ORIGINAL PAPER

Effective Results on the Size and Structure of Sumsets

Andrew Granville[2] · George Shakan[2] · Aled Walker[1]

© The Author(s) 2023

Abstract

Let $A \subset \mathbb{Z}^d$ be a finite set. It is known that NA has a particular size ($|NA| = P_A(N)$ for some $P_A(X) \in \mathbb{Q}[X]$) and structure (all of the lattice points in a cone other than certain exceptional sets), once N is larger than some threshold. In this article we give the first effective upper bounds for this threshold for arbitrary A. Such explicit results were only previously known in the special cases when $d = 1$, when the convex hull of A is a simplex or when $|A| = d + 2$ Curran and Goldmakher (Discrete Anal. Paper No. 27, 2021), results which we improve.

1 Introduction

For any given finite subset A of an abelian group G, we consider the sumset

$$NA := \{a_1 + a_2 + \cdots + a_N : a_i \in A\}.$$

If G is finite and N is sufficiently large, then

$$NA = Na_0 + \langle A - A \rangle \tag{1.1}$$

✉ Aled Walker
  aled.walker@kcl.ac.uk

1 King's College London, London, UK

2 Département de Mathématiques et Statistique, Université de Montréal, Montréal, Canada

for any $a_0 \in A$ where $\langle A - A \rangle$ is the subgroup of G generated by $A - A$, so that $|NA|$ is eventually constant. In this article we study instead the case when $G = \mathbb{Z}^d$ is infinite, and ask similar questions about the size and structure of NA when N is large.

The Size of NA

Khovanskii's 1992 theorem [8] states that if $A \subset \mathbb{Z}^d$ is finite then there exists $P_A(X) \in \mathbb{Q}[X]$ of degree $\leqslant d$ such that if $N \geqslant N_{\text{Kh}}(A)$ then

$$|NA| = P_A(N).$$

Although there are now several different proofs of Khovanskii's theorem [7, 12], the only effective bounds on $N_{\text{Kh}}(A)$ have been obtained when $d = 1$ [5, 6, 11, 14], when the convex hull of A is a d-simplex or when $|A| = d + 2$ (see [3]).

We will determine an upper bound for $N_{\text{Kh}}(A)$ for any such A in terms of the *width* of A,

$$w(A) = \text{width}(A) := \max_{a_1, a_2 \in A} \|a_1 - a_2\|_\infty. \tag{1.2}$$

Theorem 1.1 (Effective Khovanskii) *If $A \subset \mathbb{Z}^d$ is finite then*

$$|NA| = P_A(N) \text{ for all } N \geqslant (2|A| \cdot \text{width}(A))^{(d+4)|A|}.$$

The theorem states that $N_{\text{Kh}}(A) \leqslant (2\ell \, w(A))^{(d+4)\ell}$ where $\ell := |A|$. We expect that $N_{\text{Kh}}(A)$ is considerably smaller (see Sect. 2); for example, if $|A| = d + 2$ and $A - A$ generates $\mathbb{Z}^d$ then [3, Theorem 1.2] gives that

$$N_{\text{Kh}}(A) = d! \, \text{Vol}(H(A)) - d - 1, \tag{1.3}$$

where the *convex hull* $H(A)$ is defined by

$$H(A) := \left\{ \sum_{a \in A} c_a a : \text{Each } c_a \in \mathbb{R}_{\geqslant 0}, \sum_{a \in A} c_a = 1 \right\}.$$

We can replace $w(A)$ in Theorem 1.1 by $w^*(A)$ which is defined to be the minimum of $w(A')$ over all $A' \subset \mathbb{Z}^d$ that are Freiman isomorphic to A.[1]

Previous proofs of Khovanskii's theorem [7, 12] relied on the following ineffective principle.

Lemma 1.2 (The Mann–Dickson Lemma) *For any $S \subset \mathbb{Z}_{\geqslant 0}^d$ there exists a finite subset $S_{\min} \subset S$ such that for all $s \in S$ there exists $x \in S_{\min}$ with $s - x \in \mathbb{Z}_{\geqslant 0}^d$.*

---

[1] That is, there is a map $\phi : A \to A'$ such that for all $a_1, \ldots, a_k, b_1, \ldots, b_k \in A$ and $k \geqslant 1$, we have

$$a_1 + \cdots + a_k = b_1 + \cdots + b_k \text{ if and only if } \phi(a_1) + \cdots + \phi(a_k) = \phi(b_1) + \cdots + \phi(b_k).$$

For a proof see [5, Lemma 5]. Here we rework the method of Nathanson–Ruzsa from [12] as a collection of linear algebra problems which we solve quantitatively (see Sect. 6), and therefore bypass Lemma 1.2 and prove our effective threshold.

The Structure of *NA*

For a given finite set $A \subset \mathbb{Z}^d$ with $0 \in A$ we have

$$H(A) = \left\{ \sum_{a \in A} c_a a : \text{Each } c_a \in \mathbb{R}_{\geqslant 0}, \sum_{a \in A} c_a \leqslant 1 \right\}.$$

We let $\mathrm{ex}(H(A))$ be the set of extremal points of $H(A)$, that is the "corners" of the boundary of A, [2] which is a subset of A. We define the lattice generated by A,

$$\Lambda_A := \left\{ \sum_{a \in A} x_a a : x_a \in \mathbb{Z} \text{ for all } a \right\}.$$

For a domain $D \subset \mathbb{R}^d$ we set $N \cdot D := \{Nx : x \in D\}$ so that $N \cdot H(A) = NH(A)$ as $H(A)$ is convex and so, as $0 \in A$,

$$H(A) \subset 2H(A) \subset 3H(A) \cdots \subset C_A$$
$$:= \lim_{N \to \infty} NH(A) = \left\{ \sum_{a \in A} c_a a : c_a \in \mathbb{R}_{\geqslant 0} \text{ for all } a \right\},$$

the cone generated by A. Now, by definition,

$$0 \in A \subset 2A \subset 3A \cdots \subset \mathcal{P}(A) := \bigcup_{N=1}^{\infty} NA,$$

and each

$$NA \subset NH(A) \cap \Lambda_A \text{ so that } \mathcal{P}(A) \subset C_A \cap \Lambda_A.$$

Define the set of *exceptional elements*

$$\mathcal{E}(A) := (C_A \cap \Lambda_A) \setminus \mathcal{P}(A).$$

Therefore, for any finite $A \subset \mathbb{Z}^d$ and $a \in A$ we have

$$N(a - A) \subset (NH(a - A) \cap \Lambda_{a-A}) \setminus \mathcal{E}(a - A),$$

---

[2] That is, those points $p \in H(A)$ for which there is a vector $v \in \mathrm{span}(A - A) \setminus \{0\}$ and a constant c such that $\langle v, p \rangle = c$ and $\langle v, x \rangle > c$ for all $x \in H(A) \setminus \{p\}$; see Appendix A.

as $0 \in a - A$. So

$$NA \subset (NH(A) \cap (aN + \Lambda_{a-A})) \setminus (aN - \mathcal{E}(a - A)).$$

Hence, as $aN + \Lambda_{a-A}$ is independent of the choice of $a \in A$ and $\Lambda_{a-A} = \Lambda_{A-A}$, for any fixed $a_0 \in A$ we have

$$NA \subset (NH(A) \cap (a_0 N + \Lambda_{A-A})) \setminus \left(\bigcup_{a \in \mathrm{ex}(H(A))} (aN - \mathcal{E}(a - A)) \right). \tag{1.4}$$

In [5] the first two authors showed[3] there exists a constant $N_{\mathrm{Str}}(A)$ such that we get equality in (1.4) provided $N \geqslant N_{\mathrm{Str}}(A)$; that is,

$$NA = (NH(A) \cap (a_0 N + \Lambda_{A-A})) \setminus \left(\bigcup_{a \in \mathrm{ex}(H(A))} (aN - \mathcal{E}(a - A)) \right). \tag{1.5}$$

(Compare this statement to (1.1).) The proof in [5] relied on the ineffective Lemma 1.2 so did not produce a value for $N_{\mathrm{Str}}(A)$.

In this article we give an effective bound on $N_{\mathrm{Str}}(A)$:

Theorem 1.3 (Effective structure) *If $A \subset \mathbb{Z}^d$ is finite then*

$$(1.5) \text{ holds for all } N \geqslant (d|A| \cdot \mathrm{width}(A))^{13d^6}.$$

That is, Theorem 1.3 implies that $N_{\mathrm{Str}}(A) \leqslant (d\ell\, w(A))^{13d^6}$ where $|A| = \ell$.

The 1-dimensional case is easier than higher dimensions, since if $0 = \min A$ and $\Lambda_A = \mathbb{Z}$ then $\mathcal{E}(A)$ is finite, and so has been the subject of much study [5, 6, 11, 14]: We have $N_{\mathrm{Str}}(A) = 1$ if $|A| = 3$ in [5], and $N_{\mathrm{Str}}(A) \leqslant w(A) + 2 - |A|$ in [6], with equality in a family of examples. There are also effective bounds known when $H(A)$ is a d-simplex, as we will discuss in the next subsection.

Suppose that x belongs to the right-hand side of (1.5). To prove Theorem 1.3 when x is far away from the boundary of $NH(A)$ we develop an effective version of Proposition 1 of Khovanskii's original paper [8] using quantitative linear algebra. Otherwise x is close to a separating hyperplane of $NH(A)$: Suppose the hyperplane is $z_d = 0$; write each $a = (a_1, \ldots, a_d)$ and $x = (x_1, \ldots, x_d)$, so that every $a_d \geqslant 0$ and x_d is "small". Now $x = \sum_{a \in A} m_a a$ where each $m_a \in \mathbb{Z}_{\geqslant 0}$ as $x \in \mathcal{P}(A)$ and so $\sum_{a \in A, a_d \neq 0} m_a a_d \leqslant x_d$ is small. The contribution from those a with $a_d = 0$ is a "smaller dimensional problem", living in the hyperplane $z_d = 0$. Carefully formulated, one can apply induction on the dimension to bound $\sum_{a \in A} m_a$, and hence show that $x \in NA$.

The structure (1.5) is evidently related to Khovanskii's theorem. However, we have not been able to find a precise way to relate Khovanskii's theorem and Theorem 1.3. Our proofs of Theorems 1.1 and 1.3 are almost entirely disjoint, and we get a different quality of bound in each theorem.

---

[3] The result in [5] was only stated when $0 \in A$ and $\Lambda_A = \mathbb{Z}^d$, and the union was over all of A rather than just $\mathrm{ex}(H(A))$, but the methods give the general version (1.5).

The Size and Structure of NA When $H(A)$ is a d-Simplex

If $A \subset \mathbb{R}^d$ then the convex hull $H(A)$ is a *d-simplex* if there exists $B \subset A$ with $|B| = d+1$ for which $B - B$ spans $\mathbb{R}^d$ and $H(A) = H(B)$ (whence $\mathrm{ex}(H(A)) = B$).

Theorem 1.4 (Effective Khovanskii, simplex case) *If $A \subset \mathbb{Z}^d$ is finite and $H(A)$ is a d-simplex then $|NA| = P_A(N)$ for all $N \geqslant 1$ for which*

$$N \geqslant (d+1)! \, \mathrm{vol}(H(A)) - (d+1)(|A| - d) - d + 1. \qquad (1.6)$$

Theorem 1.5 (Effective structure, simplex case) *If $A \subset \mathbb{Z}^d$ is finite and $H(A)$ is a d-simplex then (1.5) holds for all $N \geqslant 1$ for which*

$$N \geqslant (d+1)! \, \mathrm{vol}(H(A)) - (d+1)(|A| - d), \qquad (1.7)$$

and if $|A| = d+1$ or $d+2$ then (1.5) holds for all $N \geqslant 1$.

Therefore if $A \subset \mathbb{Z}^d$ is finite and $H(A)$ is a d-simplex then

$$N_{\mathrm{Kh}}(A) \leqslant (d+1)! \, \mathrm{vol}(H(A)) - (d+1)(|A| - d) - d + 1 \qquad (1.8)$$

and

$$N_{\mathrm{Str}}(A) \leqslant (d+1)! \, \mathrm{vol}(H(A)) - (d+1)(|A| - d). \qquad (1.9)$$

The hypotheses imply that $|A| \geqslant d+1$. If $d = 1$ our bound gives $N_{\mathrm{Str}}(A) \leqslant 2w(A) - 2|A| + 3$ which is weaker than the bound $N_{\mathrm{Str}}(A) \leqslant w(A) - |A| + 2$ from [6], which suggests that Theorem 1.5 is still some way from being "best possible".

Even though the main bounds in Theorems 1.4 and 1.5 are very similar, we have not been able to find a way to directly deduce one theorem from the other. Instead, we present separate arguments for each theorem (in Sects. 4 and 5 respectively), albeit based on the same fundamental lemmas in Sect. 3.

Curran and Goldmakher [3] gave similar (but slightly weaker) bounds in the simplex case. In [3, Theorem 1.4] they showed that $N_{\mathrm{Kh}}(A) \leqslant (d+1)! \, \mathrm{vol}(H(A)) - 3d - 1$, and in [3, Theorem 1.3] they showed that $N_{\mathrm{Str}}(A) \leqslant (d+1)! \, \mathrm{vol}(H(A)) - 2d - 2$. (In the statement of [3, Theorem 1.3] they replace (1.5) by

$$NA = \bigcap_{b \in \mathrm{ex}(H(A))} (bN + \mathcal{P}(A - b))$$

but these expressions are equivalent.) Our bounds (1.8) and (1.9) match these expressions when $|A| = d+2$, but are an improvement as soon as $|A| \geqslant d+3$.

The proofs of Theorems 1.4 and 1.5 look seemingly very different from the work in [3]. Our method manipulates A directly using additive-combinatorial language; Curran and Goldmakher, being inspired by Ehrhart theory, used generating functions such as $S(t) := \sum_{N \geqslant 0} |NA| t^N$ and 'raised the dimension' by examining further properties of subsets of $\mathbb{Z}^{d+1}$ generated by $\{(a, 1) : a \in A\}$.

However, the two approaches are in fact closely related. The central notion of our method for the simplex case is that of a 'B-minimal element', see Definition 3.3 below; this is equivalent to the notion of 'minimal elements' defined in [3], at the end of p. 7 and in the remark following the statement of Proposition 4.1 of that paper. There are also analogies between some of our preparatory lemmas and partial results in [3], which will be discussed in Sects. 3, 4, and 5 below when they occur.

Our improvement over [3] comes from refining an additive combinatorial lemma concerning the B-minimal elements, related to the Davenport constant of the group $\mathbb{Z}^d / \Lambda_{B-B}$. The key results are Lemmas 3.5 and 3.7 below. In fact, it would have been possible to derive Theorems 1.4 and 1.5 directly by inputting the conclusions of Lemmas 3.5 and 3.7 into the relevant parts of the argument of [3], following a translation into the generating function language of [3] (the details are discussed after Lemma 3.7 below). However, we think there is extra value in showing how the analysis from [3] can be phrased—efficiently—in a classical additive-combinatorial language.

Having discussed the similarities to [3], it should be stressed that the main work of this paper—all parts of the proof of Theorem 1.1, and the technical heart of the proof of Theorem 1.3—is not related to any part of [3]. These novel elements comprise the majority of the present work.

The structure of the paper is as follows. In the next section we briefly discuss the 1-dimensional case, and in the three subsequent sections, the simplex case. In Sect. 6, we prove the effective Khovanskii theorem (Theorem 1.1). In Sect. 7 we then prove the effective structure result (Theorem 1.3); this part may be read essentially independently of the previous section, although there is one piece of quantitative linear algebra in common. An appendix collects together some facts from the theory of convex polytopes (which are useful in Sect. 7).

2 One Dimension and Speculations

It might well be that for finite $A \subset \mathbb{Z}^d$

$$N_{\mathrm{Str}}(A) \leqslant N_{\mathrm{Kh}}(A) \leqslant d! \operatorname{vol}(H(A)). \tag{2.1}$$

We refrain from calling this speculation a conjecture, since we have not even proved it for $d = 1$. However, a slight specialisation of the relation (2.1) is true when $d = 1$, and we know of no counterexample for larger d, so it is certainly worth investigating; we make a few remarks in this section.

After translating suppose that $0 \in \operatorname{ex}(H(A))$. First we note that if $\mathcal{E}(b - A) = \emptyset$ for all $b \in \operatorname{ex}(H(A))$ then $N_{\mathrm{Kh}}(A) = N_{\mathrm{Str}}(A)$. Indeed, Khovanskii's theorem [8] and Theorem 1.3 imply that the Khovanskii polynomial $P_A(N)$ is equal to $|NH(A) \cap \Lambda_A|$. Since $NA \subset NH(A) \cap \Lambda_A$, we have $|NA| \leqslant P_A(N)$ for all N, and $|NA| = P_A(N)$ if and only if (1.5) holds, and thus $N_{\mathrm{Kh}}(A) = N_{\mathrm{Str}}(A)$.

We also obtain the bounds $N_{\mathrm{Kh}}(A), N_{\mathrm{Str}}(A) < (d + 1)! \operatorname{vol}(H(A))$ in Theorems 1.4 and 1.5, bigger than in (2.1) by a factor of $d + 1$ (and one can see where this comes from in the proof). If $d = 1$ then $\operatorname{Vol}(H(A)) = w(A)$, so the inequalities $N_{\mathrm{Str}}(A), N_{\mathrm{Kh}}(A) \leqslant d! \operatorname{vol}(H(A))$ can be deduced from the following:

Lemma 2.1 *If $A \subset \mathbb{Z}$ with $\gcd_{a \in A} a = 1$ and $|A| \geqslant 3$ then $N_{\mathrm{Str}}(A), N_{\mathrm{Kh}}(A) \leqslant w(A) - 1$.*

Proof We may translate A so that it has minimal element 0 and largest element $b = w(A)$. (If $|A| = 2$ then $A = \{0, 1\}$ and $N_{\mathrm{Str}}(A) = N_{\mathrm{Kh}}(A) = 1$). The main theorem of [6] gives that $N_{\mathrm{Str}}(A) \leqslant b - |A| + 2$, which is $\leqslant w(A) - 1$ for $|A| \geqslant 3$.

If $N \geqslant N_{\mathrm{Str}}(A)$ then $NA = (NH(A) \cap \mathbb{Z}^d) \setminus (\mathcal{E}(A) \bigcup (bN - \mathcal{E}(b - A)))$. Let e_A denote the largest element of $\mathcal{E}(A)$, or $e_A = -1$ if $\mathcal{E}(A)$ is empty. If $bN > e_A + e_{b-A}$ then $\mathcal{E}(A)$ and $bN - \mathcal{E}(b - A)$ are disjoint subsets of $\{0, \ldots, bN\}$ so that $|NA| = bN - c$ where $c = |\mathcal{E}(A)| + |\mathcal{E}(b - A)| - 1$. Therefore

$$N_{\mathrm{Kh}}(A) \leqslant \max \left\{ N_{\mathrm{Str}}(A), 1 + \left\lfloor \frac{e_A + e_{b-A}}{b} \right\rfloor \right\}.$$

In particular if $A = \{0, a, b\}$ with $(a, b) = 1$ then $N_{\mathrm{Str}}(A) = 1$ by [5, Theorem 4] and $e_A = ba - b - a$ so that $N_{\mathrm{Kh}}(A) = \max(1, b - 2)$.

Now suppose that $|A| \geqslant 4$. By [4, Theorem 1] we have

$$e_A \leqslant \frac{b(b-1)}{|A| - 2} - 1 \text{ so that } 1 + \left\lfloor \frac{e_A + e_{b-A}}{b} \right\rfloor < 1 + \frac{2(b-1)}{|A| - 2} \leqslant b.$$

Therefore we have $N_{\mathrm{Kh}}(A) \leqslant b - 1 = w(A) - 1$. □

Although we do not yet know whether $N_{\mathrm{Str}}(A) \leqslant N_{\mathrm{Kh}}(A)$ in general when $d = 1$, the methods of Curran–Goldmakher do show something along these lines.[4] For each $g \in \{0, 1, \ldots, b - 1\}$, let $N_{\mathrm{Kh}, g}(A)$ denote the optimal threshold for which $|NA \cap \{n : n \equiv g \bmod b\}| = P_g(N)$ for all $N \geqslant N_{\mathrm{Kh}, g}(A)$, where P_g is some fixed polynomial; let $N_{\mathrm{Str}, g}(A)$ denote the optimal threshold for which

$$NA \cap \{n : n \equiv g \bmod b\} = ([0, bN] \cap \{n : n \equiv g \bmod b\}) \setminus (\mathcal{E}(A) \cup (bN - \mathcal{E}(b - A)))$$

for all $N \geqslant N_{\mathrm{Str}, g}(A)$. Then

$$N_{\mathrm{Str}, g}(A) \leqslant N_{\mathrm{Kh}, g}(A). \tag{2.2}$$

This is obtained by considering the proofs in [3, Sect. 3], which show that $N_{\mathrm{Kh}, g}(A) = \deg P - d$ when $H(A)$ is a simplex, where P is some auxiliary polynomial: In [3, Sect. 4] Curran–Goldmakher then show that $N_{\mathrm{Str}, g}(A) \leqslant \deg P - 1$ for the same auxiliary polynomial P. Unfortunately, although $N_{\mathrm{Str}}(A) = \max_g N_{\mathrm{Str}, g}(A)$, one could potentially get $N_{\mathrm{Kh}}(A) < \max_g N_{\mathrm{Kh}, g}(A)$, so the inequality (2.2) does not immediately give (2.1) when $d = 1$.

Curran–Goldmakher also give the precise value of $N_{\mathrm{Kh}}(A)$ in (1.3) in certain special cases including the useful example $A := \{(0, \ldots, 0), (1, \ldots, 1), m_1 e_1, \ldots, m_d e_d\} \subset \mathbb{Z}^d$ where the m_j are pairwise coprime positive integers and the $e_1, \ldots, e_d$ are the standard basis vectors. If all the m_j are close to x so that $w(A) \approx x$ for some large x

---

then $N_{\mathrm{Kh}}(A) \sim_{x \to \infty} w(A)^d$, which suggests we might be able to reduce the bound in Theorem 1.1 to $w(A)^d$. However $d! \, \mathrm{vol}(H(A))$ would be a preferable bound to $w(A)^d$, since it is smaller and more precise in the example where we let $m_2 = \cdots = m_d = 1$ and $m_1 = x$ be arbitrarily large so that $N_{\mathrm{Kh}}(A) \sim_{x \to \infty} w(A)$.

3 Preparatory Lemmas for the Simplex Case

Throughout this section, $0 \in A \subset \mathbb{Z}^d$ and A is finite. Let $N_A(0) = 0$ and for each $v \in \mathcal{P}(A) \setminus \{0\}$ let $N_A(v)$ denote the minimal positive integer N such that $v \in NA$.

Definition 3.1 (*B*-minimal elements) Suppose that $B \cup \{0\} \subset A \subset \mathbb{Z}^d$, with A finite. Let $\mathcal{S}(A, B)$ denote the set of *B-minimal elements*[5], which comprises 0 and those elements $u \in \mathcal{P}(A) \setminus \{0\}$ such that $a_i \notin B \cup \{0\}$ for every i whenever

$$u = a_1 + a_2 + \cdots + a_{N_A(u)} \text{ with each } a_i \in A.$$

B-minimal elements can be used to decompose NA and $\mathcal{P}(A)$ into simpler parts. The following is the analogous statement to [3, Proposition 4.1], although that proposition is only stated in the case when $H(A)$ is a d-simplex.

Lemma 3.2 *If* $B^* := B \cup \{0\} \subset A \subset \mathbb{Z}^d$ *with* A *finite then*

$$\mathcal{P}(A) = \mathcal{S}(A, B) + \mathcal{P}(B^*) \text{ and } NA = \bigcup_{\substack{u \in \mathcal{S}(A,B) \\ N_A(u) \leqslant N}} (u + (N - N_A(u))B^*).$$

Proof The second assertion implies the first by taking a union over all N. That each $u + (N - N_A(u))B^* \subset NA$ is immediate, so we need only show that if $v \in NA$ then $v \in u + (N - N_A(u))B^*$ for some $u \in \mathcal{S}(A, B)$ with $N_A(u) \leqslant N$.

Now, for any $v \in NA$ we can write

$$v = u + w \text{ with } u = a_1 + \cdots + a_L \text{ and } w = b_1 + \cdots + b_M,$$

where $L, M \geqslant 0$, and each $a_i \in A \setminus B$ and $b_i \in B$, with M maximal and $L + M = N_A(v)$. Then $N_A(u) = L$ and $N_A(w) = M$, else we could replace the above expression for u or w by a shorter sum of elements of A, and therefore obtain a shorter sum of elements to give v, contradicting that $L + M = N_A(v)$ is minimal. Moreover $u \in S(A, B)$ else we could replace the sum $a_1 + \cdots + a_L$ in the expression for v by a different sum of length L which includes some elements of B, contradicting the maximality of M.

Therefore $u \in S(A, B)$ with $N_A(u) = L \leqslant N_A(v) \leqslant N$ and

$$v \in u + MB^* = u + (N_A(v) - N_A(u))B^* \subset u + (N - N_A(u))B^*,$$

---

[5] We observe that $\mathcal{S}(A, B)$ is the set of $u \in \mathcal{P}(A)$ such that $(u, N_A(u)) \in \mathbb{Z}^{d+1}$ is minimal in the sense of [3, Sects. 3,4], in particular the bottom of p. 7 and the remark following Proposition 4.1 of that paper.

since $0 \in B^*$. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

It will be useful to control the complexity of the B-minimal elements.

Definition 3.3 Let $B \cup \{0\} \subset A \subset \mathbb{Z}^d$, with A finite. If $\mathcal{S}(A, B)$ is a finite set, we define

$$K(A, B) := \max_{u \in \mathcal{S}(A, B)} N_A(u).$$

In certain circumstances we will bound $K(A, B)$ using results on *Davenport's problem*, which asks for the smallest integer $D(G)$ such that any set of $D(G)$ (not necessarily distinct) elements of an abelian group G contains a subsum[6] that equals 0_G. It is known that $D(G) \leqslant m(1 + \log |G|/m)$ where m is the maximal order of an element of G.

Definition 3.4 Given a finite abelian group G, if $0 \notin H \subset G$ let $k(G, H)$ be the length of the longest sum of elements of H which contains no subsum equal to 0, and no subsum of length > 1 belonging to H.

Lemma 3.5 *Given a finite abelian group G, for any $0 \notin H \subset G$ we have $k(G, H) \leqslant |G| - |H|$. Moreover $k(G, H) \leqslant m(1 + \log |G|/m) - 1$, where m is the maximal order of an element of G.*

Proof Suppose we are given a longest sum $h_1 + \cdots + h_k$ of elements of H defining $k(G, H)$, so that $k = k(G, H)$. Then

$$0, h_1 + h_2, h_1 + h_2 + h_3, \ldots, h_1 + \cdots + h_k,$$

are all distinct in G, else subtracting would give a subsum equal to 0, and they are all contained in $G \setminus H$. Therefore $k + |H| \leqslant |G|$ and the first result follows.

By definition $k(G, H) < D(G)$ so the second result claims from the result noted for $D(G)$ above. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Curran and Goldmakher's [3, Lemma 3.1] implies the weaker upper bound $k(G, H) \leqslant |G| - 1$. This difference leads in part to the improvements in Theorems 1.4 and 1.5.

3.1 d-Dimensional Simplices

Let $B = \{b_1, \ldots, b_d\} \subset A$ be a basis for $\mathbb{R}^d$ with

$$B \cup \{0\} \subset A \subset H(B \cup \{0\}) \text{ and } A \subset \mathbb{Z}^d$$

so that A is finite. Since $C_A = C_B$, and B is a basis, there is a unique representation of every vector $r \in C_A$ as

$$r = \sum_{i=1}^{d} r_i b_i \text{ where each } r_i \geqslant 0. \qquad\qquad (3.1)$$

---

[6] A *subsum* of a given sum $\sum_{i \in I} g_i$ is a sum of the form $\sum_{i \in I'} g_i$ where $I' \subset I$ is non-empty, of *length* $|I'|$.

If $r \in H(A) = H(B \cup \{0\})$ then $\sum_{i=1}^{d} r_i \leqslant 1$.

Lemma 3.6 *Suppose $B = \{b_1, \ldots, b_d\}$ is a basis for $\mathbb{R}^d$ with $B \cup \{0\} \subset A \subset H(B \cup \{0\})$ and $A \subset \mathbb{Z}^d$ is finite. If $r \in \mathcal{P}(A)$ and $r \equiv a \pmod{\Lambda_B}$ with $a \in A$ then $r - a \in \mathcal{P}(B \cup \{0\})$ (where we choose $a = 0$ if $r \in \Lambda_B$).*

Proof Since $r \in \mathcal{P}(A) \subset C_A$, we have the representation (3.1) for r. Moreover since $a \in H(A) = H(B \cup \{0\})$ we have the representation $a = \sum_{i=1}^{d} a_i b_i$ by (3.1) with $\sum_{i=1}^{d} a_i \leqslant 1$. If $a \not\equiv 0 \pmod{\Lambda_B}$ then each $a_i \in [0, 1)$, and otherwise we choose $a = 0$ so each $a_i = 0$. Therefore $\sum_{i=1}^{d} r_i b_i = r \equiv a = \sum_{i=1}^{d} a_i b_i \pmod{\Lambda_B}$, and each $r_i \equiv a_i \pmod{1}$. As each $r_i \geqslant 0$ we write $m_i = r_i - a_i$ so that each $m_i \in \mathbb{Z}_{\geqslant 0}$ and $r - a = \sum_{i=1}^{d} m_i b_i \in \mathcal{P}(B \cup \{0\})$.   □

We use this lemma to bound $K(A, B)$.

Lemma 3.7 *Suppose $B = \{b_1, \ldots, b_d\}$ is a basis for $\mathbb{R}^d$ with $B \cup \{0\} \subset A \subset H(B \cup \{0\})$ and $A \subset \mathbb{Z}^d$ is finite. If $u = a_1 + \cdots + a_{N_A(u)} \in \mathcal{S}(A, B)$ is non-zero then any subsum with two or more elements cannot belong to $A_B := A \bmod \Lambda_B$, and no subsum can be congruent to $0 \bmod \Lambda_B$. Therefore*

$$K(A, B) \leqslant k(\Lambda_A / \Lambda_B, A_B \setminus \{0\}).$$

Proof Let r be a subsum of $a_1 + \cdots + a_{N_A(u)}$ of size $\ell > 1$. Then $\ell = N_A(r)$ and $r \in \mathcal{S}(A, B)$ as $u \in \mathcal{S}(A, B)$. We write r as in (3.1) so that $\sum_{i \leqslant d} r_i \leqslant \ell = N_A(r)$. Suppose that $r \equiv a \pmod{\Lambda_B}$ for some $a \in A$ (where we choose $a = 0$ if $r \in \Lambda_B$) so that $m := r - a \in \mathcal{P}(B \cup \{0\})$ by Lemma 3.6. Therefore $N_A(m) \geqslant \ell - N_A(a) \geqslant \ell - 1 > 0$ (so $m \neq 0$). On the other hand $N_A(m) = \sum_{i \leqslant d}(r_i - a_i) = \ell$ if $a = 0$, and $< \ell$ if $a \neq 0$, so $N_A(m) \leqslant \ell - N_A(a)$. We deduce that r can be represented as a plus the sum of $\ell - N_A(a)$ elements of B, contradicting that $r \in \mathcal{S}(A, B)$.   □

The combination of Lemmas 3.5, 3.6 and 3.7 effects an upper bound bound on $N_A(u)$ when $u \in \mathcal{S}(A, B)$, which is analogous to the bound from the statement of [3, Lemma 3.1] (albeit slightly stronger due to the stronger bound on $k(G, H)$ in this paper).

If the convex hull of A is not a simplex then $\mathcal{S}(A, B)$ need not be finite. For example, if $B = \{(0, 1), (1, 0)\} \subset A = \{(0, 0), (-1, 1), (0, 1), (1, 0)\}$ then $\mathcal{S}(A, B) = \{(-k, k) : k \in \mathbb{Z}_{\geqslant 0}\}$. This is one reason why $\mathcal{S}(A, B)$ is not used later in Sect. 7, when dealing with general sets A.

3.2 Translations

We finish by observing that under rather general hypotheses the sets $\mathcal{S}(A, B)$, and consequently the quantities $K(A, B)$, are well-behaved under translations. This observation was also made in [3, Lemma 4.2].

Lemma 3.8 *Let $B \cup \{0\} \subset A \subset \mathbb{Z}^d$, with A finite. If $b \in B$ then*

$$\mathcal{S}(b - A, b - B) = \{bN_A(u) - u : u \in \mathcal{S}(A, B)\}$$

and if $v = bN_A(u) - u$ with $u \in \mathcal{S}(A, B)$ then $N_{b-A}(v) = N_A(u)$. In particular we have $K(b - A, b - B) = K(A, B)$.

Proof Let $N = N_A(u)$. If $u = a_1 + a_2 + \cdots + a_N$ then $v := bN - u = (b - a_1) + \cdots + (b - a_N)$ so that $N_{b-A}(v) \leqslant N_A(u)$. If $N_{b-A}(v) \leqslant N - 1$ say $v = (b-a_1') + \cdots + (b-a_M')$ with $M < N$ then $u = a_1' + \cdots + a_M' + (N-M)b$ contradicting the definition of $u \in \mathcal{S}(A, B)$. We deduce that there is a 1-to-1 correspondance between the representations of u as the sum of N elements of A, and of v as the sum of N elements of $b - A$, and the result follows. $\qquad \square$

4 Structure Bounds in the Simplex Case

First we deal with the special cases.

Proof of Theorem 1.5 *for* $|A| = d + 1$ *and* $|A| = d + 2$. Let $\mathrm{ex}(H(A)) = B$ where $|B| = d + 1$ and $\mathrm{span}(B - B) = \mathbb{R}^d$. Write $B = \{b_0, \ldots, b_d\}$, and translate so that $0 = b_0 \in B$.

If $|A| = d + 1$ then $B = A$ and $\mathcal{E}(b - A) = \emptyset$ for all $b \in B$. We immediately see that $NA = NH(B) \cap \Lambda_B = NH(A) \cap \Lambda_A$ for all $N \geqslant 1$.

If $|A| = d + 2$ write $A = B \cup \{a\}$. Since $a \in H(B)$ we can write $a = \sum_{i=0}^d a_i b_i$ uniquely with each $a_i \geqslant 0$ and $\sum_{i=0}^d a_i = 1$. We know that the finite group Λ_A / Λ_B is generated by a. If a has order M in the group Λ_A / Λ_B then the classes of Λ_A / Λ_B can be represented by

$$\mathcal{S}(A, B) = \{ma : 0 \leqslant m \leqslant M - 1\}.$$

Now let

$$v \in (NH(A) \cap \Lambda_A) \setminus (\bigcup_{b \in B} (bN - \mathcal{E}(b - A))). \tag{4.1}$$

Since $v \in NH(A) = NH(B)$ we can write $v = \sum_{i=0}^d v_i b_i$ in a unique way with each $v_i \geqslant 0$ and $\sum_{i=0}^d v_i = N$. This implies that $b_i N - v = \sum_{j=0}^d v_j (b_i - b_j) \in C_{b_i - A}$, and from (4.1) we have $b_i N - v \in \Lambda_A = \Lambda_{b_i - A}$ and $b_i N - v \notin \mathcal{E}(b_i - A)$. Hence $b_i N - v \in \mathcal{P}(b_i - A)$ for all i, in particular $v \in \mathcal{P}(A)$ (from $i = 0$).

Suppose that $v \equiv ma \mod \Lambda_B$ for some $0 \leqslant m \leqslant M - 1$. This implies that $v_i - ma_i \in \mathbb{Z}$ for $i = 0, 1, \ldots, d$, and we now show that $v_i - ma_i \in \mathbb{Z}_{\geqslant 0}$ if $i \neq 0$: Since $v \in \mathcal{P}(A)$ we may write

$$v = (m + \lambda M)a + \sum_{i=1}^d (v_i - (m + \lambda M)a_i)b_i$$

for some $\lambda \in \mathbb{Z}_{\geqslant 0}$ with $v_i - (m + \lambda M)a_i \in \mathbb{Z}_{\geqslant 0}$ for $i = 1, \ldots, d$. Therefore we conclude that $v_i - ma_i \in \mathbb{Z}_{\geqslant 0}$ for all $i \geqslant 1$.

We now give an analogous argument for representations of $b_j N - v$ for each $j = 1, \ldots, d$: For each j we also have

$$b_j N - v = \sum_{i=0}^{d} v_i (b_j - b_i) \equiv \sum_{i=0}^{d} m a_i (b_j - b_i) = m(b_j - a) \bmod \Lambda_{b_j - B}$$

Since $b_j N - v \in \mathcal{P}(b_j - A)$ we may write

$$b_j N - v = (m + \lambda M)(b_j - a) + \sum_{i=0}^{d} (v_i - (m + \lambda M)a_i)(b_j - b_i)$$

for some $\lambda \in \mathbb{Z}_{\geqslant 0}$ with $v_i - (m + \lambda M)a_i \in \mathbb{Z}_{\geqslant 0}$ for $i = 0, \ldots, d$ with $i \neq j$ (we can't deduce this for $i = j$ since then $b_j - b_i = 0$). Therefore $v_i \geqslant m a_i$ for all $i \neq j$.

Combining these observations, we deduce that $v_i - m a_i \in \mathbb{Z}_{\geqslant 0}$ for all i, which implies that

$$v = ma + \sum_{i=0}^{d} (v_i - m a_i) b_i \in \left(m + \sum_{i=0}^{d} (v_i - m a_i) \right) A = NA.$$

$\square$

We now prove the rest of Theorem 1.5. We'll use our bound on $K(A, B)$ from Lemma 3.7, combined with the following theorem.

Theorem 4.1 *Let $A \subset \mathbb{Z}^d$ be a finite set, for which $H(A)$ is a d-simplex and $0 \in B := \mathrm{ex}(H(A))$. Then (1.5) holds for all $N \geqslant (d+1)(K(A, B) - 1)$.*

This result can be abstracted from the proof of [3, Lemma 3.2] and the part of the proof of [3, Theorem 1.3] following expression (11).

Proof The proof follows similar lines to [5]. For all

$$v \in (N H(A) \cap (a_0 N + \Lambda_{A-A})) \setminus (\bigcup_{b \in B} (bN - \mathcal{E}(b - A))) \tag{4.2}$$

we wish to show that $v \in NA$. Now $v \in NH(A) = NH(B)$, so if $B = \{0 = b_0, b_1, \ldots, b_d\}$ then $v = \sum_{i=0}^{d} v_i b_i$ for some $v_i \in \mathbb{R}_{\geqslant 0}$ with $\sum_{i=0}^{d} v_i = N$. We will now show that $v \in N_j A$ for each j, where $N_j = K(A, B) + \sum_{i \neq j} \lfloor v_i \rfloor$:

Taking $j = d$ (all other cases are analogous), we observe that

$$b_d N - v = \sum_{i=0}^{d-1} v_i (b_d - b_i) \in (N - v_d) \cdot H(b_d - B),$$

so that $b_d N - v \in C_{b_d - B} = C_{b_d - A}$. Therefore $b_d N - v \in \mathcal{P}(b_d - A)$, as $b_d N - v \notin \mathcal{E}(b_d - A)$ and $b_d N - v \in \Lambda_{b_d - A}$ by (4.2). So we may write

$$b_d N - v = u + w \text{ with } u \in \mathcal{S}(b_d - A, b_d - B) \text{ and } w \in \mathcal{P}(b_d - B)$$

by Lemma 3.2. Then $w = \sum_{i=0}^{d-1} w_i(b_d - b_i)$ for some $w_i \in \mathbb{Z}_{\geqslant 0}$, which implies $0 \leqslant w_i \leqslant v_i$ so that $w_i \leqslant \lfloor v_i \rfloor$ for each i. But then $w \in (\sum_{i \neq d} \lfloor v_i \rfloor)B \subset (N_d - K(A, B))A$ and $u \in K(A, B)A$ since $K(A, B) = K(b_d - A, b_d - B)$ by Lemma 3.8. Therefore $v = u + w \in N_d A$ as claimed.

We have $v \in NA$ if $\sum_{i \neq j} \lfloor v_i \rfloor \leqslant N - K$ for some j, where $K = K(A, B)$. If not then $\sum_{i \neq j} v_i \geqslant \sum_{i \neq j} \lfloor v_i \rfloor \geqslant N - K + 1$ for each j, and so

$$N = \sum_{i=0}^{d} v_i = \frac{1}{d} \sum_{j=0}^{d} \sum_{i \neq j} v_i \geqslant \frac{d+1}{d}(N - K + 1),$$

which would imply that $N \leqslant (d + 1)(K - 1)$. Therefore $v \in NA$ when $N > (d + 1)(K - 1)$.

If $N = (d + 1)(K - 1)$ and the above inequalities fail to yield a contradiction, the last two chains of inequalities must be equalities. Therefore each $v_i \in \mathbb{Z}$, and so $u = 0$, (since 0 is the only element in $\mathcal{S}(b_d - A, b_d - B)$ that is congruent to 0 mod $\Lambda_{b_d - B}$). This implies that $v = w \in (N_d - K(A, B))A = (\sum_{i \neq d} v_i)A \subset NA$ as required. $\qquad \square$

Proof of Theorem 1.5 for $|A| \geqslant d + 3$. Now $A \setminus B$ is non-empty. Replacing A with $A - b$ (for some $b \in \text{ex}(H(A))$) we may assume, without loss of generality, that $0 \in \text{ex}(H(A)) = B$. Applying Lemmas 3.7 and 3.5, we then have

$$\begin{aligned} K(A, B) &\leqslant k(\Lambda_A/\Lambda_B, A_B \setminus \{0\}) \\ &\leqslant |\Lambda_A/\Lambda_B| - |A| + |B| \\ &\leqslant |\mathbb{Z}^d/\Lambda_B| - |A| + |B| = d! \, \text{vol}(H(A)) - |A| + d + 1. \end{aligned}$$

By Theorem 4.1, we conclude that (1.5) holds for all N in the range (1.7), as required. The result follows. $\qquad \square$

5 The Khovanskii Polynomial in the Simplex Case

In this section we prove Theorem 1.4, and make various remarks about the form of the Khovanskii polynomial itself. By analogy with the previous section, the main technical result is as follows:

Theorem 5.1 *Let $A \subset \mathbb{Z}^d$ be a finite set, for which $H(A)$ is a d-simplex and $0 \in B := \text{ex}(H(A))$. Then $|NA| = P_A(N)$ for all $N \geqslant 1$ for which $N \geqslant (d+1)K(A, B) - 2d$.*

This same result may be extracted from the proofs of [3, Lemma 3.2] and [3, Theorem 1.4] on p. 9 and 10 of that paper.

Proof We write $B = \{0, b_1, \dots, b_d\}$ where $\{b_1, \dots, b_d\}$ is a basis for $\mathbb{R}^d$ and

$$B \subset A \subset H(B) \subset \mathbb{Z}^d.$$

For each $g \in G := \mathbb{Z}^d / \Lambda_B$ we have a coset representative $g = \sum_{i=1}^{d} g_i b_i$ where each $g_i \in [0, 1)$. We may partition NA as the (disjoint) union over $g \in G$ of

$$(NA)_g := \{v \in NA : v \in g + \Lambda_B\},$$

and thus we wish to count the number of elements in each $(NA)_g$. If

$$\mathcal{S}(A, B)_g := \{u \in \mathcal{S}(A, B) : u \in g + \Lambda_B\}$$

then, by Lemma 3.2,

$$(NA)_g = \bigcup_{\substack{u \in \mathcal{S}(A,B)_g \\ N_A(u) \leqslant N}} \left(u + (N - N_A(u))B\right).$$

This union is not necessarily disjoint, but we may nonetheless develop a formula for its size by using inclusion-exclusion.

It is helpful to distinguish the case when $g = 0$. In this instance $\mathcal{S}(A, B)_g = \{0\}$, and since $N_A(0) = 0$ we conclude that for all $N \geqslant 1$,

$$|(NA)_0| = |NB| = \#\{(\ell_1, \dots, \ell_d) \in \mathbb{Z}_{\geqslant 0}^d : \ell_1 + \cdots + \ell_d \leqslant N\} = \binom{N + d}{d},$$

and this is a polynomial in N, namely $\frac{1}{d!}(N + d) \cdots (N + 1)$.

Now we consider the case $g \neq 0$. Let $\mathcal{S}(A, B)_g = \{u_1, \dots, u_k\}$, as $\mathcal{S}(A, B)$ is finite by Lemma 3.7, and so write

$$u_j = g + \sum_{i=1}^{d} u_{j,i} b_i = a_1 + \cdots + a_{N_A(u_j)}$$

where each $u_{j,i} \in \mathbb{Z}_{\geqslant 0}$. Expressing each a_ℓ in terms of the basis $\{b_1, \dots, b_d\}$, and using the fact that $g \neq 0$, we deduce that

$$\sum_{i=1}^{d} u_{j,i} < N_A(u_j) \text{ so that } \Delta_j := N_A(u_j) - \sum_{i=1}^{d} u_{j,i} > 0.$$

Since the $u_{j,i}$ are integers, we conclude that

$$\sum_{i=1}^{d} u_{j,i} \leqslant N_A(u_j) - 1.$$

Therefore, if $N \geqslant N_A(u_j)$ then

$$u_j + (N - N_A(u_j))B = g + \left\{ \sum_{i=1}^{d} m_i b_i : \text{Each } m_i \in \mathbb{Z}_{\geqslant u_{j,i}} \text{ and } \sum_{i=1}^{d} m_i \leqslant N - \Delta_j \right\}$$

(and the set on the right-hand side of the above expression is empty when $N < N_A(u_j)$). Therefore for all N and for all non-empty subsets $J \subset \{1, \ldots, k\}$ we have

$$\bigcap_{j \in J} \left(u_j + (N - N_A(u_j))B \right) = g + \left\{ \sum_{i=1}^{d} m_i b_i : \text{Each } m_i \geqslant u_{J,i} \text{ and } \sum_{i=1}^{d} m_i \leqslant N - \Delta_J \right\},$$

$$(5.1)$$

where we understand the m_i to always be integers, and we let

$$u_{J,i} := \max_{j \in J} u_{j,i} \text{ and } \Delta_J := \max_{j \in J} \Delta_j.$$

Let

$$N_J := \Delta_J + \sum_{i=1}^{d} u_{J,i}.$$

To count the number of points in the intersection (5.1) we write each $m_i = u_{J,i} + \ell_i$, and then

$$\left| \bigcap_{j \in J} (u_j + (N - N_A(u_j))B) \right| = \#\{(\ell_1, \ldots, \ell_d) \in \mathbb{Z}_{\geqslant 0}^{d} : \ell_1 + \cdots + \ell_d \leqslant N - N_J\}$$

$$= \binom{N - N_J + d}{d},$$

where we define $\binom{N-N_J+d}{d} := 0$ if $N < N_J$. Hence, by inclusion-exclusion we obtain

$$\#(NA)_g = \sum_{\substack{J \subset \{1, \ldots, k\} \\ |J| \geqslant 1}} (-1)^{|J|-1} \left| \bigcap_{j \in J} (u_j + (N - N_A(u_j))B) \right|$$

$$= \sum_{\substack{J \subset \{1, \ldots, k\} \\ |J| \geqslant 1}} (-1)^{|J|-1} \binom{N - N_J + d}{d}.$$

In fact this formula extends to cover the case $g = 0$, taking $k = 1$ and $N_{\{1\}} := 0$. Therefore we have the general formula

$$\#NA = \sum_{g \in G} \#(NA)_g = \sum_{\substack{g \in G \\ S(A,B)_g = \{u_1, \ldots, u_k\}}} \sum_{\substack{J \subset \{1, \ldots, k\} \\ |J| \geqslant 1}} (-1)^{|J|-1} \binom{N - N_J + d}{d}.$$

$$(5.2)$$

We wish to replace the binomial coefficients in this formula by polynomials in N; that is,

$$\text{Replacing } \binom{N - N_J + d}{d} \text{ by } \frac{1}{d!}(N - N_J + d) \cdots (N - N_J + 1),$$

but these are only equal if $N \geqslant N_J - d$. Therefore we are guaranteed that

$$\#(NA)_g = P_g(N) \text{ where } P_g(T) := \sum_{\substack{J \subset \{1,\ldots,k\} \\ |J| \geqslant 1}} (-1)^{|J|-1} \frac{(T - N_J + d) \cdots (T - N_J + 1)}{d!},$$

provided $N \geqslant \max_J N_J - d = N_{\{1,\ldots,k\}} - d$. Therefore

$$\#NA = P_A(N) \text{ where } P_A(T) := \sum_{g \in G} P_g(T)$$

once $N \geqslant 1$ (the trivial bound from the $g = 0$ class) and $N \geqslant \max_{g \neq 0}(N_{\{1,\ldots,k\}} - d)$. It remains to bound $N_{\{1,\ldots,k\}}$. By definition we have

$$N_{\{1,\ldots,k\}} \leqslant \max_j N_A(u_j) + \sum_{i=1}^d \max_j u_{j,i} \leqslant K(A, B) + \sum_{i=1}^d \max_j u_{j,i}. \qquad (5.3)$$

Now

$$u_{j,i} \leqslant \sum_{i=1}^d u_{j,i} \leqslant N_A(u_j) - 1 \leqslant K(A, B) - 1$$

by definition. Thus

$$N_{\{1,\ldots,k\}} - d \leqslant (d + 1)K(A, B) - 2d$$

as claimed.   □

We remark that the $-2d$ term (in the $(d + 1)!K(A, B) - 2d$ bound from Theorem 5.1) was saved by two separate actions. First, $-d$ was saved through considering $g = 0$ and $g \neq 0$ separately; there is an equivalent manoeuvre on [3, P. 9] when it is assumed that 'g_i is not congruent to $\mathbf{0}$'. Then, $-d$ was saved by noting that the binomial coefficient $\binom{N - N_J + d}{d}$ agrees with the polynomial $\frac{1}{d!}(N - N_J + d) \cdots (N - N_J + 1)$ for all $N \geqslant N_J - d$ not just for all $N \geqslant N_J$. This is analogue to the $-d$ that is saved by the application of the division algorithm in [3, Proof of Theorem 1.4] at the bottom of p. 10 of that paper.

Proof of Theorem 1.4 As in the proof of Theorem 1.5 at the end of Sect. 1.9, we may replace A with $A - b$ (for some $b \in \text{ex}(H(A))$) and assume without loss of generality that $0 \in \text{ex}(H(A)) = B$. We again have the bound

$$K(A, B) \leqslant d! \text{vol}(H(A)) - |A| + d + 1,$$

which substituting into Theorem 5.1 shows that $|NA| = P_A(N)$ in the range required.
                                                                                                                     □

5.1 Smaller N

Returning to the proof of Theorem 5.1, one may sometimes show that $\#(NA)_g = P_g(N)$ for more values of N.

Proposition 5.2 *Define*

$$W(h) := \sum_{\substack{J \subset \{1,\ldots,k\} \\ |J| \geqslant 1 \\ N_J = N_{\{1,\ldots,k\}} - h}} (-1)^{|J|},$$

and let h be the smallest non-negative integer for which $W(h) \neq 0$. Then $\#(NA)_g = P_g(N)$ for all $N \geqslant N_{\{1,\ldots,k\}} - d - h$, but not for $N = N_{\{1,\ldots,k\}} - d - h - 1$.

Proof Letting $m \geqslant 0$ and $N = N_{\{1,\ldots,k\}} - d - 1 - m$ we have

$$\#(NA)_g - P_g(N) = \sum_{\substack{J \subset \{1,\ldots,k\} \\ |J| \geqslant 1 \\ N_J \geqslant N_{\{1,\ldots,k\}} - m}} (-1)^{|J|} \frac{(N - N_J + d) \cdots (N - N_J + 1)}{d!}$$

$$= (-1)^d \sum_{\kappa=0}^{m} \binom{\kappa + d}{d} W(m - \kappa)$$

since if $N_J = N_{\{1,\ldots,k\}} - (m - \kappa)$ then

$$\frac{(N - N_J + d) \cdots (N - N_J + 1)}{d!} = (-1)^d \binom{\kappa + d}{d}$$

If $m \leqslant h - 1$ then every term on the right-hand side is 0 and so $\#(NA)_g = P_g(N)$. If $m = h$ then $\#(NA)_g = P_g(N) + (-1)^d W(h)$. □

5.2 Determing $W(0)$

We do not see how to easily determine h in general, though it is sometimes possible to identify whether $W(0) = 0$.

Proposition 5.3 *Let $J_0 := \{j : \Delta_j = \Delta_{\{1,\ldots,k\}}\}$ and $J_i := \{j : u_{j,i} = u_{\{1,\ldots,k\},i}\}$ for $1 \leqslant i \leqslant d$, with $J^* := \cup_{0 \leqslant i \leqslant d} J_i$.*

(i) If J^* is a proper subset of $\{1, \ldots, k\}$ then $W(0) = 0$.
(ii) If $J^* = \{1, \ldots, k\}$ and, for each i, there exists $j_i \in J_i$ such that $j_i \notin J_\ell$ for any $\ell \neq i$, then $W(0) = (-1)^{d+1} \neq 0$. (For example, when the sets J_i are disjoint.)

Proof We have $N_J = N_{\{1,\ldots,k\}}$ if and only if $J \cap J_i \neq \emptyset$ for all $0 \leqslant i \leqslant d$. Therefore, by inclusion-exclusion we have

$$W(0) = \sum_{\substack{J \subset \{1,\ldots,k\} \\ |J \cap J_i| \geqslant 1 \text{ for each } i}} (-1)^{|J|} = \sum_{\substack{I \subset \{0,\ldots,d\} \\ I \neq \emptyset}} (-1)^{|I|} \sum_{\substack{J \subset \{1,\ldots,k\} \\ J \cap J_i = \emptyset \text{ for each } i \in I}} (-1)^{|J|}$$

$$= \sum_{\substack{I \subset \{0,\ldots,d\} \\ I \neq \emptyset}} (-1)^{|I|} \sum_{J \subset \{1,\ldots,k\} \setminus \cup_{i \in I} J_i} (-1)^{|J|} = \sum_{\substack{I \subset \{0,\ldots,d\} \\ \cup_{i \in I} J_i = \{1,\ldots,k\}}} (-1)^{|I|}$$

(i) If J^* is a proper subset of $\{1, \ldots, k\}$ then there are no terms in the sum.

(ii) If $\cup_{\ell \in I} J_\ell = \{1, \ldots, k\}$ then each $j_i \in \cup_{\ell \in I} J_\ell$, so we conclude that $i \in I$. Therefore $I = \{0, \ldots, d\}$ and the result follows. $\square$

5.3 Explicitly Enumerating the Coefficients of $P_g(T)$

It turns out that the quantities Λ_j and $u_{j,i}$ also feature in the Khovanskii polynomial itself. Indeed, expanding the polynomial $P_g(T)$ we find that the leading two terms of $P_g(T)$ are

$$\frac{1}{d!} \sum_{\substack{J \subset \{1,\ldots,k\} \\ |J| \geqslant 1}} (-1)^{|J|-1} (T^d - d(N_J - \tfrac{d+1}{2}) T^{d-1})$$

$$= \frac{T^d}{d!} + \frac{1}{2} \frac{(d+1)T^{d-1}}{(d-1)!} - \frac{T^{d-1}}{(d-1)!} \left(\min_{1 \leqslant j \leqslant k} \Delta_j + \sum_{i=1}^{d} \min_{1 \leqslant j \leqslant k} u_{j,i} \right)$$

since N_J is a sum of various maximums and we have the identity

$$\sum_{\substack{J \subset \{1,\ldots,k\} \\ |J| \geqslant 1}} (-1)^{|J|} \max_{j \in J} a_j = - \min_{1 \leqslant j \leqslant k} a_j \qquad (5.4)$$

for any sequence $\{a_j\}$. The proof of (5.4) is an exercise in inclusion-exclusion.

6 Delicate Linear Algebra and an Effective Khovanskii's Theorem

The proof of Theorem 1.1 rests on various principles of quantitative linear algebra. The first is an application of the pigeon-hole principle.

Lemma 6.1 *Let M be a non-zero m-by-n matrix with integer coefficients and $n > m$. Let K be the maximum of the absolute values of the entries of M. Then there is a solution to $MX = 0$ with $X \in \mathbb{Z}^n \setminus \{0\}$ and*

$$||X||_\infty \leqslant (Kn)^m.$$

To prove Corollary 7.9 in the next section, we will need the more sophisticated Siegel's lemma due to Bombieri–Vaaler [1], which gives a basis for ker M rather than just a

single vector X; for the results in this section, the elementary result in Lemma 6.1 suffices.

Proof Suppose first that Kn is odd. If there were two distinct vectors $X_1, X_2 \in \mathbb{Z}^n$ for which $MX_1 = MX_2$ and $\|X_i\|_\infty \leqslant \frac{1}{2}(Kn)^m$, then by choosing $X = X_1 - X_2$ we would be done. Now, the number of vectors $X \in \mathbb{Z}^n$ for which $\|X\|_\infty \leqslant \frac{1}{2}(Kn)^m$ is equal to $(2(\frac{1}{2}((Kn)^m - 1)) + 1)^n$, which is $(Kn)^{mn}$. For all such X we have $\|MX\|_\infty \leqslant \frac{1}{2}(Kn)^{m+1}$ and $MX \in \mathbb{Z}^m$. We may further assume that $MX \neq 0$, since otherwise we would be immediately done. There are exactly $(2(\frac{1}{2}((Kn)^{m+1}-1))+1)^m$ vectors $Y \in \mathbb{Z}^m \setminus \{0\}$ with $\|Y\|_\infty \leqslant \frac{1}{2}(Kn)^{m+1}$, i.e exactly $(Kn)^{m(m+1)} - 1$ such vectors. Since $n \geqslant m + 1$, by the pigeonhole principle we may find distinct X_1, X_2 with $MX_1 = MX_2$ as required.

If Kn is even, then the number of vectors $X \in \mathbb{Z}^n$ for which $\|X\|_\infty \leqslant \frac{1}{2}(Kn)^m$ is exactly $((Kn)^m + 1)^n$, and there are at most $((Kn)^{m+1} + 1)^m - 1$ vectors $Y \in \mathbb{Z}^m \setminus \{0\}$ with $\|Y\|_\infty \leqslant \frac{1}{2}(Kn)^{m+1}$. Since

$$((Kn)^m + 1)^n > ((Kn)^{m+1} + 1)^m - 1,$$

we can conclude using the pigeonhole principle as before. □

Next, we will consider solutions to the equation $My = b$ in which all the coordinates of y are positive integers.

Lemma 6.2 *Let $M = (\mu_{ij})_{i \leqslant m, \, j \leqslant n}$ be an m-by-n matrix with integer coefficients, with $m \leqslant n$ and rank $M = m$, and let $b \in \mathbb{Z}^m$. Suppose that $\max_{i,j} |\mu_{ij}| \leqslant K_1$ and $\|b\|_\infty \leqslant K_2$ (where we choose $K_1, K_2 \geqslant 1$), and suppose that there is some $x \in \mathbb{Z}^n_{>0}$ for which $Mx = b$. Then we may find $y \in \mathbb{Z}^n_{>0}$ for which $My = b$ and*

$$\|y\|_\infty \leqslant (n - m)(n^m m^m K_1^{2m} + m^m K_1^m) + m^m K_1^{m-1} K_2.$$

Proof We prove this by induction on n. The base case is $n = m$. In this case we observe that M is invertible, and so $x = y = M^{-1}b$. Using the formula $M^{-1} = \det(M)^{-1} \operatorname{adj}(M)$, and since $(\det M)^{-1} \leqslant 1$ as M has integer entries, we conclude that $\|y\|_\infty \leqslant m! K_1^{m-1} K_2 \leqslant m^m K_1^{m-1} K_2$. This gives the base case.

We proceed to the induction step, assuming that $n \geqslant m + 1$. By Lemma 6.1, there is a vector $X \in \mathbb{Z}^n \setminus \{0\}$ such that $MX = 0$ and

$$\|X\|_\infty \leqslant n^m K_1^m.$$

Replacing X by $-X$ if necessary, we may assume that X has at least one positive coordinate with respect to the standard basis. Let $S \subset \{1, \ldots, n\}$ be the set of indices where the coordinate of X is positive.

Take x from the hypotheses of the lemma, and write $x = (x_1, \ldots, x_n)^T \in \mathbb{Z}^n_{>0}$. By replacing x with $x - \lambda X$ for some $\lambda \in \mathbb{Z}_{>0}$ as appropriate, we may assume that there is some $i \in S$ for which $1 \leqslant x_i \leqslant \|X\|_\infty + 1 \leqslant n^m K_1^m + 1$. Fix such an i and x_i, and

now consider the m-by-$(n-1)$ matrix $M^{\{i\}}$ which is M with the ith column removed. Similarly define $x^{\{i\}} \in \mathbb{Z}_{>0}^{n-1}$ to be the vector x with the ith coordinate removed. Then

$$M^{\{i\}}x^{\{i\}} = b - M(x_i e_i),$$

where e_i is the ith standard basis vector in $\mathbb{R}^n$.

Observe that $b - M(x_i e_i) \in \mathbb{Z}^m$ with

$$\|b - M(x_i e_i)\|_\infty \leqslant K_2 + K_1 x_i \leqslant K_2 + K_1(1 + n^m K_1^m) \leqslant n^m K_1^{m+1} + K_1 + K_2.$$

Now rank $M^{\{i\}}$ is either m or $m-1$. If rank $M^{\{i\}} = m$ then, by the induction hypothesis (with x replaced by $x^{\{i\}}$), there is some $y^{\{i\}} \in \mathbb{Z}_{>0}^{n-1}$ for which $M^{\{i\}}y^{\{i\}} = b - M(x_i e_i)$ and

$$
\begin{aligned}
\|y^{\{i\}}\|_\infty &\leqslant (n-m-1)((n-1)^m m^m K_1^{2m} + m^m K_1^m) + m^m K_1^{m-1}(n^m K_1^{m+1} + K_1 + K_2) \\
&\leqslant (n-m-1)(n^m m^m K_1^{2m} + m^m K_1^m) + m^m K_1^{m-1}(n^m K_1^{m+1} + K_1 + K_2) \\
&= (n-m)(n^m m^m K_1^{2m} + m^m K_1^m) + m^m K_1^{m-1} K_2.
\end{aligned}
$$

Let $y := y^{\{i\}} + x_i e_i$, where we have abused notation by treating $y^{\{i\}}$ also as an element of $\mathbb{Z}_{\geqslant 0}^n$ by extending by 0 in the ith coordinate. Then we have $y \in \mathbb{Z}_{>0}^n$, $My = b$, and

$$\|y\|_\infty \leqslant \max(\|y^{\{i\}}\|_\infty, n^m K_1^m + 1) \leqslant (n-m)(n^m m^m K_1^{2m} + m^m K_1^m) + m^m K_1^{m-1} K_2$$

since $n \geqslant m+1$. Thus we have completed the induction in this case.

If rank $M^{\{i\}} = m-1$ then there are some further cases. If $m = 1$ and $M^{\{i\}}$ is the zero matrix, then we can choose any vector $y^{\{i\}} \in \mathbb{Z}_{>0}^{n-1}$. Otherwise, we may replace $M^{\{i\}}$ with $m-1$ of its rows. Call this new $(m-1)$-by-$(n-1)$ matrix $M_{\text{res}}^{\{i\}}$, and further we may assume that rank $M_{\text{res}}^{\{i\}} = m-1$. Denote the analogous restriction of the vector $b - M(x_i e_i)$ as $b_{\text{res}} - M(x_i e_i)_{\text{res}}$. Then by the induction hypothesis as applied to $M_{\text{res}}^{\{i\}}$, there is some $y^{\{i\}} \in \mathbb{Z}_{>0}^{n-1}$ for which $M_{\text{res}}^{\{i\}}y^{\{i\}} = b_{\text{res}} - M(x_i e_i)_{\text{res}}$ and

$$
\begin{aligned}
\|y^{\{i\}}\|_\infty &\leqslant (n-m)(n^{m-1} m^{m-1} K_1^{2m-2} + m^{m-1} K_1^{m-1}) + m^{m-1} K_1^{m-2} \\
&\quad (n^{m-1} K_1^m + K_1 + K_2) \\
&\leqslant (n-m)(n^m m^m K_1^{2m} + m^m K_1^m) + m^m K_1^{m-1} K_2
\end{aligned}
$$

since $m \geqslant 2$, thus completing the induction as above. $\qquad\square$

Corollary 6.3 *Let $M = (\mu_{ij})_{i \leqslant m, \, j \leqslant n}$ be an m-by-n matrix with integer coefficients, and let $b \in \mathbb{Z}^m$. Suppose that $\max_{i,j} |\mu_{ij}| \leqslant K_1$ and $\|b\|_\infty \leqslant K_2$ (where we choose $K_1, K_2 \geqslant 1$), and suppose that there is some $x \in \mathbb{Z}_{>0}^n$ for which $Mx = b$. Then we may find $y \in \mathbb{Z}_{>0}^n$ for which $My = b$ and*

$$\|y\|_\infty \leqslant 2n^{m+1} m^m K_1^{2m} + m^m K_1^{m-1} K_2.$$

Proof We restrict M to a maximal linearly independent subset of its rows and so obtain an m'-by-n matrix M' with rank $M' = m' \leqslant n$. The result follows by applying Lemma 6.2 to M'. □

We introduce a partial ordering $<_{\text{unif}}$ on $\mathbb{Z}^d$ by saying that $x \leqslant_{\text{unif}} y$ if $x_i \leqslant y_i$ for all $i \leqslant d$ (that is, $y - x \in \mathbb{Z}^d_{\geqslant 0}$ as in the Mann–Dickson lemma). The next lemma controls the set of minimal solutions (with respect to the partial ordering $<_{\text{unif}}$) to a certain kind of linear equation.

Lemma 6.4 *Let $n = n_1 + n_2 \geqslant 2$ with $n_1, n_2 \in \mathbb{Z}_{>0}$. Let $M = (\mu_{ij})_{i \leqslant m, \, j \leqslant n}$ be an m-by-n matrix with integer coefficients, and $b \in \mathbb{Z}^m$. Suppose that $\max_{i,j} |\mu_{ij}| \leqslant K_1$ and $\|b\|_\infty \leqslant K_2$ (where we choose $K_1, K_2 \geqslant 1$). Let*

$$S = S(M, b, n_1, n_2) = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^{n_1}_{>0} \times \mathbb{Z}^{n_2}_{>0} : M \begin{pmatrix} x \\ y \end{pmatrix} = b \right\},$$

and let $S_{\min} = S_{\min}(M, b, n_1, n_2)$ be defined as

$$S_{\min} = \left\{ x \in \mathbb{Z}^{n_1}_{>0} : \exists y \in \mathbb{Z}^{n_2}_{>0} \text{ with } \begin{pmatrix} x \\ y \end{pmatrix} \in S \text{ and } \nexists \begin{pmatrix} x_* \\ y_* \end{pmatrix} \in S \text{ with } x_* <_{\text{unif}} x \right\}.$$

If $x_{\min} \in S_{\min}$ then

$$\|x_{\min}\|_\infty \leqslant 2^{2n} m^{mn} K_1^{m(n+3)} n^{m+1} + 2^n m^{mn} K_1^{mn} K_2.$$

Proof We use induction on n_1. If S is empty then Lemma 6.4 is vacuously true. Otherwise S is non-empty and so is $S_{\min}$.

If $n_1 = 1$ then $S \subset \mathbb{Z}_{>0}$ so $|S_{\min}| = 1$ by the well-ordering principle. Writing $S_{\min} = \{x_{\min}\}$ we note that there exists $\binom{x}{y} \in S$ by Corollary 6.3 with $x \leqslant 2n^{m+1} m^m K_1^{2m} + m^m K_1^{m-1} K_2$, and so $x_{\min} \leqslant x \leqslant 2n^{m+1} m^m K_1^{2m} + m^m K_1^{m-1} K_2$.

If $n_1 \geqslant 2$ let $x_{\min} \in S_{\min}$ and choose $y \in \mathbb{Z}^{n_2}_{>0}$ with $\binom{x_{\min}}{y} \in S$. By Corollary 6.3 we may choose $\binom{x_*}{y_*} \in S$ with $\|x_*\|_\infty \leqslant 2n^{m+1} m^m K_1^{2m} + m^m K_1^{m-1} K_2$. Thus there is some $i \leqslant n_1$ for which

$$|x_{\min,i}| \leqslant 2n^{m+1} m^m K_1^{2m} + m^m K_1^{m-1} K_2,$$

as otherwise $x_* <_{\text{unif}} x_{\min}$, in contradiction to the fact that $x_{\min} \in S_{\min}$. Fixing such a coordinate i, as in the proof of Lemma 6.2 we let $x_{\min}^{\{i\}}$ denote the vector $x_{\min}$ with the ith coordinate removed, and let $M^{\{i\}}$ be the matrix M but with the ith column removed (from the initial set of n_1 columns). Then

$$M^{\{i\}} \begin{pmatrix} x_{\min}^{\{i\}} \\ y \end{pmatrix} = b - M \begin{pmatrix} x_{\min,i} e_i \\ 0 \end{pmatrix},$$

where e_i is the ith basis vector in $\mathbb{R}^{n_1}$. We have

$$\|b - M((x_{\min,i}e_i, 0)^T)\|_\infty \leqslant K_2 + K_1|x_{\min,i}|$$
$$\leqslant K_2 + K_1(2n^{m+1}m^m K_1^{2m} + m^m K_1^{m-1} K_2)$$
$$= 2n^{m+1}m^m K_1^{2m+1} + (m^m K_1^m + 1)K_2$$
$$\leqslant 2n^{m+1}m^m K_1^{2m+1} + 2m^m K_1^m K_2.$$

The vector $x_{\min}^{\{i\}} \in \mathbb{Z}_{>0}^{n_1-1}$ is in $S_{\min}(M^{\{i\}}, b - M(\begin{smallmatrix} x_{\min,i}e_i \\ 0 \end{smallmatrix}), n_1 - 1, n_2)$. Indeed, were there another vector $(w, z)^T \in \mathbb{Z}_{>0}^{n_1-1} \times \mathbb{Z}_{>0}^{n_2}$ with $(w, z)^T \in S(M^{\{i\}}, b - M(\begin{smallmatrix} x_{\min,i}e_i \\ 0 \end{smallmatrix}), n_1 - 1, n_2)$ and $w <_{\text{unif}} x_{\min}^{\{i\}}$, then $w + x_i e_i <_{\text{unif}} x_{\min}$ and $(\begin{smallmatrix} w + x_{\min,i}e_i \\ z \end{smallmatrix}) \in S(M, b, n_1, n_2)$, contradicting the minimality of $x_{\min}$. (We have abused notation here by treating w as both an element of $\mathbb{Z}_{>0}^{n-1}$ and, by extending by 0, an element of $\mathbb{Z}_{\geqslant 0}^n$.) So by the induction hypothesis we have

$$\|x_{\min}^{\{i\}}\|_\infty$$
$$\leqslant 2^{2(n-1)}m^{m(n-1)}K_1^{m(n+2)}n^{m+1} + 2^{n-1}m^{m(n-1)}K_1^{m(n-1)}(2n^{m+1}m^m K_1^{2m+1} + 2m^m K_1^m K_2)$$
$$\leqslant 2^{2n}m^{mn}K_1^{m(n+3)}n^{m+1} + 2^n m^{mn}K_1^{mn}K_2.$$

So

$$\|x_{\min}\|_\infty = \max(\|x_{\min}^{\{i\}}\|_\infty, |x_{\min,i}|) \leqslant 2^{2n}m^{mn}K_1^{m(n+3)}n^{m+1} + 2^n m^{mn}K_1^{mn}K_2$$

too, and the induction is completed.   □

We are now ready to prove an effective version of Khovanskii's theorem. Our method is a quantitative adaptation of Nathanson–Ruzsa's argument from [12].

Proof of Theorem 1.1 Without loss of generality, we may first translate A (which preserves the width $w(A)$) so that $0 \in A$. Therefore we can assume that $\max_{a \in A} \|a\|_\infty \leqslant w(A)$. We can also assume that $A - A$ contains d linearly independent vectors: If not we can project the question down to a smaller dimension (by removing some coordinate but keeping all the linear dependencies) and the result follows by induction on d. So $|A| =: \ell \geqslant d + 1$.

Let us now recall the lexicographic ordering on $\mathbb{Z}^d$. If $x = (x_1, \ldots, x_d)^T \in \mathbb{Z}^d$ and $y = (y_1, \ldots, y_d)^T \in \mathbb{Z}^d$ we say that $x <_{\text{lex}} y$ if there exists some $i \leqslant d$ for which $x_i < y_i$ and $x_j = y_j$ for all $j < i$. This is a total ordering on $\mathbb{Z}^d$.

Following Nathanson–Ruzsa, we say that an element $x \in \mathbb{Z}_{\geqslant 0}^\ell$ is *useless* if there exists $y \in \mathbb{Z}_{\geqslant 0}^\ell$ with $y <_{\text{lex}} x$, $\|y\|_1 = \|x\|_1$ and $\sum_{i \leqslant \ell} x_j a_j = \sum_{j \leqslant \ell} y_j a_j$. We say that element $x \in \mathbb{Z}_{\geqslant 0}^\ell$ is *minimally useless* if there does not exist a useless $x' \in \mathbb{Z}_{\geqslant 0}^\ell$ for which $x' <_{\text{unif}} x$. Let U denote the set of useless elements and $U_{\min}$ be the set of minimally useless elements. By definition see that

$$U = \bigcup_{u \in U_{\min}} \{x \in \mathbb{Z}_{\geqslant 0}^\ell : x \geqslant_{\text{unif}} u\}.$$

For $x \in U_{\min}$, let $I_1 = \{i \leqslant \ell : x_i \geqslant 1\}$ and $I_2 = \{j \leqslant \ell : y_j \geqslant 1\}$ (with y as above). Now $I_1 \cap I_2 = \emptyset$ else if $i \in I_1 \cap I_2$ then $x - e_i$ is also useless (via $y - e_i$) contradicting minimality. We may assume that both I_1 and I_2 are non-empty, since otherwise we would have $x = y = 0$. Evidently $\min I_1 < \min I_2$ as $y <_{\text{lex}} x$.

By the Mann–Dickson lemma we know that $U_{\min}$ is finite, but now we will be able to get an explicit bound on $\max(\|u\|_\infty : u \in U_{\min})$:

Fix a pair of disjoint non-empty subsets $I_1 \cup I_2 \subset \{1, \ldots, \ell\}$ with $\min I_1 < \min I_2$, and let $n_1 = |I_1|$, $n_2 = |I_2|$, with $n = n_1 + n_2 \leqslant \ell$. We define a $(d+1)$-by-n matrix M where the columns are indexed by the elements of $I_1 \cup I_2$, and the row numbers run from 0 to d. If $j \in I_1$ then $M_{0,j} = 1$ and $M_{i,j} = (a_j)_i$ for $1 \leqslant i \leqslant d$; if $j \in I_2$ then $M_{0,j} = -1$ and $M_{i,j} = -(a_j)_i$ for $1 \leqslant i \leqslant d$. Then the top row of the equation $M\binom{x}{y} = 0$ with $x \in \mathbb{Z}_{>0}^{n_1}$ and $y \in \mathbb{Z}_{>0}^{n_2}$ gives that $\|y\|_1 = \|x\|_1$ and the ith row yields that $\sum_{j \leqslant \ell} x_j (a_j)_i = \sum_{j \leqslant \ell} y_j (a_j)_i$ for $1 \leqslant i \leqslant d$, so together they yield that $\sum_{j \leqslant \ell} x_j a_j = \sum_{j \leqslant \ell} y_j a_j$.

By the minimality of x there cannot exist $(x_*, y_*) \in \mathbb{Z}_{>0}^{n_1} \times \mathbb{Z}_{>0}^{n_2}$ such that $M\binom{x_*}{y_*} = 0$ and $x_* <_{\text{unif}} x$. Indeed, by construction of I_1 and I_2 we would have (after extending by zeros) that $y_* <_{\text{lex}} x_*$, thus implying that x_* is useless—contradicting the fact that x is minimally useless.

Using Lemma 6.4, as applied to the matrix M with $K_1 = \max_{a \in A} \|a\|_\infty := K$ and $K_2 = 1$, we conclude that

$$\|x\|_\infty \leqslant 2^{2\ell}(d+1)^{\ell(d+1)}\ell^{d+2}K^{(d+1)(\ell+3)} + 2^\ell(d+1)^{\ell(d+1)}K^{\ell(d+1)}$$
$$\leqslant 2^{2\ell+1}(d+1)^{\ell(d+1)}\ell^{d+2}K^{(d+1)(\ell+3)}$$

In [12, Lemma 1], Nathanson and Ruzsa proved that for all $U' \subset U_{\min}$

$$B(N, U') := |\{x \in \mathbb{Z}_{\geqslant 0}^s : \|x\|_1 = N, \ x \geqslant_{\text{unif}} u \text{ for all } u \in U'\}|$$

is equal to a fixed polynomial in N, once $N \geqslant \ell \max_{u \in U'} \|u\|_\infty$. Indeed, let $U' = \{u_1, \ldots, u_m\}$, where each $u_j = (u_{1,j}, u_{2,j}, \ldots, u_{s,j}) \in \mathbb{Z}_{\geqslant 0}^\ell$. Letting $u_i^* = \max_{j \leqslant m} u_{i,j}$, and $u^* = (u_1^*, u_2^*, \ldots, u_\ell^*)$, we have that

$$B(N, U') = |\{x \in \mathbb{Z}_{\geqslant 0}^\ell : \|x\|_1 = N, \ x \geqslant_{\text{unif}} u^*\}|$$
$$= |\{x \in \mathbb{Z}_{\geqslant 0}^\ell : \|x\|_1 = N - \|u^*\|_1\}|$$
$$= \binom{N - \|u^*\|_1 + \ell - 1}{\ell - 1}$$

provided $N \geqslant \|u^*\|_1$, which is a polynomial in N. Since $\|u^*\|_1 \leqslant \ell \max_{u \in U'} \|u\|_\infty$, our claim follows.

Then by inclusion-exclusion we have

$$|NA| = |\{x \in \mathbb{Z}_{\geqslant 0}^\ell : \|x\|_1 = N, \ x \text{ is not useless}\}|$$

$$= \sum_{U' \subset U_{\min}} (-1)^{|U'|} B(N, U')$$

which is a polynomial in N once $N \geqslant N_{\mathrm{Kh}}(A)$ where

$$N_{\mathrm{Kh}}(A) \leqslant 2^{2\ell+1}(d+1)^{\ell(d+1)} \ell^{d+3} K^{(d+1)(\ell+3)} \leqslant (2\ell w(A))^{(d+4)\ell},$$

as $K := \max_{a \in A} \|a\|_\infty \leqslant w(A)$. To obtain the last displayed inequality we assumed that $d \geqslant 2$ (as we use Lemma 2.1 for $d = 1$ which gives $N_{\mathrm{Kh}}(A) \leqslant w(A) - 1$), and $\ell \geqslant d + 1$.   □

7 Structure Bounds in the General Case: Proof of Theorem 1.3

We start by introducing the central structural result of this section. As a reminder, we say that $p \in \mathrm{ex}(H(A))$ if there is a vector $v \in \mathrm{span}(A - A) \setminus \{0\}$ and a constant c such that $\langle v, p \rangle = c$ and $\langle v, x \rangle > c$ for all $x \in H(A) \setminus \{p\}$.

Lemma 7.1 (Decomposing $\mathcal{P}(A)$) *Let $B \cup \{0\} \subset A \subset \mathbb{Z}^d$ with $|A| = \ell$ and B a non-empty linearly independent set. Suppose that $0 \in \mathrm{ex}(H(A))$. Let A^+ denote the set of $x \in \mathcal{P}(A) \cap C_B$ with the property that, for all $b \in B$, $x - b \notin \mathcal{P}(A) \cap C_B$. Then A^+ has the following two properties:*

$$C_B \cap \mathcal{P}(A) = A^+ + \mathcal{P}(B \cup \{0\}) \tag{7.1}$$

and

$$A^+ \subset NA$$

for some $N \leqslant N_0(A) := 2^{11d^2} d^{12d^6} \ell^{3d^2} w(A)^{8d^6}$.

Lemma 7.1 is straightforward for large N ((7.1) was already given in [5, Proposition 4]) but our focus is on getting an effective bound on such N.

The only other ingredient in the proof of Theorem 1.3 is the following classical lemma:

Lemma 7.2 (Carathéodory) *Let $A \subset \mathbb{R}^d$ be a finite set, and let $V := \mathrm{span}(A - A)$. If $\dim V = r$, then*

$$H(A) = \bigcup_{\substack{B \subset \mathrm{ex}(H(A)) \\ |B| = r+1 \\ \mathrm{span}(B-B) = V}} H(B).$$

Proof After an affine transformation one may assume that $V = \mathbb{R}^d$. Then see [5, Lemma 4] for the proof, in which the union is taken over all $B \subset A$ with $|B| = d + 1$ and $\mathrm{span}(B - B) = \mathbb{R}^d$. The equality as claimed, where $B \subset \mathrm{ex}(H(A))$, then follows from general fact that $H(A) = H(\mathrm{ex}(H(A))$ (see Lemma A.1).   □

Proof of Theorem 1.3 Let

$$v \in (NH(A) \cap (a_0 N + \Lambda_{A-A})) \setminus (\bigcup_{b \in \text{ex}(H(A))} (bN - \mathcal{E}(b - A))). \tag{7.2}$$

We will show that $v \in NA$ for all $N \geqslant (d + 1)N_0(A)$.

Let $V = \text{span}(A - A)$ and $r = \dim V$ as above. By Lemma 7.2 there exists a set $B \subset \text{ex}(H(A))$ with $|B| = r + 1$ such that $v \in NH(B^*)$ and $\text{span}(B - B) = V$. Write $B = \{b_0, b_1, \ldots, b_r\}$. Since $v \in NH(B)$ we can write $v = \sum_{i=0}^{r} c_i b_i$ for some real $c_i \geqslant 0$ such that $\sum_{i=0}^{r} c_i = N$. Since $N \geqslant (d + 1)N_0(A)$ there must be some $c_i \geqslant N_0(A)$. After permuting coordinates, we will assume that $c_r \geqslant N_0(A)$. Thus

$$b_r N - v = \sum_{i=0}^{r-1} c_i (b_r - b_i) \in (N - N_0(A)) \cdot H(b_r - B),$$

so that $b_r N - v \in C_{b_r - B} \subset C_{b_r - A}$. By the assumption (7.2) we also have $b_r N - v \notin \mathcal{E}(b_r - A)$ and $b_r N - v \in \Lambda_{b_r - A}$. Hence $b_r N - v \in \mathcal{P}(b_r - A)$. We may now apply Lemma 7.1 to the sets $b_r - A$ and $(b_r - B) \setminus \{0\}$; the hypotheses are satisfied since $b_r \in \text{ex}(H(A))$ implies $0 \in \text{ex}(H(b_r - A))$. Furthermore, $w(b_r - A) = w(A)$. We thus obtain

$$b_r N - v \in C_{b_r - B} \cap \mathcal{P}(b_r - A) = A^+ + \mathcal{P}(b_r - B^*)$$

for some set $A^+ \subset C_{b_r - B} \cap \mathcal{P}(b_r - A)$ with $A^+ \subset N_0(A)(b_r - A)$.

Now let us write

$$b_r N - v = u + w,$$

with $u \in A^+$ and $w \in \mathcal{P}(b_r - B)$. Thus $u + w = \sum_{i=0}^{r-1} c_i (b_r - b_i)$, with $c_i \in \mathbb{R}_{\geqslant 0}$ for all i and $\sum_{i=0}^{r-1} c_i \leqslant N - N_0(A)$. Expressing u and w with respect to the basis $(b_r - B) \setminus \{0\}$, and noting that $u \in A^+ \subset C_{b_r - B} \cap N_0(A)(b_r - A)$, we infer that $w = \sum_{i=0}^{r-1} \gamma_i (b_r - b_i)$ with $\gamma_i \leqslant c_i$ and $\gamma_i \in \mathbb{Z}_{\geqslant 0}$ for all i. Hence $w \in (N - N_0(A))(b_r - B)$.

Putting everything together we have

$$b_r N - v = u + w \in N_0(A)(b_r - A) + (N - N_0(A))(b_r - B)$$
$$\subset N_0(A)(b_r - A) + (N - N_0(A))(b_r - A) = N(b_r - A).$$

Hence $v \in NA$ as required.

The proof shows that $N_{\text{Str}}(A) \leqslant (d+1)N_0(A) = (d+1)2^{11d^2} d^{12d^6} \ell^{3d^2} w(A)^{8d^6} \leqslant (d\ell \, w(A))^{13d^6}$ as we may take $d \geqslant 2$ (after Lemma 2.1). □

It remains to prove Lemma 7.1. The condition $x \in \mathcal{P}(A) \cap C_B$ but $x - b \notin \mathcal{P}(A) \cap C_B$ in the definition of A^+ is a minimality-type condition on x.[7] As our argument for

---

[7] In fact this intuition can be phrased precisely: viewing $\mathcal{P}(A) \cap C_B$ as a poset P, where $x \leqslant_P y$ if $y - x \in \mathcal{P}(B) \cup \{0\}$, the set A^+ is exactly the minimal elements of this poset.

analysing the set A^+ will not stay within C_B, it turns out to be convenient to separate the $\mathcal{P}(A)$ part and the C_B part of this condition; this motivates the following definition.

Definition 7.3 (Absolutely B-minimal) Let $B \cup \{0\} \subset A \subset \mathbb{Z}^d$, with A finite. We say that $u \in \mathcal{P}(A)$ is *absolutely B-minimal* with respect to A if $u - b \notin \mathcal{P}(A)$ for all $b \in B$. Let $\mathcal{S}_{\text{abs}}(A, B)$ denote the set of absolutely B-minimal elements.

Let $\mathcal{S}_{\text{abs}}(A, \emptyset) = \mathcal{P}(A)$ and use the convention that $C_\emptyset = \{0\}$. By this definition $\mathcal{S}_{\text{abs}}(A, B) \subset \mathcal{S}(A, B)$, though these sets needn't be equal, so being a B-minimal element is a weaker condition than being an absolutely B-minimal element.

For a subset $U \subset \mathbb{R}^d$ and $x \in \mathbb{R}^d$, we define

$$\text{dist}(x, U) := \inf_{u \in U} \|x - u\|_\infty.$$

Lemma 7.4 (Controlling the absolutely B-minimal elements) *Let $B \cup \{0\} \subset A \subset \mathbb{Z}^d$ with $|A| = \ell \geqslant 2$, and assume that B is a (possibly empty) linearly independent set. Let $r := \dim \text{span}(A)$ and suppose that $0 \in \text{ex}(H(A))$. If $x \in \mathcal{S}_{\text{abs}}(A, B)$ and $\text{dist}(x, C_B) \leqslant X$ then $x \in NA$ for some $N \in \mathbb{Z}_{>0}$ with*

$$N \leqslant (X + 1) 2^{10dr} d^{11d^5r} \ell^{3dr} w(A)^{7d^5r}.$$

Lemma 7.4 is the main technical result of this section. The hypotheses allow r to be less than d, even though we will only apply the lemma when $r = d$, since our proof involves induction on r. Similarly, we do not assume that $\Lambda_A = \mathbb{Z}^d \cap \text{span}(A)$, as this property would not necessarily be preserved by the induction step. Deducing Lemma 7.1 is straightforward:

Proof of Lemma 7.1 If $x \in A^+$ then we can partition $B = B' \cup B''$ so that $b' \in B'$ implies $x - b' \notin C_B$ and $b'' \in B''$ implies $x - b'' \in C_B \setminus \mathcal{P}(A)$.

Writing x with respect to the basis B, we get

$$x = \ell + \sum_{b'' \in B''} c_{b''} b'' \quad \text{where} \quad \ell = \sum_{b' \in B'} \ell_{b'} b'$$

with $c_{b''} \geqslant 1$ for all $b'' \in B''$ and $\ell_{b'} \in [0, 1)$ for all $b' \in B'$.

Since $\|\ell\|_\infty \leqslant dw(A)$, this implies that $\text{dist}(x, C_{B''}) \leqslant dw(A)$. Furthermore, for all $b'' \in B''$ we have $x - b'' \notin \mathcal{P}(A)$. Hence $x \in \mathcal{S}_{\text{abs}}(A, B'')$. By Lemma 7.4 as applied to B'' and $X = dw(A)$, we may conclude that $x \in NA$ for $N \geqslant N_0(A)$ as in Lemma 7.1.

To establish (7.1), note that $A^+ + \mathcal{P}(B \cup \{0\}) \subset \mathcal{P}(A) \cap C_B$ by definition. On the other hand if $y \in \mathcal{P}(A) \cap C_B$ and there exists some $b_1 \in B$ with $y - b_1 \in \mathcal{P}(A) \cap C_B$ then we replace y by $y - b_1$. We repeat this with $b_2, \ldots$ until the process terminates, which it must do since the sum of the coefficients of y with respect to the basis B decreases by 1 at each step. We are left with $y - b_1 - \cdots - b_k \in A^+$ so that $y \in A^+ + \mathcal{P}(B \cup \{0\})$. $\qquad\square$

It remains is to prove Lemma 7.4. Following the proofs in [3, 6] we now show that in certain favourable circumstances, $\mathcal{S}_{\text{abs}}(A, B)$ may be controlled in terms of the Davenport constant of $\mathbb{Z}^d/\Lambda_B$. However this is not used in our proof of Lemma 7.4 (except when $d = 1$) but, for reasons of motivation, it is helpful to understand why this type of argument fails.

Lemma 7.5 *Let $B \cup \{0\} \subset A \subset \mathbb{Z}^d$, with A finite and B a basis of $\mathbb{R}^d$. Suppose that $C_A = C_B$. Let $\mathbb{Z}^d/\Lambda_B := G$. Then $\mathcal{S}_{\text{abs}}(A, B) \subset NA$, where $N = \max(1, D(G)-1)$ and $D(G)$ is the Davenport constant of G.*

Proof Let $x \in \mathcal{S}_{\text{abs}}(A, B)$, and assume that $x \neq 0$. Then write

$$x = a_1 + a_2 + \cdots + a_{N_A(x)}$$

for some $a_i \in A$. If there were a subsum $\sum_{i \in I} a_i \equiv 0 \bmod \Lambda_B$, then since $C_A = C_B$ we would have $\sum_{i \in I} a_i \in C_A \cap \Lambda_B \subset C_B \cap \Lambda_B$. But since B is a basis of $\mathbb{R}^d$ we have $C_B \cap \Lambda_B = \mathcal{P}(B) \cup \{0\}$, so $\sum_{i \in I} a_i \in \mathcal{P}(B) \cup \{0\}$. By minimality of $N_A(x)$ we also have $\sum_{i \in I} a_i \neq 0$. Therefore $x \in \mathcal{P}(A) + y$ for some non-zero $y \in \mathcal{P}(B)$, contrary to the assumption that $x \in \mathcal{S}_{\text{abs}}(A, B)$. Hence $N_A(x) \leqslant \max(1, D(G) - 1)$, which also takes care of the $x = 0$ case. $\square$

If C_B is a strict subset of C_A then the above argument doesn't necessarily work, as $\sum_{i \in I} a_i \equiv 0 \bmod \Lambda_B$ does not automatically imply that $\sum_{i \in I} a_i \in \mathcal{P}(B) \cup \{0\}$: Indeed the key issue is how an element $a_1 + \cdots + a_N = x \in \mathcal{P}(A) \cap C_B$ can have partial sums $\sum_{i \in I} a_i \notin C_B$.

Sketch of Our Proof of Lemma 7.4

The easy cases are $r = 1$ (which follows from any of the existing literature [5, 6, 11, 14], or from Lemma 7.5) and $B = \emptyset$ (which is dealt with in Lemma 7.11 below). From these base cases, we will construct a proof by induction on r. We may assume, therefore, that $r \geqslant 2$ and B is non-empty. For this sketch, we will also assume that $r = d$. There are three main phases to the induction step.

• We provide an extra restriction on the region of $\mathbb{R}^d$ where $\mathcal{S}_{\text{abs}}(A, B)$ can lie, by showing that if $x \in \mathcal{S}_{\text{abs}}(A, B)$ then $\text{dist}(x, \partial(C_A)) \leqslant Y$, where $\partial(C_A)$ is the topological boundary of C_A and Y is some explicit bound.[8] The bound $\text{dist}(x, \partial(C_A)) \leqslant Y$ is a generalisation of a basic result from the one dimensional case—the classical 'Frobenius postage stamp' problem—in which the boundary of C_A is just $\{0\}$ and one shows that the exceptional set $\mathcal{E}(A)$ is finite. Since $\partial(C_A)$ is a union of $d - 1$ dimensional facets, there is some non-zero linear map $\alpha : \mathbb{R}^d \longrightarrow \mathbb{R}$ for which $\text{dist}(x, \ker \alpha) \leqslant Y$.

• We combine the distance condition from above with the hypotheses of Lemma 7.4, giving $\text{dist}(x, C_B) \leqslant X$ and $\text{dist}(x, \ker \alpha) \leqslant Y$. In turn, we show that this implies $\text{dist}(x, C_B \cap \ker \alpha) \leqslant f(X, Y, A)$ (for some explicit function $f(X, Y, A)$), by a quantitative linear algebra argument. For this part, one should have in mind the

---

[8] If $r \leqslant d - 1$ then one cannot use the topological boundary here, since $\partial(C_A) = C_A$ in this case, but this issue may be circumvented.

situation of two rays, both starting from the origin. If x is in a neighbourhood of both rays separately, then x will be in some neighbourhood of the origin. The size of this neighbourhood will be determined by the angle between the rays (the smaller the angle, the larger the neighbourhood). To study the general dimension version of this phenomenon we avoid talking explicitly about angles, relying instead on the existence of suitable bases of vectors with integer coordinates.

Defining $B' = B \cap \ker \alpha$ then $C_{B'} = C_B \cap \ker \alpha$, and so we establish that $\mathrm{dist}(x, C_{B'}) \leqslant f(X, Y, A)$.

• Let $A' = A \cap \ker \alpha$. If x is expressed as a sum $a_1 + \cdots + a_N$ with $a_i \in A$ for all i then only finitely many of the a_i are in $A \setminus A'$. This is because $\alpha(x)$ is bounded, by the assumption $\mathrm{dist}(x, \ker \alpha) \leqslant Y$, and $\alpha(a) > 0$ for all $a \in A \setminus A'$, since $\ker \alpha$ is a separating hyperplane for $H(A)$.

Now let x' be the subsum of $a_1 + \cdots + a_N$ coming just from those $a_i \in A'$. One still has an upper bound on $\mathrm{dist}(x', C_{B'})$, since $\|x - x'\|_\infty$ is bounded. One may also show that $x' \in \mathcal{S}_{\mathrm{abs}}(A', B')$. However, $\dim \mathrm{span}(A') = \dim \ker \alpha = d - 1 < r$, so by applying the induction hypothesis we conclude that $x' \in N'A'$ for some explicit N'. Adding on the elements of $A \setminus A'$, of which there are boundedly many, we end up with $x \in NA$ for some other explicit N.

Phase 1: Quantitative Details

We will prove the following.

Lemma 7.6 (Interior points are representable) *Let $A \subset \mathbb{Z}^d$ be a finite set with $0 \in A$ and $|A| = \ell \geqslant 2$. There is a constant K_A such that if $x \in C_A \cap \Lambda_A$ and*

$$(x + [-K_A, K_A]^d) \cap \mathrm{span}(A) \subset C_A,$$

then $x \in \mathcal{P}(A)$. Moreover we may take

$$K_A = 4d^d \ell^{3d} w(A)^{3d}.$$

The proof will be a quantitative adaptation of an argument of Khovanskii from his original paper (Proposition 1 of [8], repeated as Lemma 1 of [9]).

Lemma 7.7 (Quantitative representation of basis elements) *Let $A \subset \mathbb{Z}^d$ be a finite set with $|A| = \ell \geqslant 2$ and $0 \in A$. If $u \in \Lambda_A$ then there exists $(n_a(u))_{a \in A} \in \mathbb{Z}^A$ for which $u = \sum_{a \in A} n_a(u)a$ and*

$$|n_a(u)| \leqslant 2d^d \ell^{d+1} w(A)^{2d} + d^d w(A)^{d-1} \|u\|_\infty$$

for all $a \in A$.

Proof We may assume that $u \neq 0$ else the result is trivial. Pick some $(x_a(u))_{a \in A} \in \mathbb{Z}^A$ for which $\sum_{a \in A} x_a(u)a = u$. Let $A' := \{a \in A : x_a(u) \neq 0\}$ and $\ell' = |A'|$. Let M be the d-by-ℓ' matrix M whose columns are the vectors $\mathrm{sign}(x_a(u))a$ for

$a \in A'$. The absolute values of the coefficients of M are all $\leqslant \max_{a \in A} \|a\|_\infty \leqslant w(A)$. Since $x'(u) := (|x_a(u)|)_{a \in A'} \in \mathbb{Z}_{>0}^{A'}$ satisfies $Mx'(u) = u$, we may apply Corollary 6.3 and conclude that there is some $y(u) \in \mathbb{Z}_{\geqslant 0}^{A'}$ for which $My(u) = u$ and $\|y\|_\infty \leqslant 2d^d(\ell')^{d+1}w(A)^{2d} + d^d w(A)^{d-1}\|u\|_\infty$. We have $u = \sum_{a \in A} n_a(u)a$ with $n_a(u) := \mathrm{sign}(x_a(u))y_a(u)$ for $a \in A'$, and $n_a(u) := 0$ otherwise. □

Proof of Lemma 7.6 Let

$$U = \{u \in \Lambda_A : u = \sum_{a \in A} c_a a \text{ with } c_a \in [0, 1) \text{ for all } a \in A\}.$$

From Lemma 7.7, we may write $u = \sum_{a \in A} n_a(u)a$ for coefficients $n_a(u) \in \mathbb{Z}$ satisfying

$$\begin{aligned}
|n_a(u)| &\leqslant 2d^d \ell^{d+1} w(A)^{2d} + d^d w(A)^{d-1}\|u\|_\infty \\
&\leqslant 2d^d \ell^{d+1} w(A)^{2d} + d^d \ell w(A)^d \\
&\leqslant 3d^d \ell^{d+1} w(A)^{2d}
\end{aligned}$$

since $\|u\|_\infty \leqslant \ell w(A)$. We let

$$D = 1 + \max_{\substack{u \in U \\ a \in A}} |n_a(u)|,$$

and write $K_A := D\ell w(A)$.

Suppose that $x \in \Lambda_A \cap C_A$ with $(x + [-K_A, K_A]^d) \cap \mathrm{span}(A) \subset C_A$. By the construction of K_A, we have $x - D\sum_{a \in A} a \in C_A$. Therefore, we may write $x = \sum_{a \in A} \lambda_a a$ for some real coefficients λ_a which satisfy $\lambda_a \geqslant D$ for all a. Then consider

$$u := x - \sum_{a \in A} \lfloor \lambda_a \rfloor a.$$

We have $u \in U$, so writing $u = \sum_{a \in A} n_a(u)a$ we get $x = \sum_{a \in A}(\lfloor \lambda_a \rfloor + n_a(u))a$. Since $\lfloor \lambda_a \rfloor + n_a(u) \in \mathbb{Z}_{\geqslant 0}$ by the construction of D, this shows that $x \in \mathcal{P}(A)$, as required.

The bound on K_A follows from the bound $D \leqslant 4d^d \ell^{d+1} w(A)^{2d}$. □

We use a classical result due to Bombieri–Vaaler for the more complicated pieces of quantitative linear algebra to come:

Lemma 7.8 (Siegel's lemma, Theorem 2 of [1]) *With $n \geqslant m$ let M be an m-by-n matrix with integer entries. Then the equation $MX = 0$ has $n - m$ linearly independent integer solutions $X_j = (x_{j,1}, \cdots, x_{j,n}) \in \mathbb{Z}^n$ such that*

$$\prod_{j=1}^{n-m} \|X_j\|_\infty \leqslant D^{-1}\sqrt{\det(MM^T)},$$

where D is the greatest common divisor of the determinants of all the m-by-m minors of M.

Corollary 7.9 *With $n \geqslant m$ let M be an m-by-n matrix with integer entries. Let K be the maximum of the absolute values of the entries of M. Then the equation $MX = 0$ has $n - m$ linearly independent integer solutions $X_j = (x_{j,1}, \cdots, x_{j,n}) \in \mathbb{Z}^n$ such that*

$$\prod_{j=1}^{n-m} \|X_j\|_\infty \leqslant (m!)^{1/2} n^{m/2} K^m.$$

Proof In Lemma 7.8 we have $D \geqslant 1$ and, since the coefficients of MM^T are at most nK^2 in absolute value, we have $\det(MM^T) \leqslant m!(nK^2)^m$. $\square$

In our application, Lemma 7.6 will be combined with the following result. This uses Siegel's lemma to construct normal vectors to separating hyperplanes of C_A.

Lemma 7.10 (Finding a close point on the boundary) *Let $A \subset \mathbb{Z}^d$ with $0 \in A$, $|A| = \ell \geqslant 2$ and $r = \dim \operatorname{span}(A)$. Let $x \in C_A$, and suppose that there is some $y \in \operatorname{span}(A) \setminus C_A$ for which $\|x - y\|_\infty \leqslant D$. Then there are $r - 1$ linearly independent vectors $\{a_1, \ldots, a_{r-1}\} \subset A$, a vector $z \in \operatorname{span}(\{a_1, \ldots, a_{r-1}\})$ for which $\|x - z\|_\infty \leqslant D$, and a vector $v \in \mathbb{Z}^d \cap \operatorname{span}(A) \cap \operatorname{span}(\{a_1, \ldots, a_{r-1}\})^\perp$ for which*

(1) $\|v\|_\infty \leqslant d^{2d^2} w(A)^{d^2}$;
(2) $\langle v, w \rangle \geqslant 0$ *for all $w \in C_A$;*
(3) $\langle v, w \rangle > 0$ *for all $w \in C_A \setminus \operatorname{span}(\{a_1, \ldots, a_{r-1}\})$.*

Proof Since C_A is convex, we know there is some maximal $\rho \in (0, 1)$ for which

$$z := x + \rho(y - x) \in C_A.$$

Certainly $\|x - z\|_\infty \leqslant D$.

To prove the other properties, let $f : \mathbb{R}^d \longrightarrow \mathbb{R}^d$ be some linear isomorphism for which $f(\operatorname{span}(A)) = \mathbb{R}^r \times \{0\}^{d-r}$. Letting $A' = f(A)$ and $z' = f(z)$, we also have $f(C_A) = C_{A'}$. Abusing notation to neglect the final $d - r$ coordinates, we have $z' \in \partial(C_{A'})$ (since every neighbourhood of z contains a point in $\operatorname{span}(A) \setminus C_A$). The structure of $\partial(C_{A'})$ is well-understood from the theory of convex polytopes, which we recall in Appendix A below. Indeed, by Lemma A.2 there is some non-zero linear map $\alpha : \mathbb{R}^r \longrightarrow \mathbb{R}$ for which $z' \in \ker \alpha$ and $\alpha(a') \geqslant 0$ for all $a' \in A'$. Furthermore, $\ker \alpha$ is spanned by some linearly independent set $A'' \subset A'$ with $|A''| = r - 1$. Letting $\{a_1, \ldots, a_{r-1}\} = f^{-1}(A'')$, we have $z \in \operatorname{span}(\{a_1, \ldots, a_{r-1}\})$.

We finish by constructing v. By applying Corollary 7.9 to an r-by-d matrix whose rows are element of A that are a basis for $\operatorname{span}(A)$, we can construct a basis $X_1, \ldots, X_{d-r} \in \mathbb{Z}^d$ for $\operatorname{span}(A)^\perp$ with $\|X_i\|_\infty \leqslant d^d w(A)^d$ for all i. Noting that $(\operatorname{span}(A)^\perp)^\perp = \operatorname{span}(A)$, we then apply Corollary 7.9 again to the $(d - 1)$-by-d matrix whose first $r - 1$ rows consist of the vectors $a_1, \ldots, a_{r-1}$ and whose final

$d - r$ rows consist of the vectors $X_1, \ldots, X_{d-r}$; this gives a non-zero vector $v \in \mathbb{Z}^d \cap \mathrm{span}(A) \cap \mathrm{span}(\{a_1, \ldots, a_{r-1}\})^\perp$ with $\|v\|_\infty \leqslant d^d(d^d w(A)^d)^d \leqslant d^{2d^2} w(A)^{d^2}$.

Finally, let $\beta : \mathrm{span}(A) \longrightarrow \mathbb{R}$ denote the linear map $w \mapsto \langle v, w \rangle$. The kernel of β is exactly $\mathrm{span}(\{a_1, \ldots, a_{r-1}\})$ (since otherwise, writing $\mathbb{R}^d = \mathrm{span}(A) \oplus \mathrm{span}(A)^\perp$, we would get that all of $\mathbb{R}^d$ is orthogonal to v). Since the map $\beta_f : \mathbb{R}^r \longrightarrow \mathbb{R}$ given by $\beta_f(w') = \beta(f^{-1}(w'))$ is a linear map with $\ker \beta_f = \ker \alpha$, we conclude that $\beta_f = \lambda \alpha$ for some non-zero $\lambda \in \mathbb{R}$. By replacing v by $-v$ if necessary, we may assume that $\lambda > 0$. Therefore $\beta_f(w') \geqslant 0$ for all $w' \in C_{A'}$, and hence $\beta(w) \geqslant 0$ for all $w \in C_A$, as desired. $\qquad\square$

The next result deals with the $B = \emptyset$ case of Lemma 7.4. It is a generalisation to arbitrary dimension of a trivial observation from the one dimensional case, namely that if $A \subset \mathbb{Z}_{\geqslant 0}$ with $\min A = 0$, and if $v \in \mathcal{P}(A)$, then $v \in NA$ for all $N \geqslant v$.

Lemma 7.11 (Controlling small elements) *Let $A \subset \mathbb{Z}^d$ with $|A| = \ell \geqslant 2$ and $0 \in \mathrm{ex}(H(A))$. If $v \in \mathcal{P}(A) \setminus \{0\}$ and $N \geqslant 2d^{11d^3} \ell^d w(A)^{5d^3} \|v\|_\infty$ then $v \in NA$.*

Proof Suppose that $\dim \mathrm{span}(A) = r$. We start by constructing a linear isomorphism $f : \mathbb{R}^d \longrightarrow \mathbb{R}^d$ for which $f(A) \subset \mathbb{Z}^r \times \{0\}^{d-r}$. Indeed, if $r = d$ there is nothing to do. Otherwise, we take some elements $a_1, \ldots, a_r \in A$ which form a basis of $\mathrm{span}(A)$. Then, by applying Corollary 7.9 to the r-by-d matrix whose rows are given by the vectors a_i, we have vectors $v_{r+1}, \ldots, v_d \in \mathbb{Z}^d$ such that $\mathcal{B} := \{a_1, \ldots, a_r, v_{r+1}, \ldots, v_d\}$ is a basis for $\mathbb{R}^d$ and $\|v_i\|_\infty \leqslant d^d w(A)^d$ for each i.

Now let $M = (\mu_{i,j})_{i,j \leqslant d}$ denote the d-by-d matrix whose inverse M^{-1} has columns given by the vectors from $\mathcal{B}$. Thus M is the change of basis matrix that maps elements of $\mathcal{B}$ to the standard basis vectors of $\mathbb{R}^d$. By Cramer's rule, we see that

$$|\mu_{i,j}| \leqslant d^d(d^d w(A)^d)^d \leqslant d^{2d^2} w(A)^{d^2}.$$

Furthermore, $\mu_{i,j} \in \frac{1}{D}\mathbb{Z}$ where $D \in \mathbb{Z}$ with

$$|D| = \det(M^{-1}) \leqslant d^d(d^d w(A)^d)^d \leqslant d^{2d^2} w(A)^{d^2}.$$

Now let f be the linear map given by matrix DM, and let $A' = f(A)$. Then $0 \in \mathrm{ex}(H(A'))$, $A' \subset \mathbb{Z}^r \times \{0\}^{d-r}$, $\mathrm{span}(A') = \mathbb{R}^r \times \{0\}^{d-r}$ and

$$w(A') \leqslant d^{4d^2} w(A)^{2d^2+1} \leqslant d^{4d^2} w(A)^{3d^2}. \tag{7.3}$$

Henceforth we will abuse notation and consider A' as a subset of $\mathbb{Z}^r$.

We now make an appeal to facts about $C_{A'}$ and $\partial(C_{A'})$ which are laid out in Lemma A.2 below. In particular, we see that there is a collection of non-zero linear maps $\alpha_1, \ldots, \alpha_n : \mathbb{R}^r \longrightarrow \mathbb{R}$, with $n \leqslant 2r\ell^{r/2}$, for which

$$C_{A'} = \cap_{i \leqslant n} \{y \in \mathbb{R}^r : \alpha_i(y) \geqslant 0\} \tag{7.4}$$

and for which for each $i \leqslant n$ there exists a subset $A_i' \subset A' \cap \ker \alpha_i$ with $|A_i'| = r - 1$ and $\ker \alpha_i = \mathrm{span}(A_i')$. Therefore, using Corollary 7.9 on the $(r-1)$-by-r matrix

with rows given by the elements of A_i', without loss of generality we may assume the following: for all $i \leqslant n$, there exists a vector $x_i \in \mathbb{Z}^r \setminus \{0\}$ with $\|x_i\|_\infty \leqslant r^r w(A')^r$ such that for all $y \in \mathbb{R}^r$ we have $\alpha_i(y) = \langle x_i, y \rangle$. Indeed, by directly applying Corollary 7.9 we find a $z_i \in \mathbb{Z}^r \setminus \{0\}$ with $\|z_i\|_\infty \leqslant r^r w(A')^r$ that is orthogonal to $\ker \alpha_i$. Hence there is some $c_i \in \mathbb{R} \setminus \{0\}$ for which $\alpha_i(y) = c_i \langle z_i, y \rangle$ for all $y \in \mathbb{R}^r$. Then $|c_i|^{-1}\alpha_i(y) = \langle \text{sign}(c_i)z_i, y \rangle$, and without loss of generality we may rename $|c_i|^{-1}\alpha_i(y)$ as $\alpha_i(y)$ (as this preserves $C_{A'}$) and define $x_i := \text{sign}(c_i)z_i$.

We claim that for each $a' \in A' \setminus \{0\}$ there exists $i \leqslant n$ for which $\langle x_i, a' \rangle > 0$. Indeed, suppose for contradiction that there were some $a' \in A' \setminus \{0\}$ for which $\alpha_i(a') = 0$ for all i. By (7.4), this would mean that $\lambda a' \in C_{A'}$ for all $\lambda \in \mathbb{R}$. Yet $0 \in \text{ex}(H(A'))$, which means that there is a non-zero linear map $\beta : \mathbb{R}^r \longrightarrow \mathbb{R}$ for which $\beta(y) > 0$ for all $y \in C_{A'} \setminus \{0\}$. Taking $\lambda = \pm 1$ we would have both $\beta(a') > 0$ and $\beta(-a') > 0$, which gives the contradiction. Therefore for each $a' \in A' \setminus \{0\}$ we have $\langle a', \sum_{i \leqslant n} x_i \rangle > 0$, and since these are both integer vectors we have $\langle a', \sum_{i \leqslant n} x_i \rangle \geqslant 1$.

Now suppose that $v \in \mathcal{P}(A) \setminus \{0\}$. Then $f(v) \in \mathcal{P}(A') \setminus \{0\}$. Writing

$$f(v) = a_1' + \cdots + a_N'$$

with $a_i' \in A' \setminus \{0\}$, we get the inequality

$$N \leqslant \sum_{j \leqslant N} \sum_{i \leqslant n} \langle a_j', x_i \rangle = \langle f(v), \sum_{i \leqslant n} x_i \rangle$$
$$\leqslant d \|f(v)\|_\infty \Big(\sum_{i \leqslant n} \|x_i\|_\infty \Big) \leqslant \|f(v)\|_\infty 2\ell^{r/2} r^{r+2} w(A')^r.$$

Since $\|f(v)\|_\infty \leqslant d^{4d^2} w(A)^{2d^2} \|v\|_\infty$, by using the bound on $w(A')$ from (7.3) we derive

$$N \leqslant \|v\|_\infty 2d^{4d^2 + 4rd^2} w(A)^{2d^2 + 3rd^2} \ell^{r/2} r^{r+2} \leqslant \|v\|_\infty 2d^{11d^3} \ell^d w(A)^{5d^3}.$$

Writing $v = \sum_{j \leqslant N} f^{-1}(a_j')$, we have $v \in NA$ as claimed.   □

This completes all the necessary preparation for the first phase of the induction step.

Phase 2: Quantitative details. We will prove the following.

Lemma 7.12 (Intersecting Cones) *Let $d, d_1, d_2 \in \mathbb{Z}$, with $d \geqslant 1$ and $0 \leqslant d_1, d_2 \leqslant d$. Let $B_1, B_2 \subset \mathbb{Z}^d$ be finite sets with $|B_i| = d_i$ for each i, and assume that B_1 is linearly independent and B_2 is linearly independent. Let $\max_{b \in B_1 \cup B_2} \|b\|_\infty \leqslant K$ (where $K \geqslant 1$). Let $x \in \mathbb{R}^d$ and suppose $\text{dist}(x, C_{B_1}) \leqslant X_1$ and $\text{dist}(x, C_{B_2}) \leqslant X_2$. Then*

$$\text{dist}(x, C_{B_1} \cap C_{B_2}) \leqslant (X_1 + X_2) 2^{2d} d^{10d^5} K^{4d^5}.$$

First we use Siegel's lemma to construct a basis of $\mathbb{R}^d$ with certain useful properties.

Lemma 7.13 (Basis for intersections) *Let $d, d_1, d_2 \in \mathbb{Z}_{>0}$ with $d_1, d_2 \leqslant d$. Let $B_1, B_2 \subset \mathbb{Z}^d$ be finite sets with $|B_i| = d_i$ for each i, and assume that B_1 is linearly independent and B_2 is linearly independent, and let $n := \dim(\mathrm{span}(B_1) \cap \mathrm{span}(B_2))$. Let $\max_{b \in B_1 \cup B_2} \|b\|_\infty \leqslant K$.*

Then there is a basis $V = \{v_1, \ldots, v_d\}$ for $\mathbb{R}^d$ such that:

(1) $v_i \in \mathbb{Z}^d$ for all i;
(2) $\{v_1, \ldots, v_n\}$ is a basis for $\mathrm{span}(B_1) \cap \mathrm{span}(B_2)$;
(3) $\{v_1, \ldots, v_{d_1}\}$ is a basis for $\mathrm{span}(B_1)$, and $\{v_{n+1}, \ldots v_{d_1}\} \subset B_1$;
(4) $\{v_1, \ldots, v_n, v_{d_1+1}, \ldots, v_{d_1+d_2-n}\}$ is a basis for $\mathrm{span}(B_2)$, and $\{v_{d_1+1}, \ldots, v_{d_1+d_2-n}\} \subset B_2$;
(5) $\|v_i\|_\infty \leqslant d^{3d^3} K^{d^3}$ for all i;

The requirement that $\{v_{n+1}, \ldots, v_{d_1}\} \subset B_1$ and $\{v_{d_1+1}, \ldots, v_{d_1+d_2-n}\} \subset B_2$ are not vital in the application to Lemma 7.12, but will be convenient at a certain point in that proof.

Proof First we use Corollary 7.9 (as applied to the d_1-by-d matrix whose rows consist of the elements of B_1) to construct a basis $\{X_1, \ldots, X_{d-d_1}\}$ for $B_1^\perp$ consisting of vectors $X_i \in \mathbb{Z}^d$ with $\|X_i\|_\infty \leqslant (d_1!)^{1/2} d^{d/2} K^d \leqslant d^d K^d$. We construct a basis $\{Y_1, \ldots, Y_{d-d_2}\}$ for $B_2^\perp$ in the same way.

Following this, we may construct a $(d - n)$-by-d matrix M whose rows are some elements of $\{X_1, \ldots, X_{d-d_1}, Y_1, \ldots, Y_{d-d_2}\}$, where we populate the rows by choosing some X_i or Y_j that is not in the linear span of the rows that we have chosen so far, until we can no longer do so. By construction the rows of M are a basis for $B_1^\perp + B_2^\perp$. Since $B_1^\perp + B_2^\perp = (\mathrm{span}(B_1) \cap \mathrm{span}(B_2))^\perp$ (by dimension counting), the rows of M are also a basis for $(\mathrm{span}(B_1) \cap \mathrm{span}(B_2))^\perp$. Therefore applying Corollary 7.9 to the matrix M we get a basis $\{v_1, \ldots, v_n\}$ for $\mathrm{span}(B_1) \cap \mathrm{span}(B_2)$ of vectors $v_i \in \mathbb{Z}^d$ which satisfy $\|v_i\|_\infty \leqslant (d!)^{1/2} d^{d/2} (d^d K^d)^d \leqslant d^{d^2+d} K^{d^2}$ for each i.

Now we complete $\{v_1, \ldots, v_n\}$ to a basis $\{v_1, \ldots, v_d\}$ for $\mathbb{R}^d$ with all the remaining properties. For $n + 1 \leqslant i \leqslant d_1$, we let v_i list some elements of B_1 that are not in $\mathrm{span}(\{v_1, \ldots, v_{i-1}\})$. Then for $d_1 + 1 \leqslant i \leqslant d_1 + d_2 - n$, we let v_i list some elements of B_2 that are not in $\mathrm{span}(\{v_1, \ldots, v_{i-1}\})$. By dimension counting, we have that $\{v_1, \ldots, v_{d_1}\}$ is a basis for B_1 and $\{v_1, \ldots, v_n, v_{d_1+1}, \ldots, v_{d_1+d_2-n}\}$ is a basis for B_2. We choose the remaining v_i to be integer vectors that are orthogonal to the set $\{v_j : j \leqslant d_1 + d_2 - n\}$. We can again use Corollary 7.9 to bound the norms of these v_i, ending up with

$$\|v_i\|_\infty \leqslant d!^{1/2} d^{d/2} (d^{d^2+d} K^{d^2})^d \leqslant d^{d^3+d^2+d} K^{d^3} \leqslant d^{3d^3} K^{d^3}.$$

This completes the lemma. $\square$

Proof of Lemma 7.12 The proof will be by induction on $d_1 + d_2$, with the induction hypothesis being that

$$\mathrm{dist}(x, C_{B_1} \cap C_{B_2}) \leqslant (X_1 + X_2) 2^{d_1+d_2} d^{5(d_1+d_2)d^4} K^{2(d_1+d_2)d^4}.$$

If some $d_i = 0$ then $C_{B_i} = \{0\}$ and we are done. From now on we assume that $d_1, d_2 \geqslant 1$. Since $\mathrm{dist}(x, C_{B_1}) \leqslant X_1$ we can write

$$x = y_1 + z_1$$

with $y_1 \in C_{B_1}$ and $\|z_1\|_\infty \leqslant X_1$, and similarly

$$x = y_2 + z_2$$

with $y_2 \in C_{B_2}$ and $\|z_2\|_\infty \leqslant X_2$. Let us emphasise that we cannot assume that $y_1, y_2 \in \mathbb{Z}^d$, nor do we currently have any control over the norms of y_1 or y_2. Both of these issues would pose difficulties were we try to induct upon the dimension d by restricting to the two-dimensional subspace $\mathrm{span}(\{y_1, y_2\})$.

Let $n := \dim(\mathrm{span}(B_1) \cap \mathrm{span}(B_2))$, and let $\{v_1, \ldots, v_d\}$ be a basis for $\mathbb{R}^d$ that satisfies all the properties in Lemma 7.13. Expanding with respect to this basis, we write

$$y_1 = \sum_{i \leqslant n} \alpha_i v_i + \sum_{n+1 \leqslant i \leqslant d_1} \beta_i v_i$$

and

$$y_2 = \sum_{i \leqslant n} \gamma_i v_i + \sum_{d_1+1 \leqslant i \leqslant d_1+d_2-n} \delta_i v_i,$$

for some coefficients $\alpha_i, \beta_i, \gamma_i, \delta_i$.

We know that $\|y_1 - y_2\|_\infty \leqslant X_1 + X_2$, and that $\{v_1, \ldots, v_d\}$ is a basis with integer coordinates and $\max_i \|v_i\|_\infty \leqslant d^{3d^3} K^{d^3}$. By Cramer's rule (or equivalently considering the change of basis matrix), we conclude that

$$\max_i(|\alpha_i - \gamma_i|, |\beta_i|, |\delta_i|) \leqslant (X_1 + X_2)d!(d^{3d^3} K^{d^3})^d \leqslant (X_1 + X_2)d^{4d^4} K^{d^4}.$$

This implies, taking

$$y_3 := \sum_{i \leqslant n} \alpha_i v_i,$$

that there exists some $y_3 \in \mathrm{span}(B_1) \cap \mathrm{span}(B_2)$ such that

$$\|x - y_3\|_\infty \leqslant \|z_1\|_\infty + \sum_{n+1 \leqslant i \leqslant d_1} |\beta_i| \|v_i\|_\infty \leqslant (X_1 + X_2)(d^{4d^4+1} K^{d^4+1} + 1)$$

$$\leqslant 2(X_1 + X_2)d^{5d^4} K^{2d^4},$$

since $v_i \in B_1$ for all i in the range $n + 1 \leqslant i \leqslant d_1$.

If $y_3 \in C_{B_1} \cap C_{B_2}$ then we are done directly from the bound on $\|x - y_3\|_\infty$. If not, let us assume without loss of generality that $y_3 \notin C_{B_1}$. The rest of the argument proceeds as follows. We know that $y_1 \in C_{B_1}$, but since $\|y_1 - y_3\|_\infty$ is bounded it follows that y_1 is nonetheless quite close to the boundary of C_{B_1}. Thus y_1 is close to $C_{B_1'}$, for some $B_1' \subsetneq B_1$. Hence x is close to $C_{B_1'}$ as well, and we may finish off by applying the induction hypothesis on the cones $C_{B_1'}$ and C_{B_2}.

We now proceed with the details. Expanding y_1 in terms of the basis B_1, one obtains the (unique) expression

$$y_1 = \sum_{b \in B_1} c_b b$$

with $c_b \geqslant 0$ for all $b \in B_1$. We then claim that there must exist a set $B' \subset B_1$, with $B' \neq \emptyset$, for which

$$c_b \leqslant (X_1 + X_2) d^{4d^4} K^{d^4+1}$$

for all $b \in B'$. Indeed, were this not the case then $c_b > (X_1 + X_2) d^{4d^4} K^{d^4+1}$ for all $b \in B_1$. Write

$$y_3 = y_1 - \sum_{n+1 \leqslant i \leqslant d_1} \beta_i v_i \tag{7.5}$$

and recall that $|\beta_i| \leqslant (X_1 + X_2) d^{4d^4} K^{d^4}$ and $v_i \in B_1$ for each i in the range $n + 1 \leqslant i \leqslant d_1$. Then expand both sides of (7.5) with respect to the basis B_1 of $\mathrm{span}(B_1)$. We get $y_3 = \sum_{b \in B_1} c_b' b$, where c_b' is either of the form c_b or $c_b - \beta_i$ for some i. In any case, $c_b' \geqslant 0$ for all $b \in B_1$. So $y \in C_{B_1}$, but this is in contradiction with the earlier assumption that $y_3 \notin C_{B_1}$.

With this set B', we conclude that

$$\mathrm{dist}(y_1, C_{B_1 \setminus B'}) \leqslant (X_1 + X_2) d^{4d^4+1} K^{d^4+1} \leqslant (X_1 + X_2) d^{5d^4} K^{2d^4},$$

and hence that

$$\mathrm{dist}(x, C_{B_1 \setminus B'}) \leqslant X_1 + (X_1 + X_2) d^{5d^4} K^{2d^4}.$$

Since $|B_1 \setminus B'| < d_1$, we can apply the induction hypothesis to conclude that

$$\mathrm{dist}(x, C_{B_1 \setminus B'} \cap C_{B_2}) \leqslant 2^{|B_1 \setminus B'|+d_2} (X_1 + X_2 + (X_1 + X_2) d^{5d^4} K^{2d^4})$$
$$d^{5(|B_1 \setminus B'|+d_2)d^4} K^{2(|B_1 \setminus B'|+d_2)d^4}$$
$$\leqslant (X_1 + X_2) 2^{d_1+d_2} d^{5(d_1+d_2)d^4} K^{2(d_1+d_2)d^4}.$$

Since $\mathrm{dist}(x, C_{B_1} \cap C_{B_2}) \leqslant \mathrm{dist}(x, C_{B_1 \setminus B'} \cap C_{B_2})$, this closes the induction and the lemma follows. $\qquad\square$

Now let us record the precise version that we will use.

Corollary 7.14 *Let $d, d_1, d_2 \in \mathbb{Z}_{>0}$ with $d_1, d_2 \leqslant d$, and let $K \geqslant 1$. Let $B_1 \subset \mathbb{Z}^d$ be a linearly independent set with $|B_1| = d_1$ and $\max_{b \in B} \|b\|_\infty \leqslant K$. Let $V \leqslant \mathbb{R}^d$ be a subspace of dimension d_2, with a basis of d_2 vectors $B_2 := \{v_1, \ldots, v_{d_2}\} \subset \mathbb{Z}^d \cap V$ satisfying $\|v_i\|_\infty \leqslant K$ for all i.*

Suppose $\mathrm{dist}(x, C_{B_1}) \leqslant X_1$ and $\mathrm{dist}(x, V) \leqslant X_2$. Then

$$\mathrm{dist}(x, C_{B_1} \cap V) \leqslant (X_1 + X_2) 2^{2d} d^{10d^5} K^{4d^5}.$$

Proof Since $\mathrm{dist}(x, V) \leqslant X_2$, by replacing some vectors v_i with $-v_i$ as necessary we may assume that $\mathrm{dist}(x, C_{B_2}) \leqslant X_2$. Then apply Lemma 7.12. $\square$

Having prepared both the first and second phase of the induction step, we may plough ahead and resolve Lemma 7.4. (The third phase will be dealt with in situ.)

Proof of Lemma 7.4 If $B = \emptyset$ then $\|x\|_\infty \leqslant X$ and we are done by Lemma 7.11, so we may assume that $|B| \geqslant 1$. We then proceed by induction on $r := \dim \mathrm{span}(A)$. The base case is $r = 1$. For an arbitrary non-negative real X, suppose $x \in S_{\mathrm{abs}}(A, B)$ with $\mathrm{dist}(x, C_B) \leqslant X$. Since $r = 1$, we have moreover $x \in S_{\mathrm{abs}}(A, B) \subset \mathcal{P}(A) \subset C_A = C_B$, and thus in fact $\mathrm{dist}(x, C_B) = 0$. Observe further that $\Lambda_A \cap C_A = v\mathbb{Z}_{\geqslant 0}$ for some non-zero vector $v \in \mathbb{Z}^d$. Taking the linear map $f : \mathrm{span}(A) \to \mathbb{R}$ for which $f(v) = 1$, let $A' = f(A)$, $B' = f(B)$, and $x' = f(x)$. Then $w(A') \leqslant w(A)$, $\Lambda_{A'} = \mathbb{Z}$, $x' \in S_{\mathrm{abs}}(A', B')$. Applying Lemma 7.5, we conclude that $x \in NA$ with $N \leqslant D(\mathbb{Z}/\Lambda_{B'}) \leqslant w(A') \leqslant w(A)$. This settles the base case.

From now on, we assume that $r \geqslant 2$ and $x \neq 0$. Our first task is to find a vector $y \in \mathrm{span}(A) \backslash C_A$ for which $\|x - y\|_\infty$ is bounded. Indeed, choosing some $b \in B$, since $x \in S_{\mathrm{abs}}(A, B)$ we have $x - b \notin \mathcal{P}(A)$. We know that $x \in C_A$, since $\mathcal{P}(A) \subset C_A$, and so if $x - b \notin C_A$ we let $y = x - b$ and then $\|x - y\|_\infty \leqslant w(A)$. Otherwise $x - b \in (\Lambda_A \cap C_A) \backslash \mathcal{P}(A) = \mathcal{E}(A)$. By Lemma 7.6, there is therefore some $y \in \mathrm{span}(A) \backslash C_A$ for which

$$\|x - b - y\|_\infty \leqslant 8d^d \ell^{3d} w(A)^{3d}.$$

Hence,

$$\|x - y\|_\infty \leqslant 8d^d \ell^{3d} w(A)^{3d} + w(A) \leqslant 16d^d \ell^{3d} w(A)^{3d}.$$

We now apply Lemma 7.10 to this pair x and y. This gives a linearly independent set $A_{\mathrm{bas}} \subset A$, with $|A_{\mathrm{bas}}| = r - 1$, and a vector $z \in \mathrm{span}(A_{\mathrm{bas}})$ for which $\|x - z\|_\infty \leqslant 16d^d \ell^{3d} w(A)^{3d}$. In particular

$$\mathrm{dist}(x, \mathrm{span}(A_{\mathrm{bas}})) \leqslant 16d^d \ell^{3d} w(A)^{3d}. \tag{7.6}$$

We also have a vector $v \in \mathbb{Z}^d \cap \mathrm{span}(A) \cap (\mathrm{span}(A_{\mathrm{bas}}))^\perp$ for which $\|v\|_\infty \leqslant d^{2d^2} w(A)^{d^2}$ and $\langle v, u \rangle \geqslant 0$ for all $u \in C_A$.

Phase one of the induction step is complete. We now begin the second phase, in which we show that $\mathrm{dist}(x, C_{B'})$ is bounded for some suitable $B' \subset B$. Indeed, since

$\operatorname{dist}(x, C_B) \leqslant X$, Corollary 7.14 implies that

$$\operatorname{dist}(x, C_B \cap \operatorname{span}(A_{\mathrm{bas}})) \leqslant (16d^d \ell^{3d} w(A)^{3d} + X) 2^{2d} d^{10d^5} w(A)^{4d^5}.$$

Let $B' = B \cap \operatorname{span}(A_{\mathrm{bas}})$. We then have $C_B \cap \operatorname{span}(A_{\mathrm{bas}}) = C_{B'}$. To justify this assertion, note that if $u \in C_B \cap \operatorname{span}(A_{\mathrm{bas}})$ we have $u = \sum_{b \in B} c_b b$ for some coefficients $c_b \geqslant 0$. But then

$$0 = \langle v, u \rangle = \sum_{b \in B} c_b \langle v, b \rangle = \sum_{b \in B \setminus B'} c_b \langle v, b \rangle$$

since $v \in \operatorname{span}(A_{\mathrm{bas}})^{\perp}$. As $\langle v, b \rangle > 0$ for all $b \in B \setminus B'$ we must have $c_b = 0$ for all $b \in B \setminus B'$. Hence $y \in C_{B'}$. (The reverse inclusion $C_{B'} \subset C_B \cap \operatorname{span}(A_{\mathrm{bas}})$ is immediate from definitions.) Therefore,

$$\operatorname{dist}(x, C_{B'}) \leqslant (16d^d \ell^{3d} w(A)^{3d} + X) 2^{2d} d^{10d^5} w(A)^{4d^5}. \tag{7.7}$$

Now we move onto the third phase of the induction step. Let $A' = A \cap \operatorname{span}(A_{\mathrm{bas}})$. We now collect a few facts about A' and about x. Firstly, if $a \in A \setminus A'$ then $\langle v, a \rangle > 0$, and thus $\langle v, a \rangle \geqslant 1$ as both v and a are in $\mathbb{Z}^d$. Next, letting x_0 be the orthogonal projection of x onto $\operatorname{span}(A_{\mathrm{bas}})$, we have

$$\langle v, x \rangle = \langle v, x - x_0 \rangle \leqslant d \|v\|_\infty \operatorname{dist}(x, \operatorname{span}(A_{\mathrm{bas}})).$$

Finally, since $x \neq 0$, we may write $x = a_1 + \cdots + a_N$ for some $a_i \in A \setminus (B \cup \{0\})$. Putting everything together we then have

$$|\{i \leqslant N : a_i \in A \setminus A'\}| \leqslant \sum_{i=1}^{N} \langle v, a_i \rangle = \langle v, x \rangle$$
$$\leqslant d \|v\|_\infty \operatorname{dist}(x, \operatorname{span}(A_{\mathrm{bas}}))$$
$$\leqslant 16 d^{4d^2} \ell^{3d} w(A)^{4d^2}. \tag{7.8}$$

Now define

$$x' := \sum_{i \leqslant N : a_i \in A'} a_i \in \mathcal{P}(A').$$

Then

$$\|x - x'\|_\infty \leqslant 16 d^{4d^2} \ell^{3d} w(A)^{4d^2 + 1} \leqslant 16 d^{4d^2} \ell^{3d} w(A)^{5d^2}, \tag{7.9}$$

and so

$$\mathrm{dist}(x', C_{B'}) \leqslant \mathrm{dist}(x, C_{B'}) + \|x - x'\|_\infty$$
$$\leqslant (16 d^d \ell^{3d} w(A)^{3d} + X) 2^{2d} d^{10d^5} w(A)^{4d^5} + 16 d^{4d^2} \ell^{3d} w(A)^{5d^2}$$
$$\leqslant (X+1) 2^{7d} d^{11d^5} \ell^{3d} w(A)^{7d^5}. \tag{7.10}$$

What's more, $x' \in \mathcal{S}_{\mathrm{abs}}(A', B')$. Indeed, $x' \in \mathcal{P}(A')$ by construction, and if $x' - b' \in \mathcal{P}(A')$ for some $b' \in B'$ then $x - b' \in \mathcal{P}(A)$, in contradiction to the assumption that $x \in \mathcal{S}_{\mathrm{abs}}(A, B)$.

We now apply the induction hypothesis to the sets A' and B', and to the element x'. The hypotheses are satisfied (taking $\mathrm{dist}(x', C_{B'})$ from (7.10)), since B' is linearly independent (though possibly empty), and $0 \in \mathrm{ex}(H(A'))$; this is since, if $V \cap \mathrm{span}(A)$ is a separating hyperplane for $H(A)$ with $V \cap H(A) = \{0\}$, then $V \cap \mathrm{span}(A')$ is a separating hyperplane for $H(A')$ with $V \cap H(A') = 0$.

So, $x' \in N'A'$ for some

$$N' \leqslant ((X+1) 2^{7d} d^{11d^5} \ell^{3d} w(A)^{7d^5} + 1) 2^{10d(r-1)} d^{11d^5(r-1)} \ell^{3d(r-1)} w(A)^{7d^5(r-1)}$$
$$\leqslant (X+1) 2^{10dr - 3d + 1} d^{11d^5 r} \ell^{3dr} w(A)^{7d^5 r}.$$

Finally, adding in the contribution from (7.8) from those $a \in A \setminus A'$, we deduce that $x \in NA$ for

$$N \leqslant (X+1) 2^{10dr - 3d + 1} d^{11d^5 r} \ell^{3dr} w(A)^{7d^5 r} + 16 d^{4d^2} \ell^{3d} w(A)^{4d^2}$$
$$\leqslant (X+1) 2^{10dr} d^{11d^5 r} \ell^{3dr} w(A)^{7d^5 r}$$

as $d \geqslant 2$. This completes the induction, and the lemma is proved. $\qquad\square$

So Lemma 7.4 is settled, and with it our main effective structure result, Theorem 1.3.

Appendix A. Convex Sets

In this appendix we collect together some standard facts about convex polytopes (i.e. convex hulls of finite subsets of Euclidean space). Our main references will be [2] and [15].

Lemma A.1 (Extremal points) *Let $A \subset \mathbb{R}^d$ be a finite set. Then $\mathrm{ex}(H(A)) \subset A$ and $H(A) = H(\mathrm{ex}(H(A))$.*

Proof This is [2, Theorem 7.2]. □

Lemma A.2 (Structure of $H(A)$) *Let $A \subset \mathbb{R}^d$ be a finite set with $|A| = \ell$, $0 \in \mathrm{ex}(H(A))$, and assume that $\mathrm{span}(A) = \mathbb{R}^d$. Then there is a finite collection of maps $\{\alpha_1, \ldots, \alpha_n\} \in (\mathbb{R}^d)^*$ and constants $\{c_1, \ldots, c_n\} \subset \mathbb{R}_{\leqslant 0}$ for which $n \leqslant 2d\ell^{d/2}$ and*

(1) $H(A) = \cap_{i \leqslant n}\{x \in \mathbb{R}^d : \alpha_i(x) \geqslant c_i\}$;
(2) $C_A = \cap_{i \leqslant n : c_i = 0}\{x \in \mathbb{R}^d : \alpha_i(x) \geqslant 0\}$;
(3) $\partial(C_A) = \cup_{i \leqslant n : c_i = 0}(\ker \alpha_i \cap C_A)$
(4) for all i such that $c_i = 0$, there exists a set $A_i \subset A \setminus \{0\}$ with $|A_i| = d - 1$ and $\mathrm{span}(A_i) = \ker \alpha_i$.

Proof Part (1) is the fundamental theorem of convex polytopes, given as [2, Theorem 9.2]. To prove Part (2), we note that $c_i \leqslant 0$ for all i, since $0 \in A \subset H(A)$. Then

$$C_A = \cup_{N \geqslant 1} NH(A) = \cup_{N \geqslant 1} \cap_{i \leqslant n} \{x \in \mathbb{R}^d : \alpha_i(x) \geqslant Nc_i\}$$
$$= \cap_{i \leqslant n : c_i = 0}\{x \in \mathbb{R}^d : \alpha_i(x) \geqslant 0\}$$

as claimed. Part (3) follows immediately from part (2) (see [2, Theorem 8.2 (a)]).

For Part (4) we appeal to [2, Theorem 8.2 (c)], assuming as we may that the expression $H(A) = \cap_{i \leqslant n}\{x \in \mathbb{R}^d : \alpha_i(x) \geqslant c_i\}$ is irreducible (i.e. the collection of maps $\{\alpha_1, \ldots, \alpha_n\}$ cannot be replaced with a proper subset). This result tells us that

$$\{x \in \mathbb{R}^d : \alpha_i(x) = c_i\} \cap H(A)$$

is a facet of $H(A)$, i.e. is a $d - 1$ dimensional face. Now, if F is a facet of $H(A)$, [2, Theorem 7.2] and [2, Theorem 7.3] imply that F is a polytope, $F = H(\mathrm{ex}(F))$, and $\mathrm{ex}(F) \subset \mathrm{ex}(H(A)) \subset A$. Therefore, if $c_i = 0$ we see that $\ker \alpha_i \subset \mathrm{span}(A \cap \ker \alpha_i)$. Since every spanning set contains a basis we may find the set A_i as claimed in (4).

Regarding the claim that $n \leqslant 2d\ell^{d/2}$, this bound follows from the celebrated Upper Bound Theorem of McMullen ([10], or [15, Theorem 8.23] of Ziegler's textbook), which gives a tight upper bound for the number of facets of a convex polytope. This is since the pair (α_i, c_i) is determined (up to scalar multiples) by the facet $F := \{x \in \mathbb{R}^d : \alpha_i(x) = c_i\} \cap H(A)$. However, one doesn't need the full strength of the Upper Bound Theorem to get the order-of-magnitude bound $2d\ell^{d/2}$; one could instead use the easier argument of Seidel [13], summarised in the remark before Sect. 8.5 of [15]. This bounds the number of facets by $2 \sum_{i \leqslant d/2} \binom{\ell}{d}$, which is trivially at most $2d\ell^{d/2}$. □

To aid the reader seeking the references in [2], we should say that [2] uses the symbol H differently; there, H denotes a hyperplane, whereas for us H is the convex hull.

References

1. Bombieri, E., Vaaler, J.: On Siegel's lemma. Invent. Math. **73**(1), 11–32 (1983)

2. Brøndsted, A.: An Introduction to Convex Polytopes. Graduate Texts in Mathematics, vol. 90. Springer, New York (1983)
3. Curran, M.J., Goldmakher, L.: Khovanskii's theorem and effective results on sumset structure. Discrete Anal., pages Paper No. 27, 25 (2021)
4. Dixmier, J.: Proof of a conjecture by Erdős and Graham concerning the problem of Frobenius. J. Number Theory **34**(2), 198–209 (1990)
5. Granville, A., Shakan, G.: The Frobenius postage stamp problem, and beyond. Acta Math. Hungar. **161**(2), 700–718 (2020)
6. Granville, A., Walker, A.: A tight structure theorem for sumsets. Proc. Am. Math. Soc. **149**(10), 4073–4082 (2021)
7. Jelínek, V., Klazar, M.: Generalizations of Khovanskii's theorems on the growth of sumsets in abelian semigroups. Adv. Appl. Math. **41**(1), 115–132 (2008)
8. Khovanskiĭ, A.G.: The Newton polytope, the Hilbert polynomial and sums of finite sets. Funktsional. Anal. i Prilozhen. **26**(4), 57–63, 96 (1992)
9. Lee, J.: Geometric structure of sumsets. arxiv:0704.3314
10. McMullen, P.: The maximum numbers of faces of a convex polytope. Mathematika **17**, 179–184 (1970)
11. Nathanson, M.B.: Sums of finite sets of integers. Am. Math. Monthly **79**(9), 1010–1012 (1972)
12. Nathanson, M.B., Ruzsa, I.Z.: Polynomial growth of sumsets in abelian semigroups. Journal de théorie des nombres de Bordeaux **14**(2), 553–560 (2002)
13. Seidel, R.: The upper bound theorem for polytopes: an easy proof of its asymptotic version. Comput. Geom. **5**(2), 115–116 (1995)
14. Wu, J.-D., Chen, F.-J., Chen, Y.-G.: On the structure of the sumsets. Discrete Math. **311**(6), 408–412 (2011)
15. Ziegler, G.M.: Lectures on Polytopes. Graduate Texts in Mathematics, vol. 152. Springer, New York (1995)