TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 353, Number 10, Pages 3995–4024
S 0002-9947(01)02763-5
Article electronically published on June 6, 2001

A BRUNN-MINKOWSKI INEQUALITY FOR THE INTEGER LATTICE

R. J. GARDNER AND P. GRONCHI

Abstract. A close discrete analog of the classical Brunn-Minkowksi inequality that holds for finite subsets of the integer lattice is obtained. This is applied to obtain strong new lower bounds for the cardinality of the sum of two finite sets, one of which has full dimension, and, in fact, a method for computing the *exact* lower bound in this situation, given the dimension of the lattice and the cardinalities of the two sets. These bounds in turn imply corresponding new bounds for the lattice point enumerator of the Minkowski sum of two convex lattice polytopes. A Rogers-Shephard type inequality for the lattice point enumerator in the plane is also proved.

1. Introduction

The classical Brunn-Minkowski inequality states that if K and L are convex bodies in $\mathbb{E}^n$, then

$$V(K+L)^{1/n} \geq V(K)^{1/n} + V(L)^{1/n}, \tag{1}$$

with equality if and only if K and L are homothetic. Here $K+L$ is the vector or Minkowski sum of K and L, and V denotes volume; see Section 2 for notation and definitions. It has long been known that the inequality holds for nonempty bounded measurable sets, and several quite different proofs of it are known. An excellent introduction is provided in a book by Schneider [28, Section 6.1].

Always a seminal result in convex, integral, and Minkowski geometry, the Brunn-Minkowski inequality has in recent decades dramatically extended its influence in many areas of mathematics. Various applications have surfaced, for example to probability and multivariate statistics, shapes of crystals, geometric tomography, elliptic partial differential equations, and combinatorics; see [28, Section 6.1], [12], [1], and [19]. Connections to Shannon's entropy power inequality have been found (see, for example, [8] and [9]). Several remarkable analogs have been established in other areas, such as potential theory and algebraic geometry; see, for example, [6], [11], [16], [18], and [22]. Reverse forms of the inequality are important in the local theory of Banach spaces, as explained in [23].

One proof of the Brunn-Minkowski inequality, due to Blaschke, runs as follows (see, for example, [31, pp. 310–314]). Let $S_u K$ denote the Steiner symmetral of K

Received by the editors September 30, 1999.
1991 *Mathematics Subject Classification.* Primary 05B50, 52B20, 52C05, 52C07; Secondary 92C55.
Key words and phrases. Brunn-Minkowski inequality, lattice, lattice polygon, convex lattice polytope, lattice point enumerator, sum set, difference set.
First author supported in part by U.S. National Science Foundation Grant DMS-9802388.

©2001 American Mathematical Society

in the direction $u \in S^{n-1}$. If K and L are convex bodies in $\mathbb{E}^n$, then it can be shown (see, for example, [31, Theorem 6.6.3]) that

$$S_u(K+L) \supset S_uK + S_uL. \tag{2}$$

If $V(K) = V(B_K)$ and $V(L) = V(B_L)$, where B_K and B_L are balls with centers at the origin, then applying (2) successively to a suitable sequence of directions yields

$$V(K+L) \geq V(B_K + B_L), \tag{3}$$

which is easily seen to be equivalent to (1).

In Theorem 5.1 below we prove the following discrete analog of (3): If A and B are finite subsets of $\mathbb{Z}^n$ with $\dim B = n$, then

$$|A+B| \geq \left| D^B_{|A|} + D^B_{|B|} \right|. \tag{4}$$

Here $D^B_{|A|}$ and $D^B_{|B|}$ are finite subsets of $\mathbb{Z}^n$ with cardinalities equal to those of A and B, respectively, that are initial segments in a certain order on $\mathbb{Z}^n$ which depends only on $|B|$. Roughly speaking, these sets are as close as possible to being the intersection with $\mathbb{Z}^n$ of simplices of a certain fixed shape. To obtain (4), we first prove in Lemma 3.4 a discrete analog of (2): If A and B are finite subsets of $\mathbb{Z}^n_+$, and v is contained in a certain special subset of $\mathbb{Z}^n$, then

$$C_v(A+B) \supset C_vA + C_vB, \tag{5}$$

where C_vA denotes the v-compression of A. Compression in $\mathbb{Z}^n$ is a discrete analog of shaking, an antisymmetrization process introduced by Blaschke (see, for example, [5, p. 77] and [7]). Essentially, (4) is obtained by applying (5) to a sequence of suitable vectors.

The process of compression was apparently introduced by Kleitman [20], and used by him, Bollobás and Leader [3], and others to obtain certain discrete isoperimetric inequalities. There are many papers on this topic (see the survey of Bezrukov [2]). After proving (4), we learned that Bollobás and Leader [4] also use compression to obtain a result in the finite grid $\{0, 1, \ldots, k\}^n$, $k \in \mathbb{N}$, analogous to (4). However, their result is essentially different and cannot be used to deduce (4); see the discussion at the end of Section 5. We are not aware of such a close analog of the Brunn-Minkowski inequality as (4) that applies to the integer lattice.

Just as the classical Brunn-Minkowski inequality is useful in geometric tomography (see [12]), we believe the discrete Brunn-Minkowski inequality (4) will be useful in discrete tomography once this new subject is developed along the same lines. For an introduction to the latter, see [13] and [17]. Here we apply (4) to find new lower bounds for the cardinality of a sum of two finite subsets of the integer lattice. The problem of understanding the nature of the sum or difference of two finite sets has a long and rich history; it is, as Granville and Roesler [14] point out, "a central problem of combinatorial geometry and additive number theory". The book of Nathanson [21] gives an extensive account of the work of Freiman, Ruzsa, and others in this area, some of which has been used by W. T. Gowers in obtaining upper bounds in Szemerédi's theorem (see [14] and [21, Chapter 9]). The structure of differences of multisets turns out to be important in crystallography via the Patterson function; see [24].

Our methods actually produce lower bounds for the cardinality of a sum of two finite subsets of $\mathbb{E}^n$. (It is worth remarking that the obvious idea of replacing the points in the two finite sets by small congruent balls and applying the classical

Brunn-Minkowski inequality to the resulting compact sets is doomed to failure. The fact that the sum of two congruent balls is a ball of twice the radius introduces an extra factor of $1/2$ that renders the resulting bound weaker than even the trivial bound (11) below.) Ruzsa [25] proved that if A and B are finite sets in $\mathbb{E}^n$ with $|B| \leq |A|$ and $\dim(A+B) = n$, then

$$|A+B| \geq |A| + n|B| - \frac{n(n+1)}{2}. \tag{6}$$

Our technique involves new reductions (see Corollaries 3.6 and 3.8) from the case of general subsets of $\mathbb{E}^n$ to special subsets of the integer lattice. Compressions also play a role in this reduction, in which the dimension of the sum of the two sets, but not necessarily their individual dimensions, is preserved. With this method, we give a new proof of (6) in Corollary 4.2 below.

It is not hard to show (see the end of Section 4) that there is no improvement of (6) that is linear in $|A|$. However, under the slightly stronger additional assumption that $\dim B = n$, we can apply (4) to obtain in Theorem 6.5 the following inequality, considerably stronger than (6):

$$|A+B| \geq |A| + (n-1)|B| + (|A|-n)^{(n-1)/n}(|B|-n)^{1/n} - \frac{n(n-1)}{2}. \tag{7}$$

Assuming only that $\dim B = n$, we also prove in Theorem 6.6 that

$$|A+B|^{1/n} \geq |A|^{1/n} + \frac{1}{(n!)^{1/n}}(|B|-n)^{1/n}. \tag{8}$$

Inequality (7) is better when $|A|$ is small, but (8) provides an optimal second-order term as $|A|$ grows large. The latter should be compared to some inequalities obtained by Ruzsa [26, Theorem 3.3] via the classical Brunn-Minkowski inequality, which, however, hold only when $|A|$ is large enough. The novelty of (8) is that it is similar to (but not, as far as we know, derivable from) (1), yet it holds without cardinality restrictions on A and B.

Both (7) and (8) are consequences of (21) and (22) below. In fact, from these two equations the *exact* lower bound for $|A+B|$ can be found for any given n, $|A|$, and $|B|$; one simply computes the values of the variables p and r_j, $j = 1, \ldots, n$, from (21) and substitutes them into (22). In this sense, the problem of finding the lower bound is completely solved here. The authors have written a Mathematica program that does the necessary computations. When $n = 3$, $|A| = 2000$, and $|B| = 10$, for example, the exact lower bound for $|A+B|$ is 2546. By comparison, Ruzsa's estimate (6) and another stronger one of his, (14) below, give 2024 and 2027, respectively, while (7) gives 2321, and (8), remarkably, gives 2545. When $n = 10$, $|A| = 50000$, and $|B| = 1000$, the exact lower bound is 221800, while (6), (14) below, (7), and (8), give 59945, 59990, 92728, and 200828, respectively.

Inequalities (7) and (8) immediately translate into new results for the lattice point enumerator of the Minkowski sum of two convex lattice polytopes, Corollary 7.1 below. In Section 7 we give a different proof in the planar case that provides precise equality conditions for (7). We also derive a version of the Rogers-Shephard inequality, an affine isoperimetric inequality that gives the best possible upper bound for the volume of the difference body of a convex body, for the lattice point enumerator in the plane.

2. Definitions and preliminaries

As usual, S^{n-1} denotes the unit sphere and o the origin in Euclidean n-space $\mathbb{E}^n$. If $u \in S^{n-1}$, we denote by $u^\perp$ the $(n-1)$-dimensional subspace orthogonal to u. The standard orthonormal basis for $\mathbb{E}^n$ will be $\{e_1, \dots, e_n\}$.

If A is a set, we denote by $|A|$, $\operatorname{int} A$, $\operatorname{bd} A$, and $\operatorname{conv} A$ the *cardinality*, *interior*, *boundary*, and *convex hull* of A, respectively. The *dimension* of A is the dimension of its affine hull $\operatorname{aff} A$, and is denoted by $\dim A$. The notation for the usual orthogonal *projection* of A on a subspace S is $A|S$.

If A and B are subsets of $\mathbb{E}^n$, their *vector* or *Minkowski sum* is

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

and if $r \in \mathbb{R}$, then

$$rA = \{ra : a \in A\}.$$

Thus $-A$ is the reflection of A in the origin. We also write $DA = A - A = A + (-A)$ for the *difference set* of A.

We denote by $V(E)$ the *volume* of a k-dimensional body E in $\mathbb{E}^n$, that is, its k-dimensional volume.

A *convex lattice set* F is a finite subset of the n-dimensional integer lattice $\mathbb{Z}^n$ such that $F = \operatorname{conv} F \cap \mathbb{Z}^n$.

We denote by $\mathbb{Z}^n_+$ the subset of $\mathbb{Z}^n$ of points with nonnegative coordinates. Let F be a convex lattice set with $\dim F = k$, $1 \le k \le n$, such that for distinct integers i and i_j, $1 \le j \le k-1$ between 1 and n, F is of the form

$$F = \{se_i : s = 0, 1, \dots, |F| - k\} \cup \{e_{i_1}, \dots, e_{i_{k-1}}\}.$$

Note that $\operatorname{conv} F$ is a k-simplex. We call F a *long simplex*.

A *convex polytope* is the convex hull of a finite subset of $\mathbb{E}^n$. A *lattice polytope* is a polytope with its vertices in $\mathbb{Z}^n$. A *lattice polygon* is a polygon with its vertices in $\mathbb{Z}^2$.

If P is a convex lattice polytope, we denote by

$$G(P) = |P \cap \mathbb{Z}^n|$$

the value of the *lattice point enumerator* G at P. A useful survey of results involving G was made by Gritzmann and Wills [15]. Note that if K is a convex lattice set, then $\operatorname{conv} K$ is a convex lattice polytope and $|K| = G(\operatorname{conv} K)$, so results concerning the lattice point enumerator have a bearing on the cardinality of convex lattice sets and vice versa.

Let P be a lattice polytope. We denote by $i(P)$ and $b(P)$ the number of lattice points in $\operatorname{int} P$ and $\operatorname{bd} P$, respectively. *Pick's theorem* (see, for example, [10, p. 8]) states that when P is a lattice polygon in $\mathbb{E}^2$,

$$V(P) = i(P) + \frac{b(P)}{2} - 1. \tag{9}$$

If K and L are compact convex sets in $\mathbb{E}^n$, then the *Brunn-Minkowski inequality* states that

$$V(K + L)^{1/n} \ge V(K)^{1/n} + V(L)^{1/n}, \tag{10}$$

with equality if and only if K and L lie in parallel hyperplanes or are homothetic. We refer the reader to the excellent text of Schneider [28, Section 6.1] for more information.

3. Sums of sets and compressions

If A and B are finite subsets of $\mathbb{E}^n$, it is easy to see that

$$|A+B| \geq |A| + |B| - 1. \tag{11}$$

In general, this is the best possible inequality of this type; take, for example, $A = \{1, \ldots, k\}$ and $B = \{1, \ldots, l\}$, for $k, l \in \mathbb{N}$. However, many other results exist that give a lower bound for the cardinality of the sum of two finite sets. We introduce methods here and apply them in the next sections to obtain some known and new bounds, as well as a discrete version of the Brunn-Minkowski inequality.

Lemma 3.1. *Let A and B be finite subsets of $\mathbb{Z}^n$ containing the origin. Then there is a linear map $f : \mathbb{Z}^n \to \mathbb{Z}^{n-1}$ such that $f|_{A+B}$ is injective.*

Proof. Let $k \in \mathbb{N}$ be such that $k > \operatorname{diam}(A + B)$. We define $f(x)$ for $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ by

$$f(x) = (x_1 + kx_n, x_2, \ldots, x_{n-1}) \in \mathbb{Z}^{n-1}.$$

Suppose that $x, y \in A + B$ and $f(x) = f(y)$. Then $x_i = y_i$ for $2 \leq i \leq n-1$, and $x_1 - y_1 = k(x_n - y_n)$. If $x_n \neq y_n$, then $|x_1 - y_1| \geq k$, contradicting $k > \operatorname{diam}(A+B)$. It follows that $x_n = y_n$, so $x_1 = y_1$ also, and $x = y$, as required. □

Theorem 3.2. *Let A and B be finite subsets of $\mathbb{E}^n$ containing the origin. Then there is a linear and injective map $\phi : A + B \to \mathbb{Z}^n$ such that $\dim \phi(A) = \dim A$ and $\dim \phi(A + B) = \dim(A + B)$.*

Proof. Suppose first that $n = 1$. Let E be the set of all linear combinations of elements from $A + B$ with rational coefficients, that is, the vector subspace of $\mathbb{R}$ (regarded as a vector space over $\mathbb{Q}$) generated by $A + B$. Then E has dimension $d \leq |A+B|-1$. Let $c_1, \ldots, c_d$ be a basis for E. If $x \in A+B$ and $x = q_1c_1 + \cdots + q_dc_d$, we define $h(x) = (q_1, \ldots, q_d) \in \mathbb{Q}^d$. By composing h with an integer dilatation, if necessary, we obtain a linear and injective map $g : A + B \to \mathbb{Z}^d$.

One application of Lemma 3.1, with $A + B$ replaced by $g(A + B)$, produces a linear and injective map $f \circ g : A + B \to \mathbb{Z}^{d-1}$. Applying Lemma 3.1 in this way successively another $(d-2)$ times, we obtain a linear and injective map $\phi : A+B \to \mathbb{Z}$. The map ϕ clearly preserves dimension. This completes the proof for $n = 1$.

Suppose now that $n > 1$. We may assume, without loss of generality, that $\dim(A+B) = n$. By applying a nonsingular linear transformation, if necessary, we may also assume that $e_i \in A$, $1 \leq i \leq \dim A$, and $e_i \in B$, $\dim A + 1 \leq i \leq n$. If E is a finite subset of $\mathbb{Z}^n$ and $1 \leq i \leq n$, let

$$E_i = \{x_i : x = (x_1, \ldots, x_n) \in E\}.$$

Let $\phi_i : (A + B)_i \to \mathbb{Z}$ be the map just constructed when $n = 1$ and A and B are replaced by the sets A_i and B_i. Define $\phi : A + B \to \mathbb{Z}^n$ by

$$\phi(x) = (\phi_1(x_1), \ldots, \phi_n(x_n)).$$

Clearly, ϕ is linear and injective. Moreover, ϕ preserves the dimension of A and $A + B$ because for each i, $\phi(e_i) = t_ie_i$, where $t_i \neq 0$. □

Corollary 3.3. *Let A and B be finite subsets of $\mathbb{E}^n$. Then there are subsets A' and B' of $\mathbb{Z}^n$ satisfying* (i) $|A'| = |A|$, $|B'| = |B|$, *and* $|A' + B'| = |A+B|$, *and* (ii) $\dim A' = \dim A$ *and* $\dim(A' + B') = \dim(A + B)$.

Proof. By translating A and B, if necessary, we may assume that they both contain the origin. Let $A' = \phi(A)$ and $B' = \phi(B)$, where ϕ is the map from the previous theorem. □

The previous corollary allows us to focus on subsets of $\mathbb{Z}^n$. We now employ ideas introduced by Kleitman [20] (see also Bollobás and Leader [3]).

We shall need quite a bit of notation. Let

$$V = \{v = (v_1, \ldots, v_n) \in \mathbb{Z}^n : v_i < 0 \text{ for at least one } i, 1 \le i \le n\}.$$

If $v \in V$, let

$$\mathbb{Z}(v) = \{x \in \mathbb{Z}^n_+ : x + v \notin \mathbb{Z}^n_+\}.$$

Suppose that A is a finite subset of $\mathbb{Z}^n_+$, $v \in V$, and $x \in \mathbb{Z}(v)$. The *v-section* of A at x is

$$A_v(x) = \{m \in \mathbb{N} : x - mv \in A\}.$$

Note that the v-section of A is a subset of $\mathbb{N}$, not A. Since the lines parallel to v through points in $\mathbb{Z}(v)$ partition $\mathbb{Z}^n_+$, we can define the *v-compression* C_vA of A to be the unique set such that

$$(C_vA)_v(x) = \{0, 1, \ldots, |A_v(x)| - 1\},$$

for all $x \in \mathbb{Z}(v)$. The set A is called *v-compressed* if $C_vA = A$.

It is worth remarking that if L is a line parallel to v, then

$$|C_vA \cap L| = |A \cap L|,$$

so C_vA has the same discrete X-ray (see [13]) in the direction v as A, and is the subset of $\mathbb{Z}^n_+$ with this property whose points are moved as far as possible in the direction v. In particular, any compression of a set does not change its cardinality.

If $A \subset \mathbb{Z}^n_+$ is $-e_i$-compressed for each i with $1 \le i \le n$, we call A a *down set*. It is easy to see that A is a down set if and only if $x \in A$ and $x - e_i \in \mathbb{Z}^n_+$ imply that $x - e_i \in A$.

Let

$$W = \{v = (v_1, \ldots, v_n) \in \mathbb{Z}^n : v_i = -1 \text{ for some } i \text{ and } v_j \ge 0 \text{ for } j \ne i\}.$$

Note that if $v \in W$ with $v_i = -1$, then $\mathbb{Z}(v) = \mathbb{Z}^n_+ \cap e_i^\perp$.

Lemma 3.4. *Let A and B be finite subsets of $\mathbb{Z}^n_+$, and let $v \in W$. Then*

$$C_v(A + B) \supset C_vA + C_vB.$$

Proof. Let $x \in \mathbb{Z}(v)$. Suppose that $x - mv = a + b \in A + B$, where $m \in \mathbb{N}$, $a \in A$, and $b \in B$. Choose y, $z \in \mathbb{Z}(v)$ and k, $l \in \mathbb{N}$ such that $y - kv = a$ and $z - lv = b$. Then since $v \notin \mathbb{Z}^n_+$ and $\mathbb{Z}(v) = \mathbb{Z}^n_+ \cap e_i^\perp$ for some i, we must have $x = y + z$ and $m = k + l$. Using this fact, we obtain

$$\begin{aligned}(A + B)_v(x) &= \{m \in \mathbb{N} : x - mv \in A + B\} \\ &= \bigcup \{\{k \in \mathbb{N} : y - kv \in A\} \\ &\qquad + \{l \in \mathbb{N} : z - lv \in B\} : x = y + z, \text{ and } y, z \in \mathbb{Z}(v)\} \\ &= \bigcup \{A_v(y) + B_v(z) : x = y + z, \text{ and } y, z \in \mathbb{Z}(v)\}.\end{aligned}$$

Therefore, by (11),

$$\begin{aligned}
&(C_vA + C_vB)_v(x)\\
&= \bigcup\{(C_vA)_v(y) + (C_vB)_v(z) : x = y + z, \text{ and } y, z \in \mathbb{Z}(v)\}\\
&= \bigcup\{\{0, 1, \ldots, |A_v(y)| - 1\}\\
&\qquad + \{0, 1, \ldots, |B_v(z)| - 1\} : x = y + z, \text{ and } y, z \in \mathbb{Z}(v)\}\\
&\subset \{0, 1, \ldots, \max\{|A_v(y)| + |B_v(z)| - 2 : x = y + z, \text{ and } y, z \in \mathbb{Z}(v)\}\}\\
&\subset \{0, 1, \ldots, \max\{|A_v(y) + B_v(z)| - 1 : x = y + z, \text{ and } y, z \in \mathbb{Z}(v)\}\}\\
&\subset \{0, 1, \ldots, |(A + B)_v(x)| - 1\}\\
&= (C_v(A + B))_v(x).
\end{aligned}$$

The lemma follows immediately. □

Corollary 3.5. *Let A and B be finite subsets of $\mathbb{Z}_+^n$, and let $v \in W$. Then*

$$|A + B| \geq |C_vA + C_vB|. \tag{12}$$

Proof. Since $|A + B| = |C_v(A + B)|$, this follows directly from the previous lemma. □

We remark that Lemma 3.4 and Corollary 3.5 do not hold for all $v \in V$; the additive structure of $\mathbb{Z}(v)$ when $v \in W$ is needed. To see this, let

$$A = \mathbb{Z}^2 \cap \operatorname{conv}\{(0, 0), (1, 0), (1, 3), (0, 4)\}$$

and

$$B = \mathbb{Z}^2 \cap \operatorname{conv}\{(0, 0), (1, 0), (1, 2), (0, 3)\}.$$

If $v = (1, -2)$, then $|A + B| = 21$ and $|C_vA + C_vB| = 23$.

Corollary 3.6. *Let A and B be finite subsets of $\mathbb{E}^n$. Then there are down sets A' and B' in $\mathbb{Z}_+^n$ satisfying* (i) $|A'| = |A|$, $|B'| = |B|$, *and* $|A + B| \geq |A' + B'|$, *and* (ii) $\dim A' = \dim A$ *and* $\dim(A' + B') = \dim(A + B)$.

Proof. By Corollary 3.3, we may assume that A and B are subsets of $\mathbb{Z}^n$. We may also assume that $\dim(A + B) = n$, and, by translating if necessary, that A and B contain the origin. Let $\dim A = k$. Choose linearly independent vectors x_i such that $x_i \in A$, $1 \leq i \leq k$ and $x_i \in B$, $k + 1 \leq i \leq n$. Let ϕ be a linear transformation of $\mathbb{E}^n$ such that $\phi(x_i) = e_i$, $1 \leq i \leq n$. Since the matrix associated with ϕ has rational coefficients, there is an $m \in \mathbb{N}$ such that $\phi(A)$ and $\phi(B)$ are subsets of the lattice $(1/m)\mathbb{Z}^n$. Then $m\phi(A)$ and $m\phi(B)$ are subsets of $\mathbb{Z}^n$.

Let $S = \{o, e_1, \ldots, e_n\}$ and $T = \{o, e_1, \ldots, e_k\}$. Note that $mT \subset m\phi(A)$, $mS \subset m\phi(A) \cup m\phi(B)$, and that we have not changed any of the relevant cardinalities or dimensions in passing from A and B to $m\phi(A)$ and $m\phi(B)$.

Choose $t \in \mathbb{Z}^n$ so that $m\phi(A) + t$ and $m\phi(B) + t$ are subsets of $\mathbb{Z}_+^n$. Then $mT + t \subset m\phi(A) + t$, and $mS + t \subset (m\phi(A) + t) \cup (m\phi(B) + t)$. Now by $-e_i$-compressing $m\phi(A) + t$ and $m\phi(B) + t$ for each i with $1 \leq i \leq n$ we obtain down sets A' and B' such that $T \subset A'$ and $S \subset A' \cup B'$. Therefore (ii) holds, and it follows from Corollary 3.5 that A' and B' satisfy (i). □

We now give another reduction to even more special sets. Note, however, that the dimension of either of the individual sets is not guaranteed to be preserved.

Lemma 3.7. *Let A and B be down sets in $\mathbb{Z}^n_+$ with $\dim(A+B) = n$. There exists a finite sequence of vectors in W such that the corresponding compressions applied successively to both A and B result in long simplices A' and B', respectively, such that $\dim(A' + B') = n$.*

Proof. Since A and B are down sets in $\mathbb{Z}^n_+$ with $\dim(A+B) = n$, we have $o \in A \cap B$ and $S = \{o, e_1, \dots, e_n\} \subset A \cup B$.

Suppose first that $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$. Since A and B are down sets, we can assume, without loss of generality, that $e_1 \in A \cap B$. Note that, if $e_n \notin A$, then $A \subset e_n^\perp$, and similarly for B. Let $E_A = A \cap e_n^\perp$ if $e_n \in A$, $E_A = \emptyset$ if $e_n \notin A$, and define E_B analogously. Let $w_1 = y_1 - e_n$, where $y_1 \in E_A \cup E_B$ is such that $\|w_1\|$ is maximal. Then $w_1 \in W$. Since $e_1 \in A \cap B$, we have $y_1 \neq o$, and then

$$(C_{w_1} A \cup C_{w_1} B) \setminus e_n^\perp = \{e_n\}.$$

Now $-e_i$-compress for $1 \le i \le n-1$ to obtain down sets A_1 and B_1 from $C_{w_1} A$ and $C_{w_1} B$, respectively. Note that $o \in A_1 \cap B_1$, $S \subset A_1 \cup B_1$, and

$$(A_1 \cup B_1) \setminus e_n^\perp = \{e_n\}.$$

Let $F_{A_1} = A_1 \cap e_n^\perp \cap e_{n-1}^\perp$ if $e_{n-1} \in A_1$, $F_{A_1} = \emptyset$ if $e_{n-1} \notin A_1$, and define F_{B_1} analogously. Let $w_2 = y_2 - e_{n-1}$, where $y_2 \in F_{A_1} \cup F_{B_1}$ is such that $\|w_2\|$ is maximal. Then $w_2 \in W$. Since $e_1 \in A \cap B$, we have $y_2 \neq o$, and then

$$(C_{w_2} A_1 \cup C_{w_2} B_1) \setminus (e_n^\perp \cap e_{n-1}^\perp) = \{e_{n-1}, e_n\}.$$

Now $-e_i$-compress for $1 \le i \le n-2$ to obtain down sets A_2 and B_2 from $C_{w_2} A_1$ and $C_{w_2} B_1$, respectively. Note that $o \in A_2 \cap B_2$, $S \subset A_2 \cup B_2$, and

$$(A_2 \cup B_2) \setminus (e_n^\perp \cap e_{n-1}^\perp) = \{e_{n-1}, e_n\}.$$

Continuing in this fashion, we obtain sets A_n and B_n that are clearly long simplices with the first coordinate axis as axis. Let $A' = A_n$ and $B' = B_n$ and note that $\dim(A' + B') = n$. This completes the proof under the assumption that $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$.

Suppose that $B = \{o\}$. Then $A + B = A$ and the above proof still works since $S \subset A$ implies that $y_i \neq o$ for $1 \le i \le n$. Similarly, the result holds when $A = \{o\}$.

Finally, suppose that $\operatorname{aff} A \cap \operatorname{aff} B = \{o\}$, where $\dim A \ge 1$ and $\dim B \ge 1$. Then we may assume that $A \subset H = \operatorname{aff}\{o, e_1, \dots, e_k\}$ and $B \subset H^\perp$. In this case we can apply the result already proved first for the case $B = \{o\}$ (with n replaced by k, identifying H with $\mathbb{E}^k$), and then for the case $A = \{o\}$ (with n replaced by $n-k$, identifying $H^\perp$ with $\mathbb{E}^{n-k}$), to obtain long simplices $A' \subset H$ and $B' \subset H^\perp$ with the required properties. (Note that the compressions used in reducing A to a long simplex in H do not affect B, and those used in reducing B to a long simplex in $H^\perp$ do not affect A.) □

Corollary 3.8. *Let A and B be finite subsets of $\mathbb{E}^n$. Then there are long simplices A' and B' in $\mathbb{Z}^n_+$ satisfying*

(i) $|A'| = |A|$, $|B'| = |B|$, *and* $|A + B| \ge |A' + B'|$, *and*
(ii) $\dim(A' + B') = \dim(A + B)$.

If $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$, we may suppose in addition that A' and B' have the x_1-axis as common axis.

Proof. This is a direct consequence of Corollaries 3.6 and 3.5 and Lemma 3.7 (and its proof). □

4. Known lower bounds for the cardinality of the sum of sets

The following result is due to Ruzsa [25].

Proposition 4.1. *If A and B are finite sets in $\mathbb{E}^n$ with $|B| \le |A|$ and $\dim(A+B) = n$, then*

$$|A+B| \ge |A| + \sum_{i=1}^{|B|-1} \min\{n, |A|-i\}. \tag{13}$$

Proof. By translating A and B, if necessary, we may assume that $o \in A \cap B$. If $\operatorname{aff} A \cap \operatorname{aff} B = \{o\}$, then clearly $|A+B| = |A||B|$, which implies (13). Suppose that $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$. By Corollary 3.8, we can assume that A and B are long simplices in $\mathbb{Z}^n_+$ with the x_1-axis as common axis. We prove (13) by induction. For $n = 1$ it is equivalent to (9). Suppose it is true in $\mathbb{E}^k$ for $k < n$.

If $\dim A = \dim B = n$, we have $B \subset A$, and a straightforward computation shows that

$$|A+B| = n|A| + |B| - \frac{n(n+1)}{2}.$$

Suppose that $|A| = |B| + s$. If $s \ge n-1$, then the right-hand side of (13) is

$$|A| + n(|B|-1) \le n|A| + |B| - \frac{n(n+1)}{2}.$$

If $s < n-1$, then the right-hand side of (13) is

$$\begin{aligned} &|A| + n(|B|+s-n) + (n-1) + \cdots + (s+1) \\ &\quad = |A| + n|B| + ns - n^2 + \frac{n(n-1)}{2} - \frac{(s+1)s}{2} \\ &\quad \le n|A| + |B| - \frac{n(n+1)}{2}, \end{aligned}$$

proving the proposition in this case.

Suppose that $\dim B < n$. Without loss of generality, we may assume that $B \subset \{x_n = 0\}$, so that $e_n \in A$ and

$$A + B = ((A \cap \{x_n = 0\}) + B) \cup (B + e_n).$$

If $|B| < |A|$, then $|B| \le |A| - 1 = |A \cap \{x_n = 0\}|$, so by the induction hypothesis,

$$\begin{aligned} |A+B| &\ge |A| - 1 + \sum_{i=1}^{|B|-1} \min\{n-1, |A|-1-i\} + |B| \\ &= |A| + \sum_{i=1}^{|B|-1} \min\{n, |A|-i\}. \end{aligned}$$

If $|A| = |B|$, then $|A| - 1 = |A \cap \{x_n = 0\}| < |B|$, so by the induction hypothesis,

$$\begin{aligned} |A+B| &\geq |B| + \sum_{i=1}^{|A|-2} \min\{n-1, |B|-i\} + |B| \\ &= |A| + \sum_{i=1}^{|B|-2} \min\{n-1, |A|-i\} + |B| \\ &= |A| + \sum_{i=1}^{|B|-2} \min\{n, |A|-i+1\} + 2 \\ &\geq |A| + \sum_{i=1}^{|B|-1} \min\{n, |A|-i\}. \end{aligned}$$

Finally, if $\dim A < n$, we may assume that $A \subset \{x_n = 0\}$ and $e_n \in B$, in which case, again by the induction hypothesis,

$$\begin{aligned} |A+B| &\geq |A| + \sum_{i=1}^{|B|-2} \min\{n-1, |A|-i\} + |A| \\ &= |A| + \sum_{i=1}^{|B|-2} \min\{n, |A|-i+1\} + |A| - |B| + 2 \\ &\geq |A| + \sum_{i=1}^{|B|-1} \min\{n, |A|-i\}. \end{aligned}$$

□

The following corollary, also stated by Ruzsa [25], follows from (13) after a simple computation.

Corollary 4.2. *If A and B are finite sets in $\mathbb{E}^n$ with $|B| \leq |A|$ and $\dim(A+B) = n$, then*

$$|A+B| \geq |A| + n|B| - \frac{n(n+1)}{2}. \tag{14}$$

Rusza's inequality (13) and its weaker form (14) contain several previous results in the literature. For all but finitely many pairs $\{|A|, |B|\}$, Ruzsa gave an example which shows that equality can hold in (13), and thus that this inequality is the best possible under its hypotheses. In all of these examples, either $\dim A < n$ or $\dim B < n$, unless $|A| = |B|$. Other related results are given by Ruzsa in [26] and [27]; see also [30].

No inequality of the form

$$|A+B| \geq c|A| + f_1(|B|) + f_2(n) \tag{15}$$

can hold with $c > 1$ for all finite sets A and B in $\mathbb{E}^n$ (or $\mathbb{Z}^n$) with $\dim A = \dim B = n$. To see this, let $r \in \mathbb{N}$ and $E_r = S_r \cap \mathbb{Z}^n$, where S_r is the n-simplex

$$S_r = \{(x_1, \ldots, x_n) : x_i \geq 0 \text{ and } x_1 + \cdots + x_n \leq r\}.$$

We have

$$|E_r| = \begin{pmatrix} r+n \\ n \end{pmatrix}.$$

Now let $r \in \mathbb{N}$, $A = A(r) = E_r$ and $B = E_1$. Then $A + B = E_{r+1}$, so (15) would imply that

$$\begin{pmatrix} r+n+1 \\ n \end{pmatrix} \geq c \begin{pmatrix} r+n \\ n \end{pmatrix} + g(n).$$

This in turn implies that

$$r + n + 1 \geq c(r+1) + g(n),$$

which is false for large r if $c > 1$.

In Section 6 below, we offer new nonlinear inequalities that are not implied by (13); see Theorems 6.5 and 6.6.

5. A Brunn-Minkowski inequality for the integer lattice

We begin with more notation.

Let B be a finite subset of $\mathbb{Z}^n$ with $|B| \geq n+1$. For every $x \in \mathbb{Z}^n$ we denote by $w_B(x)$ the *B-weight* of $x = (x_1, \ldots, x_n)$, defined by

$$w_B(x) = \frac{x_1}{|B| - n} + \sum_{i=2}^{n} x_i.$$

Define an order on $\mathbb{Z}^n$, the *B-order*, by setting $x <_B y$ if either $w_B(x) < w_B(y)$ or $w_B(x) = w_B(y)$ and for some j we have $x_j > y_j$ and $x_i = y_i$ for all $i < j$. Note that when $|B| = n+1$, the B-order is just the simplicial order defined in [3]. Let $V^B = \{v \in \mathbb{Z}^n : v <_B o\}$.

For $m \in \mathbb{N}$, let D_m^B be the union of the first m points in $\mathbb{Z}_+^n$ in the B-order. The set D_m^B is called a *B-initial segment*. It is easy to see that $D_{|B|}^B$ is an n-dimensional long simplex and $D_{|B|-1}^B$ is an $(n-1)$-dimensional long simplex. The points of $D_{|B|}^B$ are

$$o <_B e_1 <_B 2e_1 <_B \cdots <_B (|B| - n)e_1 <_B e_2 <_B \cdots <_B e_n.$$

Notice that all the above definitions depend only on the cardinality of B. As explained in the introduction to this paper, the following theorem can be viewed as a discrete Brunn-Minkowski inequality in the integer lattice.

Theorem 5.1. *Let A and B be finite subsets of $\mathbb{Z}^n$ with $\dim B = n$. Then*

$$|A + B| \geq \left| D_{|A|}^B + D_{|B|}^B \right|.$$

The proof of Theorem 5.1 is quite long and will proceed by a succession of lemmas, throughout which the set B will be a fixed subset of $\mathbb{Z}_+^n$. Since B is fixed, we shall write $S = D_{|B|}^B$. Note that none of the definitions before Theorem 5.1 change if we replace B by S.

Lemma 5.2. *We have $z <_S y$ if and only if $z - y \in V^S$.*

Proof. This follows immediately from the definitions above. □

Lemma 5.3. *A finite set $F \subset \mathbb{Z}_+^n$ is an S-initial segment if and only if it is v-compressed for every $v \in V^S$.*

Proof. The set F is not an S-initial segment if and only if there are $y \in F$, $z \notin F$, with $z <_S y$. By Lemma 5.2, the previous condition holds if and only if S is not v-compressed where $v = z - y \in V^S$. □

The following lemma will not be needed in this section.

Lemma 5.4. *An S-initial segment is a convex lattice set.*

Proof. Let F be an S-initial segment and let $x, y \in F$ be such that $x <_S y$ and $z = (1-t)x + ty \in \mathbb{Z}^n_+$, where $0 \le t \le 1$. Then $x <_S z <_S y$, so $z \in F$ and F is a convex lattice set. □

If F is a finite subset of $\mathbb{Z}^n_+$, let the *S-height* $h_S(F)$ of F be the sum of the positions in the S-order occupied by the points of F. Then $h_S(F) \in \mathbb{N}$; for example, we have $h_S(D^S_m) = m(m+1)/2$ for each $m \in \mathbb{N}$.

Lemma 5.5. *Let F be a finite subset of $\mathbb{Z}^n_+$. Suppose that $F_1 = F$ and for each $j \in \mathbb{N}$, $F_{j+1} = C_{v_j} F_j$ for some $v_j \in V^S$. Then there is a k such that $F_j = F_k$ for each $j \ge k$.*

Proof. Regarding the v_j-compression as a bijection from F_j to F_{j+1}, we see from its definition and Lemma 5.2 that it can only lower the position of points in F_j in the S-order, and if $F_{j+1} \ne F_j$, the position in the S-order of at least one point in F_j is lowered. Therefore $h_S(F_{j+1}) < h_S(F_j)$ unless $F_{j+1} = F_j$, so there is a k such that $F_j = F_k$ for each $j \ge k$. □

Lemma 5.6. *It suffices to prove Theorem 5.1 when $B = S = D^B_{|B|}$ and $A \subset \mathbb{Z}^n_+$ is v-compressed for every $v \in W \cap V^S$.*

Proof. By translating A and B, if necessary, we may assume that they are subsets of $\mathbb{Z}^n_+$. By applying, for each $i = 1, \dots, n$, a $-e_i$-compression to A and B, we may also assume, by Corollary 3.5, that A and B are down sets.

Letting $A = B$ in Lemma 3.7, we see that there is a finite sequence of vectors in W such that the corresponding compressions applied to B result in a long simplex, which in fact is S. Suppose that the same sequence of compressions, applied to A, result in a set A'. Then by Corollary 3.5, we have $|A + B| \ge |A' + S|$. Now we apply Lemma 5.5 where $F = A'$ and $\{v_j\}$ is a sequence in which each member of the finite set $W \cap V^S$ appears infinitely often. Then the resulting set $A'' = F_k$ is clearly v-compressed for every $v \in W \cap V^S$. By Lemma 5.3, these compressions leave S unchanged, so by Corollary 3.5 again, we have $|A' + S| \ge |A'' + S|$. □

We now settle the case $n = 2$ of Theorem 5.1.

Lemma 5.7. *Let A and B be finite subsets of $\mathbb{Z}^2$ with $\dim B = 2$. Then*

$$|A + B| \ge \left| D^B_{|A|} + D^B_{|B|} \right|.$$

Proof. By Lemma 5.6, we may assume $B = S = D^B_{|B|}$. We shall prove that

$$|A + S| \ge |D^S_{|A|} + S|$$

by induction on the S-height of A. Note that $h_S(A) \ge (|A| + 1)|A|/2$, and if $h_S(A) = (|A| + 1)|A|/2$, then $A = D^S_{|A|}$ and the inequality is trivial. Suppose that $h_S(A) > (|A| + 1)|A|/2$ and that the inequality is true whenever A is replaced by a subset of $\mathbb{Z}^2$ of the same cardinality but smaller S-height than A.

Let $v \in W \cap V^S$. By Lemma 5.6, we may assume that A is v-compressed for every $v \in W \cap V^S$. In particular, A is a down set which is u-compressed, where $u = (|S| - 2)e_1 - e_2$.

Let $y = (y_1, y_2) \in A$ be of maximal position in the S-order and let $z = (z_1, z_2) \in \mathbb{Z}_+^2 \setminus A$ be of minimal position in the S-order. Then $z <_S y$, because $A \neq D^S_{|A|}$. Since A is u-compressed and $y \in A$, we have $y' = (y_1 + (|S|-2)y_2, 0) \in A$. It follows from the fact that A is a down set that $(k, 0) \in A$ for every $k \leq y_1 + (|S| - 2)y_2$. Therefore $z_2 > 0$.

Note that y' is the unique point of A with maximal first coordinate. Therefore if $A' = A \setminus \{y'\}$, we have $(y_1 + (|S| - 2)(y_2 + 1), 0) \in (A + S) \setminus (A' + S)$, implying that $|A + S| \geq |A' + S| + 1$. Now let $A'' = A' \cup \{z\}$. Then $|A''| = |A|$, and since $z <_S y'$, we have $h_S(A'') < h_S(A)$. The hypothesis on z and $z_2 > 0$ imply that $z + u \in A$, and since A is a down-set we conclude that the only point that can belong to $(A'' + S) \setminus (A' + S)$ is $z + e_2$. Therefore $|A'' + S| \leq |A' + S| + 1$. By the induction hypothesis,

$$|A + S| \geq |A' + S| + 1 \geq |A'' + S| \geq |D^S_{|A|} + S|,$$

as required. □

Let F be a finite subset of $\mathbb{Z}_+^n$. We define sets $X_i(F)$, $1 \leq i \leq n$, as follows. If $1 < i \leq n$ and $m \in \mathbb{Z}$, denote by $F[i, m]$ the projection of $F \cap \{x_i = m\}$ onto the hyperplane $\{x_i = 0\}$. For each $m \in \mathbb{Z}$, let

$$P_m = \left\{ x \in \mathbb{Z}_+^n : w_S(x) = \frac{m}{|S| - n} \right\}. \tag{16}$$

The points in P_m lie in a hyperplane containing $(m, 0, \ldots, 0)$. Denote by $F[1, m]$ the projection of $F \cap P_m$ onto the hyperplane $\{x_1 = 0\}$. Let $S_i = S \cap \{x_i = 0\}$, and note that S_i is an $(n-1)$-dimensional long simplex in $\{x_i = 0\}$. For $1 \leq i \leq n$, define $X_i(F)$ to be the subset of $\mathbb{Z}_+^n$ for which

$$X_i(F)[i, m] = D^{S_i}_{|F[i,m]|},$$

where we are identifying $\{x_i = 0\}$ with $\mathbb{Z}^{n-1}$.

In other words, if $1 < i \leq n$, the projection of $X_i(F) \cap \{x_i = m\}$ onto $\{x_i = 0\}$ is the S_i-initial segment, defined in $\{x_i = 0\}$, with the same cardinality as the projection of $F \cap \{x_i = m\}$ onto $\{x_i = 0\}$. Similarly, the projection of $X_1(F) \cap P_m$ onto $\{x_1 = 0\}$ is the S_1-initial segment, defined in $\{x_1 = 0\}$, with the same cardinality as the projection of $F \cap P_m$ onto $\{x_1 = 0\}$. Therefore these definitions constitute a sort of $(n-1)$-dimensional compression in hyperplanes parallel to a fixed subspace.

It is not difficult to see (and can be proved from the definitions in a routine exercise) that

$$(F + S)[i, m] = F[i, m - 1] \cup (F[i, m] + S_i), \tag{17}$$

for $1 < i \leq n$, and

$$\begin{aligned}(F + S)[1, m] = {} & F[1, m] \cup F[1, m - 1] \cup \cdots \cup F[1, m - |S| + n + 1] \\ & \cup (F[1, m - |S| + n] + S_1).\end{aligned} \tag{18}$$

Lemma 5.8. *Let F be a finite subset of $\mathbb{Z}_+^n$ and let $1 \leq i \leq n$. Then $h_S(X_i(F)) \leq h_S(F)$, with equality if and only if $X_i(F) = F$.*

Proof. Let $x = (x_1, \ldots, x_n) \in \mathbb{Z}_+^n$ with $x_i = m$, and let x' be the projection of x onto $\{x_i = 0\}$. Then $x'_i = 0$ and $x'_j = x_j$ for all $j \neq i$. It follows that the S-order of

two points in $\{x_i = m\}$ agrees with the S_i-order of their projections onto $\{x_i = 0\}$. It is then clear from the definition of $X_i(F)$ that $h_S(X_i(F)) \le h_S(F)$.

If $1 < i \le n$ and $X_i(F) \ne F$, there is an $m \in \mathbb{N}$ such that $F[i,m]$ is not an S_i-initial segment. Let $y' \in F[i,m]$ be of maximal position in the S_i-order and $z' \in \{x_i = 0\} \setminus F[i,m]$ be of minimal position in the S_i-order. Then $z' <_{S_i} y'$. By the definition of $X_i(F)$, we have $y' \in \{x_i = 0\} \setminus X_i(F)[i,m]$ and $z' \in X_i(F)[i,m]$. Let $y, z \in \{x_i = m\}$ be the points whose projections onto $\{x_i = 0\}$ are y', z', respectively. Then $y \in F \setminus X_i(F)$, $z \in X_i(F) \setminus F$, and $z <_S y$. Therefore $h_S(X_i(F)) < h_S(F)$. The proof for $i = 1$ is similar. □

If $F \subset \mathbb{Z}^n_+$, let $Z_F = \{z - y : y \in F,\, z \in \mathbb{Z}^n_+ \setminus F\}$.

Lemma 5.9. *If $F \subset \mathbb{Z}^n_+$, then F is v-compressed if and only if $v \notin Z_F$.*

Proof. If $v \in Z_F$, there are $y \in F$ and $z \in \mathbb{Z}^n_+ \setminus F$ with $v = z - y$, so F is not v-compressed. Conversely, if F is not v-compressed, there are $y' \in F$ and $z' \in \mathbb{Z}^n_+ \setminus F$ such that $z' = y' + mv$ for some $m \in \mathbb{N}$. Let $j \in \mathbb{N}$ be maximal such that $y' + jv \in F$. If $y = y' + jv$ and $z = y' + (j+1)v$, then $v = z - y \in Z_F$. □

Lemma 5.10. *Let F be a finite subset of $\mathbb{Z}^n_+$ and let $v \in V^S$ with $w_S(v) = 0$. If F is not v-compressed, then $F[1,m]$ is not an S_1-initial segment for some $m \in \mathbb{N}$.*

Proof. Suppose that F is not v-compressed, where $v \in V^S$ and $w_S(v) = 0$. Then for some j we have $v_j > 0$ and $v_i = 0$ for all $i < j$. By Lemma 5.9, $v \in Z_F$, so there are $y \in F$ and $z \in \mathbb{Z}^n_+ \setminus F$ with $v = z - y$. Therefore $w_S(y) = w_S(z)$, so there is an $m \in \mathbb{N}$ such that $y, z \in P_m$.

Let y', z', and v' be the projections of y, z, and v, respectively, onto $\{x_1 = 0\}$. Then $y' \in F[1,m]$, $z' \in \{x_1 = 0\} \setminus F[1,m]$, and $v' = z' - y'$. If $v_1 = 0$, then $w_{S_1}(v') = w_S(v) = 0$, $v'_j > 0$ and $v'_i = 0$ for all $i < j$, where $j \ge 2$. If $v_1 > 0$, then

$$w_{S_1}(v') = w_S(v) - \frac{v_1}{|S| - n} < w_S(v).$$

In either case we have $v' <_{S_1} o$, so $v' \in V^{S_1}$. Therefore $v' \in Z_{F[1,m]}$, so $F[1,m]$ is not v'-compressed. By Lemma 5.3, $F[1,m]$ is not an S_1-initial segment. □

Lemma 5.11. *Let F be a finite subset of $\mathbb{Z}^n_+$, $n > 2$. If $X_i(F) = F$ for $i = 1, 2$, then F is an S-initial segment.*

Proof. Let $y \in F$ be of maximal position in the S-order and let $z \in \mathbb{Z}^n_+ \setminus F$ be of minimal position in the S-order. If $y <_S z$, then F is an S-initial segment.

Suppose that $z <_S y$. By Lemma 5.10 and our assumption that $X_1(F) = F$, F is v-compressed for every $v \in V^S$ with $w_S(v) = 0$, so $w_S(y) > w_S(z)$. If $m = w_S(y)(|S| - n)$, then $y \in P_m$ and $y' = (m, 0, \dots, 0)$ is the point in P_m of minimal position in the S-order, so $y' \in F$. Similarly, if $m' = w_S(z)(|S| - n)$, then $z \in P_{m'}$, and if z' is the point in $P_{m'}$ of maximal position in the S-order, we have $z' \notin F$. By the definition of S-order and the fact that $n > 2$, $z'_2 = 0$. Since $y', z' \in \{x_2 = 0\}$, we have

$$w_{S_2}(y') = w_S(y') = w_S(y) > w_S(z) = w_S(z') = w_{S_2}(z').$$

But $y' \in F[2,0] = F \cap \{x_2 = 0\}$ and $z' \notin F[2,0]$, so $F[2,0]$ is not an S_2-initial segment. Therefore $X_2(F) \ne F$, contradicting the hypothesis. □

The previous lemma is not true when $n = 2$. For example, let

$$S = \{(0,0),(0,1),(1,0)\} \text{ and } F = \mathbb{Z}^2 \cap \operatorname{conv}\{(0,0),(0,1),(3,0),(2,1)\}.$$

Lemma 5.12. *If F is an S-initial segment, then so is $F + S$.*

Proof. The proof is by induction on n. The result is trivial when $n = 1$. Assume it is true in $\mathbb{Z}_+^{n-1}$ (for all long simplices S in $\mathbb{Z}_+^{n-1}$) and suppose that $F + S \subset \mathbb{Z}_+^n$ is not an S-initial segment.

Let $y \in F + S$ be of maximal position in the S-order. If $y = a + b$, where $a \in F$ and $b \in S$, we must have $w_S(b) = 1$. Let $z \in \mathbb{Z}_+^n \setminus (F + S)$ be of minimal position in the S-order, so that $z <_S y$ by our assumption. Every $x \in \mathbb{Z}_+^n$ with $w_S(x) < w_S(a)$ must belong to the S-initial segment F, so every $x \in \mathbb{Z}_+^n$ with $w_S(x) < w_S(a) + 1 = w_S(y)$ belongs to $F + S$.

Therefore $w_S(y) = w_S(z)$. If $v = z - y$, then $v \in V^S$, $w_S(v) = 0$, and $F + S$ is not v-compressed. By Lemma 5.10, there is an $m \in \mathbb{N}$ (in fact $m = (|S| - n)w_S(y)$) such that $(F + S)[1, m]$ is not an S_1-initial segment.

By Lemma 5.8, $h_S(X_1(F)) \le h_S(F)$. Since F is an S-initial segment, $h_S(X_1(F)) = h_S(F)$, so Lemma 5.8 implies that $X_1(F) = F$. Therefore $F[1, m-1]$ is an S_1-initial segment. By the induction hypothesis, $(F + S)[1, m] = F[1, m-1] + S_1$ is also an S_1-initial segment. This contradiction completes the proof. □

Proof of Theorem 5.1. The proof is by induction on n. For $n = 1$, Theorem 5.1 is a direct consequence of (9) and Lemma 5.7 disposes of the case $n = 2$. Suppose that $n > 2$ and that Theorem 5.1 holds in all dimensions less than n.

If $m \in \mathbb{N}$, let

$$\mathcal{F}_m = \{F \subset \mathbb{Z}_+^n : |F| = m \text{ and } |F + S| \text{ is minimal}\}.$$

Let $F \in \mathcal{F}_{|A|}$ be of minimal S-height. We will show that $F = D^S_{|A|}$.

We claim that for $1 < i \le n$, we have

$$|F + S| \ge |X_i(F) + S|.$$

To see this, let $m \in \mathbb{N}$. Using (17), Lemma 5.12, the induction hypothesis, and (17) again, we obtain

$$\begin{aligned} |(X_i(F) + S)[i, m]| &= |X_i F[i, m-1] \cup (X_i F[i, m] + S_i)| \\ &= \max\{|X_i F[i, m-1]|, |X_i F[i, m] + S_i|\} \\ &\le \max\{|F[i, m-1]|, |F[i, m] + S_i|\} \\ &\le |F[i, m-1] \cup (F[i, m] + S_i)| = |(F + S)[i, m]|. \end{aligned}$$

This proves the claim.

By our assumption on F, we must have $h_S(X_i(F)) = h_S(F)$ for $1 < i \le n$. Analogously, using (18) instead of (17), we conclude that $h_S(X_1(F)) = h_S(F)$. Then Lemma 5.8 implies that $X_i(F) = F$ for $1 \le i \le n$. By Lemma 5.11, F is an S-initial segment, so $F = D^S_{|A|}$. □

Bollobás and Leader [4] obtain a result in the finite grid $[k]^n = \{0, 1, \ldots, k\}^n$, $k \in \mathbb{N}$ analogous to (4). Addition of sets A and B in $[k]^n$ is defined by

$$A +_k B = \{x \in [k]^n : x = a + b, a \in A, b \in B\}.$$

In other words, points in the usual sum not lying in the grid are simply ignored. For every $x = (x_1, \dots, x_n) \in [k]^n$, let

$$w_k(x) = \sum_{i=1}^{n} x_i k^i,$$

and define an order on k^n by setting $x <_k y$ if and only if $w_k(x) < w_k(y)$. The main result of [4] is that the minimum of $|A +_k B|$ over down sets A and B of $[k]^n$ is attained when A and B are initial segments with respect to the order $<_k$. The restriction to down sets is generally necessary because of the definition of addition $+_k$ of sets in the grid.

We can also restrict to down sets, without loss of generality, as shown in Corollary 3.6, but the fact that some points in the usual vector sum are not counted by Bollobás and Leader is the first important difference between their result and ours. The second is that any initial segment in the order $<_k$ with cardinality less than $k + 1$ must be a one-dimensional set, whereas the initial segment $D^B_{|B|}$ in the B-order is always n-dimensional. These two differences mean that if we choose a grid $[k]^n$ that contains down sets A and B in $\mathbb{Z}^n$, the lower bound for $|A +_k B|$ from [4] will generally be smaller than the lower bound for $|A + B|$ provided by (4).

6. New lower bounds for the cardinality of the sum of sets

In the following, the usual conventions

$$\binom{n}{k} = 0 \text{ if } n < k, \text{ and } \binom{n}{0} = 1$$

apply.

Lemma 6.1. *For $n \geq 1$ and $r \geq 1$,*

$$\binom{r+n-1}{n}^{-1/n} \left(\binom{r+n-1}{n} - (n-1) \right) - \binom{r+n-1}{n-1} \leq P(r),$$

where

$$P(r) = -(n-1) \left(\prod_{j=1}^{n-2} \frac{r+j}{j+1} + \frac{n}{r+n-1} \right).$$

Proof. Since $(r + j)/(j + 1) \geq (r + n - 1)/n$ for $0 \leq j \leq n - 1$, we have

$$\binom{r+n-1}{n} \geq \left(\frac{r+n-1}{n} \right)^n, \tag{19}$$

with equality if $r = 1$. Also,

$$\binom{r+n-1}{n} - (n-1) \geq 0$$

for $r \geq 2$. Therefore we can use (19) to obtain

$$\begin{aligned}
&\binom{r+n-1}{n}^{-1/n}\left(\binom{r+n-1}{n}-(n-1)\right)-\binom{r+n-1}{n-1}\\
&\quad\leq\left(\frac{n}{r+n-1}\right)\left(\binom{r+n-1}{n}-(n-1)\right)-\binom{r+n-1}{n-1}\\
&\quad=\binom{r+n-1}{n}\left(\frac{n}{r+n-1}-\frac{n}{r}\right)-\frac{n(n-1)}{r+n-1}\\
&\quad=-(n-1)\left(\prod_{j=1}^{n-2}\frac{r+j}{j+1}+\frac{n}{r+n-1}\right).
\end{aligned}$$

□

Lemma 6.2. *For $n \geq 1$ and $r \geq 1$,*

$$\binom{r+n-1}{n}^{(n-1)/n}-\binom{r+n-1}{n-1}\leq Q(r),$$

where

$$Q(r)=-(n-1)\prod_{j=1}^{n-2}\frac{r+j}{j+1}.$$

Proof. This is proved as in the previous lemma. □

Lemma 6.3. *For $n \geq 1$ and $r \geq 1$, we have*

$$\left(\frac{n-1}{n}\right)\binom{r+n-1}{n}^{-1/n}\binom{r+n-1}{n-1}-\binom{r+n-1}{n-2}\leq-\frac{(n-1)(n-2)}{2}.$$

Proof. Using (19), we obtain

$$\begin{aligned}
&\left(\frac{n-1}{n}\right)\binom{r+n-1}{n}^{-1/n}\binom{r+n-1}{n-1}-\binom{r+n-1}{n-2}\\
&\quad\leq\left(\frac{n-1}{r+n-1}\right)\binom{r+n-1}{n-1}-\binom{r+n-1}{n-2}\\
&\quad=\frac{n(n-1)(2-n)}{r(r+1)(r+n-1)}\binom{r+n-1}{n}\\
&\quad=\frac{(n-1)(2-n)}{2}\prod_{j=2}^{n-2}\frac{r+j}{j+1}\\
&\quad\leq-\frac{(n-1)(n-2)}{2}.
\end{aligned}$$

□

Lemma 6.4. *Let $n \geq 1$ and $c > 0$, and for $r \geq -1$, let*

$$S(r)=c\binom{r+n}{n}-\binom{r+n}{n-1}.$$

If $r_1 > -1$, then the maximum value of S on $[-1, r_1]$ occurs when $r = -1$ or r_1.

Proof. If $n = 1$, S is linear and the result follows immediately. Suppose that $n \geq 2$. We have

$$S'(r) = \frac{c}{n} \binom{r+n}{n-1} \left(1 + \left(r + 1 - \frac{n}{c} \right) \sum_{j=2}^{n} \frac{1}{r+j} \right).$$

The roots of S' are solutions of the equation

$$\sum_{j=2}^{n} \frac{1}{r+j} = \frac{1}{(n/c) - 1 - r}.$$

Since the left-hand side is strictly decreasing in r and the right-hand side is strictly increasing in r, there is at most one solution. The lemma follows directly. □

When $\dim B = n$, the following nonlinear inequality is considerably stronger than (14). (A different proof of the case $n = 2$ is obtained by combining Theorem 5.1, Lemma 5.4, and Corollary 7.4 from the next section.)

Theorem 6.5. *Let A and B be finite subsets of $\mathbb{E}^n$ with $|B| \leq |A|$ and $\dim B = n$. Then*

(20)
$$|A + B| \geq |A| + (n-1)|B| + (|A| - n)^{(n-1)/n}(|B| - n)^{1/n} - \frac{n(n-1)}{2}.$$

Proof. For $n = 1$ the inequality is trivial, so we may assume $n \geq 2$. By Theorem 5.1, it is enough to prove the result when B is a long simplex and A is a B-initial segment.

Note that if A is a "perfect" B-initial segment, that is, $A = rB$ for some $r \in \mathbb{N}$, then

$$|A| = (|B| - n) \binom{r+n-1}{n} + \binom{r+n-1}{n-1} = f(r),$$

say, and of course $A + B = (r+1)B$, so $|A + B| = f(r+1)$. In general, we can write

$$\begin{aligned} |A| &= f(r_1) + p \binom{r_1 + n - 1}{n-1} + \sum_{j=2}^{n} \binom{r_j + n + 1 - j}{n+1-j} \\ &= (|B| - n) \binom{r_1 + n - 1}{n} + (p+1) \binom{r_1 + n - 1}{n-1} \\ &\quad + \sum_{j=2}^{n} \binom{r_j + n + 1 - j}{n+1-j}, \end{aligned} \tag{21}$$

where $0 \leq p \leq |B| - n - 1$, $r_1 \geq r_2 \geq \cdots \geq r_n \geq -1$ and with the condition that if $r_1 = r_2$, then $p = |B| - n - 1$. In fact, there is a unique finite sequence $(p, r_1, \ldots, r_n)$ for each natural number $|A|$ under these conditions. Our assumption $|B| \leq |A|$ implies that $r_1 \geq 1$.

It will be convenient to write

$$b = |B| - n.$$

Then

$$|A+B| = b\begin{pmatrix} r_1+n \\ n \end{pmatrix} + (p+1)\begin{pmatrix} r_1+n \\ n-1 \end{pmatrix} + \sum_{j=2}^{n}\begin{pmatrix} r_j+n+2-j \\ n+1-j \end{pmatrix} - |R|, \tag{22}$$

where $R = R(r_2,\dots,r_n) = \{i:\ 2 \le i \le n,\ r_i = -1\}$. (We omit the proof of this fact, which is a straightforward consequence of the geometry.) Using Pascal's rule, we get

$$|A+B| - |A| = b\begin{pmatrix} r_1+n-1 \\ n-1 \end{pmatrix} + (p+1)\begin{pmatrix} r_1+n-1 \\ n-2 \end{pmatrix} + \sum_{j=2}^{n}\begin{pmatrix} r_j+n+1-j \\ n-j \end{pmatrix} - |R|. \tag{23}$$

Let

$$F = (n-1)b + (|A|-n)^{(n-1)/n}b^{1/n} + \frac{n(n-1)}{2} - (|A+B|-|A|). \tag{24}$$

We must show that $F \le 0$, and claim first that this holds for $n = 2$. From (21), we obtain

$$|A| = b\begin{pmatrix} r_1+1 \\ 2 \end{pmatrix} + (p+1)(r_1+1) + r_2 + 1.$$

Substituting this and (23) into (24), we see that we must prove

$$F = b + \left(b\begin{pmatrix} r_1+1 \\ 2 \end{pmatrix} + (p+1)(r_1+1) + r_2 - 1\right)^{1/2} b^{1/2} - b(r_1+1) - (p+1) + |R| \le 0,$$

or, equivalently, that

$$F_1 = (br_1 + (p+1) - |R|)^2 - \left(b\begin{pmatrix} r_1+1 \\ 2 \end{pmatrix} + (p+1)(r_1+1) + r_2 - 1\right)b \ge 0.$$

It can easily be verified that this holds when $b = 1$, and

$$\begin{aligned} \frac{\partial F_1}{\partial b} &= 2(br_1 + (p+1) - |R|)r_1 - 2b\begin{pmatrix} r_1+1 \\ 2 \end{pmatrix} - (p+1)(r_1+1) - r_2 + 1 \\ &= (r_1-1)(r_1b + p + 1) - 2|R|r_1 - r_2 + 1. \end{aligned}$$

If $r_2 > -1$, then $|R| = 0$ and $-2|R|r_1 - r_2 + 1 \ge -r_1 + 1$. If $r_2 = -1$, then $|R| = 1$, and $-2|R|r_1 - r_2 + 1 \ge -2r_1 + 2$. Therefore

$$\frac{\partial F_1}{\partial b} \ge (r_1-1)(r_1b + p - 1) \ge 0,$$

when $b \ge 1$ and $r_1 \ge 1$. Therefore $F_1 \ge 0$, proving the claim.

For the rest of the proof we may assume that $n \ge 3$. Using the inequality

$$(x+y)^{(n-1)/n} \le x^{(n-1)/n} + \left(\frac{n-1}{n}\right)yx^{-1/n},$$

we obtain

$$\begin{aligned}
&(|A| - n)^{(n-1)/n} b^{1/n} \\
&\quad = \left(b \binom{r_1 + n - 1}{n} + (p+1) \binom{r_1 + n - 1}{n-1} \right. \\
&\qquad\qquad \left. + \sum_{j=2}^{n} \binom{r_j + n + 1 - j}{n + 1 - j} - n \right)^{(n-1)/n} b^{1/n} \\
&\quad \le b \binom{r_1 + n - 1}{n}^{(n-1)/n} \\
&\qquad + \binom{n-1}{n} \frac{(p+1) \binom{r_1 + n - 1}{n-1} + \sum_{j=2}^{n} \binom{r_j + n + 1 - j}{n + 1 - j} - n}{\binom{r_1 + n - 1}{n}^{1/n}}.
\end{aligned}$$

Substituting this estimate and (23) into (24), we have

$$F \le G = H_0 b + H_1 (p+1) + \sum_{j=2}^{n} H_j - (n-1) \binom{r_1 + n - 1}{n}^{-1/n} + \frac{n(n-1)}{2},$$

with

$$H_0 = \binom{r_1 + n - 1}{n}^{(n-1)/n} - \binom{r_1 + n - 1}{n-1} + (n-1),$$

$$H_1 = \binom{n-1}{n} \binom{r_1 + n - 1}{n}^{-1/n} \binom{r_1 + n - 1}{n-1} - \binom{r_1 + n - 1}{n-2},$$

and

$$\begin{aligned}
H_j = &\binom{n-1}{n} \binom{r_1 + n - 1}{n}^{-1/n} \binom{r_j + n + 1 - j}{n + 1 - j} \\
&- \binom{r_j + n + 1 - j}{n - j} + \varepsilon_j,
\end{aligned}$$

where $\varepsilon_j = 1$ if $r_j = -1$ and $\varepsilon_j = 0$, otherwise, $2 \le j \le n$.

By Lemma 6.2,

$$\frac{\partial G}{\partial b} = H_0 \le Q(r_1) + (n-1) \le Q(1) + (n-1) = 0,$$

and by Lemma 6.3,

$$\frac{\partial G}{\partial p} = H_1 < 0.$$

Also, by Lemma 6.4, the maximum value of H_j in V occurs when $r_j = -1$ or $r_j = r_1$, $2 \le j \le n$. Therefore it suffices to show that $G = G(b, p, r_1, \dots, r_n) \le 0$ when $b = 1$, $p = 0$, $r_i = r_1$ for $1 \le i \le k$, where $1 \le k \le n$, and $r_i = -1$ for $k + 1 \le i \le n$. Denote this value of G by $G(k, r_1)$.

We claim that $G(k,r_1) \le G(1,r_1)$ for $2 \le k \le n$. To see this, suppose that $k \ge 2$. Using (19), we find that

$$\begin{aligned}
&G(k,r_1) - G(1,r_1)\\
&= \sum_{j=2}^{k} \left(\left(\frac{n-1}{n} \right) \binom{r_1+n-1}{n}^{-1/n} \binom{r_1+n+1-j}{n+1-j} \right.\\
&\qquad\qquad \left. - \binom{r_1+n+1-j}{n-j} \right)\\
&\le \sum_{j=2}^{k} \left(\left(\frac{n-1}{r_1+n-1} \right) \binom{r_1+n+1-j}{n+1-j} - \binom{r_1+n+1-j}{n-j} \right)\\
&= \left(\frac{n-1}{r_1+n-1} \right) \left(\binom{r_1+n}{n-1} - \binom{r_1+n+1-k}{n-k} \right)\\
&\quad - \binom{r_1+n}{n-2} + \binom{r_1+n+1-k}{n-k-1}\\
&= \binom{r_1+n+1-k}{n-k} \left(\left(\frac{n-1}{r_1+n-1} \right) \left(\prod_{j=2}^{k} \frac{r_1+n+2-j}{n+1-j} - 1 \right) \right.\\
&\qquad\qquad \left. + \left(\frac{n-1}{r_1+2} \right) \left(\frac{n-k}{n-1} - \prod_{j=2}^{k} \frac{r_1+n+2-j}{n+1-j} \right) \right)\\
&\le (n-1) \binom{r_1+n+1-k}{n-k} \left(\frac{1}{r_1+n-1} - \frac{1}{r_1+2} \right)\\
&\quad \times \left(\prod_{j=2}^{k} \frac{r_1+n+2-j}{n+1-j} - 1 \right) \le 0,
\end{aligned}$$

since $n \ge 3$. It remains to show that

$$G(1,r) = H_0 + H_1 - (n-1) \binom{r+n-1}{n}^{-1/n} + \frac{n(n-1)}{2} \le 0.$$

By Lemma 6.1,

$$\begin{aligned}
H_0 - (n-1) \binom{r+n-1}{n}^{-1/n} &\le P(r) + (n-1)\\
&\le P(1) + (n-1) = -(n-1),
\end{aligned}$$

since $n \ge 3$ and a routine exercise shows that P decreases with r when $n \ge 3$. Applying this and Lemma 6.3, we obtain

$$G(1,r) \le -(n-1) - \frac{(n-1)(n-2)}{2} + \frac{n(n-1)}{2} = 0,$$

as required. □

Theorem 6.6. *Let A and B be finite subsets of $\mathbb{E}^n$ with $\dim B = n$. Then*

$$|A+B|^{1/n} \ge |A|^{1/n} + \frac{1}{(n!)^{1/n}} (|B| - n)^{1/n}. \tag{25}$$

Proof. The proof is by induction on the dimension n. When $n = 1$, (25) is just the trivial estimate (11). Suppose that $n \geq 2$. By Theorem 5.1, we may assume that B is a long simplex and A is a B-initial segment.

Let $n = 2$. By squaring and rearranging (25) we see that we require

$$(|A + B| - |A| - b/2)^2 - 2b|A| \geq 0,$$

where we write $b = |B| - n$ as in the proof of Theorem 6.5. By (21) and (22), this becomes

$$\left(b(r_1 + 1) + (p + 1) + 1 - |R| - \frac{b}{2}\right)^2 - 2b\left(\frac{b(r_1 + 1)r_1}{2} + (p + 1)(r_1 + 1) + r_2 + 1\right) \geq 0.$$

Multiplying out, we get

$$2b(r_1 - r_2 - (r_1 + 1)|R|) + \left(p + 2 - |R| - \frac{b}{2}\right)^2 \geq 0,$$

which is true since $r_1 \geq r_2$ and either $r_2 \geq 0$ and $|R| = 0$, or $r_2 = -1$ and $|R| = 1$.

Assume that $n \geq 3$ and that (25) holds for dimensions less than n. Let the maximal B-weight of any point in A be m/b, $m \in \mathbb{N}$. Then $A = X \cup Y$, where

$$X = \left\{x \in \mathbb{Z}^n_+ : w_B(x) \leq \frac{m - 1}{b}\right\}$$

and Y is a subset of the set

$$\left\{x \in \mathbb{Z}^n_+ : w_B(x) = \frac{m}{b}\right\}$$

contained in a hyperplane (compare (16)). We can choose an $r \geq 0$ such that

$$|X| = b\begin{pmatrix} r + n - 1 \\ n \end{pmatrix} + q\begin{pmatrix} r + n - 1 \\ n - 1 \end{pmatrix},$$

for some q with $1 \leq q \leq b$. (Compare (21), where r_1 and $p + 1$ have been replaced here by r and q, respectively.) Notice that

$$|X + B| = b\begin{pmatrix} r + n \\ n \end{pmatrix} + q\begin{pmatrix} r + n \\ n - 1 \end{pmatrix}$$

and that $Y \subset X + B$. Therefore $|A + B| = |X + B| + |(Y + B) \setminus Y|$.

The set $(Y + B) \setminus Y$ is contained in a hyperplane H parallel to the one containing Y. It can be viewed as the vector sum of a translate of Y in $H \cap \mathbb{Z}^n_+$ and an $(n - 1)$-dimensional simplex in $H \cap \mathbb{Z}^n_+$ containing n points (a translate of the set $\{x \in \mathbb{Z}^n_+ : w_B(x) = 1\}$). Applying (25) to these translates in the $(n-1)$-dimensional lattice $H \cap \mathbb{Z}^n_+$, we obtain

$$|(Y + B) \setminus Y|^{1/(n-1)} \geq |Y|^{1/(n-1)} + \frac{1}{((n - 1)!)^{1/(n-1)}}.$$

Let $y = |Y|$,

$$\phi(y) = \left(y^{1/(n-1)} + \frac{1}{((n - 1)!)^{1/(n-1)}}\right)^{n-1} \tag{26}$$

for $y \geq 1$, and $\phi(0) = 0$. Then

$$|A + B| \geq b \begin{pmatrix} r+n \\ n \end{pmatrix} + q \begin{pmatrix} r+n \\ n-1 \end{pmatrix} + \phi(y).$$

It remains to show that

$$F(b,q,r,y) = \left(b \begin{pmatrix} r+n \\ n \end{pmatrix} + q \begin{pmatrix} r+n \\ n-1 \end{pmatrix} + \phi(y) \right)^{1/n} - \left(b \begin{pmatrix} r+n-1 \\ n \end{pmatrix} + q \begin{pmatrix} r+n-1 \\ n-1 \end{pmatrix} + y \right)^{1/n} - \left(\frac{b}{n!} \right)^{1/n} \geq 0$$

for the appropriate values of b, q, r, and y. We shall consider these as real variables to allow differentiation with respect to them. In view of (21), (22), and the identity $F(b,b,r,y) = F(b,0,r+1,y)$, it will suffice to show that $F \geq 0$ in the two regions

$$\Omega_1 = \{(b,q,r,y) \in \mathbb{R}^4 : b \geq 1, 0 \leq q \leq b-1, r \geq 0, y = 0\}$$

and

$$\Omega_2 = \{(b,q,r,y) \in \mathbb{R}^4 : b \geq 1, 0 \leq q \leq b-1, r \geq 0, 1 \leq y \leq \begin{pmatrix} r+n-1 \\ n-1 \end{pmatrix}\},$$

where the lower bound for q in Ω_1 has been lowered by one to simplify some of the calculations.

Consider first the region Ω_1. Let

$$G(b,q,r) = \left(b \begin{pmatrix} r+n \\ n \end{pmatrix} + q \begin{pmatrix} r+n \\ n-1 \end{pmatrix} \right)^{1/n}.$$

In Ω_1, the inequality $F \geq 0$ is equivalent to

$$G(b,q,r) - G(b,q,r-1) \geq \left(\frac{b}{n!} \right)^{1/n},$$

so by the mean-value theorem it suffices to prove that

$$\frac{\partial G}{\partial r} \geq \left(\frac{b}{n!} \right)^{1/n}.$$

We have

$$n \frac{\partial G}{\partial r} = \frac{b \begin{pmatrix} r+n \\ n \end{pmatrix} \sum_{i=1}^{n} \frac{1}{r+i} + q \begin{pmatrix} r+n \\ n-1 \end{pmatrix} \sum_{i=2}^{n} \frac{1}{r+i}}{G(b,q,r)^{n-1}}.$$

Then

$$n\frac{\partial^2 G}{\partial r\partial q} = \frac{G(b,q,r)^n \binom{r+n}{n-1} \sum_{i=2}^{n} \frac{1}{r+i}}{G(b,q,r)^{2n-1}} - \frac{-\frac{n-1}{n}\left(b\binom{r+n}{n}\sum_{i=1}^{n}\frac{1}{r+i} + q\binom{r+n}{n-1}\sum_{i=2}^{n}\frac{1}{r+i}\right)\binom{r+n}{n-1}}{G(b,q,r)^{2n-1}}$$

$$= \frac{\binom{r+n}{n-1}}{nG(b,q,r)^{2n-1}}\left(q\binom{r+n}{n-1}\sum_{i=2}^{n}\frac{1}{r+i} + b\binom{r+n}{n}\sum_{i=2}^{n}\frac{1}{r+i} - \frac{n-1}{r+1}b\binom{r+n}{n}\right).$$

It follows that $\partial G/\partial r$ has a unique minimum when

$$q = \frac{b}{n}\left(\frac{n-1}{\sum_{i=2}^{n}\frac{1}{r+i}} - (r+1)\right).$$

Substituting this value of q, we obtain

$$n\frac{\partial G}{\partial r} \geq \frac{\frac{nb}{r+1}\binom{r+n}{n}}{\left(\frac{b}{r+1}\binom{r+n}{n}\left(\frac{n-1}{\sum_{i=2}^{n}\frac{1}{r+i}}\right)\right)^{(n-1)/n}}$$

$$= n\left(\frac{b}{n!}\right)^{1/n}\left(\frac{\frac{1}{n-1}\sum_{i=2}^{n}\frac{1}{r+i}}{\left(\prod_{i=2}^{n}\frac{1}{r+i}\right)^{1/(n-1)}}\right)^{(n-1)/n} > n\left(\frac{b}{n!}\right)^{1/n},$$

by the arithmetic-geometric mean inequality. (Note that equality cannot hold in the latter because $n \geq 3$.) Therefore $F > 0$ in Ω_1.

Now consider the region Ω_2. Suppose $F(b',q',r',y') < 0$ for some $(b',q',r',y') \in \Omega_2$. We claim that F has a minimum in the set $\Omega_2(r') = \{(b,q,r,y) \in \Omega_2 : r = r'\}$. To see this, let $\{(b_i,q_i,r',y_i)\}$, $i \in \mathbb{N}$, be a sequence such that $F(b_i,q_i,r',y_i)$ tends to the infimum of F in $\Omega_2(r')$. Since $\Omega_2(r')$ is closed, this infimum is a minimum if the sequence $\{b_i\}$ is bounded. However, if $\{b_i\}$ is unbounded, we may, by taking a subsequence if necessary, assume $\lim_{i\to\infty} b_i = \infty$. Then

$$0 \geq \lim_{i\to\infty}\frac{F(b_i,q_i,r',y_i)}{b_i^{1/n}} = \lim_{i\to\infty} F\left(1,\frac{q_i}{b_i},r',0\right) > 0,$$

the last inequality holding because $(1,q_i/b_i,r',0) \in \Omega_1$ and Ω_1 is closed. This contradiction proves the claim. Writing $r' = r_0$, we conclude that F has a minimum at some point $z_0 = (b_0,q_0,r_0,y_0)$ in $\Omega_2(r_0)$.

The following notation will be convenient. Let

$$C = b_0\binom{r_0+n}{n} + q_0\binom{r_0+n}{n-1} + \phi(y_0),$$

$$D = b_0 \begin{pmatrix} r_0+n-1 \\ n \end{pmatrix} + q_0 \begin{pmatrix} r_0+n-1 \\ n-1 \end{pmatrix} + y_0,$$

$$x = \left(\frac{C}{D}\right)^{(n-1)/n},$$

and

$$\lambda = \left(\prod_{i=1}^{n-1}(r_0+i)\right)^{1/(n-1)} - r_0.$$

The curve $z(t) = (tb_0, tq_0, r_0, y_0)$, $t \geq 1$ is contained in $\Omega_2(r_0)$. By the minimality of $F(z_0)$ and direct calculation, we find that

$$\begin{aligned} F(z_0) - \frac{\phi(y_0)}{C^{(n-1)/n}} + \frac{y_0}{D^{(n-1)/n}} &= nb_0 \left.\frac{\partial F}{\partial b}\right|_{t=1} + nq_0 \left.\frac{\partial F}{\partial q}\right|_{t=1} \\ &= n\frac{\partial F}{\partial t}(z_0) \geq 0. \end{aligned} \tag{27}$$

Also, using the fact that $y\phi'(y) \leq \phi(y)$, the inequality

$$\frac{1}{n}F(z) \geq b\frac{\partial F}{\partial b} + p\frac{\partial F}{\partial p} + y\frac{\partial F}{\partial y} \tag{28}$$

can be verified by expanding the right-hand side. Consequently, the assumption $F(z_0) < 0$ and (27) imply that $\partial F/\partial y < 0$. By the minimality of $F(z_0)$, y_0 must be the maximal value of y in $\Omega_2(r_0)$, namely

$$y_0 = \begin{pmatrix} r_0+n-1 \\ n-1 \end{pmatrix} = \frac{(r_0+\lambda)^{n-1}}{(n-1)!}.$$

Then, by (26),

$$\phi(y_0) = \frac{(r_0+\lambda+1)^{n-1}}{(n-1)!}.$$

Using (27) again, we obtain the estimate

$$x > \frac{\phi(y_0)}{y_0} = \left(\frac{r_0+\lambda+1}{r_0+\lambda}\right)^{n-1}. \tag{29}$$

Next, we evaluate $F(z_0)$ from its definition as follows:

$$\begin{aligned} F(z_0) &= -\left(\frac{b_0}{n!}\right)^{1/n} + (x^{1/(n-1)}-1)\left(\frac{(r_0+\lambda)^{n-1}}{n!}\right)^{1/n}(b_0r_0+nq_0+n)^{1/n} \\ &> \left(\frac{b_0}{n!}\right)^{1/n}\left(\left(\frac{r_0+\lambda+1}{r_0+\lambda}-1\right)(r_0+\lambda)^{(n-1)/n}\left(\frac{b_0r_0+nq_0+n}{b_0}\right)^{1/n} - 1\right) \\ &= \left(\frac{b_0}{n!}\right)^{1/n}\left(\left(\frac{b_0r_0+nq_0+n}{b_0r_0+b_0\lambda}\right)^{1/n} - 1\right). \end{aligned}$$

Since $F(z_0) < 0$ by assumption,

$$nq_0 + n < b_0\lambda. \tag{30}$$

By the arithmetic-geometric inequality, $\lambda \leq n/2$, so $b_0 > 2(q_0+1) \geq 2$. It follows that the curve $z(t)$ is contained in $\Omega_2(r_0)$ for t in an open neighborhood of 1, so

that there must be equality in (27). Also, since $q_0 < b_0/2$, $(\partial F/\partial q)(z_0) \geq 0$, and computing the latter yields

$$x \leq \frac{r_0 + n}{r_0 + 1}. \tag{31}$$

We claim that $(\partial F/\partial q)(z_0) = 0$. Indeed, suppose that $(\partial F/\partial q)(z_0) > 0$. Then the minimality of $F(z_0)$ implies that $q_0 = 0$. Since $b_0 > 2$, $(\partial F/\partial b)(z_0) = 0$, and expanding this equation, we obtain

$$\begin{aligned}(r_0 + n)(r_0 + \lambda)^{n-1} - r_0 x(r_0 + \lambda)^{n-1} &= x\left(\frac{n!C}{b}\right)^{(n-1)/n} \\ &= x\left(r_0(r_0 + \lambda)^{n-1} + n(r_0 + \lambda)^{n-1}/b\right)^{(n-1)/n},\end{aligned}$$

that is,

$$(r_0 + n)(r_0 + \lambda)^{n-1} = x\left(r_0(r_0 + \lambda)^{n-1} + (r_0 + \lambda)^{(n-1)^2/n}\left(r_0 + \frac{n}{b}\right)^{(n-1)/n}\right).$$

By (30), $n/b_0 < \lambda$, so

$$(r_0 + n)(r_0 + \lambda)^{n-1} < x(r_0 + 1)(r_0 + \lambda)^{n-1}.$$

This implies that $x > (r_0 + n)/(r_0 + 1)$, contradicting (31) and establishing the claim.

Therefore $(\partial F/\partial q)(z_0) = 0$ and then $x = (r_0+n)/(r_0+1)$. From $(\partial F/\partial b)(z_0) = 0$ we now obtain

$$\begin{aligned}&(r_0 + n)(r_0 + \lambda)^{n-1} \\ &\quad = xr_0(r_0 + \lambda)^{n-1} + x\left(r_0(r_0 + \lambda)^{n-1} + \left(\frac{nq_0 + n}{b_0}\right)(r_0 + \lambda)^{n-1}\right)^{(n-1)/n} \\ &\quad = \frac{r_0 + n}{r_0 + 1}\left(r_0(r_0 + \lambda)^{n-1} + \left(r_0 + \frac{nq_0 + n}{b_0}\right)^{(n-1)/n}(r_0 + \lambda)^{(n-1)^2/n}\right).\end{aligned}$$

This yields

$$r_0 + 1 = r_0 + \left(r_0 + \frac{nq_0 + n}{b_0}\right)^{(n-1)/n}(r_0 + \lambda)^{(1-n)/n},$$

or

$$\lambda = \frac{nq_0 + n}{b_0}.$$

This contradicts (30) and completes the proof. □

7. Inequalities for the lattice point enumerator

The following result is an immediate consequence of Theorems 5.1 and 6.6.

Corollary 7.1. *Let P and Q be convex lattice polytopes in $\mathbb{E}^n$ with $\dim Q = n$. Then*

$$\begin{aligned}G(P + Q) \geq\ & G(P) + (n-1)G(Q) \\ &+ (G(P) - n)^{(n-1)/n}(G(Q) - n)^{1/n} - \frac{n(n-1)}{2},\end{aligned} \tag{32}$$

if $G(Q) \leq G(P)$, *and*

$$G(P+Q) \geq \left(G(P)^{1/n} + \frac{1}{(n!)^{1/n}} (G(Q)-n)^{1/n} \right)^n. \tag{33}$$

In two dimensions, the symmetry of (32) with respect to P and Q is restored. It turns out that with the extra assumption that $\dim P = 2$, a quite different approach yields a slightly better inequality than (32) when $n = 2$, together with precise equality conditions.

Theorem 7.2. *Let* P *and* Q *be convex lattice polygons with* $\dim P = \dim Q = 2$. *Then*

(34)

$$G(P+Q) \geq G(P) + G(Q) + ((2G(P) - b(P) - 2)(2G(Q) - b(Q) - 2))^{1/2} - 1,$$

with equality if and only if P *and* Q *are homothetic.*

Proof. By Pick's theorem (9), we have

$$V(P) = i(P) + \frac{b(P)}{2} - 1 = G(P) - \frac{b(P)}{2} - 1,$$

and similarly with P replaced by Q. By the Brunn-Minkowski inequality (10), we obtain

$$\left(G(P+Q) - \frac{b(P+Q)}{2} - 1 \right)^{1/2} \geq \left(G(P) - \frac{b(P)}{2} - 1 \right)^{1/2} + \left(G(Q) - \frac{b(Q)}{2} - 1 \right)^{1/2}.$$

Then (34) follows from squaring both sides and applying the equation

$$b(P+Q) = b(P) + b(Q), \tag{35}$$

which is easily proved by comparing the edges of P and Q parallel to a fixed edge of $P+Q$. The equality conditions for (34) follow directly from those of (10). □

It is worth noting that (34) is not always better than the case $n = 2$ of (33). Indeed, when $i(P) = i(Q) = 0$, (34) becomes

$$G(P+Q) \geq G(P) + G(Q) + (G(P)-2)^{1/2} (G(Q)-2)^{1/2} - 1.$$

So (33) is better if

$$(G(Q)-2)^{1/2} \left((2G(P))^{1/2} - (G(P)-2)^{1/2} \right) \geq G(Q)/2. \tag{36}$$

Now let $P = \operatorname{conv}\{(j,0),(j,1) : j = 1,\ldots,m\}$ and $Q = \operatorname{conv}\{(0,0),(1,0),(0,1)\}$. Then (36) becomes

$$(4m)^{1/2} - (2m-2)^{1/2} \geq 3/2,$$

or

$$36m^2 - 51m + \left(\frac{17}{4}\right)^2 \geq 32m(m-1),$$

which is true for large enough m.

Corollary 7.3. *Let P and Q be convex lattice polygons with* $\dim P = \dim Q = 2$. *Then*

$$G(P+Q) \geq G(P) + G(Q) + ((G(P)-2)(G(Q)-2))^{1/2} - 1, \tag{37}$$

with equality if and only if (i) *Q is a translate of P and $i(P) = 0$, or* (ii) *Q is a translate of $2P$ and $G(P) = 3$.*

Proof. We obtain (37) from (34) on noting that $b(P) \leq G(P)$. Using the equality conditions for (34), we see that equality holds in (37) if and only if P and Q are homothetic and $i(P) = i(Q) = 0$. Then either (i) holds or, translating P if necessary, we have $Q = rP$, $r \in \mathbb{Q}$, and $i(P) = i(Q) = 0$. Clearly, we may assume that $r = k/l > 1$, where k and l are integers with the greatest common divisor equal to 1. Then $P' = (1/l)P$ is also a nondegenerate convex lattice polygon and $Q = kP'$. Now P' contains three noncollinear lattice points, so their centroid c is such that $3c$ is a lattice point in the interior of $3P'$. Therefore $i(3P') > 0$. It follows that $k = 2$ and hence that $l = 1$ and $Q = 2P$. If $G(P) > 3$, then there are lattice points x, y in $\operatorname{bd} P$ such that the line segment $[x, y]$ meets $\operatorname{int} P$. This implies that the lattice point $x + y$ belongs to the interior of Q, so $i(Q) > 0$. Therefore we must have $G(P) = 3$ and $Q = 2P$, and this also satisfies (37). □

Corollary 7.4. *Let K and L be convex lattice sets in $\mathbb{Z}^2$ with* $\dim K = \dim L = 2$. *Then*

$$|K+L| \geq |K| + |L| + ((|K|-2)(|L|-2))^{1/2} - 1, \tag{38}$$

with equality if and only if (i) *L is a translate of K and $i(\operatorname{conv} K) = 0$, or* (ii) *$L$ is a translate of $2K$ and $|K| = 3$.*

If $|L| \leq |K|$, then the restriction on the dimension of L is generally necessary in the previous corollary. To see this, take, for example, K to be the long simplex $K = \{o, e_2, e_1, 2e_1, \ldots, 5e_1\}$, with $|K| = 7$, and $L = \{o, e_1, 2e_1\}$ with $|L| = 3$. Then $|K + L| = 11$, while the right-hand side of (38) is $9 + \sqrt{5}$.

For the remainder of this section, we investigate difference sets.

If A is a finite subset of $\mathbb{E}^n$, it is easy to see that

$$|DA| \leq |A|^2 - |A| + 1.$$

(See, for example, [29]. This paper also provides a useful introduction to results concerning lower bounds for $|DA|$; precise estimates are available when $n \leq 3$, but in general the problem appears to be open.) In general, this is all one can say, even for finite subsets of $\mathbb{Z}^n$. For example, equality holds for the subset $A = \{(k, k^2) : k = 0, 1, \ldots, m\}$ of $\mathbb{Z}^2$. The following Rogers-Shephard type inequality for the lattice point enumerator provides a much stronger bound for planar convex lattice sets.

Theorem 7.5. *Let P be a convex lattice polygon. Then*

$$G(DP) \leq 6G(P) - 2b(P) - 5, \tag{39}$$

with equality if and only if P is a triangle.

Proof. By Pick's theorem (9), we have

$$G(P) = V(P) + \frac{b(P)}{2} + 1. \tag{40}$$

The Rogers-Shephard inequality in the plane (see [28, Section 7.3] and [5, Section 53]; this special case is due to Blaschke and Rademacher) states that if K is a planar convex body, then

$$V(DK) \le 6V(K), \tag{41}$$

with equality if and only if K is a triangle. From (40), (35), and (41), we obtain

$$G(DP) = V(DP) + \frac{b(DP)}{2} + 1 \le 6V(P) + b(P) + 1 = 6G(P) - 2b(P) - 5,$$

with equality if and only if P is a triangle. □

Corollary 7.6. *Let K be a convex lattice set in $\mathbb{Z}^2$. Then*

$$|DK| \le 6|K| - 2b(\operatorname{conv} K) - 5, \tag{42}$$

where equality holds if and only if $\operatorname{conv} K$ *is a triangle.*

References

1. I. J. Bakelman, *Convex Analysis and Nonlinear Geometric Elliptic Equations*, Springer, Berlin, 1994. MR **95k:**35063
2. S. L. Bezrukov, *Isoperimetric problems in discrete spaces*, Extremal Problems for Finite Sets, Visegrád, Hungary (1991), Bolyai Society Mathematical Studies 3 (Budapest), János Bolyai Math. Soc., 1994, pp. 59–91. MR **96c:**05181
3. B. Bollobás and I. Leader, *Compressions and isoperimetric inequalities*, J. Comb. Theory A **56** (1991), 47–62. MR **92h:**05133
4. ———, *Sums in the grid*, Discrete Math. **162** (1996), 31–48. MR **97h:**05179
5. T. Bonnesen and W. Fenchel, *Theory of Convex Bodies*, BCS Associates, Moscow, Idaho, U.S.A., 1987. German original: Springer, Berlin, 1934. MR **88j:**52001
6. C. Borell, *Capacitary inequalities of the Brunn-Minkowski type*, Math. Ann. **263** (1983), 179–184. MR **84e:**31005
7. S. Campi, A. Colesanti, and P. Gronchi, *Shaking compact sets*, Contributions to Algebra and Geometry **42** (2001), 123–136.
8. M. H. M. Costa and T. Cover, *On the similarity of the entropy power inequality and the Brunn-Minkowksi inequality*, IEEE Trans. Information Theory **30** (1984), 837–839. MR **86d:**26029
9. A. Dembo, T. M. Cover, and J. A. Thomas, *Information theoretic inequalities*, IEEE Trans. Information Theory **37** (1991), 1501–1518. MR **92h:**94005
10. P. Erdös, P. M. Gruber, and J. Hammer, *Lattice Points*, Longman Scientific and Technical, and John Wiley, Bath and New York, 1989. MR **90g:**11081
11. G. Ewald, *Combinatorial Convexity and Algebraic Geometry*, Springer-Verlag, New York, 1996. MR **97i:**52012
12. R. J. Gardner, *Geometric Tomography*, Cambridge University Press, New York, 1995. MR **96j:**52006
13. R. J. Gardner and P. Gritzmann, *Discrete tomography: Determination of finite sets by X-rays*, Trans. Amer. Math. Soc. **349** (1997), 2271–2295. MR **97h:**52021
14. A. Granville and F. Roesler, *The set of differences of a given set*, Amer. Math. Monthly **106** (1999), 338–344. MR **2000f:**05080
15. P. Gritzmann and J. M. Wills, *Lattice points*, Handbook of Convexity, ed. by P. M. Gruber and J. M. Wills (Amsterdam), North-Holland, 1993, pp. 765–797. MR **94k:**52026
16. M. Gromov, *Convex sets and Kähler manifolds*, Advances in Differential Geometry and Topology (Teaneck, NJ), World Scientific Publishing, 1990, pp. 1–38. MR **92d:**52018
17. G. T. Herman and A. Kuba (eds.), *Discrete Tomography: Foundations, Algorithms and Application*, Birkhäuser, Boston, 1999. MR **2000h:**92015
18. D. Jerison, *A Minkowski problem for electrostatic capacity*, Acta Math. **176** (1996), 1–47. MR **97e:**31003
19. J. Kahn and N. Linial, *Balancing extensions via Brunn-Minkowski*, Combinatorica **11** (1991), 363–368. MR **93e:**52017

20. D. L. Kleitman, *Extremal hypergraph problems*, Surveys in Combinatorics, ed. by B. Bollobás (Cambridge), Cambridge University Press, 1979, pp. 44–65. MR **81d:**05061
21. M. B. Nathanson, *Additive Number Theory - Inverse Problems and the Geometry of Sumsets*, Springer-Verlag, New York, 1996. MR **98f:**11011
22. A. Okounkov, *Brunn-Minkowski inequality for multiplicities*, Invent. Math. **125** (1996), 405–411. MR **99a:**58074
23. G. Pisier, *The Volume of Convex Bodies and Banach Space Geometry*, Cambridge University Press, Cambridge, 1989. MR **91d:**52005
24. J. Rosenblatt and P. D. Seymour, *The structure of homometric sets*, SIAM J. Alg. Disc. Meth. **3** (1982), 343–350.
25. I. Z. Ruzsa, *Sum of sets in several dimensions*, Combinatorica **14** (1994), 485–490. MR **95m:**11018
26. ———, *Sets of sums and commutative graphs*, Studia Sci. Math. Hungar. **30** (1995), 127–148. MR **96i:**11013
27. ———, *Sums of finite sets*, Number Theory, New York Seminar 1991–5 (New York), Springer, 1996, pp. 281–293. MR **97i:**11019
28. R. Schneider, *Convex Bodies: The Brunn-Minkowski Theory*, Cambridge University Press, Cambridge, 1993. MR **94d:**52007
29. Y. Stanchescu, *On finite difference sets*, Acta Math. Hungar. **79** (1998), 123–138. MR **99c:**05034
30. ———, *On the simplest inverse problem for sums of sets in several dimensions*, Combinatorica **18** (1998), 139–149. MR **2000a:**05052
31. R. Webster, *Convexity*, Oxford University Press, Oxford, 1994. MR **98h:**52001

Department of Mathematics, Western Washington University, Bellingham, Washington 98225-9063
E-mail address: gardner@baker.math.wwu.edu

Istituto di Analisi Globale ed Applicazioni, Consiglio Nazionale delle Ricerche, Via S. Marta 13/A, 50139 Firenze, Italy
E-mail address: paolo@iaga.fi.cnr.it