On the discrete Brunn-Minkowski inequality by Gradner&Gronchi

David Iglesias [1]

Departamento de Matemáticas
Universidad de Murcia
Murcia, Spain

Abstract

In 2002 Gardner and Gronchi obtained a discrete analogue of the Brunn-Minkowski inequality. They proved that for finite subsets $A, B \subset \mathbb{R}^n$ with $\dim B = n$, the inequality $|A+B| \geq \left|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}\right|$ holds, where $\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|}, \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ are particular subsets of the integer lattice, called B-initial segments. The aim of this paper is to provide a method in order to compute $\left|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}\right|$ and so, to implement this inequality.

Keywords: The Brunn-Minkowski inequality, cardinality, Minkowski addition, integer lattice, B-order.

1 Introduction and notation

Let $\mathbb{R}^n$ denote the n-dimensional Euclidean space, let e_i be the i-th canonical unit vector. The n-dimensional volume (Lebesgue measure) of a compact set $K \subset \mathbb{R}^n$ is denoted by $\mathrm{vol}(K)$, and we use $|A|$ to represent the cardinality of a finite subset $A \subset \mathbb{R}^n$. Let $\mathbb{Z}^n$ be the integer lattice, i.e., the lattice of all points with integral coordinates in $\mathbb{R}^n$, and we write $\mathbb{Z}^n_+ = \left\{x \in \mathbb{Z}^n : x_i \geq 0\right\}$.

[1] Email: `david.iglesias@um.es`

The classical Brunn-Minkowski inequality states that if $K, L \subset \mathbb{R}^n$ are compact, then

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

with equality, when $\mathrm{vol}(K)\mathrm{vol}(L) > 0$, if and only if K and L are homothetic compact convex sets. Here, $K + L = \{x + y : x \in K, y \in L\}$ is the *Minkowski* (vectorial) addition. The Brunn-Minkowski inequality is one of the most powerful results in Convex Geometry and beyond. For an extensive survey on it we refer to [2].

There are several equivalent forms of the Brunn-Minkowski inequality (the multiplicative version, the minimal version, the analytic one called the Prékopa-Leindler inequality..., see e.g. [4, s. 7.1]). Among them, one can find the so-called Blaschke form of the Brunn-Minkowski inequality: if $K, L \subset \mathbb{R}^n$ are compact and convex and B_K, B_L are the balls (centered at 0) such that $\mathrm{vol}(K) = \mathrm{vol}(B_K)$, $\mathrm{vol}(L) = \mathrm{vol}(B_L)$, then

$$\mathrm{vol}(K+L) \geq \mathrm{vol}(B_K + B_L). \tag{2}$$

Next we move it to the discrete setting, i.e., we consider finite subsets of (integer) points. It can be easily seen that one cannot expect to obtain a Brunn-Minkowski inequality for the cardinality in the classical form (1). Indeed, simply taking $A = \{0\}$ to be the origin and any finite set $B \subset \mathbb{Z}^n$, then $|A + B|^{1/n} < |A|^{1/n} + |B|^{1/n}$. So, in [3] Gardner and Gronchi proposed to obtain an analogue of (2) for the cardinality, and proved the following beautiful and powerful discrete Brunn-Minkowski inequality:

Theorem 1.1 *Let $A, B \subset \mathbb{Z}^n$ be finite with* $\dim B = n$. *Then*

$$|A + B| \geq \left|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}\right|. \tag{3}$$

Here $\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|}, \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ are *B-initial segments*: for $m \in \mathbb{N}$, D^B_m is the set of the first m points of $\mathbb{Z}^n_+$ in the "B-order", which is a particular order defined on $\mathbb{Z}^n_+$ depending only on $|B|$ (see Section 2). Roughly speaking, these sets are close to the intersection of certain simplices with $\mathbb{Z}^n$. In order to show (3) the authors use the technique of the so-called "compression in a direction v", which might be seen as a discrete analog of shaking (see e.g. [1, p. 77]).

2 The B-weight and the B-order

In order to define the main object in Gardner&Gronchi's result, i.e. the initial segments, we need a certain order, depending on one of the sets, say B, in $\mathbb{Z}^n$.

This B-order is defined via a linear function that the authors called B-weight. As usual we write $x = (x_1, \ldots, x_n)^\intercal$.

Definition 2.1 [B-weight] Let $B \subset \mathbb{Z}^n$ be finite with $|B| \geq n+1$. The *B-weight function* $w_B : \mathbb{Z}^n \longrightarrow \mathbb{R}$ is defined as

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

The B-weight function allows to define the B-order in $\mathbb{Z}^n$:

Definition 2.2 [B-order] Given $x, y \in \mathbb{Z}^n$, we say that $x <_B y$ if

- $w_B(x) < w_B(y)$ or
- $w_B(x) = w_B(y)$ and there exists $j \in \{1, \ldots, n\}$ such that $x_j > y_j$ and $x_i = y_i$ for all $i < j$.

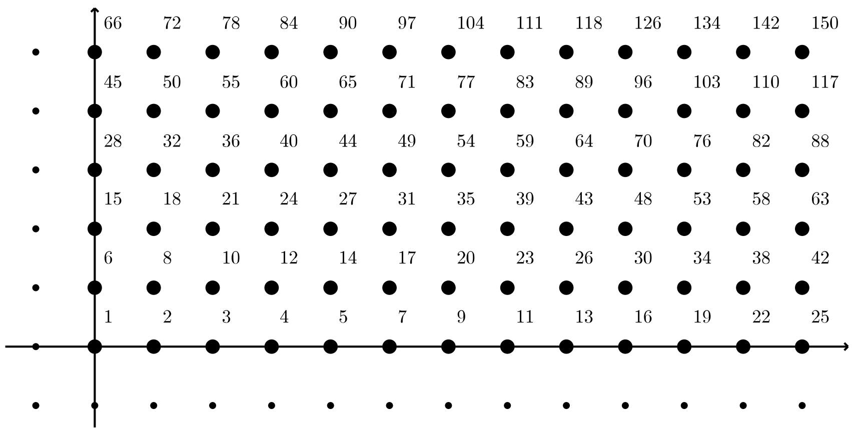

Fig. 1. The B-order in $\mathbb{Z}^2_+$ for $|B| = 6$.

We note that the minimum of $\mathbb{Z}^n_+$ in any B-order is always the origin. Moreover, one can check that the first $|B|$ points in any B-order are

$$0 <_B \mathrm{e}_1 <_B 2\mathrm{e}_1 <_B 3\mathrm{e}_1 \cdots <_B (|B| - n)\mathrm{e}_1 <_B \mathrm{e}_2 <_B \mathrm{e}_3 <_B \cdots <_B \mathrm{e}_n. \quad (4)$$

Another important observation is that initial segments behave well with the Minkowski addition: if $F = D^B_m$ is the m-initial segment in the B-order, then $F + D^B_{|B|}$ is also a initial segment in the same B-order.

3 Computing the cardinality $\left|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}\right|$

If we want to estimate the cardinality of the sum of two finite sets $A, B \subset \mathbb{Z}^n$ by below, one might have the impression that inequality (3) cannot help us, because we are replacing the problem of estimating $|A+B|$ by the one of computing the cardinality of another Minkowski addition, namely, $\left|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|}+\mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}\right|$. However, $\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|}$ and $\mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ are very special sets: they are B-initial segments, and therefore $\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ is also a B-initial segment. And so, in order to know its cardinality, it is enough to find the point $p \in \mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ of maximum position in the B-order, because

$$x \in \mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|} \text{ if and only if } x <_B p;$$

or equivalently, $|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}|$ is the position of the "last" point $p \in \mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ in the B-order.

We also note that $p = a + b \in \mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ is the maximum position point in the B-order if and only if $a \in \mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|}$ and $b \in \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ are the maximum position points (in the B-order) of A and B, respectively. And moreover, we already know that the maximum position point in $\mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}$ is always e_n (cf. (4)).

Thus, the problem of computing the cardinality $|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}|$ is reduced to have a method which allows to know the position in the B-order of any point of $\mathbb{Z}^n_+$, and vice versa. Once we have such a method, we may compute $|\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}|$ as follows:

Step 1: To find the point $a \in \mathbb{Z}^n_+$ whose position is $|A|$ (in the B-order).
Step 2: To compute the position s (in the B-order) of $p = a + \mathrm{e}_n$.
Step 3: Then $|A + B| \geq s$.

Example 3.1 In the example shown in Figure 1, if $|A| = 54$ then $a = (6, 3)^\intercal$, and hence $p = a + \mathrm{e}_2 = (6, 4)^\intercal$. Therefore, $|A + B| \geq |\mathrm{D}^{\mathrm{B}}_{|\mathrm{A}|} + \mathrm{D}^{\mathrm{B}}_{|\mathrm{B}|}| = 77$.

If we want to know the position of a point in a certain B-order, we just need to "B-order" the points of $\mathbb{Z}^n_+$, taking also into account that the B-order depends only on the cardinality of B but not on its "shape". In order to make this process easier, one can group the points of $\mathbb{Z}^n_+$, according to their B-weight. Following this idea we can use the sets P_m, also a key-point in the proof of Gardner&Gronchi, which are defined as

$$P_m = \left\{ x \in \mathbb{Z}^n_+ : w_B(x) = \frac{m}{|B| - n} \right\} \quad m \in \mathbb{N}.$$

Since the B-order organizes the points according to their B-weight, if we know the cardinality of each set P_m, $m \in \mathbb{N}$, then we will also know the B-weight of the point $x \in \mathbb{Z}_+^n$ occupying the s-th position for any $s \in \mathbb{N}$; in fact,

$$x \in P_m \quad \text{if and only if} \quad \sum_{i=0}^{m-1} |P_i| < s \leq \sum_{i=0}^{m} |P_i|.$$

In this regard, we have proved the following result. As usual in the literature, we write $\lfloor \cdot \rfloor$ to represent the floor function.

Theorem 3.2 *Let $m \in \mathbb{N}$ and let $B \in \mathbb{Z}_+^n$ be finite. Then*

$$|P_m| = \binom{n + \left\lfloor \frac{m}{|B|-n} \right\rfloor - 1}{\left\lfloor \frac{m}{|B|-n} \right\rfloor}. \tag{5}$$

Proof. First we prove that the cardinality of P_m does not depend on m but on $\left\lfloor \frac{m}{|B|-n} \right\rfloor$. Indeed, let $m, k \in \mathbb{Z}$ such that $0 \leq k < |B| - n$ and

$$\frac{m}{|B| - n} = \left\lfloor \frac{m}{|B| - n} \right\rfloor \in \mathbb{Z}.$$

On the one hand, if $x \in P_m$, then $x + k\mathrm{e}_1 \in P_{m+k}$, which implies that $P_m + k\mathrm{e}_1 \subset P_{m+k}$. On the other hand, if $y \in P_{m+k}$, then

$$w_B(y) = \frac{y_1}{|B| - n} + \sum_{i=2}^{n} y_i = \frac{m + k}{|B| - n},$$

and so

$$\frac{y_1 - k}{|B| - n} \in \mathbb{Z}.$$

Therefore, since $0 \leq k/\big(|B| - n\big) < 1$, we infer that $k/\big(|B| - n\big)$ is the fractional part of $w_B(y)$. Hence $y_1 - k \geq 0$ and thus

$$y' = y - k\mathrm{e}_1 = (y_1 - k, y_2, \ldots, y_n) \in \mathbb{Z}_+^n.$$

Now, since $w_B(y') = m/\big(|B| - n\big)$, we have $y' \in P_m \cap \mathbb{Z}_+^n$ and, consequently, $P_{m+k} - k\mathrm{e}_1 \subset P_m$, i.e., $P_{m+k} \subset P_m + k\mathrm{e}_1$. This shows that $P_m + k\mathrm{e}_1 = P_{m+k}$ and, therefore, $|P_m| = |P_{m+k}|$, as required.

So, it is enough to prove (5) when

$$r := \frac{m}{|B| - n} \in \mathbb{Z}.$$

We observe that, for any $x \in P_m$,

$$\frac{x_1}{|B| - n} = r - \sum_{i=2}^{n} x_i \in \mathbb{Z},$$

and hence we can consider the function $c_m : P_m \longrightarrow \{0,1\}^{n+r-1}$ given by

$$c_m(x) = \left(0, \overset{\left(\frac{x_1}{|B|-n}\right)}{\cdots}, 0, 1, 0, \overset{(x_2)}{\cdots}, 0, 1, \ldots, 0, \overset{(x_n)}{\cdots}, 0\right).$$

This function $c_m(x)$ is a bijection between P_m and $\{0,1\}^{n+r-1}$ and, moreover, in $c_m(x)$ exactly r zeros appear. So, the cardinality of P_m is precisely the number of possible combinations we can have if we take r elements from a family with $n + r - 1$ elements, i.e., $|P_m| = \binom{n+r-1}{r}$. □

The "coding function" c_m can be also used to B-order the points in each P_m. Indeed, given $x, y \in P_m$, then $x <_B y$ if and only if $c_m(x) < c_m(y)$ in the lexicographical order. Moreover, since the points in P_{m+1} are "B-greater" than the ones of P_m, and since we know $|P_m|$ (see Theorem 3.2), the function c_m allows to determine, as a consequence, the position of any point of $\mathbb{Z}_+^n$ in the B-order.

References

[1] Bonnesen, T., and W. Fenchel, "Theory of Convex Bodies," BCS Associates, Moscow, Idaho, U.S.A., 1987. German original: Springer, Berlin, 1934.

[2] Gardner, R. J., *The Brunn-Minkowski inequality*, Bull. Amer. Math. Soc. **39** (3) (2002), 355–405.

[3] Gardner, R. J., and P. Gronchi, *A Brunn-Minkowski inequality for the integer lattice*, Trans. Amer. Math. Soc. **353** (10) (2001), 3995-4024.

[4] Schneider, R., "Convex bodies: The Brunn-Minkowski theory," Cambridge University Press, Cambridge, 2nd expanded edition, 2014.