emptyset$, we set $\mathrm{LD}(A; \mathcal{F}) = \emptyset$.

For $k > 1$, let $a_1, \ldots, a_m \in L_k$ be any set of coset representatives of L_k / L_{k-1}, where $m = [L_k : L_{k-1}]$. Let $D_j = \mathrm{LD}(A + a_j; \mathcal{F} \setminus L_k) \subseteq [0,1]^{k-1}$ for each $j \in [m]$ and

$$D = \bigcup_{j=1}^{m} \left(D_j \times \left[\frac{j-1}{m}, \frac{j}{m} \right] \right) \subseteq [0,1]^k.$$

Finally, set $\mathrm{LD}(A; \mathcal{F}) = C_k(D)$, where C_k is the compression in the k-th direction, defined as follows.

In our case, we will only be compressing sets which are finite unions of axis-aligned closed boxes. Let $X \subset \mathbb{R}^d$ be such a set and $1 \leq i \leq d$. Let $\pi_i : \mathbb{R}^d \to \mathbb{R}^{d-1}$ be the projection along the i-th axis. For $x \in \mathbb{R}^{d-1}$, let $X_x = \pi_i^{-1}(x)$, viewed as a subset of $\mathbb{R}$, and write $|X_x|$ for the measure of X_x. Now define $C_i'(X)$ to be the set Y such that $\pi_i(X) = \pi_i(Y)$ and, for each $x \in \pi_i(X)$, Y_x is the interval $[0, |X_x|]$. However, because of boundary issues, this is not quite the compression we want. For example, if $X = [0,1]^2 \cup [1,2]^2 \subset \mathbb{R}^2$, then $C_2'(X) = [0,2] \times [0,1] \cup \{1\} \times [1,2]$. The artifact $\{1\} \times [1,2]$ is undesirable and only arises because the boundaries of the two squares $[0,1]^2$ and $[1,2]^2$ overlap in the projection. To remove this artifact, we formally define $C_i(X)$ to be the closure of the interior of $C_i'(X)$. Since we will only be compressing sets which are finite unions of axis-aligned closed boxes, we still enjoy the main properties of compressions, such as preservation of the measure of X and that $C_i(X)$ is also a finite union of axis-aligned closed boxes. We will say that X is *C_i-compressed* if $C_i(X) = X$ and *compressed* if it is C_i-compressed for all i.

Observe that, because of the compression, $\mathrm{LD}(A; \mathcal{F})$ is independent of the ordering $a_1, \ldots, a_m$.

Example 6.1. Suppose $d = 1$, $k = 2$, $L = \mathbb{Z}$, $\mathcal{F} = \{3\mathbb{Z} \subset \mathbb{Z}\}$ and $A = 12\mathbb{Z} \cup (12\mathbb{Z} + 1) \cup (6\mathbb{Z} + 3)$. Pick $a_i = -i$ for $i = 1, 2, 3$ to be the coset representatives of $\mathbb{Z}/3\mathbb{Z}$. Let $A_i = (A - i) \cap 3\mathbb{Z}$ for $i = 1, 2, 3$. Thus, A_1, A_2, A_3 are the parts of A in the residue classes mod 3, translated so they all lie in $3\mathbb{Z}$. We can easily check that

- $A_1 = 12\mathbb{Z}$,
- $A_2 = \emptyset$,
- $A_3 = 12\mathbb{Z} + \{0, 6, 9\}$.

From the definition, $D_i = \mathrm{LD}(A_i; \{3\mathbb{Z}\}) = [0, \rho_{3\mathbb{Z}}(A_i)]$, so we have $D_1 = [0, 1/4]$, $D_2 = \emptyset$ and $D_3 = [0, 3/4]$. Stacking these intervals vertically and compressing, we get $\mathrm{LD}(A; \mathcal{F}) \subset [0,1]^2$ as shown in Figure 3.

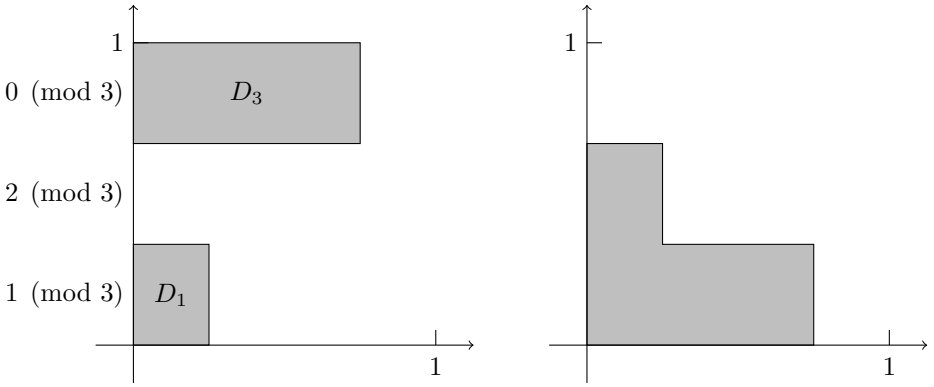

Figure 3: On the left, the D_i are stacked, while on the right they are compressed to give the final lattice density.

Throughout the rest of this section, $\mathcal{F} = \{L_1 \subseteq \cdots \subseteq L_k\}$ will be a flag of full-rank sublattices of a lattice $L \cong \mathbb{Z}^d$ and $A \subseteq L$ a d-periodic subset of L, our aim being to understand the properties of the lattice density $\mathrm{LD}(A; \mathcal{F})$. We begin with some basic observations.

Lemma 6.2. *The following are true:*

1. *For any $a \in L_k$, $\mathrm{LD}(A; \mathcal{F}) = \mathrm{LD}(A + a; \mathcal{F})$.*
2. *$\mathrm{LD}(A; \mathcal{F})$ is compressed.*
3. *If $B \subseteq A$ is d-periodic, then $\mathrm{LD}(B; \mathcal{F}) \subseteq \mathrm{LD}(A; \mathcal{F})$.*
4. *$\rho_{L_k}(A) = \mathrm{Vol}(\mathrm{LD}(A; \mathcal{F}))$.*
5. *$\mathrm{LD}(A; \mathcal{F})$ is a finite union of boxes of the form*

$$[0, r] \times \left[0, \frac{m_2}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{m_k}{[L_k : L_{k-1}]}\right],$$

where $r \in (0, 1]$ and $m_2, \ldots, m_k$ are positive integers.

Proof. We proceed by induction on k. In the base case $k = 1$, we have $\mathrm{LD}(A; \mathcal{F}) = [0, \rho_{L_1}(A)]$ and it is easy to check that all of the required properties hold.

Assume therefore that $k > 1$. Let $D_1, \ldots, D_k, D$ be as defined above. We verify each property in turn:

1. Addition by a permutes the cosets L_k/L_{k-1}, so let $a'_1, \ldots, a'_m$ be a permutation of $a_1, \ldots, a_m$ such that $a_j + a = a'_j + b_j$ for some $b_j \in L_{k-1}$. Let $D'_j = \mathrm{LD}(A + a + a_j; \mathcal{F} \setminus L_k)$. By the induction hypothesis, $D'_j = \mathrm{LD}(A + a'_j + b_j; \mathcal{F} \setminus L_k) = \mathrm{LD}(A + a'_j; \mathcal{F} \setminus L_k)$, so $D'_1, \ldots, D'_m$ is a permutation of $D_1, \ldots, D_m$. After compression, it follows that $\mathrm{LD}(A; \mathcal{F}) = \mathrm{LD}(A + a; \mathcal{F})$.
2. Each of the D_j are C_l-compressed for $l = 1, \ldots, k-1$. Thus, D is C_l-compressed for $l = 1, \ldots, k-1$ and, therefore, $\mathrm{LD}(A; \mathcal{F}) = C_k(D)$ is C_l-compressed for $l = 1, \ldots, k$.

3. Let $D'_j = \mathrm{LD}(B + a_j; \mathcal{F} \setminus L_k)$. By the induction hypothesis, $D'_j \subseteq D_j$, so the corresponding D' satisfies $D' \subseteq D$. Therefore, $\mathrm{LD}(B; \mathcal{F}) \subseteq \mathrm{LD}(A; \mathcal{F})$.

4. By definition, $D_j = \mathrm{LD}(A + a_j; \mathcal{F} \setminus L_k)$ and, by the induction hypothesis, we have $\rho_{L_{k-1}}(A + a_j) = \mathrm{Vol}(D_j)$. Therefore,

$$\begin{aligned}\mathrm{Vol}(\mathrm{LD}(A;\mathcal{F})) = \mathrm{Vol}(D) &= \frac{1}{m}\sum_{j=1}^{m}\mathrm{Vol}(D_j) = \frac{1}{m}\sum_{j=1}^{m}\rho_{L_{k-1}}(A+a_j)\\ &= \frac{[L_k : L_{k-1}]}{m}\sum_{j=1}^{m}\rho_{L_k}((A+a_j)\cap L_{k-1})\\ &= \sum_{j=1}^{m}\rho_{L_k}(A\cap(L_{k-1}-a_j)) = \rho_{L_k}(A).\end{aligned}$$

5. We show by induction that $\mathrm{LD}(A; \mathcal{F})$ is an interior-disjoint union of boxes of the form

$$v + [0, r] \times \left[0, \frac{1}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{1}{[L_k : L_{k-1}]}\right],$$

where v is of the form

$$\left(0, \frac{m_2}{[L_2 : L_1]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right)$$

with $m_2, \ldots, m_k$ non-negative integers. The base case is trivial since $\mathrm{LD}(A; \mathcal{F})$ is an interval.

By the induction hypothesis, each D_j is an interior-disjoint union of boxes of the form

$$v + [0, r] \times \left[0, \frac{1}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{1}{[L_{k-1} : L_{k-2}]}\right].$$

Thus, D is also the interior-disjoint union of boxes of the same kind and compressing preserves this property.

Finally, since $\mathrm{LD}(A; \mathcal{F})$ is compressed, it is the finite union of boxes of the required form. □

The next lemma fully determines $\mathrm{LD}(A; \mathcal{F})$ by giving a precise condition for when the lattice density contains any given point.

Lemma 6.3. *Suppose $k \geq 2$, $r \in (0, 1]$ is real and $m_2, \ldots, m_k$ are positive integers. Then the following are equivalent:*

1. $\mathrm{LD}(A; \mathcal{F})$ *contains the point*

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right).$$

2. *For each $l = 2, \ldots, k$ and $(i_l, i_{l+1}, \ldots, i_k) \in [m_l] \times [m_{l+1}] \times \cdots \times [m_k]$, there exist $b_{i_l,\ldots,i_k} \in L_k$ such that:*

   (a) *For $l < k$, $b_{i_l,i_{l+1},\ldots,i_k} \in b_{i_{l+1},\ldots,i_k} + L_l$.*

(b) $b_{i,i_{l+1},\ldots,i_k} - b_{j,i_{l+1},\ldots,i_k} \notin L_{l-1}$ *for each* $i \neq j$ *with* $i, j \in [m_l]$.

(c) $\rho_{L_1}(A + b_{i_2,\ldots,i_k}) \geq r$ *for each* $i_2, \ldots, i_k$.

Proof. We proceed by induction on k. Let $a_1, \ldots, a_m$ be any coset representatives of L_k/L_{k-1} with $m = [L_k : L_{k-1}]$ and $D_i = \mathrm{LD}(A + a_i; \mathcal{F} \setminus L_k)$.

$1 \Rightarrow 2$: From the construction of $\mathrm{LD}(A; \mathcal{F})$, m_k of the D_i contain the point

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_{k-1}}{[L_{k-1} : L_{k-2}]}\right).$$

Without loss of generality, assume that they are $D_1, \ldots, D_{m_k}$. Set $b_i = a_i \in L_k$ for $i = 1, \ldots, m_k$. Then $b_i - b_j \notin L_{k-1}$ for $i \neq j$.

If $k = 2$, then each D_i with $i \in [m_k]$ contains r, meaning that $\rho_{L_1}(A + a_i) \geq r$. Thus, $\rho_{L_1}(A + b_i) \geq r$ for each $i \in [m_k]$, completing the proof of the base case.

Now suppose that $k > 2$. By the induction hypothesis applied to each D_{i_k}, there exist $b'_{i_l,\ldots,i_k} \in L_{k-1}$ for each $(i_l, i_{l+1}, \ldots, i_k) \in [m_l] \times [m_{l+1}] \times \cdots \times [m_k]$ such that

(a) For $l < k-1$, $b'_{i_l,\ldots,i_k} \in b'_{i_{l+1},\ldots,i_k} + L_l$.

(b) For $l < k$, $b'_{i,i_{l+1},\ldots,i_k} - b'_{j,i_{l+1},\ldots,i_k} \notin L_{l-1}$ for each $i \neq j$ with $i, j \in [m_l]$.

(c) $\rho_{L_1}(A + b_{i_k} + b'_{i_2,\ldots,i_k}) \geq r$ for each $i_2, \ldots, i_k$.

Set $b_{i_l,\ldots,i_k} = b'_{i_l,\ldots,i_k} + b_{i_k}$. Then property (a) holds for $l < k-1$; property (b) holds for $l < k$ and property (c) holds. It remains to check that $b_{i_{k-1},i_k} \in b_{i_k} + L_{k-1}$ and $b_i - b_j \notin L_{k-1}$ for each $i \neq j$. The former holds since $b_{i_{k-1},i_k} = b'_{i_{k-1},i_k} + b_{i_k} \in b_{i_k} + L_{k-1}$ and the latter was observed earlier.

$2 \Leftarrow 1$: Since $a_1, \ldots, a_m$ are any coset representatives, we may pick $a_i = b_i$ for $i = 1, \ldots, m_k$.

For $k = 2$, since $\rho_{L_1}(A + b_i) \geq r$, D_i contains r for $i = 1, \ldots, m_2$. Thus, $\mathrm{LD}(A; \mathcal{F})$ contains the point $(r, \frac{m_2}{|L_2/L_1|})$.

Now assume $k > 2$. Let $b'_{i_l,\ldots,i_k} = b_{i_l,\ldots,i_k} - b_{i_k}$. Then we have the following properties, inherited from the b:

(a) For $l < k-1$, $b'_{i_l,\ldots,i_k} \in b'_{i_{l+1},\ldots,i_k} + L_l$.

(b) For $l < k$, $b'_{i,i_{l+1},\ldots,i_k} - b'_{j,i_{l+1},\ldots,i_k} \notin L_{l-1}$ for each $i \neq j$ with $i, j \in [m_l]$.

(c) $\rho_{L_1}(A + b_{i_k} + b'_{i_2,\ldots,i_k}) \geq r$ for each $i_2, \ldots, i_k$.

By the induction hypothesis, for $i = 1, \ldots, m_k$, D_i contains the point

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_{k-1}}{[L_{k-1} : L_{k-2}]}\right).$$

Therefore, by the definition of $\mathrm{LD}(A; \mathcal{F})$, it contains the point

$$\left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right),$$

as required. □

As an application of this lemma, we now show how to compute the projections of lattice densities.

Lemma 6.4. *The following are true:*

1. $\pi_1(\mathrm{LD}(A;\mathcal{F}))$ *is the interval* $[0,r]$*, where*

$$r = \max_{a\in L_k} \{\rho_{L_1}(A+a)\}.$$

In particular, $\pi_1(\mathrm{LD}(A;\mathcal{F}))$ *depends only on* A*,* L_1 *and* L_k*.*

2. *For* $2 \le l \le k$*,* $\pi_l(\mathrm{LD}(A;\mathcal{F}))$ *is the interval*

$$\left[0, \frac{m}{[L_l : L_{l-1}]}\right],$$

where $m \in \mathbb{Z}$ *is the maximum number of elements* $a_1,\dots,a_m \in A \cap L_k$ *such that* $a_i - a_j \in L_l \setminus L_{l-1}$ *for any* $i \neq j$*. In particular,* $\pi_l(\mathrm{LD}(A;\mathcal{F}))$ *depends only on* A*,* L_{l-1}*,* L_l *and* L_k*.*

Proof. We first observe that the maxima are well-defined. Indeed, ρ_{L_1} is invariant under translations by elements of L_1, so, for (1), we may take the maximum over the finitely many coset representatives of L_k/L_1. For (2), we see that each a_i must belong to a different coset of L_l/L_{l-1}, so $m \le [L_l : L_{l-1}]$.

1. If $\pi_1(\mathrm{LD}(A;\mathcal{F})) = [0,r]$, then $\mathrm{LD}(A;\mathcal{F})$ contains the point

$$\left(r, \frac{1}{[L_2 : L_1]}, \frac{1}{[L_3 : L_2]}, \dots, \frac{1}{[L_k : L_{k-1}]}\right)$$

and r is the maximum such real number. By Lemma 6.3, this is equivalent to the existence of some $b \in L_k$ such that $\rho_{L_1}(A+b) \ge r$. Thus,

$$r = \max_{b\in L_k} \{\rho_{L_1}(A+b)\}.$$

2. Suppose $\mathrm{LD}(A;\mathcal{F})$ contains the point

$$\left(r, \frac{1}{[L_2 : L_1]}, \dots, \frac{m}{[L_{l+1} : L_l]}, \dots, \frac{1}{[L_k : L_{k-1}]}\right)$$

for some $r > 0$ and m is the maximum such integer. By Lemma 6.3, this is equivalent to the existence of $b \in L_k$ and $b_1,\dots,b_m \in b + L_l$ such that $b_i - b_j \notin L_{l-1}$ for each $i \neq j$ and $\rho_{L_1}(A+b_i) \ge r$ for each i. Since we may take r to be the minimum of $\rho_{L_1}(A+b_i)$ over all i, we are just requiring that $\rho_{L_1}(A+b_i) > 0$, that is, $(A+b_i) \cap L_1 \neq \emptyset$ for each i.

Suppose such b, b_i exist. Let $a_i \in A$ be such that $a_i + b_i \in L_1$, which exists since $(A + b_i) \cap L_1 \neq \emptyset$. Note that $a_i \in L_k$ since $a_i \in -b_i + L_1 \subseteq L_k$. Moreover, for any $i \neq j$, $a_i - a_j \in b_j - b_i + L_1 \subseteq L_l \setminus L_{l-1}$, as required.

On the other hand, suppose we have $a_1,\dots,a_m \in A \cap L_k$ such that $a_i - a_j \in L_l \setminus L_{l-1}$ for all $i \neq j$. Set $b = -a_1$ and $b_i = -a_i$ for each i. Then $b_i = b + a_1 - a_i \in b + L_l$ and $b_i - b_j = a_j - a_i \notin L_{l-1}$ for $i \neq j$. Finally, note that $(A+b_i) \cap L_1 \neq \emptyset$ for each i, since it contains 0. □

The next result, which again makes use of Lemma 6.3, describes lattice densities of sumsets.

Theorem 6.5. *Suppose $B \subseteq L$ is d-periodic. If $p = (p_1, \ldots, p_k) \in \mathrm{LD}(A; \mathcal{F})$ and $q = (q_1, \ldots, q_k) \in \mathrm{LD}(B; \mathcal{F})$, then*

$$\max(p, q) \in \mathrm{LD}(A + B; \mathcal{F}),$$

where $\max(p, q) = (\max(p_1, q_1), \ldots, \max(p_k, q_k))$.

Proof. Since $\mathrm{LD}(A; \mathcal{F})$ and $\mathrm{LD}(B; \mathcal{F})$ are both unions of boxes of the form

$$[0, r] \times \left[0, \frac{m_2}{[L_2 : L_1]}\right] \times \cdots \times \left[0, \frac{m_k}{[L_k : L_{k-1}]}\right]$$

for $r \in (0, 1]$ and $m_2, \ldots, m_k$ positive integers, we may assume that p, q are of the form

$$p = \left(r, \frac{m_2}{[L_2 : L_1]}, \frac{m_3}{[L_3 : L_2]}, \ldots, \frac{m_k}{[L_k : L_{k-1}]}\right),$$

$$q = \left(r', \frac{m_2'}{[L_2 : L_1]}, \frac{m_3'}{[L_3 : L_2]}, \ldots, \frac{m_k'}{[L_k : L_{k-1}]}\right).$$

Without loss of generality, we assume that $r \geq r'$. By Lemma 6.3, we obtain $b_{i_l,\ldots,i_k}, b'_{i_l,\ldots,i_k} \in L_k$ with the properties given in the lemma. Let $I = \{i \in [2, k] \mid m_i \geq m_i'\}$ and $J = [2, k] \setminus I$. Set $c_{i_l,\ldots,i_k} = b_{i_l',\ldots,i_k'} + b'_{i_l'',\ldots,i_k''}$, where

$$i_j' = \begin{cases} i_j & \text{if } j \in I \\ 1 & \text{otherwise} \end{cases} \quad \text{and} \quad i_j'' = \begin{cases} i_j & \text{if } j \in J \\ 1 & \text{otherwise} \end{cases}$$

for $(i_l, \ldots, i_k) \in [\max(m_l, m_l')] \times \cdots \times [\max(m_k, m_k')]$. We wish to show that the $c_{i_l,\ldots,i_k}$ satisfy properties (a)–(c) in Lemma 6.3 for $\mathrm{LD}(A + B; \mathcal{F})$. Note that we have $c_{i_l,\ldots,i_k} \in L_k$ since $b_{i_l',\ldots,i_k'}, b'_{i_l'',\ldots,i_k''} \in L_k$. We now prove each of (a)–(c) in turn:

(a) For $l < k$, we have $b_{i_l', i_{l+1}', \ldots, i_k'} \in b_{i_{l+1}', \ldots, i_k'} + L_l$ and $b'_{i_l'', i_{l+1}'', \ldots, i_k''} \in b'_{i_{l+1}'', \ldots, i_k''} + L_l$. Thus, $c_{i_l, i_{l+1}, \ldots, i_k} \in c_{i_{l+1}, \ldots, i_k} + L_l$.

(b) Suppose $l \in I$. Then, for $i \neq j$, $c_{i, i_{l+1}, \ldots, i_k} - c_{j, i_{l+1}, \ldots, i_k} = b_{i, i_{l+1}', \ldots, i_k'} - b_{j, i_{l+1}', \ldots, i_k'} \notin L_{l-1}$. The case $l \in J$ is similar.

(c) We have $\rho_{L_1}(B + b'_{i_2'', \ldots, i_k''}) \geq r' > 0$. In particular, $B + b'_{i_2'', \ldots, i_k''}$ contains some element $x \in L_1$. Thus, $A + B + c_{i_2, \ldots, i_k} \supseteq A + b_{i_2', \ldots, i_k'} + x$, so we have $\rho_{L_1}(A + B + c_{i_2, \ldots, i_k}) \geq \rho_{L_1}(A + b_{i_2', \ldots, i_k'} + x) = \rho_{L_1}(A + b_{i_2', \ldots, i_k'}) \geq r$. □

The final result of this subsection relates projections of lattice densities with respect to different flags.

Lemma 6.6. *Suppose $\mathcal{F}' = \{L_1' \subseteq \cdots \subseteq L_{k-1}' \subseteq L_k\}$ is a flag of full-rank sublattices of L. Then the following are true:*

1. *If $L_1' \subseteq L_1$, then*

$$|\pi_1(\mathrm{LD}(A; \mathcal{F}))| \leq |\pi_1(\mathrm{LD}(A; \mathcal{F}'))|.$$

2. *For $2 \le l \le k$, if $L'_l = L_l$ and $L'_{l-1} \subseteq L_{l-1}$, then*

$$|\pi_l(\mathrm{LD}(A;\mathcal{F}))| \ge |\pi_l(\mathrm{LD}(A;\mathcal{F}'))|.$$

Proof. 1. Let

$$r = \max_{a \in L_k} \{\rho_{L_1}(A+a)\} \quad \text{and} \quad r' = \max_{a \in L_k} \left\{\rho_{L'_1}(A+a)\right\}.$$

By Lemma 6.4, it suffices to show that $r \le r'$. Suppose r is attained by $a \in L_k$. Let $s = [L_1 : L'_1]$ and $c_1, \dots, c_s$ be coset representatives of L_1/L'_1. We can split $(A+a) \cap L_1$ into the disjoint union $\bigcup_{i=1}^{s} (A + a + c_i) \cap L'_1$, so that

$$\rho_{L_1}(A+a) = \frac{1}{s} \sum_{i=1}^{s} \rho_{L'_1}(A + a + c_i).$$

Therefore, there is some i such that $\rho_{L'_1}(A + a + c_i) \ge r$, so $r' \ge r$.

2. Suppose $|\pi_l(\mathrm{LD}(A;\mathcal{F}'))| = \frac{n}{[L'_l : L'_{l-1}]}$. By Lemma 6.4, there are $b_1, \dots, b_n \in A \cap L_k$ such that $b_i - b_j \in L'_l \setminus L'_{l-1}$. Let $s = [L_{l-1} : L'_{l-1}]$. Define an equivalence relation by setting $b_i \sim b_j$ if $b_i - b_j \in L_{l-1}$. Then each equivalence class has at most s elements, since no two elements belong to the same coset of L_{l-1}/L'_{l-1}. Let $a_1, \dots, a_m$ be any representatives of the equivalence classes of $b_1, \dots, b_n$, so that $ms \ge n$. Since the a_i are in different equivalence classes, we have $a_i - a_j \notin L_{l-1}$ for $i \ne j$. By Lemma 6.4 again, we have

$$|\pi_l(\mathrm{LD}(A;\mathcal{F}))| \ge \frac{m}{[L_l : L_{l-1}]} = \frac{ms}{[L_l : L'_{l-1}]} \ge \frac{n}{[L_l : L'_{l-1}]} = |\pi_l(\mathrm{LD}(A;\mathcal{F}'))|,$$

as required. □

6.2 Local lattice densities

In practice, we will make use of a local variant of lattice density. Intuitively, the local lattice density of A at some point x is the lattice density of a tiny region of A around x. However, A is a discrete set, so we cannot simply take an infinitesimally small ball around x. Instead, we define the local lattice density of A in some small region $S \subset \mathbb{R}^d$ to be the lattice density of a collection of copies of $A \cap S$, placed so as to be d-periodic. To make this work, we require that S be tileable, which we now define. Note that we will continue to use notation from the previous subsection. In particular, $\mathcal{F} = \{L_1 \subseteq \cdots \subseteq L_k\}$ is a flag of full-rank sublattices of a lattice $L \cong \mathbb{Z}^d$.

Let $L_{\mathbb{R}} = L \otimes \mathbb{R} \cong \mathbb{R}^d$. We say that $S \subset L_{\mathbb{R}}$ is *tileable* if there is a sublattice $P \subseteq L_1$ of full rank such that $S \oplus P = L_{\mathbb{R}}$. In this case, we say that S is *tiled* by P. For example, if $L = \mathbb{Z}^d$, the box $[0, M)^d \subset \mathbb{R}^d$ is tileable as long as $M\mathbb{Z}^d \subseteq L_1$. In all of our applications, S will be a half-open box of the form $[0, M)^d$ or an affine transformation of it.

Let $P \subseteq L_1$ and $S \subset L_{\mathbb{R}}$ be such that S is tiled by P. For any $A \subseteq L$, define the *local lattice density*

$$\mathrm{LD}_S(A;\mathcal{F}) := \mathrm{LD}((A \cap S) + P; \mathcal{F}),$$

noting that $(A \cap S) + P$ is d-periodic. Using Lemma 6.3, it is not hard to check that $\mathrm{LD}_S(A;\mathcal{F})$ is independent of the choice of P as long as $P \subseteq L_1$.

Before moving on, we note some basic properties of these local lattice densities.

Lemma 6.7. *Let $S, T \subset L_{\mathbb{R}}$ be tileable and $A \subseteq S \cap T \cap L$. Then*

$$\mathrm{LD}_S(A;\mathcal{F}) = \Psi(\mathrm{LD}_T(A;\mathcal{F})),$$

where $\Psi : \mathbb{R}^d \to \mathbb{R}^d$ is given by

$$(x_1, \ldots, x_k) \mapsto \left(\frac{\mathrm{Vol}(T)}{\mathrm{Vol}(S)} x_1, x_2, \ldots, x_k\right).$$

Proof. Suppose T is tiled by $P \subseteq L_1$. Let $x = \left(r, \frac{m_2}{[L_2:L_1]}, \ldots, \frac{m_k}{[L_k:L_{k-1}]}\right) \in \mathrm{LD}_T(A;\mathcal{F})$. By Lemma 6.3, there exist $b_{i_l,\ldots,i_k} \in L_k$ satisfying the conditions in the lemma, one of which is that $\rho_{L_1}(A + P + b_{i_2,\ldots,i_k}) \geq r$.

Suppose S is tiled by $Q \subseteq L_1$. Since $T \oplus P = L_{\mathbb{R}}$, $\det(P) = \mathrm{Vol}(T)$ and, similarly, $\det(Q) = \mathrm{Vol}(S)$. Since $A + Q + b_{i_2,\ldots,i_k}$ is a union of translates of $A + b_{i_2,\ldots,i_k}$, one for each point of Q, its density within L_1, $\rho_{L_1}(A + Q + b_{i_2,\ldots,i_k})$, is inversely proportional to $\det(Q)$. In particular, $\rho_{L_1}(A + Q + b_{i_2,\ldots,i_k}) \det(Q) = \rho_{L_1}(A + P + b_{i_2,\ldots,i_k}) \det(P)$. Hence,

$$\rho_{L_1}(A + Q + b_{i_2,\ldots,i_k}) = \frac{\det(P)}{\det(Q)} \rho_{L_1}(A + P + b_{i_2,\ldots,i_k}) \geq \frac{\mathrm{Vol}(T)}{\mathrm{Vol}(S)} r.$$

Therefore, by Lemma 6.3, $\Psi(x) \in \mathrm{LD}_S(A;\mathcal{F})$, so we have $\mathrm{LD}_S(A;\mathcal{F}) \supseteq \Psi(\mathrm{LD}_T(A;\mathcal{F}))$. The converse follows similarly. □

Lemma 6.8. *Let $S, T \subset L_{\mathbb{R}}$ be tileable with $T \subseteq S$. Then, for $2 \leq l \leq k$,*

$$|\pi_l(\mathrm{LD}_T(A;\mathcal{F}))| \leq |\pi_l(\mathrm{LD}_S(A;\mathcal{F}))|.$$

Proof. By Lemma 6.7,

$$\begin{aligned} |\pi_l(\mathrm{LD}_T(A;\mathcal{F}))| &= |\pi_l(\mathrm{LD}_T(A \cap T;\mathcal{F}))| \\ &= |\pi_l(\mathrm{LD}_S(A \cap T;\mathcal{F}))| \\ &\leq |\pi_l(\mathrm{LD}_S(A;\mathcal{F}))|, \end{aligned}$$

as required. □

Lemma 6.9. *Let $S \subset L_{\mathbb{R}}$ be tileable and $A \subseteq L_k$. Then*

$$\frac{|A \cap S|}{|L_k \cap S|} = \mathrm{Vol}(\mathrm{LD}_S(A;\mathcal{F})).$$

Proof. Suppose S is tiled by $P \subseteq L_1$. Then

$$\mathrm{Vol}(\mathrm{LD}_S(A;\mathcal{F})) = \mathrm{Vol}(\mathrm{LD}((A \cap S) + P;\mathcal{F})) = \rho_{L_k}((A \cap S) + P) = \frac{|A \cap S|}{|L_k \cap S|},$$

as required. □

7 Families of flags

In this section, we construct flags such that "the projection π_{l+1} of the lattice density is preserved under multiplication by λ_l". More precisely, we want to find a flag $\mathcal{F}$ in $\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$ and a flag $\mathcal{G}$ in $\mathcal{O}_K$ such that, for any d-periodic $A \subseteq \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$,

$$\pi_{l+1}(\mathrm{LD}(A;\mathcal{F})) \subseteq \pi_{l+1}(\mathrm{LD}(\lambda_l \cdot A;\mathcal{G})) \tag{9}$$

for $l = 0, 1, \dots, k$. We can find such flags for each l, but, unfortunately, it may not be possible to find $\mathcal{F}, \mathcal{G}$ that work simultaneously for all l. To overcome this, we construct families of flags $\mathcal{F}_{\vec{n}}, \mathcal{G}_{\vec{n}}$ and show that for $\vec{n}$ "sufficiently large" these pairs satisfy (9) approximately for all l.

7.1 Algebraic families of flags

Recall that $\lambda_1, \dots, \lambda_k \in K = \mathbb{Q}(\lambda_1, \dots, \lambda_k)$ and $d = \deg(K/\mathbb{Q})$. Let $\mathfrak{a}_l$ be the ideal $\mathcal{O}_K \cap \lambda_1^{-1}\mathcal{O}_K \cap \cdots \cap \lambda_l^{-1}\mathcal{O}_K$ for $l = 0, 1, \dots, k$. In particular, $\mathfrak{a}_k = \mathfrak{D}_{\lambda_1,\dots,\lambda_k;K}$. Then $\mathfrak{a}_l^{-1}$ is the fractional ideal $\mathcal{O}_K + \lambda_1\mathcal{O}_K + \cdots + \lambda_l\mathcal{O}_K$. We also have $\mathcal{O}_K = \mathfrak{a}_0 \mid \mathfrak{a}_1 \mid \cdots \mid \mathfrak{a}_k$. Let $\mathfrak{b}_l \subseteq \mathcal{O}_K$ be the ideal such that $\mathfrak{a}_l = \mathfrak{b}_l\mathfrak{a}_{l-1}$ for each $l = 1, \dots, k$. For each $\vec{n} = (n_1, \dots, n_k) \in \mathbb{Z}^k_{\geq 0}$ and $l = 0, 1, \dots, k$, let $\mathfrak{c}_{\vec{n},l} = \mathfrak{b}_{l+1}^{n_{l+1}} \cdots \mathfrak{b}_k^{n_k}$. Define two flags of lattices by

$$\begin{aligned}\mathcal{F}^K_{\vec{n}} &:= \left\{\mathfrak{a}_k\mathfrak{c}_{\vec{n},0} \subseteq \mathfrak{a}_k\mathfrak{c}_{\vec{n},1} \subseteq \cdots \subseteq \mathfrak{a}_k\mathfrak{c}_{\vec{n},k-1} \subseteq \mathfrak{a}_k\right\},\\ \mathcal{G}^K_{\vec{n}} &:= \left\{\mathfrak{c}_{\vec{n},0} \subseteq \mathfrak{c}_{\vec{n},1} \subseteq \cdots \subseteq \mathfrak{c}_{\vec{n},k-1} \subseteq \mathcal{O}_K\right\}.\end{aligned}$$

These families of flags will serve as candidates for satisfying (9). The following two lemmas make this precise. Note that for any two vectors $\vec{n}, \vec{m} \in \mathbb{Z}^k$, we write $\vec{n} \geq \vec{m}$ if $n_i \geq m_i$ for all i. We also write $\vec{n} + c$ to denote the vector $(n_1 + c, \dots, n_k + c)$.

Lemma 7.1. *Let $A \subseteq \mathfrak{a}_k$ be d-periodic. Then, for any $\vec{n} \geq 0$,*

$$\pi_1(\mathrm{LD}(A;\mathcal{F}^K_{\vec{n}})) = \pi_1(\mathrm{LD}(A;\mathcal{G}^K_{\vec{n}+1})).$$

Proof. Let

$$r = \max_{a \in \mathfrak{a}_k}\left\{\rho_{\mathfrak{a}_k\mathfrak{c}_{\vec{n},0}}(A + a)\right\} \quad \text{and} \quad r' = \max_{a \in \mathcal{O}_K}\left\{\rho_{\mathfrak{a}_k\mathfrak{c}_{\vec{n},0}}(A + a)\right\}.$$

Note that $\mathfrak{b}_1 \cdots \mathfrak{b}_k = \mathfrak{a}_k$, so that $\mathfrak{c}_{\vec{n}+1,0} = \mathfrak{a}_k\mathfrak{c}_{\vec{n},0}$. By Lemma 6.4(1), it suffices to show that $r = r'$. Since $\mathfrak{a}_k \subseteq \mathcal{O}_K$, we clearly have $r' \geq r$. To see that $r \geq r'$, observe that, since $A \subseteq \mathfrak{a}_k$, $(A + a) \cap \mathfrak{a}_k = \emptyset$ for any $a \in \mathcal{O}_K \setminus \mathfrak{a}_k$. In particular, $\rho_{\mathfrak{a}_k\mathfrak{c}_{\vec{n},0}}(A + a) = 0$. □

For the next lemma, recall that $\mathcal{M}_l : K \to K$ is the $\mathbb{Q}$-linear map corresponding to multiplication by λ_l and each $\mathcal{M}_l$ restricts to the map $\mathfrak{a}_k \to \mathcal{O}_K$.

Lemma 7.2. *Let $A \subseteq \mathfrak{a}_k$ be d-periodic and $l \in [k]$. Then, for $\vec{n}, \vec{m} \geq 0$ with $m_i = n_i + 1$ for $i = l+1, l+2, \dots, k$ and $m_l = n_l$,*

$$|\pi_{l+1}(\mathrm{LD}(A;\mathcal{F}^K_{\vec{n}}))| \leq |\pi_{l+1}(\mathrm{LD}(\mathcal{M}_l A;\mathcal{G}^K_{\vec{m}}))|.$$

Proof. Let r be the maximum number of elements $a_1, \dots, a_r \in A$ such that $a_i - a_j \in \mathfrak{a}_k\mathfrak{c}_{\vec{n},l} \setminus \mathfrak{a}_k\mathfrak{c}_{\vec{n},l-1}$ for $i \neq j$. Then, by Lemma 6.4(2), $|\pi_{l+1}(\mathrm{LD}(A;\mathcal{F}^K_{\vec{n}}))| = r/[\mathfrak{a}_k\mathfrak{c}_{\vec{n},l} : \mathfrak{a}_k\mathfrak{c}_{\vec{n},l-1}]$. Since $m_l = n_l$, we have $[\mathfrak{a}_k\mathfrak{c}_{\vec{n},l} : \mathfrak{a}_k\mathfrak{c}_{\vec{n},l-1}] = [\mathfrak{c}_{\vec{n},l} : \mathfrak{c}_{\vec{n},l-1}] = N_{K/\mathbb{Q}}(\mathfrak{b}_l^{n_l}) = [\mathfrak{c}_{\vec{m},l} : \mathfrak{c}_{\vec{m},l-1}]$. By Lemma 6.4(2) applied to $|\pi_{l+1}(\mathrm{LD}(\mathcal{M}_l A;\mathcal{G}^K_{\vec{m}}))|$, it suffices to find $b_1, \dots, b_r \in \mathcal{M}_l A = \lambda_l \cdot A$ such that $b_i - b_j \in \mathfrak{c}_{\vec{m},l} \setminus \mathfrak{c}_{\vec{m},l-1}$ for $i \neq j$.

Set $b_i = \lambda_l a_i$, so it is clear that $b_i \in \lambda_l \cdot A$. It suffices to show that:

(a) $b_i - b_j \in \mathfrak{c}_{\vec{m},l}$,

(b) $b_i - b_j \notin \mathfrak{c}_{\vec{m},l-1}$ for $i \neq j$.

For (a), observe that $\lambda_l \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \subseteq \mathfrak{a}_l^{-1} \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} = \mathfrak{b}_{l+1} \cdots \mathfrak{b}_k \mathfrak{c}_{\vec{n},l} = \mathfrak{c}_{\vec{m},l}$. Thus, $b_i - b_j = \lambda_l(a_i - a_j) \in \lambda_l \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \subseteq \mathfrak{c}_{\vec{m},l}$.

For (b), suppose that $b_i - b_j \in \mathfrak{c}_{\vec{m},l-1}$ for some $i \neq j$. Then $a_i - a_j \in \lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1}$. On the other hand, $a_i - a_j \in \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}$. Together, we have $a_i - a_j \in \lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}$.

We claim that $\lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l} \subseteq \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}$, which will lead to a contradiction, since $a_i - a_j \notin \mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}$. We prove the claim by proving it locally at every prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, that is, we will show that $\nu_\mathfrak{p}(\lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}) \geq \nu_\mathfrak{p}(\mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1})$.

Recall that $\mathfrak{a}_l = \mathfrak{a}_{l-1} \cap \lambda_l^{-1} \mathcal{O}_K$, so $\nu_\mathfrak{p}(\mathfrak{a}_l) = \max(\nu_\mathfrak{p}(\mathfrak{a}_{l-1}), \nu_\mathfrak{p}(\lambda_l^{-1}))$, which implies that $\nu_\mathfrak{p}(\mathfrak{b}_l) = \max(0, \nu_\mathfrak{p}(\lambda_l^{-1}) - \nu_\mathfrak{p}(\mathfrak{a}_{l-1}))$. We have

$$\begin{aligned}\nu_\mathfrak{p}(\lambda_l^{-1} \mathfrak{c}_{\vec{m},l-1} \cap \mathfrak{a}_k \mathfrak{c}_{\vec{n},l}) &= \nu_\mathfrak{p}(\lambda_l^{-1} \mathfrak{a}_k \mathfrak{a}_l^{-1} \mathfrak{c}_{\vec{n},l-1} \cap \mathfrak{a}_k \mathfrak{b}_l^{-n_l} \mathfrak{c}_{\vec{n},l-1}) \\ &= \nu_\mathfrak{p}(\mathfrak{a}_k \mathfrak{c}_{\vec{n},l-1}) + \max(\nu_\mathfrak{p}(\lambda_l^{-1}) - \nu_\mathfrak{p}(\mathfrak{a}_l), -n_l \nu_\mathfrak{p}(\mathfrak{b}_l)).\end{aligned}$$

If $\nu_\mathfrak{p}(\mathfrak{a}_{l-1}) \geq \nu_\mathfrak{p}(\lambda_l^{-1})$, then $\nu_\mathfrak{p}(\mathfrak{b}_l) = 0$. Otherwise, $\nu_\mathfrak{p}(\mathfrak{a}_l) = \nu_\mathfrak{p}(\lambda_l^{-1})$. In either case, $\max(\nu_\mathfrak{p}(\lambda_l^{-1}) - \nu_\mathfrak{p}(\mathfrak{a}_l), -\nu_\mathfrak{p}(\mathfrak{b}_l)) \geq 0$, proving the claim and the lemma. □

Unfortunately, there are no pairs of flags $\mathcal{F}_{\vec{n}}^K$ and $\mathcal{G}_{\vec{m}}^K$ that simultaneously satisfy Lemmas 7.1 and 7.2 for all l. Indeed, in order for $\pi_1(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}^K)) = \pi_1(\mathrm{LD}(A; \mathcal{G}_{\vec{m}}^K))$ and $|\pi_{l+1}(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}^K))| \leq |\pi_{l+1}(\mathrm{LD}(\mathcal{M}_l A; \mathcal{G}_{\vec{m}}^K))|$ to hold for all l via the lemmas, we would require that $m_l = n_l$ and $m_l = n_l + 1$ simultaneously. To overcome this, in the next subsection, we will show that for $\vec{n}$ sufficiently large the projections of the lattice densities stabilise, so we may use $\mathcal{F}_{\vec{n}}^K$ and $\mathcal{G}_{\vec{n}}^K$. This seems to suggest that, as $\vec{n}$ tends to infinity, the lattice densities $\mathrm{LD}(A; \mathcal{F}_{\vec{n}})$ themselves converge as compact subsets. However, we make no attempt to formally prove this, since all we require is that their projections converge.

7.2 Regularity

For this subsection, we consider a more general setup, where we have, for each $\vec{n} = (n_1, \ldots, n_k) \in \mathbb{N}^k$, two flags

$$\begin{aligned}\mathcal{F}_{\vec{n}} &= \left\{ L_{\vec{n},1} \subseteq L_{\vec{n},2} \subseteq \cdots \subseteq L_{\vec{n},k} \subseteq \mathbb{Z}^d \right\}, \\ \mathcal{G}_{\vec{n}} &= \left\{ M_{\vec{n},1} \subseteq M_{\vec{n},2} \subseteq \cdots \subseteq M_{\vec{n},k} \subseteq \mathbb{Z}^d \right\},\end{aligned}$$

where $L_{\vec{n},l}$ depends only on $n_l, n_{l+1}, \ldots, n_k$ and $L_{\vec{n},l} \subseteq L_{\vec{n}',l}$ if $\vec{n} \geq \vec{n}'$ and similarly for $M_{\vec{n},l}$. We also fix a set $A \subseteq \mathbb{Z}^d$.

For a positive integer R, an *R-cube* is a set that comes from taking the set $[0, R)^d \subset \mathbb{R}^d$ and shifting it by an element of $R\mathbb{Z}^d$. Let P be an R-cube for some R. For natural numbers $M, n_l, n_{l+1}, \ldots, n_k$ with $M > 0$ and a real number $\delta > 0$, we say that P is *$(M, \delta, n_l, \ldots, n_k)$-regular* if each of the M^d different R/M-subcubes Q of P satisfies

$$|\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}'}))| \geq (1 - \delta) |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}}))|, \tag{10}$$

where $\vec{n} = (0, \ldots, 0, n_l, \ldots, n_k)$ and $\vec{n}' = (0, \ldots, 0, n_l + 1, \ldots, n_k)$.

Remark. *Here we are implicitly assuming that R/M is an integer. Throughout the remainder of the paper, whenever we mention a local density $\mathrm{LD}_P(A;\mathcal{F})$, we will assume that P is tileable. In particular, this means that R and R/M will always be multiples of every bounded number, so that the lattices $R\mathbb{Z}^d$ and $(R/M)\mathbb{Z}^d$ are contained in $L_{\vec{n},1}$. In practice, we will only be considering $\mathcal{F}_{\vec{n}}$ where $\vec{n}$ is bounded and (N/M)-cubes where M is bounded and N can be taken to be a multiple of a sufficiently large integer.*

By Lemmas 6.6 and 6.8, we always have

$$|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}'}))| \leq |\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))| \leq |\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))|,$$

so regularity says that both inequalities are close to equalities. In other words, our notion of regularity really encompasses two different types of regularity. The first is that the size of the projection π_{l+1} does not change much when we replace $\vec{n}$ with $\vec{n}'$. The second is that the local lattice density does not change much when we shrink the local region from P to Q. Note that in the definition of regularity, we may replace $\vec{n}, \vec{n}'$ with $\vec{n} = (*, \ldots, *, n_l, \ldots, n_k)$ and $\vec{n}' = (*, \ldots, *, n_l + 1, \ldots, n_k)$, where the $*$'s could be any (possibly distinct) natural numbers, since that does not change the relevant projection of the lattice density.

Before proving our main result on regularity, we note some simple consequences of the definition.

Lemma 7.3. *Let M_1, M_2 be positive integers and P be an $(M_1M_2, \delta, n_l, \ldots, n_k)$-regular R-cube. Then the following hold:*

1. *P is $(M_1, \delta, n_l, \ldots, n_k)$-regular.*
2. *For any R/M_1-subcube Q of P, Q is $(M_2, \delta, n_l, \ldots, n_k)$-regular.*

Proof. Let Q be any R/M_1-subcube of P and S be any $R/(M_1M_2)$-subcube of Q. By regularity, we have

$$|\pi_{l+1}(\mathrm{LD}_S(A;\mathcal{F}_{\vec{n}'}))| \geq (1-\delta)|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))|.$$

By Lemma 6.8, we have $|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))| \geq |\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))|$ and $|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}'}))| \geq |\pi_{l+1}(\mathrm{LD}_S(A;\mathcal{F}_{\vec{n}'}))|$. Therefore,

$$|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}'}))| \geq (1-\delta)|\pi_{l+1}(\mathrm{LD}_P(A;\mathcal{F}_{\vec{n}}))|,$$
$$|\pi_{l+1}(\mathrm{LD}_S(A;\mathcal{F}_{\vec{n}'}))| \geq (1-\delta)|\pi_{l+1}(\mathrm{LD}_Q(A;\mathcal{F}_{\vec{n}}))|,$$

which prove the first and second parts of the lemma, respectively. □

We now come to our main result on regularity, which says that, for any dense $A \subseteq [0,N)^d$, one can cut the box $[0,N)^d$ into a bounded number of subcubes, most of which are regular and where the union of the regular subcubes covers most of A. We first prove such a result with respect to a single projection π_{l+1}, before iterating to establish regularity with respect to all projections.

Lemma 7.4. *Fix $\varepsilon, \delta > 0$ and $l \in [k]$, a positive integer M and non-negative integers $n_{l+1}, \ldots, n_k$. Then there exists $R_0 = R_0(M, \varepsilon, \delta)$ such that if $A \subseteq [0,N)^d$ is of size at least εN^d and $N' \mid N$, there exists a natural number $r \leq R_0$ and a collection $\mathcal{P}$ of disjoint N'/M^r-cubes such that, for $A' = A \cap \bigcup_{P\in\mathcal{P}} P$,*

1. *$|A'| \geq (1-\delta)|A|$,*

2. P is $(M, \delta, r, n_{l+1}, \ldots, n_k)$-regular for all $P \in \mathcal{P}$.

Proof. Let $\mathcal{P}^{(r)}$ be the collection of N'/M^r-cubes in $[0, N)^d$, $\mathcal{P}_0^{(r)}$ be the subcollection of all $(M, \delta, r, n_{l+1}, \ldots, n_k)$-regular cubes in $\mathcal{P}^{(r)}$ and $A^{(r)} = A \cap \bigcup_{P \in \mathcal{P}_0^{(r)}} P$. We will set $A' = A^{(r)}$ and $\mathcal{P} = \mathcal{P}_0^{(r)}$, so we wish to show that there is some bounded r such that $|A^{(r)}| \geq (1 - \delta)|A|$.

Let $\mathcal{P}_1^{(r)}$ be the collection of all cubes in $\mathcal{P}^{(r)}$ which are not $(M, \delta, r, n_{l+1}, \ldots, n_k)$-regular. Writing $\vec{n}^{(r)} = (0, \ldots, 0, r, n_{l+1}, \ldots, n_k)$, consider the quantity

$$D_r := \frac{(N'/N)^d}{M^{rd}} \sum_{P \in \mathcal{P}^{(r)}} |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))| \leq \frac{(N'/N)^d}{M^{rd}} |\mathcal{P}^{(r)}| = 1.$$

For any $P \in \mathcal{P}^{(r)}$ and subcube $Q \in \mathcal{P}^{(r+1)}$, we have the inequalities

$$|\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))| \geq |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r+1)}}))| \geq |\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}^{(r+1)}}))|.$$

Therefore, D_r is decreasing in r.

Set $R_0 := \frac{M^d}{\varepsilon \delta^2}$. Since D_r is decreasing and in $[0, 1]$, there is some $r \leq R_0$ such that $D_r \geq D_{r+1} \geq D_r - \frac{\varepsilon \delta^2}{M^d}$. For each $P \in \mathcal{P}_1^{(r)}$, since P is not regular, there is some subcube $Q \in \mathcal{P}^{(r+1)}$ of P such that

$$|\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}^{(r+1)}}))| \leq (1 - \delta)|\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))|.$$

Therefore,

$$\begin{aligned} D_r - D_{r+1} &= \frac{(N'/N)^d}{M^{rd}} \sum_{P \in \mathcal{P}^{(r)}} \left(|\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))| - \frac{1}{M^d} \sum_{\substack{Q \in \mathcal{P}^{(r+1)} \\ Q \subset P}} |\pi_{l+1}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}^{(r+1)}}))| \right) \\ &\geq \frac{(N'/N)^d}{M^{rd}} \sum_{P \in \mathcal{P}_1^{(r)}} \frac{\delta}{M^d} |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))| \\ &= \frac{(N'/N)^d \delta}{M^{(r+1)d}} \sum_{P \in \mathcal{P}_1^{(r)}} |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))|. \end{aligned} \tag{11}$$

By Lemma 6.9, for any $P \in \mathcal{P}_1^{(r)}$, we have

$$\mathrm{Vol}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}})) = \frac{|A \cap P|}{|\mathbb{Z}^d \cap P|} = \frac{M^{rd}}{N'^d} |A \cap P|.$$

Therefore,

$$\begin{aligned} |A \setminus A^{(r)}| &= \sum_{P \in \mathcal{P}_1^{(r)}} |A \cap P| = \frac{N'^d}{M^{rd}} \sum_{P \in \mathcal{P}_1^{(r)}} \mathrm{Vol}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}})) \\ &\leq \frac{N'^d}{M^{rd}} \sum_{P \in \mathcal{P}_1^{(r)}} |\pi_{l+1}(\mathrm{LD}_P(A; \mathcal{F}_{\vec{n}^{(r)}}))|. \end{aligned} \tag{12}$$

Combining (11) and (12), we have

$$|A \setminus A^{(r)}| \leq \frac{N^d M^d}{\delta}(D_r - D_{r+1}) \leq \varepsilon\delta N^d \leq \delta|A|,$$

as required. □

Lemma 7.5. *Fix $\varepsilon, \delta > 0$ and a positive integer M and suppose that $A \subseteq [0,N)^d$ is of size at least εN^d. Then there exist $n_1, \ldots, n_k$, $r \leq R_1 = R_1(M, \varepsilon, \delta)$ and a collection $\mathcal{P}$ of disjoint N/M^r-cubes such that, for $A' = A \cap \bigcup_{P\in\mathcal{P}} P$,*

1. *$|A'| \geq (1-\delta)|A|$,*
2. *P is $(M, \delta, n_l, \ldots, n_k)$-regular for all $P \in \mathcal{P}$ and $l \in [k]$.*

Proof. Following the notation of Lemma 7.4, set $S_1 = R_0(M, \varepsilon/2, \delta/k)$ and, for $l = 2, \ldots, k$,

$$S_l = R_0(M^{S_1+\cdots+S_{l-1}+1}, \varepsilon/2, \delta/k).$$

We then set $R_1 := S_1 + \cdots + S_k$. We shall apply Lemma 7.4 k times in succession to obtain $n_k, n_{k-1}, \ldots, n_1 \leq R_1$.

First, we obtain $n_k \leq S_k$ and a collection $\mathcal{P}^{(k)}$ of disjoint N/M^{n_k}-cubes such that, for $A^{(k)} = A \cap \bigcup_{P\in\mathcal{P}^{(k)}} P$, we have

1. $|A^{(k)}| \geq \left(1 - \frac{\delta}{k}\right)|A|$,
2. P is $(M^{S_1+\cdots+S_{k-1}+1}, \delta, n_k)$-regular for all $P \in \mathcal{P}^{(k)}$.

Suppose we have constructed $n_k, n_{k-1}, \ldots, n_{l+1}$ for some $l \geq 1$. Then, using Lemma 7.4, we obtain $n_l \leq S_l$ and a collection $\mathcal{P}^{(l)}$ of disjoint $N/M^{n_k+\cdots+n_l}$-cubes such that, for $A^{(l)} = A^{(l+1)} \cap \bigcup_{P\in\mathcal{P}^{(l)}} P$, we have

1. $|A^{(l)}| \geq \left(1 - \frac{\delta}{k}\right)|A^{(l+1)}|$,
2. P is $(M^{S_1+\cdots+S_{l-1}+1}, \delta, n_l, \ldots, n_k)$-regular for all $P \in \mathcal{P}^{(l)}$.

We may also assume that the collection $\mathcal{P}^{(l)}$ is a subset of a refinement of $\mathcal{P}^{(l+1)}$.

Finally, set $\mathcal{P} = \mathcal{P}^{(1)}$, a collection of N/M^r-cubes, where $r = n_1 + \cdots + n_k \leq R_1$. Then, for $A' = A \cap \bigcup_{P\in\mathcal{P}} P$, we have

1. $|A'| \geq \left(1 - \frac{\delta}{k}\right)^k |A| \geq (1-\delta)|A|$,
2. for each $l \in [k]$ and each $P \in \mathcal{P}$, P is a subcube of some $P^{(l)} \in \mathcal{P}^{(l)}$, which is, by construction, $(M^{S_1+\cdots+S_{l-1}+1}, \delta, n_l, \ldots, n_k)$-regular. But then, by Lemma 7.3, P is $(M, \delta, n_l, \ldots, n_k)$-regular. □

8 Proof of the dense case

In this section, we make use of the results of the last two sections to prove Lemma 5.1, which we restate for the reader's convenience. As noted in Section 5, this will complete the proof of our main result. Recall, from Section 2, that we have isomorphisms $\Phi' : \mathfrak{D} \to \mathbb{Z}^d$ and $\Phi : \mathcal{O}_K \to \mathbb{Z}^d$. Multiplication of the elements of $\mathfrak{D}$ by λ_l then corresponds to the map $\mathcal{L}_l : \mathbb{Z}^d \to \mathbb{Z}^d$ given by $\mathcal{L}_l = \Phi \circ \mathcal{M}_l \circ \Phi'^{-1}$. In particular, one may check that $|\det \mathcal{L}_0| = N_{K/\mathbb{Q}}(\mathfrak{D})$.

Lemma 8.1. *For any $\varepsilon > 0$, there exists N_0 such that if $N \geq N_0$ and $A \subset [0, N)^d$ with $|A| \geq \varepsilon N^d$, then*

$$|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| \geq H(\lambda_1, \ldots, \lambda_k)|A| - o_\varepsilon(|A|).$$

Proof. Suppose $A \subseteq [0, N)^d$ with $|A| \geq \varepsilon N^d$. Let $\delta > 0$ be arbitrary, D be a large integer and M be a sufficiently large multiple of D. M will depend on both ε and δ, but not on N, which is assumed to be very large. By Lemma 7.5, there are bounded $n_1, \ldots, n_k, r$ and a collection $\mathcal{P}$ of disjoint N/M^r-cubes such that, for $A' = A \cap \bigcup_{P \in \mathcal{P}} P$, we have

1. $|A'| \geq (1 - \delta)|A|$,
2. P is $(M^2, \delta, n_l, \ldots, n_k)$-regular for all $P \in \mathcal{P}$ and $l \in [k]$.

Let $\mathcal{Q}$ be the collection of N/M^{r+1}-cubes Q such that $Q \subset P$ for some $P \in \mathcal{P}$ and Q is at least at a distance of DN/M^{r+1} away from the boundary of P. In particular, $|\mathcal{Q}| = (M - 2D)^d|\mathcal{P}|$. By Lemma 7.3, each Q is $(M, \delta, n_l, \ldots, n_k)$-regular for all $l \in [k]$. Set $A'' = A \cap \bigcup_{Q \in \mathcal{Q}} Q$. Then $A' \setminus A''$ consists of points covered by $\mathcal{P}$ but not $\mathcal{Q}$, so

$$\begin{aligned} |A' \setminus A''| &\leq \left(1 - \left(\frac{M - 2D}{M}\right)^d\right) N^d \leq \varepsilon^{-1} \left(1 - \left(\frac{M - 2D}{M}\right)^d\right) |A| \\ &\leq \frac{2Dd}{M\varepsilon}|A| \leq \delta|A| \end{aligned}$$

for $M \geq 2Dd/\delta\varepsilon$. It follows that $|A''| \geq (1 - 2\delta)|A|$. Let $\mathcal{Q}_0$ be the collection of all N/M^{r+1}-cubes, including those outside $[0, N)^d$. For $Q \in \mathcal{Q}_0$, denote by Q^+ the slightly expanded cube $Q + [-\frac{DN}{M^{r+2}}, \frac{DN}{M^{r+2}}]^d$. Then, for M sufficiently large ($M \geq 4Dd/\delta$ suffices),

$$\operatorname{Vol}(Q^+) = \left(1 + \frac{2D}{M}\right)^d \operatorname{Vol}(Q) \leq (1 + \delta) \operatorname{Vol}(Q). \tag{13}$$

Let $\mathcal{F}^K_{\vec{n}}, \mathcal{G}^K_{\vec{n}}$ be the families of flags of sublattices of $\mathfrak{D}$ and $\mathcal{O}_K$ defined in Section 7.1. Under the isomorphisms Φ, Φ', these families translate to families $\mathcal{F}_{\vec{n}}, \mathcal{G}_{\vec{n}}$ in $\mathbb{Z}^d$ given by $\mathcal{F}_{\vec{n}} := \Phi'(\mathcal{F}^K_{\vec{n}})$ and $\mathcal{G}_{\vec{n}} := \Phi(\mathcal{G}^K_{\vec{n}})$. By Lemmas 7.1 and 7.2, we have the following two properties:

1. For d-periodic $A \subseteq \mathbb{Z}^d$,
$$\pi_1(\mathrm{LD}(A; \mathcal{F}_{\vec{n}})) = \pi_1(\mathrm{LD}(\mathcal{L}_0 A; \mathcal{G}_{\vec{n}+1})). \tag{14}$$
2. For d-periodic $A \subseteq \mathbb{Z}^d$ and $l \in [k]$,
$$|\pi_{l+1}(\mathrm{LD}(A; \mathcal{F}_{\vec{n}}))| \leq |\pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A; \mathcal{G}_{\vec{m}}))| \tag{15}$$
if $m_i = n_i + 1$ for $i = l + 1, \ldots, k$ and $m_l = n_l$.

Define the bodies $X, Y \subset \mathbb{R}^{d+k+1} = \mathbb{R}^d \times \mathbb{R}^{k+1}$ by

$$X := \bigcup_{Q \in \mathcal{Q}} (Q \times \mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}})),$$
$$Y := \bigcup_{Q \in \mathcal{Q}_0} (\mathcal{L}_0 Q \times (1+2\delta)\,\mathrm{LD}_{\mathcal{L}_0(Q^+)}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1})).$$

We remark that in order for $\mathrm{LD}_{\mathcal{L}_0(Q^+)}$ to make sense, we require that $\mathcal{L}_0(Q^+)$ be tileable with respect to the sparsest lattice in $\mathcal{G}_{\vec{n}+1}$. But this is possible for N a multiple of a large enough number, since $\vec{n}$ is bounded.

For each $l = 0, \ldots, k$, let $\mathcal{L}'_l : \mathbb{R}^{d+k+1} \to \mathbb{R}^{d+k+1}$ be the linear map given by

$$\mathcal{L}'_l(\vec{x}, y_0, y_1, \ldots, y_k) = (\mathcal{L}_l \vec{x}, 0, \ldots, 0, y_l, 0, \ldots, 0).$$

We make the following claim.

Claim 8.2. $\mathcal{L}'_0 X + \cdots + \mathcal{L}'_k X \subseteq Y$.

Before proving this key claim, we first finish the proof of Lemma 8.1 assuming it. Let $\mathcal{L}^* : \mathbb{R}^{d+k+1} \to \mathbb{R}^{d+k+1}$ be given by $\mathcal{L}^*(x, y) = (\mathcal{L}_0^{-1} x, y)$ for $x \in \mathbb{R}^d$ and $y \in \mathbb{R}^{k+1}$. Note that $\mathcal{L}_0^{-1}\mathcal{L}_l$ is conjugate to $\mathcal{M}_l$, the map corresponding to multiplication by λ_l on K. By Lemma 2.3, the maps $1, \mathcal{L}_0^{-1}\mathcal{L}_1, \ldots, \mathcal{L}_0^{-1}\mathcal{L}_k$ are simultaneously diagonalisable over $\mathbb{C}$, where the diagonal matrix corresponding to $\mathcal{L}_0^{-1}\mathcal{L}_l$ has diagonal entries $(\sigma_1(\lambda_l), \ldots, \sigma_d(\lambda_l))$. Therefore, the $\mathcal{L}^*\mathcal{L}'_l$ are simultaneously diagonalisable with corresponding diagonal matrix entries $(1, \ldots, 1, 1, 0, \ldots, 0)$ for $l = 0$ and $(\sigma_1(\lambda_l), \ldots, \sigma_d(\lambda_l), 0, \ldots, 0, 1, 0, \ldots, 0)$ otherwise. Thus, by Theorem 3.1, we have

$$\mu(\mathcal{L}^*\mathcal{L}'_0 X + \cdots + \mathcal{L}^*\mathcal{L}'_k X) \geq \prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + |\sigma_i(\lambda_2)| + \cdots + |\sigma_i(\lambda_k)|)\mu(X).$$

Therefore, using Claim 8.2 and the fact that $|\det \mathcal{L}_0| = N_{K/\mathbb{Q}}(\mathfrak{D})$,

$$\begin{aligned}
\mu(Y) &\geq \mu(\mathcal{L}'_0 X + \cdots + \mathcal{L}'_k X) \\
&= \frac{1}{|\det(\mathcal{L}^*)|}\mu(\mathcal{L}^*\mathcal{L}'_0 X + \cdots + \mathcal{L}^*\mathcal{L}'_k X) \\
&\geq |\det(\mathcal{L}_0)| \prod_{i=1}^{d} (1 + |\sigma_i(\lambda_1)| + |\sigma_i(\lambda_2)| + \cdots + |\sigma_i(\lambda_k)|)\mu(X) \\
&= H(\lambda_1, \ldots, \lambda_k)\mu(X).
\end{aligned}$$

By Lemma 6.9,

$$\begin{aligned}
\mu(X) &= \sum_{Q \in \mathcal{Q}} \mathrm{Vol}(Q) \times \mathrm{Vol}(\mathrm{LD}_Q(A; \mathcal{F}_{\vec{n}})) \\
&= \sum_{Q \in \mathcal{Q}} |A \cap Q| = |A''| \geq (1 - 2\delta)|A|.
\end{aligned}$$

By the definition of C_1 (see Lemma 4.1), since A lies in the cube $(-N, N)^d$, the sum $A + \mathcal{L}_0^{-1}\mathcal{L}_1 A + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k A$ lies in the cube $(-(k+1)C_1 N, (k+1)C_1 N)^d \subset \mathbb{R}^d$. There are at most

$(4(k+1)C_1)^d M^{d(r+1)}$ different $Q \in \mathcal{Q}_0$ such that Q^+ intersects $(-(k+1)C_1N, (k+1)C_1N)^d$. For simplicity, assume that $D > (4(k+1)C_1)^d$, so that there are at most $DM^{d(r+1)}$ such Q. Thus, there are at most $DM^{d(r+1)}$ different $Q \in \mathcal{Q}_0$ such that $\mathcal{L}_0(Q^+) \cap (\mathcal{L}_0 A + \cdots + \mathcal{L}_k A) \neq \emptyset$. For each such Q, we have

$$\begin{aligned}|\mathcal{L}_0(Q^+) \cap (\mathcal{L}_0 A + \cdots + \mathcal{L}_k A)| - |\mathcal{L}_0 Q \cap (\mathcal{L}_0 A + \cdots + \mathcal{L}_k A)| &\leq \det(\mathcal{L}_0)(\mathrm{Vol}(Q^+) - \mathrm{Vol}(Q)) \\ &= O\left(\frac{DN^d}{M^{(r+1)d+1}}\right) \\ &\leq \delta(N/M^{r+1})^d.\end{aligned}$$

Therefore, again using Lemma 6.9,

$$\begin{aligned}\mu(Y) &= \sum_{Q \in \mathcal{Q}_0} \mathrm{Vol}(\mathcal{L}_0 Q) \times (1+2\delta)^{k+1} \mathrm{Vol}(\mathrm{LD}_{\mathcal{L}_0(Q^+)}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1})) \\ &= (1+2\delta)^{k+1} \sum_{Q \in \mathcal{Q}_0} \frac{\mathrm{Vol}(\mathcal{L}_0 Q)}{\mathrm{Vol}(\mathcal{L}_0(Q^+))} |\mathcal{L}_0(Q^+) \cap (\mathcal{L}_0 A + \cdots + \mathcal{L}_k A)| \\ &\leq (1+2\delta)^{k+1} \sum_{Q \in \mathcal{Q}_0} |\mathcal{L}_0(Q^+) \cap (\mathcal{L}_0 A + \cdots + \mathcal{L}_k A)| \\ &\leq (1+2\delta)^{k+1} \left(\sum_{Q \in \mathcal{Q}_0} |\mathcal{L}_0 Q \cap (\mathcal{L}_0 A + \cdots + \mathcal{L}_k A)| + DM^{d(r+1)} \cdot \delta(N/M^{r+1})^d \right) \\ &= (1+2\delta)^{k+1} (|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| + D\delta N^d).\end{aligned}$$

Thus, we have

$$\begin{aligned}|\mathcal{L}_0 A + \cdots + \mathcal{L}_k A| &\geq (1+2\delta)^{-(k+1)} \mu(Y) - O_D(\delta) N^d \\ &= (1 - O(\delta)) \mu(Y) - O_D(\delta) N^d \\ &\geq (1 - O(\delta)) H(\lambda_1, \ldots, \lambda_k) \mu(X) - O_D(\delta) N^d \\ &\geq (1 - O(\delta)) H(\lambda_1, \ldots, \lambda_k)(1-2\delta)|A| - O_D(\delta) N^d \\ &= H(\lambda_1, \ldots, \lambda_k)|A| - O_D(\delta) N^d.\end{aligned}$$

Since δ was arbitrary, this proves the lemma. □

In order to complete the proof, we now return to Claim 8.2.

Proof of Claim 8.2. Let $(x_l, y_l) \in X$ for $l = 0, \ldots, k$ with $Q_l \in \mathcal{Q}$ the cube containing x_l and $y_l \in \mathrm{LD}_{Q_l}(A; \mathcal{F}_{\vec{n}})$. Our aim is to show that $(\sum_l \mathcal{L}_l x_l, y) \in Y$, where $y = (\pi_1(y_0), \ldots, \pi_{k+1}(y_k))$.

Let $Q^* \in \mathcal{Q}_0$ be the cube containing $x := x_0 + \mathcal{L}_0^{-1}\mathcal{L}_1 x_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k x_k$. Then $\mathcal{L}_0 x_0 + \cdots + \mathcal{L}_k x_k = \mathcal{L}_0 x \in \mathcal{L}_0 Q^*$, so it suffices to show that $y \in (1+2\delta)\,\mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1})$.

Suppose $Q^* = Q_0 + t$ for some translate $t \in \frac{N}{M^{r+1}}\mathbb{Z}^d$. Then $t = \mathcal{L}_0^{-1}\mathcal{L}_1 x_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k x_k + t_0$ for some $t_0 \in (-\frac{N}{M^{r+1}}, \frac{N}{M^{r+1}})^d$. Let $x_k^* = x_k + \mathcal{L}_k^{-1}\mathcal{L}_0 t_0$, so that

$$x_k^* - x_k = \mathcal{L}_k^{-1}\mathcal{L}_0 t_0 \in \left[-\frac{C_1 N}{M^{r+1}}, \frac{C_1 N}{M^{r+1}}\right]^d \subseteq \left[-\frac{DN}{M^{r+1}}, \frac{DN}{M^{r+1}}\right]^d.$$

Therefore, if $P_k \in \mathcal{P}$ is the cube containing Q_k and $Q_k^* \in \mathcal{Q}_0$ is the cube containing x_k^*, we must have $Q_k^* \subset P_k$, since $Q_k \in \mathcal{Q}$ is at least a distance DN/M^{r+1} away from the boundary of P_k.

Let R_l be the N/M^{r+2}-cube containing x_l for each $l = 1, \ldots, k-1$ and R_k^* the N/M^{r+2}-cube containing x_k^*, so that $R_k^* \subset P_k$. Define the following sets:

- $A_0 = A \cap Q_0$,
- $A_l = A \cap R_l$ for $l = 1, \ldots, k-1$,
- $A_k = A \cap R_k^*$.

We have $x_l \in A_l$ for $l = 0, \ldots, k-1$, $x_k^* \in A_k$ and $t = \mathcal{L}_0^{-1}\mathcal{L}_1 x_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k x_k^*$. Since A_l is contained in an N/M^{r+2}-cube for $l = 1, \ldots, k$, $\mathcal{L}_0^{-1}\mathcal{L}_1 A_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k A_k$ is contained in a cube of side length DN/M^{r+2} if D is sufficiently large. Since $t \in \mathcal{L}_0^{-1}\mathcal{L}_1 A_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k A_k$ and $A_0 \subseteq Q_0$, we have $A_0 + \mathcal{L}_0^{-1}\mathcal{L}_1 A_1 + \cdots + \mathcal{L}_0^{-1}\mathcal{L}_k A_k \subseteq Q_0^+ + t = Q^{*+}$.

Suppose L is a lattice such that Q^+ is tiled by L for every $Q \in \mathcal{Q}_0$, such as $L = ((N/M^{r+1} + 2DN/M^{r+2})\mathbb{Z})^d$. Then $\mathcal{L}_0(Q^+)$ is tiled by $\mathcal{L}_0 L$. By repeatedly applying Theorem 6.5, we have that

$$\begin{aligned}\prod_{l=0}^{k} \pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A_l + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1})) &\subseteq \mathrm{LD}(\mathcal{L}_0 A_0 + \cdots + \mathcal{L}_k A_k + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1}) \\ &= \mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A_0 + \cdots + \mathcal{L}_k A_k; \mathcal{G}_{\vec{n}+1}).\end{aligned}$$

We will now show that $|\pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A_l + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1}))| \geq (1-\delta)\pi_{l+1}(y_l)$ for all l, looking at each of the three cases $l = 0$, $1 \leq l \leq k-1$ and $l = k$ separately. For $l = 0$, we have

$$\begin{aligned}|\pi_1(\mathrm{LD}(\mathcal{L}_0 A_0 + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1}))| &= |\pi_1(\mathrm{LD}(A_0 + L; \mathcal{F}_{\vec{n}}))| && \text{by (14)} \\ &= |\pi_1(\mathrm{LD}_{Q_0^+}(A_0; \mathcal{F}_{\vec{n}}))| \\ &= \frac{\mathrm{Vol}(Q_0)}{\mathrm{Vol}(Q_0^+)} |\pi_1(\mathrm{LD}_{Q_0}(A_0; \mathcal{F}_{\vec{n}}))| && \text{by Lemma 6.7} \\ &\geq (1-\delta)|\pi_1(\mathrm{LD}_{Q_0}(A; \mathcal{F}_{\vec{n}}))| && \text{by (13)} \\ &\geq (1-\delta)\pi_1(y_0).\end{aligned}$$

For $l = 1, \ldots, k-1$, since Q_l is $(M, \delta, n_l, \ldots, n_k)$-regular, by (10), we have, for $\vec{n}^{(l)} = (n_1+1, \ldots, n_l+1, n_{l+1}, \ldots, n_k)$, that

$$|\pi_{l+1}(\mathrm{LD}_{R_l}(A; \mathcal{F}_{\vec{n}^{(l)}}))| \geq (1-\delta)|\pi_{l+1}(\mathrm{LD}_{Q_l}(A; \mathcal{F}_{\vec{n}}))|.$$

Note that $\mathcal{L}_l^{-1}\mathcal{L}_0(Q^+)$ is tiled by $\mathcal{L}_l^{-1}\mathcal{L}_0 L$ for any $Q \in \mathcal{Q}_0$. Let S_l be a translate of $\mathcal{L}_l^{-1}\mathcal{L}_0(Q^{*+})$ containing R_l. Such a translate exists for M sufficiently large since R_l is an N/M^{r+2}-cube and Q^* is an N/M^{r+1}-cube. Therefore,

$$\begin{aligned}|\pi_{l+1}(\mathrm{LD}(\mathcal{L}_l A_l + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1}))| &\geq |\pi_{l+1}(\mathrm{LD}(A_l + \mathcal{L}_l^{-1}\mathcal{L}_0 L; \mathcal{F}_{\vec{n}^{(l)}}))| && \text{by (15)} \\ &= |\pi_{l+1}(\mathrm{LD}_{S_l}(A_l; \mathcal{F}_{\vec{n}^{(l)}}))| \\ &= |\pi_{l+1}(\mathrm{LD}_{R_l}(A_l; \mathcal{F}_{\vec{n}^{(l)}}))| && \text{by Lemma 6.7} \\ &= |\pi_{l+1}(\mathrm{LD}_{R_l}(A; \mathcal{F}_{\vec{n}^{(l)}}))| \\ &\geq (1-\delta)|\pi_{l+1}(\mathrm{LD}_{Q_l}(A; \mathcal{F}_{\vec{n}}))| && \text{by regularity} \\ &\geq (1-\delta)\pi_{l+1}(y_l).\end{aligned}$$

Finally, for $l = k$, similarly define S_k to be a translate of $\mathcal{L}_k^{-1}\mathcal{L}_0(Q_k^{*+})$ containing R_k^*. Then, we have

$$\begin{aligned}
|\pi_{k+1}(\mathrm{LD}(\mathcal{L}_k A_k + \mathcal{L}_0 L; \mathcal{G}_{\vec{n}+1}))| &\geq |\pi_{k+1}(\mathrm{LD}(A_k + \mathcal{L}_k^{-1}\mathcal{L}_0 L; \mathcal{F}_{\vec{n}^{(k)}}))| && \text{by (15)} \\
&= |\pi_{k+1}(\mathrm{LD}_{S_k}(A_k; \mathcal{F}_{\vec{n}^{(k)}}))| \\
&= |\pi_{k+1}(\mathrm{LD}_{R_k^*}(A_k; \mathcal{F}_{\vec{n}^{(k)}}))| && \text{by Lemma 6.7} \\
&= |\pi_{k+1}(\mathrm{LD}_{R_k^*}(A; \mathcal{F}_{\vec{n}^{(k)}}))| \\
&\geq (1-\delta)|\pi_{k+1}(\mathrm{LD}_{P_k}(A; \mathcal{F}_{\vec{n}}))| && \text{by regularity of } P_k \\
&\geq (1-\delta)|\pi_{k+1}(\mathrm{LD}_{Q_k}(A; \mathcal{F}_{\vec{n}}))| && \text{by Lemma 6.8} \\
&\geq (1-\delta)\pi_{k+1}(y_k).
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
(1-\delta)y &= ((1-\delta)\pi_1(y_0), \ldots, (1-\delta)\pi_{k+1}(y_k)) \\
&\in \mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A_0 + \cdots + \mathcal{L}_k A_k; \mathcal{G}_{\vec{n}+1}) \\
&\subseteq \mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1}),
\end{aligned}$$

which implies that $y \in (1+2\delta)\,\mathrm{LD}_{\mathcal{L}_0(Q^{*+})}(\mathcal{L}_0 A + \cdots + \mathcal{L}_k A; \mathcal{G}_{\vec{n}+1})$, as required. □

9 Sums of linear transformations

In this section, we prove Theorem 1.7, our main result about sums of pre-commuting linear transformations. As mentioned in the introduction, the idea of the proof is to show that the general case reduces to the seemingly special case of sums of algebraic dilates.

9.1 Algebraic number theory preliminaries

Recall that, for $\alpha_1, \ldots, \alpha_k \in K$, the denominator ideal $\mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K}$ is given by

$$\mathfrak{D}_{\alpha_1,\ldots,\alpha_k;K} := \{x \in \mathcal{O}_K \mid x\alpha_i \in \mathcal{O}_K \text{ for all } i = 1, \ldots, k\}.$$

Abbreviating this again as $\mathfrak{D}$, the ideal norm $N_{K/\mathbb{Q}}(\mathfrak{D})$ is the index $[\mathcal{O}_K : \mathfrak{D}]$. The main result of this short subsection gives an alternative way to compute the norm of the denominator ideal. In the statement, we also use the notation $N_{K/\mathbb{Q}}(\alpha)$, but this now refers to the field norm of an element α of K, which is the product of the conjugates of α.

Theorem 9.1. *Let $\alpha_1, \ldots, \alpha_k \in K$ and consider the polynomial*

$$F(x_0, \ldots, x_k) := N_{K/\mathbb{Q}}(x_0 + x_1\alpha_1 + \cdots + x_k\alpha_k) \in \mathbb{Q}[x_0, x_1, \ldots, x_k].$$

If $D > 0$ is the smallest positive integer such that DF has integer coefficients, then $D = N_{K/\mathbb{Q}}(\mathfrak{D})$.

To prove this, we require a variant of Gauss's lemma over the ring of integers $\mathcal{O}_K$. We first need a definition.

Definition 9.2. Let $F(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$. Define the *content* of F, denoted by $\mathrm{cont}_K(F)$, to be the fractional ideal $a_0\mathcal{O}_K + a_1\mathcal{O}_K + \cdots + a_n\mathcal{O}_K \subseteq K$. If it is clear from context, we omit the subscript and simply write $\mathrm{cont}(F)$.

If $F \in \mathbb{Z}[x]$, then $\mathrm{cont}_{\mathbb{Q}}(F) = c\mathbb{Z}$, where $c \in \mathbb{Z}$ is the content of F as used in the usual Gauss's lemma, that is, the greatest common divisor of the coefficients of F. If L is a field extension of K and $F \in K[x]$, then $\mathrm{cont}_L(F) = \mathrm{cont}_K(F) \cdot \mathcal{O}_L$. In particular, if $F \in \mathbb{Q}[x]$, then $\mathrm{cont}_K(F) = \mathrm{cont}_{\mathbb{Q}}(F) \cdot \mathcal{O}_K$. Our variant of Gauss's lemma over $\mathcal{O}_K$ is now as follows.

Lemma 9.3 (Gauss's lemma over $\mathcal{O}_K$)**.** *For any two polynomials $F, G \in K[x]$, $\mathrm{cont}(FG) = \mathrm{cont}(F)\,\mathrm{cont}(G)$.*

Remark. *This result also follows from the Dedekind–Mertens lemma, which says that for any ring R and polynomials $F, G \in R[x]$ there exists a positive integer n such that $\mathrm{cont}(F)^n\,\mathrm{cont}(FG) = \mathrm{cont}(F)^{n+1}\,\mathrm{cont}(G)$. Our lemma then follows, since every non-zero fractional ideal in $\mathcal{O}_K$ is invertible. We give a direct proof here for completeness.*

Proof of Lemma 9.3. Let $F(x) = a_0 + a_1x + \cdots + a_nx^n$ and $G(x) = b_0 + b_1x + \cdots + b_mx^m$. Then their product $F(x)G(x) = c_0 + c_1x + \cdots + c_{n+m}x^{n+m}$ has coefficients $c_j = a_0b_j + a_1b_{j-1} + \cdots + a_jb_0$. It is clear that $\mathrm{cont}(FG) \subseteq \mathrm{cont}(F)\,\mathrm{cont}(G)$. To show that $\mathrm{cont}(FG) \supseteq \mathrm{cont}(F)\,\mathrm{cont}(G)$, it suffices to show that, for any prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, $\nu_{\mathfrak{p}}(\mathrm{cont}(FG)) \leq \nu_{\mathfrak{p}}(\mathrm{cont}(F)) + \nu_{\mathfrak{p}}(\mathrm{cont}(G))$.

Suppose $\nu_{\mathfrak{p}}(\mathrm{cont}(F)) = s$ and $\nu_{\mathfrak{p}}(\mathrm{cont}(G)) = t$. Since $\nu_{\mathfrak{p}}(\mathrm{cont}(F)) = \min(\nu_{\mathfrak{p}}(a_0), \ldots, \nu_{\mathfrak{p}}(a_n))$, there exists an index k such that $\nu_{\mathfrak{p}}(a_k) = s$. Let k be the smallest such index, so that $\nu_{\mathfrak{p}}(a_j) \geq s+1$ for $j = 0, \ldots, k-1$. Similarly, let l be the smallest index such that $\nu_{\mathfrak{p}}(b_l) = t$, so that $\nu_{\mathfrak{p}}(b_j) \geq t+1$ for $j = 0, \ldots, l-1$.

Consider the coefficient $c_{k+l} = \sum_{j=0}^{k+l} a_jb_{k+l-j}$. For $j = k$, the term a_kb_l satisfies $\nu_{\mathfrak{p}}(a_kb_l) = \nu_{\mathfrak{p}}(a_k) + \nu_{\mathfrak{p}}(b_l) = s + t$. For every other $j \neq k$, either $j < k$ (for which $\nu_{\mathfrak{p}}(a_j) \geq s+1$) or $j > k$ (for which $\nu_{\mathfrak{p}}(b_{k+l-j}) \geq t+1$). In either case, we have $\nu_{\mathfrak{p}}(a_jb_{k+l-j}) \geq s + t + 1$. Therefore, $\nu_{\mathfrak{p}}(c_{k+l}) = s + t$, so we have $\nu_{\mathfrak{p}}(\mathrm{cont}(FG)) \leq s + t$, as required. □

Observe that we may similarly define content for multivariate polynomials $F \in K[x_0, \ldots, x_k]$ and our variant of Gauss's lemma then also holds for multivariate polynomials. Indeed, the set of coefficients for $F(x_0, \ldots, x_k)$ is the same as for $F(x, x^{N_1}, \ldots, x^{N_k})$ for sufficiently large $N_k \gg N_{k-1} \gg \cdots \gg N_1 \gg 1$. Thus, the content of F is the same as the content of $F(x, x^{N_1}, \ldots, x^{N_k})$, so we may apply the univariate case.

Proof of Theorem 9.1. Let $\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$ be the complex embeddings of K, with σ_1 being the identity. Then

$$F(x_0, \ldots, x_k) = N_{K/\mathbb{Q}}(x_0 + x_1\alpha_1 + \cdots + x_k\alpha_k) = \prod_{i=1}^{d}(x_0 + x_1\sigma_i(\alpha_1) + \cdots + x_k\sigma_i(\alpha_k)).$$

Let $K' \subseteq \mathbb{C}$ be the smallest field containing $\sigma_1(K), \ldots, \sigma_d(K)$, that is, K' is the normal closure of K over $\mathbb{Q}$. By definition, $D^{-1}\mathbb{Z} = \mathrm{cont}_{\mathbb{Q}}(F)$, so we have $\mathrm{cont}_{K'}(F) = D^{-1}\mathcal{O}_{K'}$. On the other hand, by Lemma 9.3,

$$\mathrm{cont}_{K'}(F) = \prod_i \mathrm{cont}_{K'}(x_0 + x_1\sigma_i(\alpha_1) + \cdots + x_k\sigma_i(\alpha_k)).$$

For any subset $S \subset K'$, denote by $S\mathcal{O}_{K'}$ the $\mathcal{O}_{K'}$-fractional ideal generated by S, i.e., the set of elements of the form $s_1a_1 + \cdots + s_na_n$ for some non-negative integer n, $s_i \in S$ and $a_i \in \mathcal{O}_{K'}$. Then

$$\begin{aligned}\mathrm{cont}_{K'}(x_0 + x_1\sigma_i(\alpha_1) + \cdots + x_k\sigma_i(\alpha_k)) &= \mathcal{O}_{K'} + \sigma_i(\alpha_1)\mathcal{O}_{K'} + \cdots + \sigma_i(\alpha_k)\mathcal{O}_{K'} \\ &= \sigma_i(\mathcal{O}_{K'} + \alpha_1\mathcal{O}_{K'} + \cdots + \alpha_k\mathcal{O}_{K'}) \\ &= \sigma_i(\mathfrak{D}^{-1}\mathcal{O}_{K'}) = \sigma_i(\mathfrak{D}^{-1})\mathcal{O}_{K'}.\end{aligned}$$

Multiplying over all i, we get $\mathrm{cont}_{K'}(F) = \prod_i \sigma_i(\mathfrak{D}^{-1})\mathcal{O}_{K'} = N_{K/\mathbb{Q}}(\mathfrak{D}^{-1})\mathcal{O}_{K'}$, where the last equality follows from the fact that, for any $\mathcal{O}_K$-fractional ideal $\mathfrak{a}$, we have $\prod_i \sigma_i(\mathfrak{a})\mathcal{O}_{K'} = N_{K/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_{K'}$. Indeed, this holds when $\mathfrak{a} = \alpha\mathcal{O}_K$ is principal (since $N_{K/\mathbb{Q}}(\alpha) = \prod_i \sigma_i(\alpha)$ and $N_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = N_{K/\mathbb{Q}}(\alpha)\mathcal{O}_K$), so the general case follows since $\mathfrak{a}^m$ is always principal for some $m \geq 0$. Therefore, we have $D^{-1}\mathcal{O}_{K'} = N_{K/\mathbb{Q}}(\mathfrak{D}^{-1})\mathcal{O}_{K'}$, so $D = N_{K/\mathbb{Q}}(\mathfrak{D})$, as required. □

9.2 Pre-commuting matrices

In this subsection, we prove the following result, which allows us to regard sums of pre-commuting linear transformations as sums of algebraic dilates.

Theorem 9.4. *Suppose $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are non-zero, pre-commuting, irreducible and coprime. Then they are invertible over $\mathbb{Q}$ and there exist a number field K with $\deg(K/\mathbb{Q}) = d$, $\lambda_1, \ldots, \lambda_k \in K$ and a $\mathbb{Q}$-isomorphism $\Phi : K \to \mathbb{Q}^d$ such that $|\det(\mathcal{L}_0)| = N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K})$ and, for all $u \in \mathbb{Q}^d$ and $l = 1, \ldots, k$,*

$$\mathcal{L}_0^{-1}\mathcal{L}_l(u) = \Phi(\lambda_l \cdot \Phi^{-1}(u)).$$

Before proving this theorem, we prove a structure theorem for pairwise commuting matrices with no non-trivial common invariant subspace. A folklore result (e.g., [9, Corollary 2.4.6.4]) says that pairwise commuting maps are simultaneously upper-triangularisable over $\mathbb{C}$ and so have a common eigenvector.

Lemma 9.5. *If $\mathcal{L}_1, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{C})$ are pairwise commuting matrices, then they have a common eigenvector $v \in \mathbb{C}^d$.*

Suppose $\lambda_1, \ldots, \lambda_k$ generate the field K and multiplication by these elements correspond to the matrices $\mathcal{M}_1, \ldots, \mathcal{M}_k \in \mathrm{Mat}_d(\mathbb{Q})$, as spelled out in Section 2. Then $\mathcal{M}_1, \ldots, \mathcal{M}_k$ are pairwise commuting and have no non-trivial common invariant subspace over $\mathbb{Q}$. Conversely, we now show that any such tuple of matrices $\mathcal{M}_1, \ldots, \mathcal{M}_k$ arise from some $\lambda_1, \ldots, \lambda_k$ in some field K.

Lemma 9.6. *Suppose $\mathcal{M}_1, \ldots, \mathcal{M}_k \in \mathrm{Mat}_d(\mathbb{Q})$ are pairwise commuting and have no non-trivial common invariant subspace over $\mathbb{Q}$. Then there is a number field K of degree d, algebraic numbers $\lambda_1, \ldots, \lambda_k \in K$ and a $\mathbb{Q}$-isomorphism $\Phi : K \to \mathbb{Q}^d$ such that*

1. *$K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$,*
2. *for $l = 1, \ldots, k$, the map $\Phi^{-1}\mathcal{M}_l\Phi : K \to K$ is given by multiplication by λ_l.*

Proof. By Lemma 9.5, there is a common eigenvector $v \in \mathbb{C}^d$ for $\mathcal{M}_1, \ldots, \mathcal{M}_k$ with eigenvalues $\lambda_1, \ldots, \lambda_k$. Let $K = \mathbb{Q}(\lambda_1, \ldots, \lambda_k)$. Then we may assume without loss of generality that $v \in K^d$. Let $d' = \deg(K/\mathbb{Q})$ and $\sigma_1, \ldots, \sigma_{d'} : K \to \mathbb{C}$ be the complex embeddings. Then $\sigma_i(v)$ is also a common eigenvector for $\mathcal{M}_1, \ldots, \mathcal{M}_k$ with eigenvalues $\sigma_i(\lambda_1), \ldots, \sigma_i(\lambda_k)$. Since the tuples $(\sigma_i(\lambda_1), \ldots, \sigma_i(\lambda_k))$ are distinct for $i = 1, \ldots, d'$ (as each tuple uniquely determines the map $\sigma_i : K \to K$), the common eigenvectors $\sigma_1(v), \ldots, \sigma_{d'}(v) \in \mathbb{C}^d$ are linearly independent, implying that $d' \leq d$.

Note that $U = \langle \sigma_1(v), \ldots, \sigma_{d'}(v) \rangle \cap \mathbb{Q}^d$ is a common invariant subspace. We will show that this subspace has dimension d'. Clearly it has dimension at most d'. Let $\lambda \in K$ be a generator, so that $1, \lambda, \ldots, \lambda^{d'-1}$ is a $\mathbb{Q}$-basis for K. For $i = 0, \ldots, d' - 1$, let $u_i = \sigma_1(\lambda^i v) + \cdots + \sigma_{d'}(\lambda^i v) =$

$\mathrm{Tr}_{K/\mathbb{Q}}(\lambda^i v) \in \mathbb{Q}^d$, so that $u_i \in U$. We claim that $u_0, \ldots, u_{d'-1}$ are linearly independent. Indeed, since $u_i = \sigma_1(\lambda)^i \sigma_1(v) + \cdots + \sigma_{d'}(\lambda)^i \sigma_{d'}(v)$ and $\sigma_1(v), \ldots, \sigma_{d'}(v)$ are linearly independent, it suffices to show that the $d' \times d'$ matrix

$$\begin{pmatrix} 1 & \sigma_1(\lambda) & \cdots & \sigma_1(\lambda)^{d'-1} \\ 1 & \sigma_2(\lambda) & \cdots & \sigma_2(\lambda)^{d'-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \sigma_{d'}(\lambda) & \cdots & \sigma_{d'}(\lambda)^{d'-1} \end{pmatrix}$$

is non-singular. But this is true since it is a Vandermonde matrix and $\sigma_1(\lambda), \ldots, \sigma_{d'}(\lambda)$ are distinct, which in turn follows from the fact that λ generates K.

Since $\mathcal{M}_1, \ldots, \mathcal{M}_k$ have no non-trivial common invariant subspace, we must have $d' = d$. We deduce that $\mathcal{M}_1, \ldots, \mathcal{M}_k$ are simultaneously diagonalisable with eigenvalue tuples $(\sigma_i(\lambda_1), \ldots, \sigma_i(\lambda_k))$ for $i = 1, \ldots, d$. Define the linear map $\Phi : K \to \mathbb{Q}^d$ as follows. First, let $e_1 \in \mathbb{Q}^d$ be any non-zero vector and set $\Phi(1) = e_1$. Then, for any $\alpha \in K$, express α as a polynomial $P(\lambda_1, \ldots, \lambda_k)$ with rational coefficients in $\lambda_1, \ldots, \lambda_k$. Such a polynomial exists since $\lambda_1, \ldots, \lambda_k$ generate K, though it is not unique. Set $\Phi(\alpha) = P(\mathcal{M}_1, \ldots, \mathcal{M}_k)e_1$. Observe that this is independent of the choice of P. Indeed, it suffices to show that if P is a polynomial with rational coefficients such that $P(\lambda_1, \ldots, \lambda_k) = 0$, then $P(\mathcal{M}_1, \ldots, \mathcal{M}_k) = 0$. The matrix $P(\mathcal{M}_1, \ldots, \mathcal{M}_k)$ is diagonalisable with eigenvalues $P(\sigma_i(\lambda_1), \ldots, \sigma_i(\lambda_k))$ for $i = 1, \ldots, d$. Since P has rational coefficients, we have $P(\sigma_i(\lambda_1), \ldots, \sigma_i(\lambda_k)) = \sigma_i(P(\lambda_1, \ldots, \lambda_k)) = 0$ for all i and thus $P(\mathcal{M}_1, \ldots, \mathcal{M}_k) = 0$.

Notice that if $P(\lambda_1, \ldots, \lambda_k) = \alpha \neq 0$, then $P(\mathcal{M}_1, \ldots, \mathcal{M}_k)$ is diagonalisable with eigenvalues $\sigma_1(\alpha), \ldots, \sigma_k(\alpha)$. Thus, $P(\mathcal{M}_1, \ldots, \mathcal{M}_k)$ is non-singular and so $\Phi(\alpha) \neq 0$. It follows that Φ is injective and hence an isomorphism. Since Φ also satisfies condition 2, the result follows. □

We now return to Theorem 9.4.

Proof of Theorem 9.4. Let $\mathcal{P} \in \mathrm{GL}_d(\mathbb{Q})$ be such that $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ are pairwise commuting. Since $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are irreducible, $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$ have no non-trivial common invariant subspace. Let $K, \lambda_0, \ldots, \lambda_k, \Phi$ be as in the conclusion of Lemma 9.6 when applied to $\mathcal{P}\mathcal{L}_0, \ldots, \mathcal{P}\mathcal{L}_k$.

Since all of $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are non-zero, all of $\lambda_0, \ldots, \lambda_k$ are also non-zero. In particular, $\mathcal{L}_0, \ldots, \mathcal{L}_k$ are invertible over $\mathbb{Q}$. Since $I, (\mathcal{P}\mathcal{L}_0)^{-1}\mathcal{P}\mathcal{L}_1, \ldots, (\mathcal{P}\mathcal{L}_0)^{-1}\mathcal{P}\mathcal{L}_k$ are also pairwise commuting, we may assume without loss of generality that $\mathcal{P} = \mathcal{L}_0^{-1}$, so we have $\lambda_0 = 1$. From Lemma 9.6, we have that, for all $u \in \mathbb{Q}^d$ and $l = 1, \ldots, k$,

$$\mathcal{L}_0^{-1}\mathcal{L}_l(u) = \Phi(\lambda_l \cdot \Phi^{-1}(u)).$$

It remains to show that $|\det(\mathcal{L}_0)| = N_{K/\mathbb{Q}}(\mathfrak{D})$, where $\mathfrak{D} = \mathfrak{D}_{\lambda_1,\ldots,\lambda_k;K}$. Consider the integer polynomial

$$\begin{aligned} G(x_0, \ldots, x_k) &= \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k) \\ &= \det(\mathcal{L}_0)\det(x_0 + x_1\mathcal{L}_0^{-1}\mathcal{L}_1 + \cdots + x_k\mathcal{L}_0^{-1}\mathcal{L}_k) \\ &= \det(\mathcal{L}_0)N_{K/\mathbb{Q}}(x_0 + x_1\lambda_1 + \cdots + x_k\lambda_k). \end{aligned}$$

By Theorem 9.1, $N_{K/\mathbb{Q}}(\mathfrak{D})$ is the smallest positive integer required to scale $N_{K/\mathbb{Q}}(x_0 + x_1\lambda_1 + \cdots + x_k\lambda_k)$ into an integer polynomial. Thus, $N_{K/\mathbb{Q}}(\mathfrak{D})$ divides $\det(\mathcal{L}_0)$, so that $|\det(\mathcal{L}_0)| \geq N_{K/\mathbb{Q}}(\mathfrak{D})$.

Let $\Phi_1 : \mathcal{O}_K \to \mathbb{Z}^d$ and $\Phi_2 : \mathfrak{D} \to \mathbb{Z}^d$ be linear isomorphisms of lattices, so that $\Phi_1 \circ \Phi_2^{-1} : \mathbb{Z}^d \to \mathbb{Z}^d$ is a $d \times d$ integer matrix with absolute determinant $N_{K/\mathbb{Q}}(\mathfrak{D})$. Since $\lambda_l \cdot \mathfrak{D} \subseteq \mathcal{O}_K$, we have $\Phi_1(\lambda_l \cdot \Phi_2^{-1}(u)) \in \mathbb{Z}^d$ for any $u \in \mathbb{Z}^d$. Thus, the linear map $u \mapsto \Phi_1(\lambda_l \cdot \Phi_2^{-1}(u))$ is represented by an integer matrix. But this map is also equal to the composition $(\Phi_1 \circ \Phi^{-1})(\mathcal{L}_0^{-1}\mathcal{L}_l)(\Phi \circ \Phi_2^{-1})$. Since $\mathcal{L}_0, \dots, \mathcal{L}_k$ are coprime, we have $|\det((\Phi_1 \circ \Phi^{-1})(\mathcal{L}_0^{-1})(\Phi \circ \Phi_2^{-1}))| \geq 1$, which implies that $N_{K/\mathbb{Q}}(\mathfrak{D}) = |\det(\Phi_1 \circ \Phi_2^{-1})| \geq |\det(\mathcal{L}_0)|$. Therefore, $|\det(\mathcal{L}_0)| = N_{K/\mathbb{Q}}(\mathfrak{D})$, as required. □

9.3 Sums of pre-commuting linear transformations

We are now ready to prove Theorem 1.7, our main result about sums of linear transformations, which we restate for convenience. Recall that if $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are non-zero, pre-commuting, irreducible and coprime and the polynomial $G(x_0, \dots, x_k) = \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k)$ factorises as

$$G(x_0, \dots, x_k) = \prod_{i=1}^{d}(a_{0i}x_0 + \cdots + a_{ki}x_k),$$

then $H(\mathcal{L}_0, \dots, \mathcal{L}_k)$ is defined by

$$H(\mathcal{L}_0, \dots, \mathcal{L}_k) = \prod_{i=1}^{d}(|a_{0i}| + \cdots + |a_{ki}|).$$

The statement that we wish to prove is then as follows.

Theorem 9.7. *Suppose that $\mathcal{L}_0, \dots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are pre-commuting, irreducible and coprime. Then*

$$|\mathcal{L}_0A + \cdots + \mathcal{L}_kA| \geq H(\mathcal{L}_0, \dots, \mathcal{L}_k)|A| - o(|A|)$$

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

Proof. We may assume that $\mathcal{L}_0, \dots, \mathcal{L}_k$ are non-zero. Let $\lambda_1, \dots, \lambda_k$ be the algebraic numbers given by applying Theorem 9.4 to $\mathcal{L}_0, \dots, \mathcal{L}_k$. Then the required estimate follows from Theorem 1.2 provided only that $H(\mathcal{L}_0, \dots, \mathcal{L}_k) = H(\lambda_1, \dots, \lambda_k)$. To check this, note that the map corresponding to multiplication by λ_l is similar to $\mathcal{L}_0^{-1}\mathcal{L}_l$, so we have

$$\begin{aligned}
G(x_0, \dots, x_k) &= \det(x_0\mathcal{L}_0 + \cdots + x_k\mathcal{L}_k) \\
&= \det(\mathcal{L}_0)\det(x_0I + x_1\mathcal{L}_0^{-1}\mathcal{L}_1 + \cdots + x_k\mathcal{L}_0^{-1}\mathcal{L}_k) \\
&= \det(\mathcal{L}_0)N_{K/\mathbb{Q}}(x_0 + x_1\lambda_1 + \cdots + x_k\lambda_k) \\
&= \det(\mathcal{L}_0)\prod_{i=1}^{d}(x_0 + \sigma_i(\lambda_1)x_1 + \cdots + \sigma_i(\lambda_k)x_k).
\end{aligned}$$

Therefore,

$$\begin{aligned}
H(\mathcal{L}_0, \dots, \mathcal{L}_k) &= |\det(\mathcal{L}_0)|\prod_{i=1}^{d}(1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \\
&= N_{K/\mathbb{Q}}(\mathfrak{D}_{\lambda_1,\dots,\lambda_k;K})\prod_{i=1}^{d}(1 + |\sigma_i(\lambda_1)| + \cdots + |\sigma_i(\lambda_k)|) \\
&= H(\lambda_1, \dots, \lambda_k),
\end{aligned}$$

completing the proof. □

10 Concluding remarks

Lower-order terms. A close inspection of our arguments shows that the $o(|A|)$ term in our bound

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

can be taken to be $O(|A|/\sqrt{\log_{(k)} |A|})$, where $\log_{(k)}$ is the k-times iterated logarithm. This is clearly not best possible. The lower bound in Section 3.1 suggests that one should be able to improve the error term to $O(|A|^{1-1/d})$, where $d = \deg(K/\mathbb{Q})$, though this is likely to be difficult. Given this, it would already be interesting to obtain $O(|A|^{1-\sigma})$ for some σ depending only on $\lambda_1, \ldots, \lambda_k$. In the particular case where $k = 1$ and λ is of the form $(p/q)^{1/d}$, this was already achieved in our earlier paper [7]. However, the methods of that paper and this one are quite orthogonal, so a novel approach is likely to be necessary for the general case.

An interesting example. The main problem left open by this paper is to prove an analogue of Theorem 1.2 when the matrices $\mathcal{L}_0, \ldots, \mathcal{L}_k \in \mathrm{Mat}_d(\mathbb{Z})$ are not necessarily pre-commuting. Our own attentions in this direction have focused on the specific example where

$$\mathcal{L}_0 = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \mathcal{L}_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad \mathcal{L}_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

These matrices can be shown to be irreducible and coprime, though they are not pre-commuting. We believe that

$$|\mathcal{L}_0 A + \mathcal{L}_1 A + \mathcal{L}_2 A| \geq 8|A| - o(|A|)$$

for all finite $A \subset \mathbb{Z}^3$, with the box $[0, N)^3$ showing that this would be asymptotically best possible. However, we were unable to even prove that there is some $C > 0$ such that

$$|\mathcal{L}_0 A + \mathcal{L}_1 A + \mathcal{L}_2 A| \geq C|A|$$

for all finite $A \subset \mathbb{Z}^3$. Resolving this issue would be a promising first step towards understanding the general problem.

References

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

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

[3] A. L. Bruch, Y. Jing and A. Mudgal, Brunn–Minkowski type estimates for certain discrete sumsets, preprint available at arXiv:2409.05638 [math.CO].

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

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

[6] D. Conlon and J. Lim, Sums of transcendental dilates, *Bull. London Math. Soc.* **55** (2023), 2400–2406.

[7] D. Conlon and J. Lim, Sums of linear transformations, to appear in *Trans. Amer. Math. Soc.*

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

[9] R. A. Horn and C. R. Johnson, **Matrix Analysis**, Cambridge University Press, Cambridge, 1985.

[10] F. John, Extremum problems with inequalities as subsidiary conditions, in Studies and Essays Presented to R. Courant on his 60th Birthday, 187–204, Interscience Publishers, New York, 1948.

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

[12] D. Krachun and F. Petrov, On the size of $A + \lambda A$ for algebraic λ, *Mosc. J. Comb. Number Theory* **12** (2023), 117–126.

[13] D. Krachun and F. Petrov, Tight lower bound on $|A + \lambda A|$ for algebraic integer λ, preprint available at arXiv:2311.09399 [math.CO].

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

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

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

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

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

[19] D. Singhal and Y. Lin, Primes in denominators of algebraic numbers, *Int. J. Number Theory* **20** (2024), 327–348.

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

[21] T. Tao and V. Vu, John-type theorems for generalized arithmetic progressions and iterated sumsets, *Adv. Math.* **219** (2008), 428–449.