TRABAJO DE FIN DE MÁSTER

UNIVERSIDAD DE MURCIA
FACULTAD DE MATEMÁTICAS

LA DESIGUALDAD DE BRUNN-MINKOWSKI DISCRETA

David Iglesias López

Dirigido por
María de los Ángeles Hernández Cifre

Julio 2016

DECLARACIÓN DE ORIGINALIDAD

David Iglesias López, autor del TFM titulado "*La desigualdad de Brunn-Minkowski discreta*", bajo la tutela de la profesora **María de los Ángeles Hernández Cifre**,

DECLARA

que el trabajo que presenta es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas.

En Murcia, a 5 de Julio de 2016

Fdo.: David Iglesias López

Nota: En la Secretaría de la Facultad de Matemáticas se ha depositado una copia firmada de esta declaración.

Índice general

Introducción

La Teoría de Brunn-Minkowski es una de las piezas fundamentales de la Geometría de los Cuerpos Convexos. Tuvo su origen, como tal, en la Tesis de Hermann Brunn en 1887 y es, en su parte más esencial, creación de Hermann Minkowski alrededor del cambio de siglo. Precisamente, el 10 de Diciembre de 1900, Minkowski escribió a David Hilbert informándole de que su estudio sobre el área de superficie y el volumen en $\mathbb{R}^3$ estaba completo, siendo su avance más importante la introducción de una idea asociada a tres cuerpos convexos que él denominó, provisionalmente, sus *volúmenes mixtos*. La siguiente cita pertenece al obituario de Minkowski escrito por Hilbert en 1911, e ilustra el significado y la importancia de este nuevo concepto:

> *...Thus the concept of mixed volume appears as the simplest generalization which comprises the notions of volume, surface area and total mean curvature as special cases. In this way the latter notions are related much more closely to each other. Thus we may expect now to obtain a deeper understanding than was possible before, of the mutual relations of these notions...*

Si queremos definir brevemente la Teoría de Brunn-Minkowski, podríamos decir que ésta es el resultado de asociar dos conceptos elementales para los conjuntos del espacio euclídeo: la *suma vectorial* y el *volumen*. La suma vectorial o suma de Minkowski, combinada con el volumen, nos conduce a la desigualdad fundamental de Brunn-Minkowski, quizá la desigualdad más conocida relacionando el volumen de conjuntos convexos compactos.

La desigualdad de Brunn-Minkowski fue demostrada primero por Brunn con un argumento ingenioso e inteligente, aunque algo impreciso, donde además no se establecía el caso de la igualdad. Fue Minkowski quien proporcionó una demostración correcta y completa del resultado:

Teorema (La desigualdad de Brunn-Minkowski)**.** *Sean K y L dos conjuntos convexos y compactos de $\mathbb{R}^n$ no vacíos, y sea $0 \leq \lambda \leq 1$. Entonces*

$$\mathrm{vol}\left((1-\lambda)K + \lambda L\right)^{1/n} \geq (1-\lambda)\mathrm{vol}(K)^{1/n} + \lambda \mathrm{vol}(L)^{1/n},$$

dándose la igualdad, para algún $\lambda \in (0,1)$, si y sólo si o K y L están en hiperplanos paralelos (si tienen dimensión menor que n), o son homotéticos (si tienen dimensión n).

A la vista de un resultado tan "sencillo", parece difícil intuir las potentes extensiones que se pueden obtener de él, algunas muy recientes, así como su impacto en las Matemáticas y más allá de ellas.

La desigualdad de Brunn-Minkowski estuvo inspirada en el problema iosperimétrico: éste establece que, entre todos los conjuntos convexos de $\mathbb{R}^n$ con área de superficie dada, la bola n-dimensional encierra el mayor volumen. De hecho, la *desigualdad isoperimétrica* puede obtenerse como una consecuencia inmediata de la de Brunn-Minkowski. Así, durante muchos años se consideró que la desigualdad de Brunn-Minkowski "pertenecía" a la Geometría, donde su importancia ha sido ampliamente reconocida.

Sin embargo, alrededor de la mitad del siglo XX, diversos matemáticos (Lusternik, Hadwiger, Ohmann, ...) extendieron este resultado a contextos mucho más generales, incluyendo la clase de los conjuntos medibles Lebesgue, comenzando entonces la desigualdad a moverse en los dominios del Análisis.

Los últimos 30 años han visto consolidar el papel de la desigualdad de Brunn-Minkowski como una potente herramienta analítica, mostrando su estrecha relación con otras desigualdades del Cálculo. La versión integral de la desigualdad de Brunn-Minkowski se conoce como la *desigualdad de Prékopa-Leinder*, inversa de la conocida desigualdad de Hölder, donde ya la geometría parece haber desaparecido. Entre otras desigualdades relacionadas con la de Brunn-Minkowski en este contexto general nos encontramos, por ejemplo, con las de Young, Brascamp-Lieb, Barthe, Sobolev, etc.

Se necesitaría un artículo aparte sobre la desigualdad de Brunn-Minkowski para poder mencionar cada una de sus implicaciones dentro y fuera de la Geometría. Un magnífico *survey* sobre este resultado es [3]. En palabras de su autor, Richard Gardner,

> *...In a sea of Mathematics, the Brunn-Minkowski inequality appears like an octopus, tentacles reaching far and wide, its shape and color changing as it roams from one area to the next.*

En esta memoria demostraremos la desigualdad de Brunn-Minkowski clásica y, partiendo de ese punto, "bucearemos" por los conjuntos finitos demostrando algunas desigualdades clásicas hasta encontrar, parafraseando a Gardner, nuestro "pulpo camuflado a base de puntos" de la portada[1], es decir, demostrar la que se conoce como la desigualdad de Brunn-Minkowski discreta:

Teorema (Desigualdad de Brunn-Minkowski discreta)**.** *Sean $A, B \subset \mathbb{Z}^n$ finitos con $\dim B = n$. Enonces el cardinal de su suma $|A+B|$ verifica*

$$|A+B| \geq |D^B_{|A|} + D^B_{|B|}|.$$

[1] Ilustración *"Funny octopus"* de A. Enshina, englobada en su proyecto *Colorful dotted animals*: https://www.behance.net/anaensh, consultado en Julio 2016.

Aquí $D^B_{|A|}$ y $D^B_{|B|}$ son conjuntos finitos de $\mathbb{Z}^n$ con cardinales igual a los de A y B, respectivamente, los cuales son segmentos iniciales para un cierto orden sobre $\mathbb{Z}^n$ que depende sólo de $|B|$. De manera informal, podemos asumir que estos conjuntos son lo más parecido a la intersección de $\mathbb{Z}^n$ con símplices de una cierta forma.

Ambas versiones son complementarias la una de la otra ya que la desigualdad clásica trabaja con cuerpos convexos, por tanto con el funcional volumen, mientras que la desigualdad discreta involucra conjuntos finitos, y consecuentemente el cardinal, lo que hace imposible aplicar una en el contexto de la otra.

Sin embargo, ambas desigualdades mantienen una estrecha relación: dada una cierta información de dos conjuntos A y B (ya sea su volumen o su cardinal en cada caso) las desigualdades nos proporcion cotas inferiores sobre la suma de Minkowski $A + B$.

La estructura del texto está dividida en tres capítulos. En el primer capítulo haremos un breve repaso de los conceptos más básicos que necesitaremos tanto de los cuerpos convexos como de los retículos. Este capítulo, más que ser una guía detallada de dichos conceptos, servirá para fijar la notación que usaremos durante el resto del texto.

Durante el segundo capítulo se realizarán tanto una justificación como la prueba de la desigualdad de Brunn-Minkowski clásica, caracterizando también la igualdad.

Finalmente, en el tercer capítulo trabajaremos con conjuntos finitos, introduciendo conceptos asociados a dichos conjuntos, hasta enunciar y demostrar la que se conoce como la versión discreta de la desigualdad de Brunn-Minkowski.

Capítulo 1

Preliminares

Durante este capítulo, introduciremos las definiciones y primeros resultados que necesitaremos para el resto del texto. Estos contenidos se estudian durante el Grado en Matemáticas y el Máster en Matemática Avanzada de la Universidad de Murcia y, por este mismo motivo, no se realizarán pruebas de los resultados que aquí aparezcan. Para ver con más detalle estos resultados, véanse [4] y [7].

A lo largo de este trabajo, usaremos la notación estándar para el espacio euclídeo n-dimensional y las nociones fundamentales asociadas al mismo. Así, denotaremos con $\mathbb{R}^n$ el espacio euclídeo n-dimensional, dotado con la métrica estándar $\langle \cdot, \cdot \rangle$ del producto escalar, que da lugar a la norma euclídea $|| \cdot ||$. Asímismo, usaremos la notación $\mathbb{S}^{n-1}$ y o para la esfera unidad y el origen de coordenadas del espacio euclídeo n-dimensional $\mathbb{R}^n$. Además, dado $x \in \mathbb{R}^n$, representaremos por x_i sus coordenadas (respecto a la base canónica $\{e_1, \ldots, e_n\}$), es decir, $x = (x_1, \ldots, x_n)$.

1.1. Primeras definiciones. Los cuerpos convexos

En esta sección introduciremos los conceptos que necesitamos sobre cuerpos convexos.

Definición 1.1.1 (Combinación lineal, afín, positiva, convexa)**.**
Se dice que $x \in \mathbb{R}^n$ es una *combinación lineal* de los vectores $v_1, \ldots, v_k$, y se representa por $x \in \text{lin}\{v_1, \ldots, v_k\}$, si existen $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ tales que $x = \lambda_1 v_1 + \cdots + \lambda_k v_k$. Además:

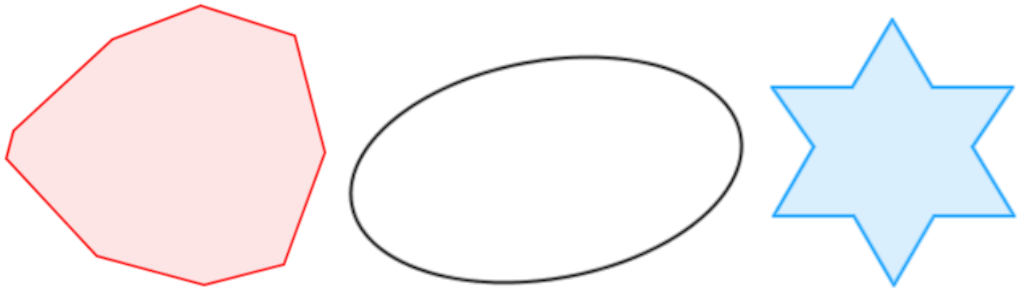
- Si los λ_i verifican $\lambda_1 + \cdots + \lambda_k = 1$, entonces se dice que x es *combinación afín* de los v_i ($x \in \text{aff}\{v_1, \ldots, v_k\}$).
- Si los λ_i verifican $\lambda_i \geq 0$ para todo i, entonces se dice que x es *combinación positiva* de los v_i ($x \in \text{pos}\{v_1, \ldots, v_k\}$).
- Finalmente, si se verifican ambas condiciones para los λ_i, entonces se dice que x es una *combinación convexa* de los v_i ($x \in \text{conv}\{v_1, \ldots, v_k\}$).

Dados $x, y \in \mathbb{R}^n$ puntos distintos, escribiremos $[x, y]$ para denotar el segmento determinado por x e y, esto es, el conjunto de todas las combinaciones convexas de x e y.

$$[x, y] = \{(1 - \lambda)x + \lambda y \ : \ 0 \leq \lambda \leq 1\}.$$

A partir de esto, podemos definir la noción de conjunto convexo.

Definición 1.1.2 (Conjunto convexo)**.**
Se dice que un conjunto $K \subset \mathbb{R}^n$ es *convexo* si, dados dos puntos cualesquiera de K, el segmento que los une está contenido en K. Es decir, si cualquier combinación convexa $\lambda x + (1 - \lambda)y \in K$, para todo $x, y \in K$ y $0 \leq \lambda \leq 1$.



(a) Los polígonos son convexos.

(b) Las elipses son convexas.

(c) Las estrellas no son convexas.

Figura 1.1: Algunos ejemplos de conjuntos convexos y no convexos.

Definición 1.1.3 (Cono)**.**
Un *cono (convexo)* es un subconjunto $A \subset \mathbb{R}^n$ que es convexo, no vacío y tal que si $x \in A$, entonces $\lambda x \in A$ para todo $\lambda \geq 0$.

Definición 1.1.4 (Envoltura convexa, afín y positiva)**.**
Dado un conjunto arbitrario $A \subset \mathbb{R}^n$ se define la *envoltura convexa* de A, y se representa por $\operatorname{conv} A$, como la intersección de todos los subconjuntos convexos que contienen a A.

Análogamente se define la *envoltura afín (positiva)* de A, y se representa por $\operatorname{aff} A$ ($\operatorname{pos} A$), a la intersección de todos los subespacios afines (conos) de $\mathbb{R}^n$ que contienen a A.

Observación 1.1.5. Podemos reescribir las definiciones de *envolturas afín, positiva y convexa* de otra forma: dado $M \subset \mathbb{R}^n$ las definiciones anteriores son equivalentes a que

- $\operatorname{aff} M$ es el plano afín de menor dimensión que contiene a M.
- $\operatorname{pos} M$ es el cono con vértice en el origen más pequeño que contiene a M.
- $\operatorname{conv} M$ es el menor conjunto convexo que contiene a M.

Ejemplo. Consideramos el conjunto $M = \{x_1 = (1,2), x_2 = (2,1)\} \subset \mathbb{R}^2$, procedemos al cálculo de $\operatorname{lin} M$, $\operatorname{aff} M$, $\operatorname{pos} M$ y $\operatorname{conv} M$:

$$\operatorname{lin} M = \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1, \lambda_2 \in \mathbb{R}\} = \mathbb{R}^2,$$

dado que x_1 y x_2 son linealmente independientes.

$$\begin{aligned}\operatorname{aff} M &= \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1 + \lambda_2 = 1\} = \{(\lambda_1 + 2\lambda_2, 2\lambda_1 + \lambda_2) : \lambda_1 + \lambda_2 = 1\} \\ &= \{(\lambda_1 + 2(1-\lambda_1), 2\lambda_1 + (1-\lambda_1)) : \lambda_1 \in \mathbb{R}\} = \{(2-\lambda_1, 1+\lambda_1) : \lambda_1 \in \mathbb{R}\} \\ &= \{(2,1) + \lambda \cdot (-1,1) : \lambda \in \mathbb{R}\},\end{aligned}$$

$$\operatorname{pos} M = \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1, \lambda_2 \geq 0\} = \{\lambda \cdot (\alpha_1 x_1 + \alpha_2 x_2) : \lambda, \alpha_1, \alpha_2 \geq 0, \alpha_1 + \alpha_2 = 1\},$$

y finalmente

$$\operatorname{conv} M = \{\lambda_1 x_1 + \lambda_2 x_2 : \lambda_1 + \lambda_2 = 1, \lambda_1, \lambda_2 \geq 0\} = \{\lambda x_1 + (1-\lambda) x_2 : 0 \leq \lambda \leq 1\}.$$

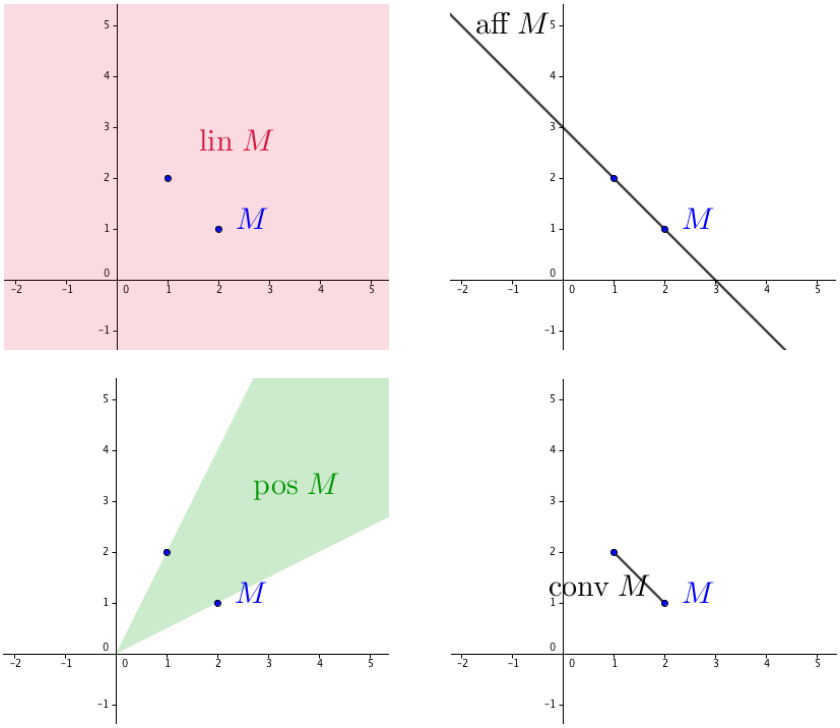


Figura 1.2: Los conjuntos M, $\operatorname{lin} M$, $\operatorname{aff} M$, $\operatorname{pos} M$ y $\operatorname{conv} M$

Si M es un conjunto de $\mathbb{R}^n$, con $\dim M$ nos referiremos a la dimensión de su envoltura afín. Además, denotaremos por $|M|$, $\operatorname{int} M$ y $\operatorname{fr} M$ el cardinal, interior y frontera de M, respectivamente.

Definición 1.1.6 (Suma de Minkowski)**.**
Sean $A, B \in \mathbb{R}^n$. Entonces denotaremos por $A+B$ la suma vectorial de ambos conjuntos, es decir

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

y si $r \in \mathbb{R}$, entonces

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

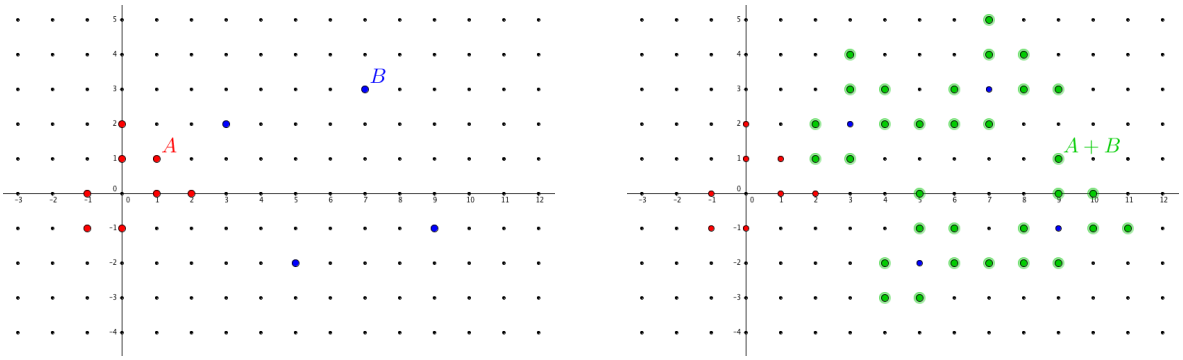


Figura 1.3: Un ejemplo de la suma de dos conjuntos discretos

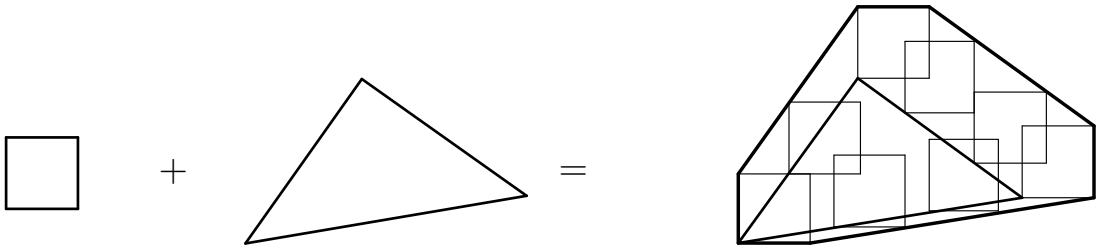


Figura 1.4: Un ejemplo de la suma de dos conjuntos convexos

Definición 1.1.7 (Cuerpo)**.**
Sea K un conjunto compacto de $\mathbb{R}^n$. Entonces decimos que K es un *cuerpo*.

Denotamos al conjunto de todos los *cuerpos convexos* de $\mathbb{R}^n$ como $\mathcal{K}^n$.

Definición 1.1.8 (Símplice)**.**
Sean $x_0, \ldots, x_n \in \mathbb{R}^n$ $n+1$ puntos afínmente independientes. Entonces el cuerpo convexo $S = \text{conv}\{x_0, \ldots, x_n\}$ se denomina *símplice* n-dimensional.

Notación. Denotamos como $\mathcal{K}_0^n$ el conjunto de todos los cuerpos convexos *simétricos respecto al origen (o-simétricos)* de $\mathbb{R}^n$.

$$\mathcal{K}_0^n = \{K \in \mathcal{K}^n : K = -K\}$$

Un ejemplo clásico de cuerpo convexo o-simétrico son las bolas para la norma euclídea, es decir

$$\mathbb{B}_n(r) := \left\{ x = (x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{n} x_i^2 \leq r^2 \right\}.$$

En el caso particular de la bola unidad, es decir, para $r = 1$, escribiremos simplemente $\mathbb{B}_n = \mathbb{B}_n(1)$.

$$\mathbb{B}_n := \left\{ x = (x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{n} x_i^2 \leq 1 \right\}.$$

Aunque las funciones convexas aparecen en numerosos contextos y aplicaciones, existen algunas de particular interés por su estrecha relación con la geometría de los conjuntos.

Una de ellas es la denominada función soporte. Dado que un conjunto convexo cerrado K es la intersección de sus semiespacios soporte, para describir dicho conjunto bastará con describir la posición de sus hiperplanos soporte, es decir, los hiperplanos que contienen al conjunto K en uno de los semiespacios que determinan y que intersecan a K en al menos un punto. Esta descripción se lleva a cabo por medio de la función soporte.

Definición 1.1.9 (Función soporte)**.**
Si $K \in \mathcal{K}^n$ es un cuerpo convexo de $\mathbb{R}^n$ no vacío, se define la *función soporte* $h(K, \cdot) = h_K$ de K como

$$h(K, u) = \text{máx}\{\langle x, u\rangle : x \in K\},$$

para cada $u \in \mathbb{R}^n$.

Usando la definición de función soporte deducimos las siguientes propiedades.

Lema 1.1.10. *Sea $K \in \mathcal{K}^n$ un cuerpo convexo de $\mathbb{R}^n$ no vacío. Entonces:*

1. *$h(K, \lambda u) = \lambda h(K, u)$ si $\lambda \geq 0$ y $h(K, u + v) \leq h(K, u) + h(K, v)$.*
2. *$h_K \leq h_L$ si, y sólo si, $K \subset L$.*
3. *$h(\lambda K, \cdot) = \lambda h(K, \cdot)$ para todo $\lambda \geq 0$, y además $h(-K, u) = h(K, -u)$.*

Notación. Sean $\alpha \in \mathbb{R}$ y $u \in \mathbb{S}^{n-1}$. Entonces denotaremos por $H_{\alpha,u}$ el hiperplano

$$H_{\alpha,u} = \{x \in \mathbb{R}^n : \langle x, u\rangle = \alpha\},$$

y por $H^-_{\alpha,u}$ uno de los semiespacios delimitados por $H_{\alpha,u}$, concretamente

$$H^-_{\alpha,u} = \{x \in \mathbb{R}^n : \langle x, u\rangle \leq \alpha\}.$$

Además, usaremos una notación abreviada para referirnos a los conocidos como hiperplanos coordenados, es decir, aquéllos en los que el vector normal pertenece a la base canónica. De esta forma denotaremos como

$$\{x_i = \alpha\} = H_{\alpha,e_i},$$

para todo $1 \leq i \leq n$.

Definición 1.1.11 (Volumen)**.**
Si $K \subset \mathbb{R}^n$, entonces definimos su *volumen* como la medida de Lebesgue asociada a K,

$$\mathrm{vol}(K) := \mathcal{H}^n(K).$$

$\mathcal{H}^n$ es la notación que usaremos para la medida de Lebesgue n-dimensional.

En los casos en los que necesitemos precisar la dimensión del espacio al que aplicamos el funcional volumen, lo incluiremos como subíndice: si K está contenido en un subespacio (afín) j-dimensional,

$$\mathrm{vol}_j(K) := \mathcal{H}^j(K).$$

El volumen (n-dimensional) es un funcional monótono y homogéneo de grado n, es decir, si $K \subset L$ y $\lambda > 0$, entonces $\mathrm{vol}(K) \leq \mathrm{vol}(L)$ y $\mathrm{vol}(\lambda K) = \lambda^n \mathrm{vol}(K)$.

Notación. Sea $K \subset \mathcal{K}^n$, y sea $t \in \mathbb{R}$ tal que $K \cap \{x_n = t\} \neq \emptyset$. Entonces denotaremos como K_t la sección $(n-1)$-dimensional de K a través del hiperplano $\{x_n = t\}$, es decir

$$K_t := \{(x_1, x_2, \ldots, x_{n-1}) \in \mathbb{R}^{n-1} : (x_1, x_2, \ldots, x_{n-1}, t) \in K\}.$$

Teorema 1.1.12 (Fubini)**.** *Sea K un cuerpo convexo de $\mathbb{R}^n$. Entonces,*

$$\mathrm{vol}(K) = \int_{-\infty}^{\infty} \mathrm{vol}_{n-1}(K_t)\, dt. \tag{1.1}$$

Notación. Denotamos al volumen de la bola unidad por $\kappa_n := \mathrm{vol}_n(\mathbb{B}_n)$.

1.2. Primeras definiciones. Retículos

En esta sección introduciremos los conceptos que necesitamos sobre retículos.

Definición 1.2.1 (Retículo)**.**
Sean $b_1, \ldots, b_n \in \mathbb{R}^n$ linealmente independientes. El conjunto

$$\Lambda = \{z_1 b_1 + z_2 b_2 + \cdots + z_n b_n : z_i \in \mathbb{Z}, 1 \leq i \leq n\}$$

se denomina *retículo*.

El conjunto de los *vectores generadores* $\{b_1, \ldots, b_n\}$ o la matriz $B = (b_1, \ldots, b_n)$ con columnas b_i recibe el nombre de *base* de Λ. Un elemento $b \in \Lambda$ se denomina *punto reticular de* Λ. Denotaremos por $\mathcal{L}^n$ al conjunto de todos los retículos de $\mathbb{R}^n$.

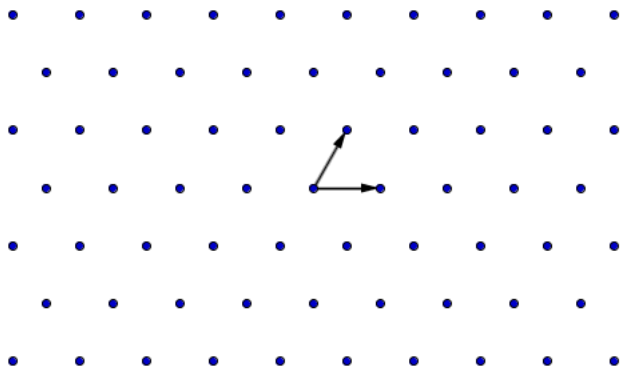


Figura 1.5: El retículo hexagonal generado por los vectores $(1, 0)$ y $(\frac{1}{2}, \frac{\sqrt{3}}{2})$.

Definición 1.2.2 (Retículo entero)**.**
Definimos el *retículo entero* n-dimensional $\mathbb{Z}^n$ como el retículo generado por los vectores de la base canónica $\{e_1, \ldots, e_n\}$, es decir, el subconjunto de los puntos del espacio euclídeo n-dimensional $\mathbb{R}^n$ con coordenadas enteras.

$$\mathbb{Z}^n := \{x = (x_1, \ldots, x_n) \in \mathbb{R}^n : x_i \in \mathbb{Z} \text{ para todo } i = 1, \ldots, n\}.$$

Notación. Denotaremos por $\mathbb{Z}^n_+$ el subconjunto de $\mathbb{Z}^n$ de los puntos con coordenadas no negativas.

$$\mathbb{Z}^n_+ := \{x = (x_1, \ldots, x_n) \in \mathbb{Z}^n : x_i \geq 0,\ \forall\ 1 \leq i \leq n\ \}.$$

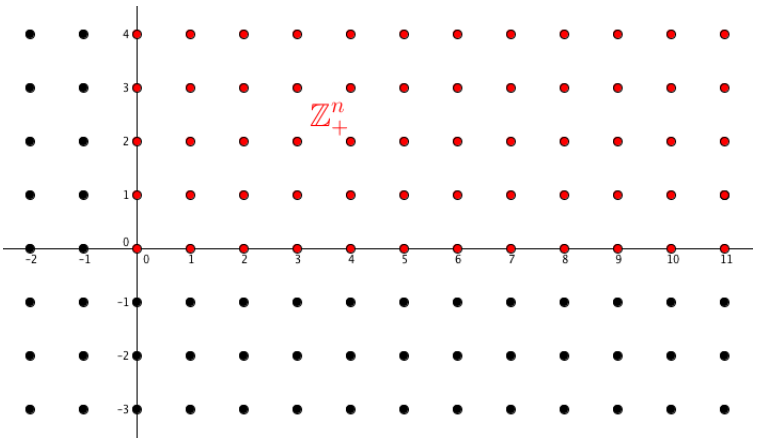


Figura 1.6: El conjunto $\mathbb{Z}^n_+ \subset \mathbb{Z}^n$ en rojo.

Vamos a representar por $\mathbb{Z}^n_c$ el conjunto complementario de $\mathbb{Z}^n_+$ en el retículo entero $\mathbb{Z}^n$, es decir,

$$\mathbb{Z}^n_c := \mathbb{Z}^n \setminus \mathbb{Z}^n_+ = \{v = (v_1, \ldots, v_n) \in \mathbb{Z}^n : v_i < 0 \text{ para al menos un } i\}.$$

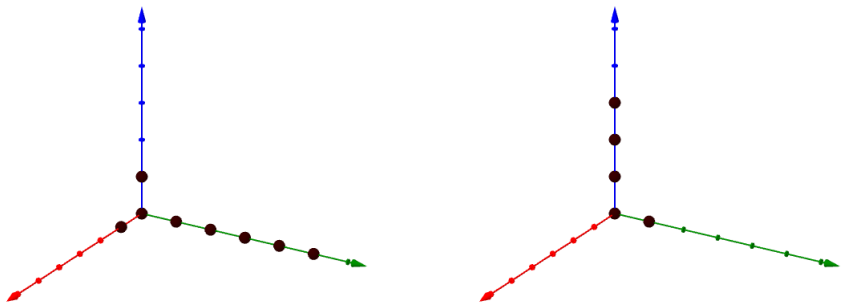
Definición 1.2.3 (Conjunto reticular convexo)**.**
Un conjunto finito F, subconjunto del retículo entero n-dimensional $\mathbb{Z}^n$, se denomina *conjunto reticular convexo* si

$$F = \text{conv}(F) \cap \mathbb{Z}^n.$$

Definición 1.2.4 (Símplice elongado)**.**
Sea F un conjunto reticular convexo con $\dim F = k$, $1 \leq k \leq n$. Si existen enteros i e i_j, $1 \leq j \leq k-1$, entre 1 y n tales que

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

entonces diremos que F es un *símplice elongado* en la dirección de e_i.



(a) Símplice elongado de cardinal 8, dimensión 3, con $i = 2$, $i_1 = 1$, $i_2 = 3$.

(b) Símplice elongado de cardinal 5, dimensión 2, con $i = 3$, $i_1 = 2$.

Figura 1.7: Dos ejemplos de símplice elongado en $\mathbb{R}^3$.

Lema 1.2.5. *Sean $F \subset S \subset \mathbb{Z}^n$ dos símplices elongados en la dirección de e_1 con $\dim F = \dim S = n$. Entonces se tiene que*

$$|F + S| = n|S| + |F| - \frac{n(n+1)}{2}.$$

Demostración. Dado que $F \subset S$ son símplices elongados en la dirección de e_1 con $\dim F = \dim S = n$, podemos asegurar la existencia de dos números naturales l, k tales que

$$F = \{o, e_1, 2e_1, \ldots, le_1, e_2, \ldots, e_n\}$$

y

$$S = \{o, e_1, \ldots, (l+k)e_1, e_2, \ldots, e_n\}.$$

En esta situación, se tiene que

$$S + F = (\{o\} + F) \cup \bigcup_{i=2}^{n} (S + e_i) \cup (S + le_1).$$

Pero en esta expresión de $S + F$ hay puntos comunes en las uniones anteriores: en efecto,

- $(S + e_i) \cap (S + e_j) = \{e_i + e_j\}$, si $i, j \in \{2, \ldots, n\}$ con $j \neq i$;
- $(S + le_1) \cap (S + e_i) = \{e_i + le_1\}$, si $i \in \{2, \ldots, n\}$;
- $(\{o\} + F) \cap (S + e_i) = \{o + e_i\} = \{e_i\}$, si $i = 2, \ldots, n$;
- $(\{o\} + F) \cap (S + le_1) = \{le_1\}$;
- además, dado que las intersecciones anteriores (dos a dos) son distintas, las intersecciones de tres o más conjuntos son vacías.

Así pues, usando el principio de inclusión-exclusión concluimos que

$$|F + S| = n|S| + |F| - \frac{n(n+1)}{2}. \qquad \square$$

Capítulo 2

La desigualdad clásica de Brunn-Minkowski

Esta sección está dedicada fundamentalmente a estudiar la llamada desigualdad de Brunn-Minkowski, la cual ha constituido la pieza clave para el desarrollo de la llamada *Teoría de Brunn-Minkowski*, núcleo de la Geometría Convexa.

2.1. Motivación y contexto de la desigualdad

Consideramos un cuerpo convexo en $\mathbb{R}^3$ sobre el que efectuamos tres cortes paralelos. Resulta intuitivo el hecho de que el corte intermedio no puede tener área más pequeña que los otros dos (aunque su demostración no es algo evidente).

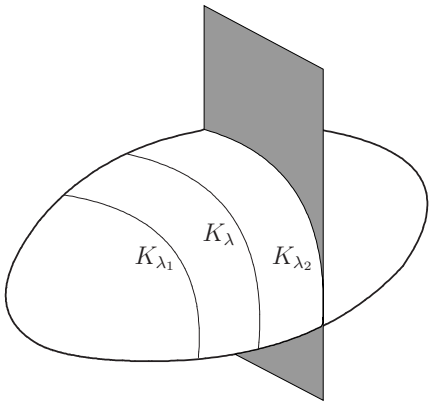


Figura 2.1: Si $\lambda_1 < \lambda < \lambda_2$, entonces $A(K_\lambda) \geq \text{mín}\{A(K_{\lambda_1}), A(K_{\lambda_2})\}$.

Formulemos el problema con mayor precisión: elegimos un sistema de coordenadas de

tal forma que las secciones sean perpendiculares al eje x_1, y representamos por $v(\lambda)$ el área de la sección determinada por el plano de corte $\{x_1 = \lambda_1\}$. Entonces, la afirmación anterior puede enunciarse del siguiente modo:

$$\text{para cada } \lambda_1 < \lambda < \lambda_2 \text{ se tiene que } v(\lambda) \geq \text{mín}\{v(\lambda_1), v(\lambda_2)\},$$

siendo λ_1, λ_2 dos valores cualesquiera del dominio de definición de $v(\lambda)$. Por tanto, existe un λ_0 para el cual la aplicación $\lambda \to v(\lambda)$ es no decreciente en un cierto intervalo $[\lambda_m, \lambda_0]$, y es no creciente en otro intervalo $[\lambda_0, \lambda_M]$.

Un resultado "similar" va a ser cierto también en $\mathbb{R}^{n+1}$, si $v(\lambda)$ representa el volumen n-dimensional de la intersección del cuerpo K con el hiperplano $\{x_1 = \lambda\}$. Pero, ¿cómo demostrar tal afirmación? En el caso plano es fácil ver que $v(\lambda)$ es una función cóncava en el intervalo obtenido al "proyectar" el cuerpo K sobre el eje x_1 (véase la figura 2.2), lo que prueba a su vez la afirmación anterior.

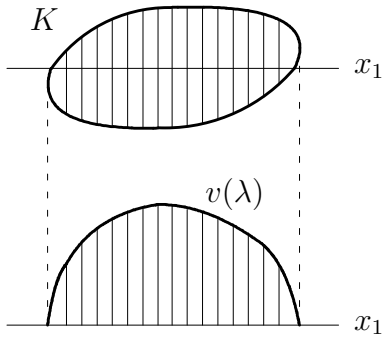
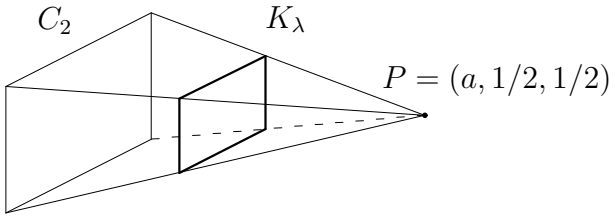


Figura 2.2: La función $v(\lambda)$ es una función cóncava en el plano.

Esto podría llevar a pensar que, para un intervalo apropiado, $v(\lambda)$ es cóncava en dimensión arbitraria. Sin embargo, esto es falso, lo que puede comprobarse fácilmente incluso en el caso más sencillo de dimensión tres: basta considerar como cuerpo K la envoltura convexa del cuadrado $C_2 = [0,1] \times [0,1]$ y el punto $P = (a, 1/2, 1/2) \notin \text{aff}\, C_2$.



$$v(\lambda) = A(K_\lambda) = \left(\frac{a-\lambda}{a}\right)^2$$

Figura 2.3: Una función $v(\lambda) = A(K_\lambda)$ en $\mathbb{R}^3$ que no es cóncava.

Claramente, $v(\lambda)$ no es una función cóncava. Sí va a existir, sin embargo, concavidad en juego, aunque la función correcta que hay que considerar en $\mathbb{R}^{n+1}$ no es $v(\lambda)$ sino $v(\lambda)^{1/n}$.

La *desigualdad de Brunn-Minkowski*, uno de los resultados fundamentales de la Teoría de los Conjuntos Convexos, da respuesta a la cuestión que nos hemos planteado.

Teorema 2.1.1 (La desigualdad de Brunn-Minkowski)**.** *Sean K y L dos conjuntos convexos y compactos de $\mathbb{R}^n$ no vacíos, y sea $0 \leq \lambda \leq 1$. Entonces*

$$\mathrm{vol}\left((1-\lambda)K + \lambda L\right)^{1/n} \geq (1-\lambda)\mathrm{vol}(K)^{1/n} + \lambda \mathrm{vol}(L)^{1/n}, \tag{2.1}$$

dándose la igualdad, para algún $\lambda \in (0,1)$, si y sólo si o K y L están en hiperplanos paralelos (si tienen dimensión menor que n), o son homotéticos (si tienen dimensión n).

Como $K, L \in \mathcal{K}^n$, podemos verlos embebidos en $\mathbb{R}^{n+1}$, y contenidos a su vez en dos hiperplanos n-dimensionales paralelos, digamos $\{x_1 = 0\}$ y $\{x_1 = 1\}$. En esas condiciones podemos determinar $(1-\lambda)K + \lambda L$ (véase la figura 2.4) como

$$(1-\lambda)K + \lambda L = \Big\{ \mathrm{conv}(K \cup L) \Big\} \cap \Big\{ (x_1, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} : x_1 = \lambda \Big\}.$$

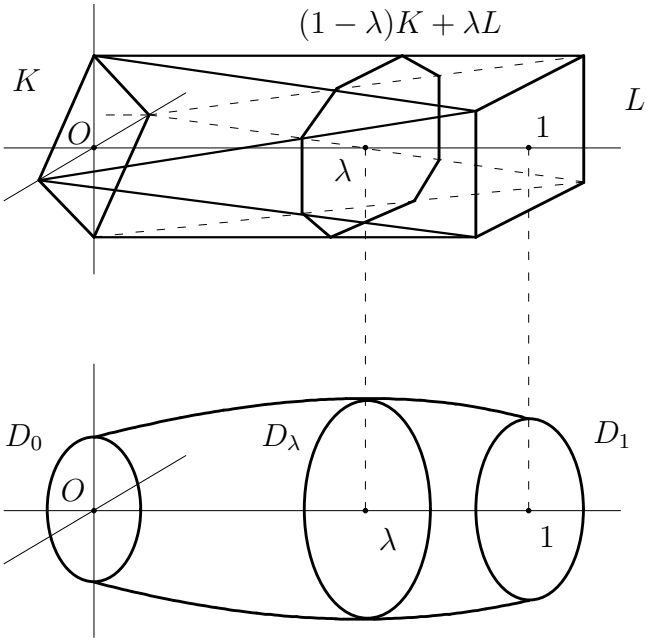


Figura 2.4: La geometría de la desigualdad de Brunn-Minkowski.

Representamos por B_n^λ la bola n-dimensional de $\mathbb{R}^{n+1}$ que está contenida en el hiperplano $\{x_1 = \lambda\}$, con centro en el eje x_1 y con volumen n-dimensional

$$\mathrm{vol}(B_n^\lambda) = v(\lambda) = \mathrm{vol}((1-\lambda)K + \lambda L).$$

Si construimos el cuerpo $D = \bigcup_{0\leq\lambda\leq 1} B_n^\lambda$, el teorema de Brunn-Minkowski 2.1.1 nos asegura que D es convexo. O en otras palabras: si $r(\lambda)$ es el radio de la bola B_n^λ, esto es,

$$r(\lambda) = \frac{\mathrm{vol}(B_n^\lambda)^{1/n}}{\kappa_n^{1/n}} = \frac{v(\lambda)^{1/n}}{\kappa_n^{1/n}},$$

el teorema de Brunn-Minkowski 2.1.1 nos asegura que $r(\lambda)$ es una función cóncava. De aquí se deduce además que $v(\lambda)^{1/n}$ es también una función cóncava, lo que da respuesta al problea que nos planteábamos al comienzo de esta sección.

2.2. Demostración de la desigualdad

Demostración del teorema 2.1.1. Si K, L están en hiperplanos paralelos, $(1-\lambda)K + \lambda L$ lo está también y por lo tanto $\mathrm{vol}\big((1-\lambda)K+\lambda L\big) = 0$ y se da la igualdad.

Si $\dim K < n$ y $\dim L < n$, entonces tenemos $\mathrm{vol}(K) = 0$ y $\mathrm{vol}(L) = 0$ y en consecuencia se satisface (2.1) trivialmente. Además, si hay igualdad, entonces $\dim\big((1-\lambda)K+\lambda L\big) < n$, es decir, $(1-\lambda)K+\lambda L$ está en un hiperplano H y por tanto, K y L están en hiperplanos paralelos a H.

Si $\dim K < n$ y $\dim L = n$, consideramos la inclusión $(1-\lambda)K + \lambda L \supset (1-\lambda)x + \lambda L$ para cualquier $x \in K$, entonces

$$\mathrm{vol}\left((1-\lambda)K+\lambda L\right)^{1/n} \geq \mathrm{vol}\left((1-\lambda)x+\lambda L\right)^{1/n} = \lambda \mathrm{vol}(L)^{1/n},$$

dándose además la igualdad si, y sólo si $K = \{x\}$. En tal caso, K y L son homotéticos (por convenio).

Por tanto, podemos suponer que $\dim K = \dim L = n$. Podemos asumir sin pérdida de generalidad además que $\mathrm{vol}(K) = \mathrm{vol}(L) = 1$: en efecto, si tenemos (2.1) probada bajo esta hipótesis y $K, L \in \mathcal{K}^n$ arbitrarios, basta tomar $\overline{K} = \mathrm{vol}(K)^{-1/n}K$, $\overline{L} = \mathrm{vol}(L)^{-1/n}L$,

$$\overline{\lambda} = \frac{\lambda \mathrm{vol}(L)^{1/n}}{(1-\lambda)\mathrm{vol}(K)^{1/n} + \lambda \mathrm{vol}(L)^{1/n}}.$$

Como $\mathrm{vol}(\overline{K}) = \mathrm{vol}(\overline{L}) = 1$ y $0 \leq \overline{\lambda} \leq 1$, podemos aplicar nuestra desigualdad, es decir,

$$\begin{aligned}\mathrm{vol}((1-\overline{\lambda})\overline{K} + \overline{\lambda}\overline{L}) &\geq \big((1-\overline{\lambda})\mathrm{vol}(\overline{K})^{1/n} + \overline{\lambda}\mathrm{vol}(\overline{L})^{1/n}\big)^n \\ &= (1-\overline{\lambda}+\overline{\lambda})^n = 1.\end{aligned}$$

Y sustituyendo los valores de $\overline{K}$, $\overline{L}$ y $\overline{\lambda}$ se tiene que

$$(1-\overline{\lambda})\overline{K} + \overline{\lambda}\overline{L} = \frac{1-\lambda}{(1-\lambda)\mathrm{vol}(K)^{1/n} + \lambda\mathrm{vol}(L)^{1/n}}K + \frac{\lambda}{(1-\lambda)\mathrm{vol}(K)^{1/n} + \lambda\mathrm{vol}(L)^{1/n}}L,$$

de donde se deduce (2.1) para K y L.

Buscamos entonces obtener

$$\mathrm{vol}\big((1-\lambda)K+\lambda L\big)\geq 1 \tag{2.2}$$

para covexos $K, L \in \mathcal{K}^n$ con $\dim K = \dim L = n$ y $\mathrm{vol}(K) = \mathrm{vol}(L) = 1$.

Demostraremos (2.2) por inducción sobre la dimensión de nuestros conjuntos. El caso $n = 1$ es evidente: dadas las hipótesis sobre K y L no hay otra opción que sean segmentos de longitud 1 sobre la misma recta, con lo que tenemos igualdad en (2.2).

Supongamos pues $n \geq 2$ y que (2.2) es cierto para $n-1$. Fijamos $u \in \mathbb{S}^{n-1}$ arbitrario y, en consecuencia, simplificamos la notación de los hiperplanos $H_\alpha = H_{\alpha,u}$.

Sean $\alpha_\lambda = -h((1-\lambda)K+\lambda L, -u)$, $\beta_\lambda = h((1-\lambda)K+\lambda L, u)$ con $\lambda \in [0,1]$.

Para $c \in \mathbb{R}$, definimos

$$v_0(c) = \mathrm{vol}_{n-1}(K \cap H_c), \quad v_1(c) = \mathrm{vol}_{n-1}(L \cap H_c),$$

$$w_0(c) = \mathrm{vol}_n(K \cap H_c^-) \quad \text{y} \quad w_1(c) = \mathrm{vol}_n(L \cap H_c^-).$$

Entonces, usando el teorema de Fubini 1.1.12, tenemos que

$$w_i(c) = \int_{-\infty}^{c} v_i(t)dt = \int_{\alpha_i}^{c} v_i(t)dt, \text{ para } i = 0, 1.$$

Obsérvese que tenemos que integrar entre el $\max\langle x, u\rangle$ (o c, en nuestro caso) y el $\min\langle x, u\rangle$, es decir, "donde empieza" el conjunto y "donde acaba". Y sabemos que

$$\min_{x\in K}\langle x, u\rangle = -\max_{x\in K}\langle x, -u\rangle = -h(K, -u) = \alpha_0,$$

y que

$$\min_{x\in L}\langle x, u\rangle = -\max_{x\in L}\langle x, -u\rangle = -h(L, -u) = \alpha_1$$

Para cada $i = 0, 1$, la función v_i es continua en el intervalo (α_i, β_i), luego w_i es diferenciable y se tiene por tanto que $w_i'(c) = v_i(c) > 0$, si $c \in (\alpha_i, \beta_i)$. Tomamos la función inversa de w_i, $z_i = w_i^{-1}$. Entonces

$$z_i'(t) = \frac{1}{w_i'(z_i(t))} = \frac{1}{v_i(z_i(t))}, \tag{2.3}$$

para $t \in (0, 1)$, pues w_i representa el volumen de partes de K (o L) que, a lo sumo valen $\mathrm{vol}(K) = \mathrm{vol}(L) = 1$.

Dado que

$$\big((1-\lambda)K+\lambda L\big) \cap H_{(1-\lambda)z_0(t)+\lambda z_1(t)} \supset (1-\lambda)\big(K \cap H_{z_0(t)}\big) + \lambda\big(L \cap H_{z_1(t)}\big),$$

si denotamos por $z_\lambda(t) = (1-\lambda)z_0(t)+\lambda z_1(t)$, $K_t = K \cap H_{z_0(t)}$ y $L_t = L \cap H_{z_1(t)}$, podemos escribir

$$\big((1-\lambda)K+\lambda L\big) \cap H_{z_\lambda(t)} \supset (1-\lambda)K_t + \lambda L_t \tag{2.4}$$

para todo $0 < t < 1$. Además,

$$z'_\lambda(t) = (1-\lambda)z'_0(t) + \lambda z'_1(t) = \frac{1-\lambda}{v_0(z_0(t))} + \frac{\lambda}{v_1(z_1(t))},$$

por lo que si usamos el cambio de variable $s = z_\lambda(t)$, $0 < t < 1$, la inclusión (2.4), la hipótesis de inducción y las definiciones de v_0 y v_1 (en ese orden) llegamos a que

$$\begin{aligned}
\mathrm{vol}\big((1-\lambda)K + \lambda L\big) &= \int_{\alpha_\lambda}^{\beta_\lambda} \mathrm{vol}_{n-1}\Big(\big[(1-\lambda)K + \lambda L\big] \cap H_s\Big) ds \\
&= \int_0^1 \mathrm{vol}_{n-1}\Big(\big[(1-\lambda)K + \lambda L\big] \cap H_{z_\lambda(t)}\Big) z'_\lambda(t) dt \\
&\geq \int_0^1 \mathrm{vol}_{n-1}\Big((1-\lambda)K_t + \lambda L_t\Big) \left(\frac{1-\lambda}{v_0(z_0(t))} + \frac{\lambda}{v_1(z_1(t))}\right) dt \\
&\geq \int_0^1 \Big((1-\lambda)\mathrm{vol}_{n-1}(K_t)^{\frac{1}{n-1}} + \lambda \mathrm{vol}_{n-1}(L_t)^{\frac{1}{n-1}}\Big)^{n-1} \left(\frac{1-\lambda}{v_0(z_0(t))} + \frac{\lambda}{v_1(z_1(t))}\right) dt \\
&= \int_0^1 \Big((1-\lambda)v_0(z_0(t))^{\frac{1}{n-1}} + \lambda v_1(z_1(t))^{\frac{1}{n-1}}\Big)^{n-1} \left(\frac{1-\lambda}{v_0(z_0(t))} + \frac{\lambda}{v_1(z_1(t))}\right) dt.
\end{aligned}$$

Podemos asegurar, tomando logaritmos y usando la convexidad estricta de la función $f(x) = x^{-p}$, que se verifica la desigualdad numérica

$$\big((1-\lambda)v_0^p + \lambda v_1^p\big)^{1/p} \left(\frac{1-\lambda}{v_0} + \frac{\lambda}{v_1}\right) \geq 1,$$

para $v_0, v_1, p > 0$, $0 < \lambda < 1$, dándose la igualdad si, y sólo si $v_0 = v_1$.

Deducimos así la veracidad de (2.2):

$$\mathrm{vol}\big((1-\lambda)K + \lambda L\big) \geq \int_0^1 1 \, dt = 1.$$

Supongamos ahora que $\mathrm{vol}\big((1-\lambda)K + \lambda L\big) = 1$ para algún $\lambda \in (0,1)$. Entonces tenemos que $v_0(z_0(t)) = v_1(z_1(t))$ y, usando (2.3), deducimos que $z'_0(t) = z'_1(t)$ para $0 \leq t \leq 1$, lo que implica que $z_1(t) - z_0(t)$ es constante.

Suponemos, sin pérdida de generalidad, que el centro de gravedad de K y L se encuentra en el origen, lo que implica que

$$0 = \int_K \langle x, u\rangle dx.$$

Si consideramos los hiperplanos H_s, $\alpha_0 \leq s \leq \beta_0$, podemos resolver la integral anterior para cada valor de la altura s, $\langle x, u\rangle = s$, y además la medida de la sección correspondiente a esa altura viene dada por $\mathrm{vol}_{n-1}(K \cap H_s)$; en consecuencia

$$0 = \int_K \langle x, u\rangle dx = \int_{\alpha_0}^{\beta_0} \mathrm{vol}_{n-1}(K \cap H_s) \; s \; ds.$$

Realizando el cambio de variable $s = z_0(t)$, utilizando la definición de v_0 y gracias a (2.3), obtenemos que

$$\begin{aligned} 0 &= \int_{\alpha_0}^{\beta_0} \mathrm{vol}_{n-1}(K \cap H_s)\ s\ ds \\ &= \int_0^1 \mathrm{vol}_{n-1}\big(K \cap H_{z_0(t)}\big) z_0(t) z_0'(t) dt \\ &= \int_0^1 v_0(z_0(t)) z_0(t) \frac{1}{v_0(z_0(t))} dt \\ &= \int_0^1 z_0(t) dt. \end{aligned}$$

Análogamente

$$\int_0^1 z_1(t) dt = 0,$$

de donde concluimos, puesto que $z_1(t) - z_0(t)$ es constante, que $z_1(t) - z_0(t) = 0$, es decir, $z_1(t) = z_0(t)$ para todo $t \in [0, 1]$.

Recordemos que hemos definido z_i como la función inversa de w_i, por lo que si $z_0(1) = c$, entonces tenemos que

$$1 = w_0(c) = \mathrm{vol}\big(K \cap H_c^-\big).$$

En consecuencia, para que $w_0(c) = 1$, debemos tener $K = K \cap H_c^-$ y por tanto debe ser $c = \beta_0 = h(K, u)$.

Análogamente, $z_1(1) = h(L, u)$, luego

$$h(K, u) = z_0(1) = z_1(1) = h(L, u)$$

para todo $u \in \mathbb{S}^{n-1}$. Usando el lema 1.1.10, concluimos que $K = L$. □

Capítulo 3

La desigualdad discreta de Brunn-Minkowski

Puesto que la desigualdad de Brunn-Minkowski viene expresada en términos de volúmenes, en este capítulo nos vamos a centrar en el caso que no queda contemplado cuando se trabaja con el funcional volumen: el caso discreto (finito). Por supuesto, ahora no disponemos del funcional volumen pero, puesto que vamos a manejar conjuntos finitos, podemos usar el cardinal.

Ahora comenzamos con las preguntas más básicas: dados los cardinales $|A|$ y $|B|$ de dos conjuntos finitos de $\mathbb{R}^n$, ¿qué podemos decir del cardinal $|A+B|$?

Tenemos una cota superior muy simple,

$$|A+B| \leq |A||B|,$$

y la igualdad se alcanza cuando A y B son conjuntos, digamos genéricos, que no tienen ninguna estructura. De forma más precisa, se tiene igualdad siempre que cada punto de $A+B$ se exprese de forma única como suma de un punto de A más un punto de B. De todas formas, al igual que ocurre con la desigualdad de Brunn-Minkowski (2.1), los resultados más interesantes vienen de buscar cotas inferiores para el cardinal $|A+B|$.

En este capítulo vamos a extender la desigualdad clásica de Brunn-Minkowski a una versión válida para conjuntos discretos. El capítulo se basa en un artículo de R. J. Gardner y P. Gronchi (véase [2]).

3.1. Cotas previas para $|A+B|$

Anteriormente a los resultados que vamos a introducir y demostrar, ya existían algunas desigualdades para obtener información sobre el cardinal de la suma de dos conjuntos.

Uno de los ejemplos más simples por su expresión, utilidad y demostración es el siguiente. Cabe destacar la fórmula es lineal sobre los cardinales de los conjuntos finitos y da una cota muy fácil de calcular.

Primero hagamos una observación básica: si trasladamos nuestros conjuntos A, B en cualquier dirección, esto no afecta a los cardinales $|A|$, $|B|$, o $|A+B|$ (o $|A-B|$, etc.).

Proposición 3.1.1. *Si $A, B \subset \mathbb{R}^n$ son conjuntos finitos, entonces*

$$|A+B| \geq |A| + |B| - 1. \tag{3.1}$$

Demostración. Necesitamos recordar el *orden lexicográfico* de $\mathbb{R}^n$: dados $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ diremos que $x < y$ si existe $j \in \{1, \ldots, n\}$ tal que $x_j < y_j$ y $x_i = y_i$ para todo i con $1 \leq i < j$.

Basta entonces con trasladar A haciendo que el máximo punto de A en el orden lexicográfico coincida con el origen de coordenadas y trasladar B haciendo que el mínimo punto de B en el orden coincida también con el origen de coordenadas.

De esta forma, los cardinales de A, B, y $A+B$ no cambian, pero tenemos garantizado que $A \cup B \subset A + B$. Esto concluye la prueba puesto que

$$|A \cup B| = |A| + |B| - |A \cap B| = |A| + |B| - 1,$$

ya que $A \cap B = \{o\}$. □

Observación 3.1.2. En general, ésta es la mejor cota posible de este tipo. Por ejemplo, si $A = \{1, \ldots, k\}$ y $B = \{1, \ldots, l\}$, para $k, l \in \mathbb{N}$, la ecuación (3.1) se satisface con igualdad.

Cabe destacar que (3.1) se puede generalizar al contexto de los grupos ordenados y libres de torsión (véase, por ejemplo, [5]).

En 1994, Ruzsa [6] demostró una cota inferior para $|A+B|$ más fina que (3.1). Concretamente, probó el siguiente resultado.

Teorema 3.1.3. *Si $A, B \subset \mathbb{R}^n$ son conjuntos finitos con $|B| \leq |A|$ y $\dim(A+B) = n$, entonces*

$$|A+B| \geq |A| + \sum_{i=1}^{|B|-1} \text{mín}\{n, |A| - i\}. \tag{3.2}$$

La demostración original de Ruzsa es más larga que la que aquí presentamos, en la que utilizaremos algunos de los resultados que vamos a desarrollar para la prueba de la desigualdad de Brunn-Minkowski discreta. Por tanto, veremos su demostración en la sección 3.3.1.

3.2. Reducción al retículo entero

En esta sección veremos que es suficiente trabajar con conjuntos del retículo entero $\mathbb{Z}^n$ cuando se trata de estudiar el cardinal de la suma de Minkowski (corolario 3.2.3).

Lema 3.2.1. *Sean $A, B \subset \mathbb{Z}^n$ conjuntos finitos conteniendo al origen. Entonces existe una aplicación lineal $f : \mathbb{Z}^n \to \mathbb{Z}^{n-1}$ tal que $f|_{A+B}$ es inyectiva.*

Demostración. Sea $k \in \mathbb{N}$ tal que $k > \operatorname{diam}(A + B)$. Si $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$, definimos f como

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

Veamos que es inyectiva. Si suponemos que $x, y \in A + B$ con $f(x) = f(y)$, entonces $x_i = y_i$, para $2 \leq i \leq n-1$, y $x_1 + kx_n = y_1 + ky_n$, es decir $x_1 - y_1 = k(y_n - x_n)$. Si $x_n \neq y_n$, entonces $|x_1 - y_1| = k|y_n - x_n| \geq k$, contradiciendo que $k > \operatorname{diam}(A+B)$. Se sigue entonces que $x_n = y_n$, por lo que $x_1 = y_1$ y concluimos que $x = y$, como queríamos. □

Teorema 3.2.2. *Sean $A, B \subset \mathbb{R}^n$ conjuntos finitos conteniendo al origen. Entonces existe una aplicación lineal e inyectiva $\phi : A + B \to \mathbb{Z}^n$ tal que preserva las dimensiones de A y $A + B$, es decir, tal que $\dim \phi(A) = \dim A$ y $\dim \phi(A + B) = \dim(A + B)$.*

Demostración. Haremos la demostración por inducción en la dimensión. Supongamos primero que $n = 1$. Sea E el conjunto de todas las combinaciones lineales de los elementos de $A + B$ con coeficientes racionales, esto es, el subespacio vectorial sobre $\mathbb{Q}$ generado por $A + B$. Entonces E tiene dimensión $d \leq |A + B| - 1$.

Sea $\{c_1, \ldots, c_d\}$ una base del conjunto E. Si $x \in A + B$ y $x = q_1c_1 + \cdots + q_dc_d$, definimos $h : A + B \to \mathbb{Q}^d$ como

$$h(x) := (q_1, \ldots, q_d) \in \mathbb{Q}^d.$$

Al ser $A+B$ un conjunto finito, es posible encontrar un entero r tal que $r \cdot h(x) \in \mathbb{Z}^d$ para todo $x \in A+B$. De esta forma conseguimos una aplicación lineal inyectiva $g : A+B \to \mathbb{Z}^d$.

Como aplicación del lema 3.2.1, reemplazando $A + B$ por $g(A + B)$ conseguiríamos una aplicación $f \circ g : A + B \to \mathbb{Z}^{d-1}$. Aplicando el lema 3.2.1 otras $d - 2$ veces, podemos llegar hasta una aplicación lineal e inyectiva $\phi : A+B \to \mathbb{Z}$. Esta aplicación ϕ claramente preserva las dimensiones, lo que completa la prueba para $n = 1$.

Pasamos ahora a considerar el caso $n > 1$. Podemos asumir, sin pérdida de generalidad, que $\dim(A+B) = n$. Aplicando una transformación lineal no-singular (multiplicando por una matriz invertible), si fuera necesario, podemos asumir que $e_i \in A$, $1 \leq i \leq \dim A$, y que $e_i \in B$, $\dim A + 1 \leq i \leq n$.

Si C es un conjunto finito de $\mathbb{Z}^n$ y $1 \leq i \leq n$, denotamos por

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

Sean $\phi_i : (A+B)_i \to \mathbb{Z}$ las aplicaciones construidas en el caso $n = 1$ y reemplazando A y B por los conjuntos A_i y B_i. Definimos $\phi : A + B \to \mathbb{Z}^n$ por

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

Claramente ϕ es lineal e inyectiva. Más aún, ϕ preserva las dimensiones de A y $A + B$ dado que para cada i, $\phi(e_i) = t_i e_i$, donde $t_i \neq 0$. □

Corolario 3.2.3. *Sean $A, B \subset \mathbb{R}^n$ conjuntos finitos. Entonces existen subconjuntos $A', B' \subset \mathbb{Z}^n$ satisfaciendo*

1. $|A'| = |A|$, $|B'| = |B|$, *y* $|A' + B'| = |A + B|$.
2. $\dim A' = \dim A$ *y* $\dim(A' + B') = \dim(A + B)$.

Demostración. Trasladando A y B, si fuera necesario, podemos asumir que ambos contienen al origen. Basta considerar $A' := \phi(A)$ y $B' := \phi(B)$, donde ϕ es la aplicación lineal inyectiva garantizada por el teorema 3.2.2. □

3.3. Compresiones

Gracias al corolario 3.2.3 podemos centrar nuestros esfuerzos en trabajar con subconjuntos del retículo entero n-dimensional $\mathbb{Z}^n$. En esta sección emplearemos las conocidas como compresiones (véase [1]).

Definición 3.3.1 (líneas paralelas a un vector)**.**
Para vectores $v \in \mathbb{Z}_c^n$ definiremos *las líneas paralelas a v* sobre el punto $x \in \mathbb{Z}^n$ como

$$L_v(x) = \{x + mv \in \mathbb{Z}^n : m \in \mathbb{Z}\}.$$

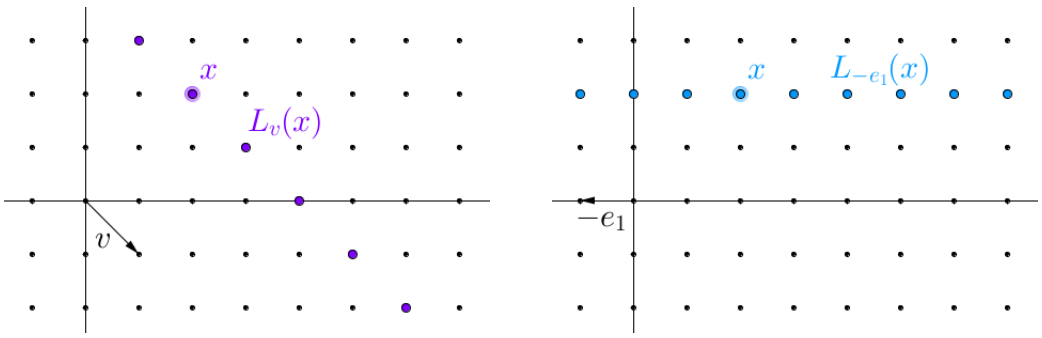


Figura 3.1: Ejemplos de líneas paralelas a distintos vectores sobre el punto $(2, 2) \in \mathbb{Z}^2$.

Notación. Si $v \in \mathbb{Z}_c^n$, denotaremos entonces

$$\mathbb{Z}(v) = \{x \in \mathbb{Z}_+^n : x + v \in \mathbb{Z}_c^n\}.$$

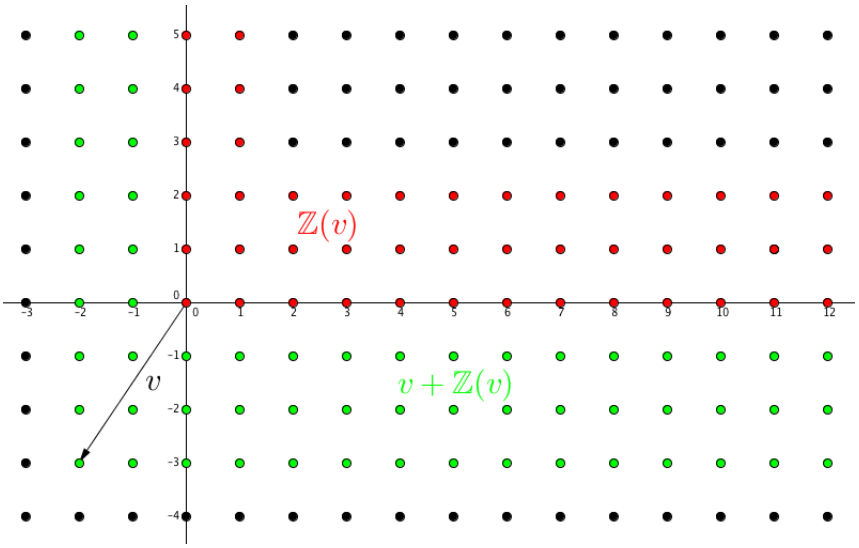


Figura 3.2: El conjunto $\mathbb{Z}(v)$ (en rojo) junto a $v + \mathbb{Z}(v) \subset \mathbb{Z}_c^2$ (en verde).

Proposición 3.3.2. *Dado $v \in \mathbb{Z}_c^n$, las líneas paralelas $L_v(a)$ sobre puntos de $a \in \mathbb{Z}(v)$ forman una partición de $\mathbb{Z}_+^n$, cuyos representantes podemos tomar en $\mathbb{Z}(v)$.*

Demostración. Tenemos que comprobar que

$$|L_v(a) \cap \mathbb{Z}(v)| = 1.$$

Primero vamos a probar que $L_v(a) \cap \mathbb{Z}(v) \neq \emptyset$, es decir, existe $x \in \mathbb{Z}(v)$ con $a + mv = x$ para cierto $m \in \mathbb{N}$:

Tomamos $m = \text{máx}\{p \in \mathbb{N} : a + pv \in \mathbb{Z}_+^n\}$. Tenemos garantizada la existencia de dicho máximo ya que para todo $w \in \mathbb{Z}_c^n$ se tiene que $L_w(y) \not\subset \mathbb{Z}_+^n$ para cualquier $y \in \mathbb{Z}_+^n$. Como $x = a + mv \in \mathbb{Z}_+^n$ y $x + v = a + (m+1)v \notin \mathbb{Z}_+^n$ tenemos que $x \in L_v(a) \cap \mathbb{Z}(v)$.

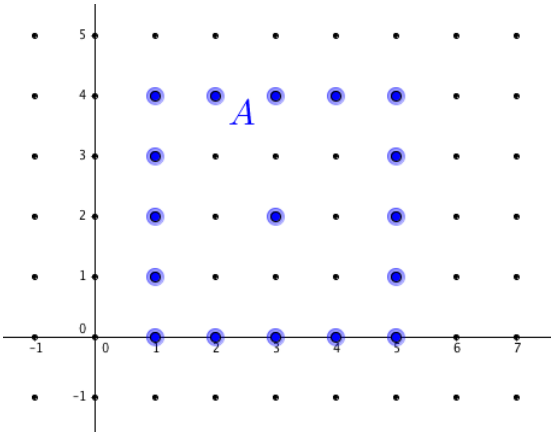
Ahora vamos a ver que si $x \in \mathbb{Z}(v)$, entonces $x - v \notin \mathbb{Z}(v)$, lo que acabaría la prueba.

Si $x - v \in \mathbb{Z}(v)$, entonces por definición tendríamos que $x = (x - v) + v \in \mathbb{Z}(v)$, en contra de que $x \in \mathbb{Z}(v)$. □

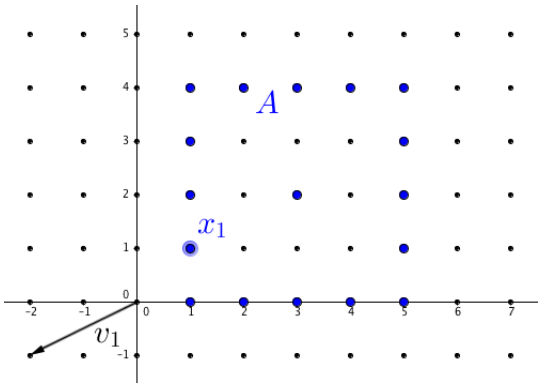
Definición 3.3.3 (Sección)**.**
Supongamos que $A \subset \mathbb{Z}_+^n$ es un conjunto finito, que $v \in \mathbb{Z}_c^n$, y que $x \in \mathbb{Z}(v)$. Definimos la *v-sección* de A en x como

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

Cabe remarcar que las v-secciones de A son conjuntos de números naturales, no conjuntos sobre A, ni sobre $\mathbb{Z}^n$.

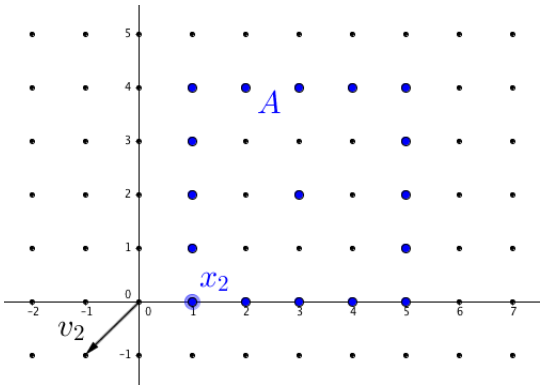


(a) El conjunto A.



(b) $v_1 = (-2, -1) \in \mathbb{Z}_c^n$, $x_1 = (1, 1) \in \mathbb{Z}(v_1)$

(c) $A_{v_1}(x_1)$



(d) $v_2 = (-1, -1) \in \mathbb{Z}_c^n$, $x_2 = (1, 0) \in \mathbb{Z}(v_2)$

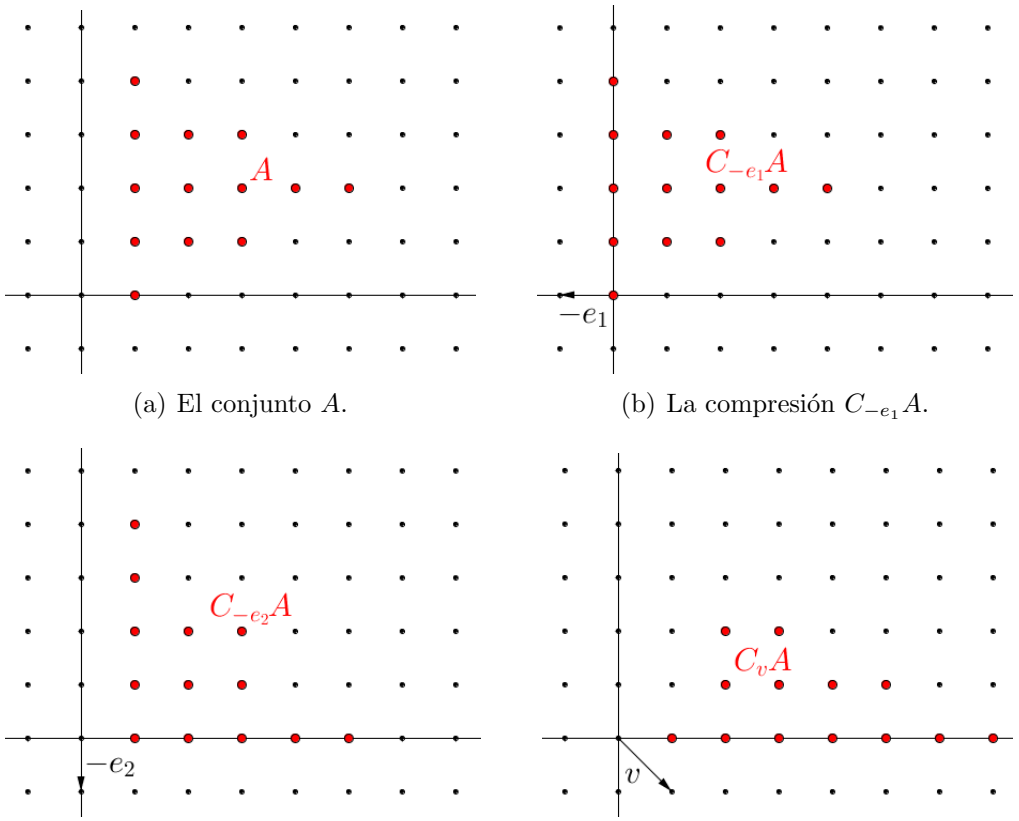
(e) $A_{v_2}(x_2)$

Figura 3.3: Un conjunto $A \subset \mathbb{Z}_+^n$, dos vectores $v_1, v_2 \in \mathbb{Z}_c^n$, dos puntos x_1, x_2 y sus respectivas secciones $A_{v_1}(x_1), A_{v_2}(x_2)$.

Definición 3.3.4 (Compresión)**.**
Si $A \subset \mathbb{Z}_+^n$ es un conjunto finito, entonces definimos la *v-compresión* C_vA de A, $v \in \mathbb{Z}_+^n$, como el único conjunto tal que

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

para todo $x \in \mathbb{Z}^n$. El conjunto A se dice *v-compreso* si $C_vA = A$.



(a) El conjunto A.
(b) La compresión $C_{-e_1}A$.
(c) La compresión $C_{-e_2}A$.
(d) La compresión C_vA con $v = e_1 - e_2$.

Figura 3.4: Un conjunto A finito y sus v-compresiones para distintos vectores $v \in \mathbb{Z}_c^2$.

Obsérvese que dado $v \in \mathbb{Z}_c^n$ y un conjunto finito $A \subset \mathbb{Z}_+^n$, podemos construir C_vA sustituyendo los puntos $a \in A$ por $a + kv$, siempre que $a + kv \in \mathbb{Z}_+^n$ y que $a + kv$ no estuviera previamente en el conjunto, con $k \in \mathbb{N}$ el máximo de los números naturales para los cuales se dan estas dos condiciones.

Cabe destacar además que las v-compresiones no modifican el cardinal de las líneas paralelas a v, es decir, que

$$|C_vA \cap L_v(x)| = |A \cap L_v(x)|,$$

para todo $v \in \mathbb{Z}_c^n$ y $x \in \mathbb{Z}(v)$.

La observación anterior permite obtener de forma inmediata la siguiente propiedad.

Lema 3.3.5. *Si $A \subset \mathbb{Z}_+^n$ es un conjunto finito, entonces A es v-compreso si y sólo si $x \in A$ y $x + v \in \mathbb{Z}_+^n$ implican que $x + v \in A$.*

Definición 3.3.6 (Conjunto inferior)**.**
Decimos que $A \subset \mathbb{Z}_+^n$ es un *conjunto inferior* si es $-e_i$-compreso para todo i con $1 \leq i \leq n$.

Notación. Denotamos por W a

$$W = \{v = (v_1, \ldots, v_n) \in \mathbb{Z}^n : v_i = -1 \text{ para algún } i \text{ y } v_j \geq 0 \ \forall j \neq i\}.$$

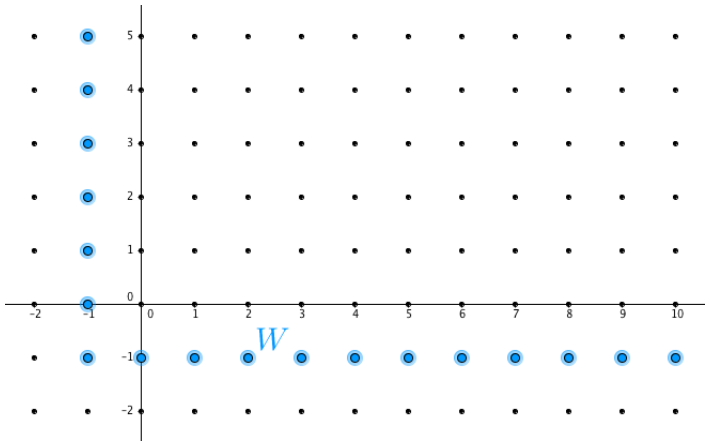


Figura 3.5: El conjunto $W \subset \mathbb{Z}_c^2$.

Observación 3.3.7. Si $v \in W$ con $v_i = -1$, entonces $\mathbb{Z}(v) = \mathbb{Z}_+^n \cap e_i^{\perp}$.

Lema 3.3.8. *Sean $A, B \subset \mathbb{Z}_+^n$ conjuntos finitos, y sea $v \in W$. Entonces*

$$C_v A + C_v B \subset C_v(A + B).$$

Demostración. Lo primero que razonamos es que es suficiente con ver que

$$(C_v A + C_v B)_v(x) \subset (C_v(A + B))_v(x),$$

para todo $x \in \mathbb{Z}(v)$, ya que por definición de v-sección, esto significaría que para $x \in \mathbb{Z}(v)$, $m \in \mathbb{N}$, si $x - mv \in C_v A + C_v B$ tenemos que $x - mv \in C_v(A + B)$. Lo que implica necesariamente

$$C_v A + C_v B \subset C_v(A + B).$$

Sea $x \in \mathbb{Z}(v)$. Supongamos que $x - mv = a + b \in A + B$, donde $m \in \mathbb{N}$, $a \in A$ y $b \in B$. Elegimos $y, z \in \mathbb{Z}(v)$ y $k, l \in \mathbb{N}$ tales que $y - kv = a$ y $z - lv = b$.

Entonces tenemos $x - mv = y + z - (l+k)v$ y como $v \in W$, por la observación 3.3.7 tenemos que $x, y, z \in \mathbb{Z}(v) \subset e_i^{\perp}$, para cierto $1 \leq i \leq n$. Por tanto

$$-m\langle v, e_i\rangle = \langle x - mv, e_i\rangle = \langle y + z - (l+k)v, e_i\rangle = -(l+k)\langle v, e_i\rangle,$$

lo que implica que $m = l + k$ y que $x = y + z$.

Usando esto, obtenemos

$$\begin{aligned}(A+B)_v(x) &= \{m \in \mathbb{N} : x - mv \in A + B\} \\ &= \bigcup_{\substack{x=y+z \\ y,z\in\mathbb{Z}(v)}} \Big\{\{k \in \mathbb{N} : y - kv \in A\} + \{l \in \mathbb{N} : z - lv \in B\}\Big\} \\ &= \bigcup_{\substack{x=y+z \\ y,z\in\mathbb{Z}(v)}} \Big\{A_v(y) + B_v(z)\Big\}.\end{aligned} \tag{3.3}$$

Utilizando (3.3), la definición de v-compresión, la ecuación (3.1), (3.3) de nuevo y finalmente la definición v-compresión, en este orden, concluimos que

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

□

Corolario 3.3.9. *Sean $A, B \subset \mathbb{Z}_+^n$ conjuntos finitos, y sea $v \in W$. Entonces*

$$|A + B| \geq |C_vA + C_vB|.$$

Demostración. Como $|A + B| = |C_v(A + B)|$, es consecuencia directa del lema 3.3.8. □

Lema 3.3.10. *Sean $A, B \subset \mathbb{R}^n$ conjuntos finitos. Entonces existen conjuntos inferiores $A', B' \subset \mathbb{Z}_+^n$ satisfaciendo*

1. $|A| = |A'|$, $|B| = |B'|$, *y* $|A + B| \geq |A' + B'|$.
2. $\dim A = \dim A'$ *y* $\dim(A + B) = \dim(A' + B')$.

Demostración. Por el corolario 3.2.3, podemos suponer que $A, B \subset \mathbb{Z}^n$. También podemos suponer que $\dim(A+B) = n$ y, trasladándolos si fuera necesario, que ambos contienen al origen de coordenadas.

Sea $k = \dim A$. Elegimos vectores $\{x_1, \ldots, x_n\}$ linealmente independientes, con $x_i \in A$, $1 \leq i \leq k$ y $x_i \in B$, $k+1 \leq i \leq n$. Sea $\phi : \mathbb{R}^n \to \mathbb{R}^n$ la aplicación lineal tal que $\phi(x_i) = e_i$, $1 \leq i \leq n$. Al tener coeficientes racionales la matriz asociada a ϕ, existe un $m \in \mathbb{N}$ tal que $\phi(A), \phi(B) \subset (1/m)\mathbb{Z}^n$. O lo que es lo mismo: $m\phi(A), m\phi(B) \subset \mathbb{Z}^n$.

Sean $S := \{o, e_1, \ldots, e_n\}$ y $T := \{o, e_1, \ldots, e_k\}$. Ya que $T \subset \phi(A)$ y $S \subset \phi(A) \cup \phi(B)$, tenemos $mT \subset m\phi(A)$ y $mS \subset m\phi(A) \cup m\phi(B)$.

Sea $t \in \mathbb{Z}^n_+$ tal que $m\phi(A)+t, m\phi(B)+t \subset \mathbb{Z}^n_+$. Entonces tenemos que $mT+t \subset m\phi(A)+t$ y $mS+t \subset (m\phi(A)+t) \cup (m\phi(B)+t)$. Si $-e_i$-comprimimos ahora $m\phi(A)+t$ y $m\phi(B)+t$ para todo $1 \leq i \leq n$ (en cualquier orden) obtendremos conjuntos $A', B' \subset \mathbb{Z}^n_+$ para los cuales $T \subset A'$, $S \subset A' \cup B'$. Por lo tanto *2.* se cumple y, gracias al corolario 3.3.9, sabemos que se cumple también *1.* para A', B'. □

Ahora daremos otra reducción a unos conjuntos todavía más especiales. Cabe destacar, sin embargo, que las dimensiones de los conjuntos no tienen por qué preservarse.

Lema 3.3.11. *Sean $A, B \subset \mathbb{Z}^n_+$ conjuntos inferiores con $\dim(A+B) = n$. Entonces existe una sucesión finita de vectores de W tal que las correspondientes compresiones aplicadas sucesivamente a A y B dan como resultado dos símplices elongados A', B', respectivamente, tales que $\dim(A'+B') = n$.*

Demostración. Como A, B son conjuntos inferiores de $\mathbb{Z}^n_+$ con $\dim(A+B) = n$, tenemos que $o \in A \cap B$ y $S := \{o, e_1, \ldots, e_n\} \subset A \cup B$.

Supongamos primero que $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$. Al ser A, B conjuntos inferiores, podemos asumir sin pérdida de generalidad que $e_1 \in A \cap B$. Además, si $e_n \notin A$, entonces $A \subset e_n^\perp$, y similarmente para B.

Sea E_A el conjunto

$$E_A := \begin{cases} A \cap e_n^\perp & \text{si } e_n \in A, \\ \emptyset & \text{si } e_n \notin A, \end{cases}$$

y definimos E_B análogamente. Sea $w_1 = y_1 - e_n$, donde $y_1 \in E_A \cup E_B$ es tal que $||w_1||$ es maximal. Entonces, como $\langle w_1, e_n \rangle = -1$, tendríamos que $w_1 \in W$. Además, al ser $e_1 \in A \cap B$, tenemos que $y_1 \neq o$, y por tanto

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

Ahora $-e_i$-comprimimos $C_{w_1}A$, $C_{w_1}B$ para $1 \leq i \leq n-1$, obteniendo conjuntos inferiores A_1, B_1. Remarcamos que seguimos teniendo $o \in A_1 \cap B_1$, $S \subset A_1 \cup B_1$, y

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

Sean ahora F_{A_1}

$$F_{A_1} := \begin{cases} A_1 \cap e_n^{\perp} & \text{si } e_{n-1} \in A_1, \\ \emptyset & \text{si } e_{n-1} \notin A_1, \end{cases}$$

y definimos F_{B_1} análogamente. Sea $w_2 = y_2 - e_{n-1}$, donde $y_2 \in F_{A_1} \cup F_{B_1}$ es tal que $||w_2||$ es maximal. Entonces $w_2 \in W$. Como $e_1 \in A_1 \cap B_1$, tenemos que $y_2 \neq o$, y por tanto

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

Ahora $-e_i$-comprimimos $C_{w_2}A_1, C_{w_2}B_1$ para $1 \leq i \leq n-2$ obteniendo conjuntos inferiores A_2, B_2. Remarcamos que $o \in A_2 \cap B_2$, $S \subset A_2 \cup B_2$, y

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

Si continuamos de esta forma, obtendremos conjuntos A_n, B_n que son símplices elongados en la dirección e_1. Tomando $A' = A_n$ y $B' = B_n$, esto completa la prueba bajo la hipótesis de que $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$ dado que $S \subset A_n \cup B_n$ y, por tanto, que $\dim(A' + B') = n$.

Supongamos ahora que $B = \{o\}$. Entonces $A + B = A$ y la prueba anterior sigue funcionando puesto que $S \subset A$ implica que $y_i \neq o$ para $1 \leq i \leq n$. Similarmente, el resultado se satisface cuando $A = \{o\}$.

Finalmente, supongamos que $\operatorname{aff} A \cap \operatorname{aff} B = \{o\}$, donde $\dim A \geq 1$ y $\dim B \geq 1$. Entonces podemos asumir que $A \subset H = \operatorname{aff}\{o, e_1, \ldots, e_k\}$ y $B \subset H^{\perp}$. En este caso podemos aplicar el resultado ya probado para el caso $B = \{o\}$ (con n reemplazado por k, identificando H con $\mathbb{R}^k$), y hacer lo mismo en el caso $A = \{o\}$ (con n reemplazado por $n-k$, identificando $H^{\perp}$ con $\mathbb{R}^{n-k}$), para obtener símplices elongados $A' \subset H$ y $B' \subset H^{\perp}$ con las propiedades requeridas.

Destacamos que las compresiones usadas para reducir A a un símplice elongado en H no afectan a B, y aquéllas utilizadas con B en $H^{\perp}$ no afectan a A. □

Corolario 3.3.12. *Sean $A, B \subset \mathbb{R}^n$ conjuntos finitos. Entonces existen símplices elongados $A', B' \subset \mathbb{Z}_+^n$ satisfaciendo*

1. $|A| = |A'|$, $|B| = |B'|$, *y* $|A + B| \geq |A' + B'|$.
2. $\dim(A + B) = \dim(A' + B')$.

Demostración. Es una consecuencia directa del corolario 3.3.9 y los lemas 3.3.10 y 3.3.11 (y su prueba). □

Observación 3.3.13. Cabe destacar que si $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$, por el procedimiento llevado a cabo en la prueba del lema 3.3.11, podemos suponer además que A' y B' están alargados en la dirección e_1.

Visto lo que hemos aprendido sobre las compresiones durante esta sección, podemos asegurar, usando el corolario 3.3.12, que cada vez que deseemos obtener una cota para el cardinal $|A + B|$ será suficiente con probar dicha cota para símplices elongados.

3.3.1. Desigualdad de Ruzsa para el cardinal $|A+B|$

A continuación vamos a demostrar la ya anunciada desigualdad de Ruzsa para $|A+B|$, desigualdad (3.2), que mejora la cota $|A|+|B|-1$.

Demostración del teorema 3.1.3. Trasladando A y B si fuera necesario, podemos asumir que $o \in A \cap B$. Si $\operatorname{aff} A \cap \operatorname{aff} B = \{o\}$, entonces tenemos que $|A+B| = |A||B|$ y por tanto

$$|A| + \sum_{i=1}^{|B|-1} \min\{n, |A|-i\} \leq |A| + \sum_{i=1}^{|B|-1} |A| = |A| + (|B|-1)|A| = |A||B| = |A+B|.$$

Supongamos ahora que $\operatorname{aff} A \cap \operatorname{aff} B \neq \{o\}$. Por el corolario 3.3.12, podemos asumir que A y B son símplices elongados en $\mathbb{Z}_+^n$. Además, podemos aplicar la observación 3.3.13 para asegurar que dichos símplices elongados están alargados en la dirección de e_1.

Procederemos a probar (3.2) por inducción sobre la dimensión de $A+B$. Para $n=1$, ya que $|B| \leq |A|$, tenemos que $1 \leq |A|-i$, para todo $i \in \{1, \ldots, |B|-1\}$ y por tanto, usando (3.1),

$$|A| + \sum_{i=1}^{|B|-1} \min\{1, |A|-i\} = |A| + \sum_{i=1}^{|B|-1} 1 = |A| + |B| - 1 \leq |A+B|.$$

Supongamos ahora que (3.2) es cierta en $\mathbb{R}^k$ para todo $k < n$.

Si $\dim A = \dim B = n$, como $|B| \leq |A|$ y ambos son símplices elongados, tenemos que $B \subset A$ y, usando el lema 1.2.5, se tiene que

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

Supongamos que $|A| = |B| + s$. Si $s \geq n-1$, entonces

$$n \leq s+1 = |A| - (|B|-1) \leq |A| - i,$$

para todo $i \in \{1, \ldots, |B|-1\}$. Además, $|A|-|B| = s \geq n-1$ lo que implica que $|B| \leq |A| - (n-1)$ y, usando todo esto, tenemos que

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

Finalmente, como

$$\frac{n(n+1)}{2} = 1 + 2 + \cdots + (n-1) + n \leq (n-1)(n-1) + n,$$

obtenemos (3.2) para este caso puesto que

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

Si ahora suponemos $s < n-1$, entonces

$$\text{mín}\{n, |A| - i\} = \begin{cases} n & \text{si } i = 1, \ldots, |A| - n = |B| + s - n, \\ |A| - i & \text{si } i = |A| - n + 1, \ldots, |B| - 1. \end{cases}.$$

Así pues, considerando la igualdad

$$\frac{n(n+1)}{2} + \frac{(n-1)n}{2} = n^2,$$

el lado derecho de (3.2) pasa a valer

$$\begin{aligned} |A| + \sum_{i=1}^{|B|-1} \text{mín}\{1, |A| - i\} &= |A| + n(|B| + s - n) + (n-1) + \cdots + (s+1) \\ &= |A| + n|B| + ns - n^2 + \frac{(n-1)n}{2} - \frac{s(s+1)}{2} \\ &= |A| + (n-1)(|B| + s) + |B| + s - n^2 + \frac{(n-1)n}{2} - \frac{s(s+1)}{2} \\ &= n|A| + |B| + s - \frac{n(n+1)}{2} - \frac{s(s+1)}{2} \\ &\leq n|A| + |B| - \frac{n(n+1)}{2} = |A+B|, \end{aligned}$$

probando la proposición en este caso.

Supongamos que $\dim B < n$. Sin pérdida de generalidad, asumimos que $B \subset \{x_n = 0\}$, con lo que $e_n \in A$ y

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

Como para aplicar la hipótesis de inducción a dos conjuntos $\overline{A}$ y $\overline{B}$ debemos verificar que $|\overline{B}| \leq |\overline{A}|$, estamos obligados a distinguir dos casos:

Si $|B| < |A|$, entonces $|B| \leq |A| - 1 = |A \cap \{x_n = 0\}|$, y aplicando la hipótesis de inducción a $\overline{A} = A \cap \{x_n = 0\}, \overline{B} = B \subset \mathbb{R}^{n-1}$, obtenemos que

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

Si $|A| = |B|$, entonces $|A|-1 = |A\cap\{x_n = 0\}| < |B|$, y aplicamos la hipótesis de indución sobre $\overline{A} = B, \overline{B} = A \cap \{x_n = 0\} \subset \mathbb{R}^{n-1}$ para obtener

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

Finalmente, si $\dim A < n$, podemos asumir que $A \subset \{x_n = 0\}$ y $e_n \in B$, y descomponer entonces $A+B$ como $A+B = \big(A + (B \cap \{x_n = 0\})\big) \cup (A + e_n)$.

Aplicando otra vez la hipótesis de inducción sobre $\overline{A} = A, \overline{B} = B \cap \{x_n = 0\} \subset \mathbb{R}^{n-1}$ concluimos que

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

3.4. La desigualdad de Brunn-Minkowski para el retículo entero

Siguiendo con la teoría que hemos desarrollado anteriormente con las compresiones, nos es necesario definir un orden especial en el retículo entero $\mathbb{Z}^n$ y, más concretamente, en el subconjunto $\mathbb{Z}^n_+$ de dicho retículo. Esto nos permitirá no sólo enunciar el teorema 3.4.3, sino ver unos primeros casos llegando a ver la prueba para el caso 2-dimensional.

Definición 3.4.1 (F-peso, F-orden)**.**
Dado $F \subset \mathbb{Z}^n$ finito con $|F| \geq n+1$, definiremos la función $w_F : \mathbb{Z}^n \longrightarrow \mathbb{R}$ como

$$w_F(x) = \frac{x_1}{|F|-n} + \sum_{i=2}^{n} x_i,$$

para $x = (x_1, \ldots, x_n)$. La llamaremos función *F-peso*.

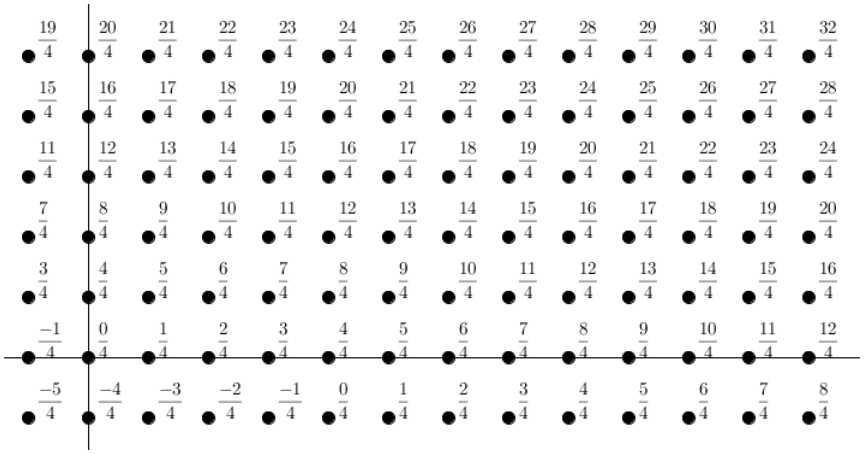


Figura 3.6: Los valores de la función F-peso en $\mathbb{Z}^2$ para un F con $|F| = 6$.

Gracias a la función F-peso definimos un *F-orden* para $\mathbb{Z}^n$: dados $x, y \in \mathbb{Z}^n$ diremos que $x <_F y$ si

- $w_F(x) < w_F(y)$ o
- $w_F(x) = w_F(y)$ y existe $j \in \{1, \ldots, n\}$ con $x_j > y_j$ y $x_i = y_i$ para todo $i < j$.

Fijado $F \subset \mathbb{Z}^n$, los primeros $|F|$ puntos de $\mathbb{Z}^n_+$ son

$$o <_F e_1 <_F 2e_1 <_F 3e_1 <_F \ldots <_F (|F| - n)e_1 <_F e_2 <_F e_3 <_F \ldots <_F e_n.$$

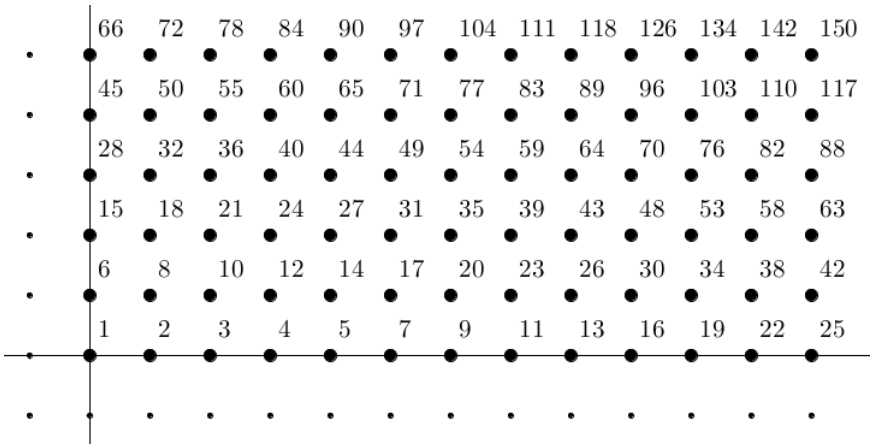


Figura 3.7: Los puntos de $\mathbb{Z}^2_+$ junto a su posición en el F-orden ($|F| = 6$).

Sea $\mathbb{Z}^F$ el conjunto de puntos anteriores al origen de coordenadas en el F-orden:

$$\mathbb{Z}^F = \{v \in \mathbb{Z}^n : v <_F o\}.$$

Claramente tenemos que $\mathbb{Z}^F \subset \mathbb{Z}^n_c$.

Definición 3.4.2 (F-segmento inicial)**.**
Para un $m \in \mathbb{N}$, representamos por D^F_m el conjunto unión de los primeros m puntos de $\mathbb{Z}^n_+$ según el F-orden. D^F_m se denomina *F-segmento inicial* de cardinal m.

Es fácil ver que $D^F_{|F|}$ es un símplice elongado n-dimensional y que $D^F_{|F|-1}$ es un símplice elongado $(n-1)$-dimensional.

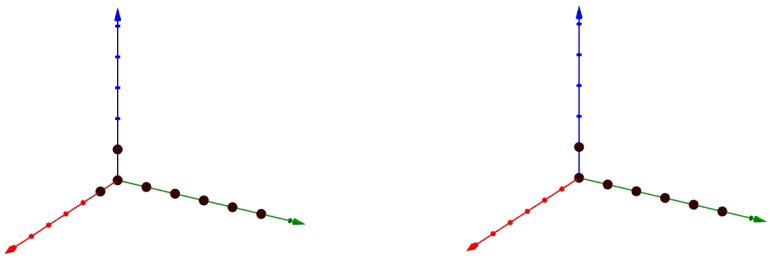


Figura 3.8: Los conjuntos $D^F_{|F|}$ (izquierda) y $D^F_{|F|-1}$ (derecha) en $\mathbb{Z}^3$ para $|F| = 8$.

Cabe destacar que todas las definiciones anteriores no dependen del conjunto F, sino de su cardinal.

El siguiente teorema puede ser visto como la versión discreta de la desigualdad de Brunn-Minkowski para el retículo entero.

Teorema 3.4.3 (Desigualdad de Brunn-Minkowski discreta)**.** *Sean $A, B \subset \mathbb{Z}^n$ finitos con $\dim B = n$. Entonces*

$$|A + B| \geq |D^B_{|A|} + D^B_{|B|}|.$$

3.4.1. Lemas sobre la ordenación

La prueba del teorema 3.4.3 es muy larga y procederemos demostrando una serie de lemas, en los cuales nuestro conjunto B será un conjunto fijo de $\mathbb{Z}^n_+$ con $\dim B = n$. Cabe destacar que para los lemas y resultados siguientes aplicaremos el orden asociado al conjunto B, por lo que al fijar B, establecemos el B-orden así como el conjunto $D^B_{|B|}$.

Lema 3.4.4. *Tenemos $z <_B y$ si y sólo si $z - y \in \mathbb{Z}^B$.*

Demostración. Observemos que la función B-peso es una función lineal y por tanto $z <_B y$ si y sólo si $z - y <_B o$. □

Lema 3.4.5. *Un conjunto finito $F \subset \mathbb{Z}_+^n$ es un B-segmento inicial si y sólo si es v-compreso para todo $v \in \mathbb{Z}^B$.*

Demostración. El conjunto F no es un B-segmento inicial si y sólo si existen $y \in F$, $z \in \mathbb{Z}_+^n \setminus F$, con $z <_B y$. Por el lema 3.4.4, la condición anterior se satisface si y sólo si F no es v-compreso para $v = z - y \in \mathbb{Z}^B$. □

Definición 3.4.6 (B-altura)**.**
Dado $F \subset \mathbb{Z}_+^n$ un conjunto finito definiremos la función *B-altura* $h_B(F)$ como la suma de las posiciones en el B-orden que ocupan los puntos de F.

Ejemplo. Sean $A = \{(0,0),(1,0),(2,0),(3,0),(4,0),(1,1),(2,2),(3,1)\}$ y B un conjunto con $|B| = 6$. Dado que conocemos las posiciones de todos los puntos de A en el B-orden (véase figura 3.7), calculamos la altura de A como la suma de estas posiciones:

$$h_B(A) = 1 + 2 + 3 + 4 + 5 + 8 + 21 + 12 = 56.$$

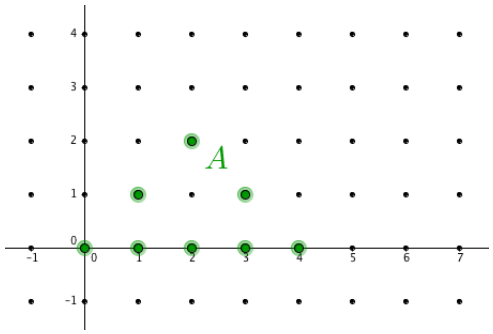


Figura 3.9: El conjunto A.

Así mismo, como D_m^B es, por definición, la unión de los primeros m puntos en el B-orden tenemos que

$$h_B(D_m^B) = \frac{m(m+1)}{2}, \text{ para cada } m \in \mathbb{N}.$$

Lema 3.4.7. *Sea $F \subset \mathbb{Z}_+^n$ un conjunto finito. Tomamos $F_1 = F$ y para cada $j \in \mathbb{N}$, sea $F_{j+1} = C_{v_j} F_j$ para ciertos $v_j \in \mathbb{Z}^B$. Entonces existe $k \in \mathbb{N}$ tal que $F_j = F_k$ para todo $j \geq k$.*

Demostración. Si vemos cada v_j-compresión como una biyección de F_j a F_{j+1}, realizar una compresión es mantener $x \in F_j$ fijo o sustituirlo por $x + v_j$ (siempre que $x + v_j \in \mathbb{Z}_+^n$).

Gracias al lema 3.4.4 tenemos entonces que como $v_j <_B o$, entonces $x + v_j <_B x$ y por tanto al realizar una compresión se rebaja el orden de los puntos de F_j y, en consecuencia, la B-altura.

Si suponemos que $F_{j+1} \neq F_j$, entonces disminuye la posición de un punto en el B-orden al menos. Así, tenemos $h_B(F_{j+1}) < h_B(F_j)$ a menos que $F_{j+1} = F_j$, por lo que al ser $|F|$ finito tiene que haber un $k \in \mathbb{N}$ tal que $F_j = F_k$ para todo $j \geq k$. □

Lema 3.4.8. *Es suficiente probar el teorema 3.4.3 cuando* $B = D^B_{|B|}$ *y* $A \subset \mathbb{Z}^n_+$ *es* v*-compreso para todo* $v \in W \cap \mathbb{Z}^B$.

Demostración. Trasladando A y B, si fuera necesario, podemos asumir que ambos son subconjuntos de $\mathbb{Z}^n_+$. Aplicando, para cada $i = 1, \ldots, n$, $-e_i$-compresiones a A y B, podemos además suponer, por el corolario 3.3.9, que A y B son conjuntos inferiores.

Si aplicamos el lema 3.3.11 a B y B, sabemos que existe una sucesión finita de vectores de W tal que sus correspondientes compresiones transforman B en un símplice elongado, que es de hecho $D^B_{|B|}$. Sea A' el resultado de aplicar esas mismas compresiones a A. Entonces por el corolario 3.3.9 tenemos que

$$|A + B| \geq |A' + D^B_{|B|}.|$$

Ahora aplicamos el lema 3.4.7 donde tomamos $F = A'$ y $\{v_j\}$ es una sucesión en la que cada elemento del conjunto finito $W \cap \mathbb{Z}^B$ aparece infinitas veces. Entonces existe un $A'' = F_k$ que es claramente v-compreso para todo $v \in W \cap \mathbb{Z}^B$.

Por el lema 3.4.5 sabemos que estas compresiones no cambian $D^B_{|B|}$. Así que por el corolario 3.3.9 otra vez, tenemos que

$$|A' + D^B_{|B|}| \geq |A'' + D^B_{|B|}|.$$ □

Gracias al lema 3.4.8, a partir de ahora consideraremos que el conjunto B es un segmento inicial ($B = D^B_{|B|}$) para el resto de lemas y resultados de este capítulo.

3.4.2. Demostración del teorema 3.4.3 para $n = 2$

Ahora estamos en condiciones de ver el caso 2-dimensional del teorema 3.4.3.

Lema 3.4.9. *Sean* $A, B \subset \mathbb{Z}^2$ *finitos con* $\dim B = 2$. *Entonces*

$$|A + B| \geq |D^B_{|A|} + D^B_{|B|}|.$$

Demostración. Por el lema 3.4.8, podemos asumir que $B = D^B_{|B|}$. Por lo que probaremos entonces que

$$|A + B| \geq |D^B_{|A|} + B| \tag{3.4}$$

por inducción en la B-altura de A, el cual podemos suponer en $\mathbb{Z}_+^2$. Cabe destacar que siempre tenemos que

$$h_B(A) \geq \frac{(|A|+1)|A|}{2},$$

y que si $h_B(A) = (|A|+1)|A|/2$ entonces $A = D_{|A|}^B$ y la desigualdad es trivial.

Supongamos entonces que $h_B(A) > (|A|+1)|A|/2$ y que la desigualdad (3.4) es cierta cuando remplazamos A por un subconjunto de $\mathbb{Z}_+^2$ del mismo cardinal pero menor B-altura que A.

Por el lema 3.4.8, podemos asumir que A es v-compreso para todo $v \in W \cap \mathbb{Z}^B$. En particular, dado que

$$-e_1, -e_2, u = (|B|-2)e_1 - e_2 \in W \cap \mathbb{Z}^B,$$

sabemos que A es un conjunto inferior u-compreso.

Sea $y = (y_1, y_2) \in A$ el punto de máxima posición en el B-orden y sea $z = (z_1, z_2) \in \mathbb{Z}_+^2 \setminus A$ el punto de mínima posición en el B-orden. Entonces como $A \neq D_{|A|}^B$ tenemos $z <_B y$. Como A es u-compreso e $y \in A$, tenemos que

$$y' = y + y_2 u = (y_1 + (|B|-2)y_2, 0) \in A.$$

Se sigue entonces que, como A es un conjunto inferior, los puntos $(k, 0) \in A$ para todo $k \leq y_1 + (|B|-2)y_2$.

Esto implica que $z_2 > 0$ dado que si $z_2 = 0$ entonces, como $z = (z_1, 0) <_B y$, tendríamos

$$\frac{z_1}{|B|-2} = w_B(z) \leq w_B(y) = \frac{y_1}{|B|-2} + y_2,$$

lo que implicaría que $z_1 \leq y_1 + (|B|-2)y_2$ y por tanto que $z \in A$.

Cabe destacar también que y' es el único punto de A con primera coordenada maximal: en efecto, si $a = (a_1, a_2) \in A$ con $a_1 \geq y_1 + (|B|-2)y_2$ entonces

$$w_B(y) = \frac{y_1}{|B|-2} + y_2 \leq \frac{a_1}{|B|-2} \leq w_B(a),$$

en contra de que $y \in A$ sea el punto con posición maximal en el B-orden, salvo que $w_B(y) = w_B(a)$, en cuyo caso se tendría que $a = (a_1, 0) = (y_1, y_2) = y'$.

Por tanto, si $A' = A \setminus \{y'\}$ tenemos

$$y' + (|B|-2)e_1 = (y_1 + (|B|-2)(y_2+1), 0) \in (A+B) \setminus (A'+B),$$

lo que implica que

$$|A+B| \geq |A'+B| + 1.$$

Si ahora consideramos $A'' = A' \cup \{z\}$, entonces $|A''| = |A|$ y, como $z <_B y'$, tenemos que $h_B(A'') < h_B(A)$. Afirmamos que

$$(A'' + B) \setminus (A' + B) = \{z + e_2\}, \tag{3.5}$$

con lo que tendríamos $|A'' + B| \leq |A' + B| + 1$.

Usando ahora la hipotesis de inducción sobre A'', tenemos que

$$|A + B| \geq |A' + B| + 1 \geq |A'' + B| \geq |D^B_{|A''|} + B| = |D^B_{|A|} + B|,$$

como queríamos demostrar.

Falta por lo tanto demostrar (3.5): Dado que $A'' = A' \cup \{z\}$ tenemos que verificar solamente que $z+b \subset A'+B$ cuando $b = ke_1$ con $k \in \mathbb{N}$, $0 \leq k \leq (|B|-2)$. Si $b = ke_1$ en esas condiciones, entonces usamos que $z_2 > 0$ para decir que $z+u = (z_1+(|B|-2), z_2-1) \in \mathbb{Z}^n_+$ y, como $z + u <_B z$ y z es el primer punto de $\mathbb{Z}^n_+$ que no pertenece a A, tenemos que $z + u \in A$. Además, dado que $z + u <_B z <_B y'$, sabemos que $z + u \neq y'$ y por tanto $z + u \in A'$.

Al ser A $-e_1$-compreso sabemos incluso que $z + u - re_1 \in A'$ siempre que $r \in \mathbb{N}$ cumpla que $z + u - re_1 \in \mathbb{Z}^n_+$. Luego tomando $r = |B| - 2 - k$ sabemos que

$$z + u + re_1 = z + (|B| - 2 - r)e_1 - e_2 = z + ke_1 - e_2 \in A',$$

y por tanto que $z + ke_1 = z + ke_1 - e_2 + e_2 \in A' + B$ como queríamos. □

3.4.3. Compresiones por hiperplanos paralelos

Antes de continuar con los lemas necesarios para probar el teorema 3.4.3, necesitamos profundizar aún más en la teoría de las compresiones.

En este apartado definiremos y comprobaremos las consecuencias de comprimir ciertas partes de nuestro conjunto por separado y no todo a la vez. Concretamente, fijaremos una serie de hiperplanos paralelos entre sí para después comprimir independientemente las intersecciones de nuestro conjunto con dichos hiperplanos.

Sea $F \subset \mathbb{Z}^n_+$ un conjunto finito. Definimos ahora unos nuevos conjuntos $X_i(F)$, $1 \leq i \leq n$ como sigue:

Si $1 < i \leq n$ y $m \in \mathbb{Z}$, denotamos por $F[i, m]$ la proyección de $F \cap \{x_i = m\}$ sobre el hiperplano $\{x_i = 0\}$, es decir,

$$F[i, m] = \{(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \in \mathbb{Z}^n_+ : (x_1, \ldots, x_n) \in F\}.$$

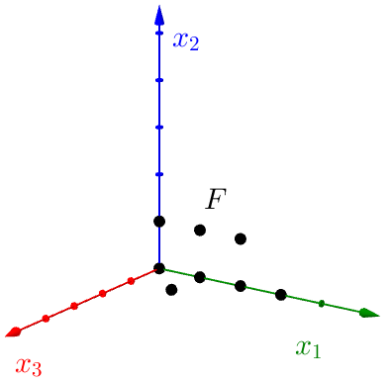
Por otro lado, para $m \in \mathbb{Z}$, sea

$$P_m = \left\{ x \in \mathbb{Z}^n_+ : w_B(x) = \frac{m}{|B| - n} \right\} = \{x \in \mathbb{Z}^n_+ : x_1 + \sum_{i=2}^{n} (|B| - n)x_i = m\}.$$

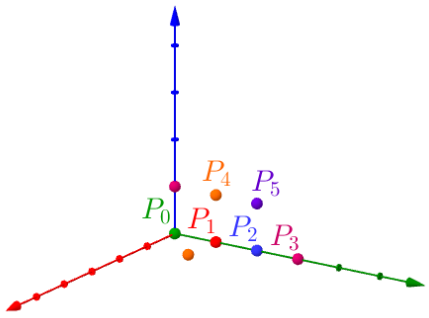
Obsérvese que P_m es un conjunto finito de puntos (pues las coordenadas x_i son no-negativas en $\mathbb{Z}^n$) que está contenido en el hiperplano

$$\left\{ x \in \mathbb{R}^n : x_1 + \sum_{i=2}^{n} (|B| - n)x_i = m \right\}.$$

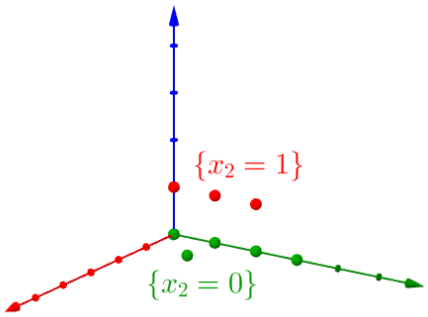
Además, el punto $(m, 0, \ldots, 0) \in P_m$. Denotamos por $F[1, m]$ la proyección de $F \cap P_m$ sobre el hiperplano $\{x_1 = 0\}$.



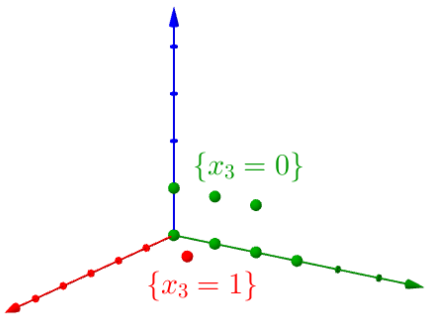
(a) El conjunto F original.



(b) Conjuntos P_m (considerando un conjunto con $|B| = 6$).



(c) Hiperplanos $\{x_2 = m\}$.



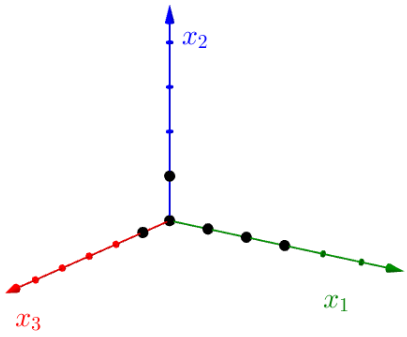
(d) Hiperplanos $\{x_3 = m\}$.

Figura 3.10: Los puntos de F coloreados según su pertenencia a distintos conjuntos.

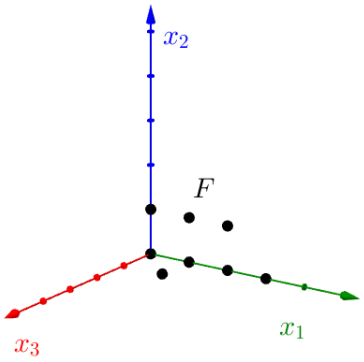
Sea $B_i = B \cap \{x_i = 0\}$, que es B_i un símplice elongado $(n-1)$-dimensional en $\{x_i = 0\}$. Finalmente, para $1 \leq i \leq n$, definimos $X_i(F)$ como el subconjunto de $\mathbb{Z}_+^n$ para el cual

$$X_i(F)[i, m] = D^{B_i}_{|F[i,m]|} \text{ para todo } m \in \mathbb{N},$$

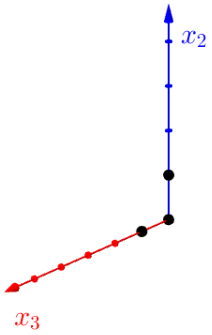
donde para construir $D^{B_i}_{|F[i,m]|}$ trabajamos en $\mathbb{Z}^{n-1}$ que identificamos con $\mathbb{Z}^n \cap \{x_i = 0\}$.



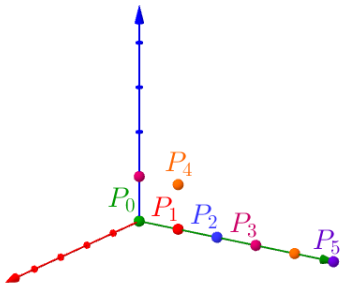
(a) El conjunto B.



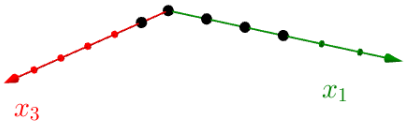
(b) El conjunto F original.



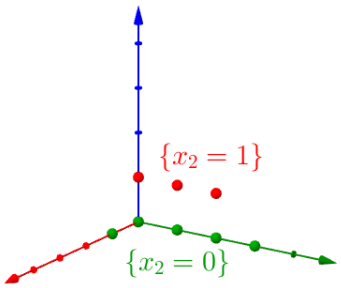
(c) El conjunto B_1.



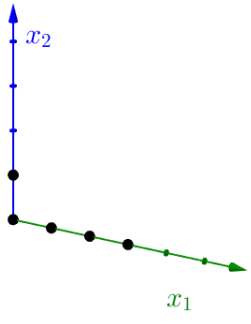
(d) El conjunto $X_1(F)$.



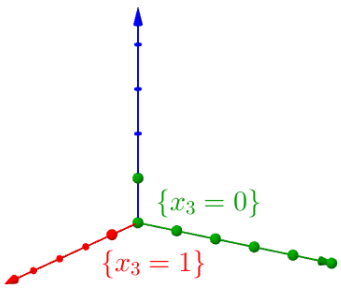
(e) El conjunto B_2.



(f) El conjunto $X_2(F)$.



(g) El conjunto B_3.



(h) El conjunto $X_3(F)$.

Figura 3.11: Un ejemplo concreto de compresión de un conjunto F por hiperplanos.

Observación 3.4.10. Dicho de otra forma, si $1 < i \leq n$, la proyección de $X_i(F) \cap \{x_i = m\}$ sobre $\{x_i = 0\}$ es el B_i-segmento inicial (los primeros puntos del B_i-orden), definido en $\{x_i = 0\}$, con el mismo cardinal que la proyección de $F \cap \{x_i = m\}$. Similarmente, la proyección de $X_1(F) \cap P_m$ sobre $\{x_1 = 0\}$ es el B_1-segmento inicial, definido en $\{x_1 = 0\}$, con el mismo cardinal que la proyección de $F \cap P_m$.

Por lo tanto podemos considerar estas definiciones como unas compresiones $(n-1)$-dimensionales concretas que no alteran la cardinalidad del conjunto respecto a unos hiperplanos paralelos (que cambian según el $1 \leq i \leq n$).

Observación 3.4.11. Usando las definiciones anteriores tenemos que

$$(F + B)[i, m] = F[i, m-1] \cup (F[i, m] + B_i), \tag{3.6}$$

para $1 < i \leq n$, y

$$\begin{aligned}(F + B)[1, m] = F[1, m] \cup F[1, m-1] \cup \cdots \cup F[1, m - |B| + n + 1] \\ \cup (F[1, m - |B| + n] + B_1).\end{aligned} \tag{3.7}$$

La justificación de (3.6) se sigue del hecho de que si $a \in F \cap \{x_i = m-1\}$, entonces $a + e_i \in (F+B) \cap \{x_i = m\}$, de donde se tiene inmediatamente $F[i, m-1] \subset (F+B)[i, m]$.

De igual modo, si $a \in F \cap \{x_i = m\}$ y $b \in B_i = B \cap \{x_i = 0\}$, entonces el punto $a + b \in (F + B) \cap \{x_i = m\}$, y por tanto $F[i, m] + B_i \subset (F + B)[i, m]$.

Por otro lado, si $a + b \in (F + B) \cap \{x_i = m\}$, entonces tenemos que

$$a \in \begin{cases} F \cap \{x_i = m-1\} & \text{si } b = e_i \in B, \\ F \cap \{x_i = m\} & \text{si } b \in B \cap \{x_i = 0\} = B_i, \end{cases}$$

y dado que $B = B_i \cup \{e_i\}$ no hay más casos y queda probado (3.6).

Análogamente, se tiene que

$$F[1, m - s] + se_1 \in (F + B)[1, m] \text{ para todo } 0 \leq s < |B| - n$$

y

$$F[1, m - |B| + n] + B_1 \in (F + B)[1, m].$$

Además, si $a + b \in (F + B) \cap \{x_1 = m\}$, entonces tenemos que

$$a \in \begin{cases} F \cap P_{m-s} & \text{si } b = se_1 \in P_s, \text{ para } 0 \leq s < |B| - n, \\ F \cap P_{m-(|B|-n)} & \text{si } b \in P_{(|B|-n)}. \end{cases}$$

Esto demuestra (3.7).

Lema 3.4.12. *Sea $F \subset \mathbb{Z}_+^n$ finito y sea $1 \leq i \leq n$. Entonces $h_B(X_i(F)) \leq h_B(F)$, con igualdad si y sólo si $X_i(F) = F$.*

Demostración. Sea $x = (x_1, \ldots, x_n) \in \mathbb{Z}_+^n$ con $x_i = m$, y sea x' la proyección de x sobre el hiperplano $\{x_i = 0\}$ (entonces $x'_i = 0$ y $x'_j = x_j$ para todo $j \neq i$). Se sigue de la definición de B-orden que el orden de dos puntos en $\{x_i = m\}$ se preserva considerando el B_i-orden de sus proyecciones sobre $\{x_i = 0\}$. Por tanto, la definición de $X_i(F)$ (junto con la observación 3.4.10) dan lugar a que $h_B(X_i(F)) \leq h_B(F)$.

Si $1 < i \leq n$ y $X_i(F) \neq F$, entonces existe un $m \in \mathbb{N}$ tal que $F[i,m]$ no es un B_i-segmento inicial. Sea $y' \in F[i,m]$ el punto de posición máxima en el B_i-orden y $z' \in \{x_i = 0\} \setminus F[i,m]$ el punto de mínima posición en el B_i-orden. Entonces $z' <_{B_i} y'$. Por la definición de $X_i(F)$, tenemos que $y' \in \{x_i = 0\} \setminus X_i(F)[i,m]$ y $z' \in X_i(F)[i,m]$. Sean $y, z \in \{x_i = m\}$ los puntos cuyas proyecciones sobre $\{x_i = 0\}$ son respectivamente y', z'. Entonces $y \in F \setminus X_i(F)$, $z \in X_i(F) \setminus F$, y $z <_B y$. Por lo que $h_B(X_i(F)) < h_B(F)$. La prueba para $i = 1$ es completamente análoga. □

Definición 3.4.13 (Z_F)**.**
Si $F \subset \mathbb{Z}_+^n$, definimos el conjunto Z_F como

$$Z_F = \{z - y : y \in F, z \in \mathbb{Z}_+^n \setminus F\}.$$

Lema 3.4.14. *Si $F \subset \mathbb{Z}_+^n$, entonces F es v-compreso si y sólo si $v \notin Z_F$.*

Demostración. Si $v \in Z_F$, entonces existen $y \in F$ y $z \in \mathbb{Z}_+^n \setminus F$ tales que $v = z - y$ y por tanto $z = y + v \notin F$, por lo que F no puede ser v-compreso. Recíprocamente, si F no es v-compreso, entonces existen $y' \in F$ y $z' \in \mathbb{Z}_+^n \setminus F$ tales que $y' + mv = z'$ para cierto $m \in \mathbb{N}$. Sea $j \in \mathbb{N}$ maximal tal que $y' + jv \in F$. Si definimos entonces $y = y' + jv \in F$ y $z = y' + (j+1)v \in \mathbb{Z}_+^n \setminus F$, entonces $v = z - y \in Z_F$. □

Lema 3.4.15. *Sea $F \subset \mathbb{Z}_+^n$ un conjunto finito y sea $v \in \mathbb{Z}^B$ con $w_B(v) = 0$. Si F no es v-compreso, entonces $F[1,m]$ no es un B_1-segmento inicial para cierto $m \in \mathbb{N}$.*

Demostración. Supongamos que F no es v-compreso, donde $v \in \mathbb{Z}^B$ con $w_B(v) = 0$. Entonces para algún j tenemos $v_j > 0$ y $v_i = 0$ para todo $i < j$. Por el lema 3.4.14, $v \in Z_F$, y existen $y \in F$ y $z \in \mathbb{Z}_+^n \setminus F$ con $v = z - y$. En consecuencia, $w_B(y) = w_B(z)$ y, por tanto, hay un $m \in \mathbb{N}$ tal que $y, z \in P_m$.

Sean y', z', v' las proyecciones de y, z y v sobre $\{x_1 = 0\}$. Entonces $y' \in F[1,m]$, $z' \in \{x_1 = 0\} \setminus F[1,m]$, y $v' = z' - y'$. Luego $v' \in Z_{F[1,m]}$ y, por el lema 3.4.14, $F[1,m]$ no es v'-compreso. Si $v_1 = 0$, entonces $w_{B_1}(v') = w_B(v) = 0$, $v'_j > 0$ y $v'_i = 0$ para todo $i < j$, donde $j \geq 2$. Si $v_1 > 0$, entonces

$$w_{B_1}(v') = w_B(v) - \frac{v_1}{|B| - n} < w_B(v) = 0.$$

En cualquier caso tenemos $v' <_{B_1} o$, por lo que $v' \in \mathbb{Z}^{B_1}$. Finalmente, usando el lema 3.4.5, tenemos que $F[1,m]$ no es un B_1-segmento inicial. □

Lema 3.4.16. *Sea $F \subset \mathbb{Z}_+^n$ un conjunto finito, con $n > 2$. Si $X_i(F) = F$ para $i = 1, 2$, entonces F es un B-segmento inicial.*

Demostración. Sea $y \in F$ el punto de posición maximal en el B-orden y sea $z \in \mathbb{Z}_+^n \setminus F$ el punto de posición minimal en el B-orden. Si $y <_B z$, entonces F es un B-segmento inicial.

Supongamos entonces que tenemos $z <_B y$, lo que implica que $w_B(z) \leq w_B(y)$. Obsérvese que

$$F \text{ es } v\text{-compreso para todo } v \in \mathbb{Z}^B \text{ con } w_B(v) = 0 : \tag{3.8}$$

en efecto, gracias al lema 3.4.15 basta ver que que $F[1, m]$ es un segmento inicial, lo cual es cierto, ya que

$$F[1, m] = X_1[1, m] = D^{B_1}_{F[1,m]}.$$

Esto descarta el caso $w_B(z) = w_B(y)$, ya que en ese caso tendríamos $y \in F$, $z = y + (z - y) \notin F$ con $z - y \in \mathbb{Z}^B$ y con $w_B(z - y) = w_B(z) - w_B(y) = 0$, lo que contradiría el que F sea $(z - y)$-compreso. Por tanto sólo queda que $w_B(z) < w_B(y)$.

Si $m = w_B(y)(|B| - n)$, entonces $y \in P_m$ e $y' = (m, 0, \ldots, 0)$ es el punto de P_m de mínima posición en el B-orden. Además, $w_B(y' - y) = 0$ y al ser la primera coordenada de $y' - y$ estrictamente positiva se tiene que $y' - y <_B o$. Por tanto, $y' - y \in \mathbb{Z}^B$ y (3.8) nos asegura que F es $(y' - y)$-compreso. Luego $y' \in F$. Similarmente, si $m' = w_B(z)(|B| - n)$, entonces $z \in P_{m'}$, y si z' es el punto de $P_{m'}$ de máxima posición en el B-orden entonces, como F es $(z - z')$-compreso (vease (3.8)), tenemos que $z' \notin F$.

Por la definición de B-orden y el hecho de que $n > 2$, $z'_2 = 0$. Como $y', z' \in \{x_2 = 0\}$, tenemos

$$w_{B_2}(y') = w_B(y') = w_B(y) > w_B(z) = w_B(z') = w_{B_2}(z').$$

Pero $y' \in F[2, 0] = F \cap \{x_2 = 0\}$ y $z' \notin F[2, 0]$, así que $F[2, 0]$ no puede ser un B_2-segmento inicial. Por tanto $X_2(F) \neq F$, en contra de las hipótesis del enunciado. □

Ejemplo. Cabe destacar que el lema 3.4.16 no es cierto en general cuando se omite la hipótesis $n > 2$. Por ejemplo basta tomar los conjuntos

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

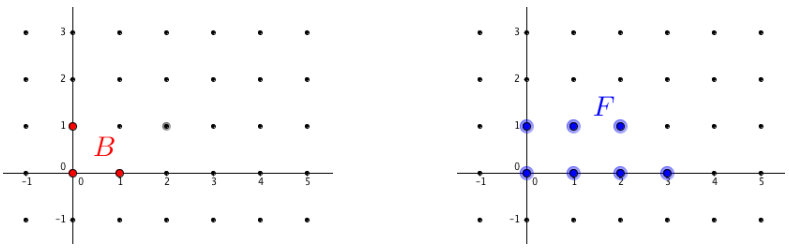


Figura 3.12: F no es un B-segmento inicial, puesto que $(2, 0) <_B (3, 0)$, pero $(2, 0) \notin F$.

Lema 3.4.17. *Si $F \subset \mathbb{Z}_+^n$ es un B-segmento inicial, entonces también lo es $F + B$.*

Demostración. Realizamos la prueba aplicando inducción sobre la dimensión del conjunto F ($n = \dim F$). El resultado es trivial para $n = 1$. Asumimos ahora que es cierto el lema en $\mathbb{Z}_+^{n-1}$ (para todos los símplices elongados $B \subset \mathbb{Z}_+^{n-1}$) y supongamos que $F + B \subset \mathbb{Z}_+^n$ no es un B-segmento inicial.

Sea $y \in F + B$ el punto de máxima posición en el B-orden. Si $y = a + b$, donde $a \in F$, $b \in B$, entonces debe darse que $w_B(b) = 1$. Sea $z \in \mathbb{Z}_+^n \setminus (F + B)$ el punto de posición minimal en el B-orden. En tal caso, como $F+B$ no es un B-segmento inicial, tenemos que $z <_B y$ y por tanto $w_B(z) \leq w_B(y)$. Todo $x \in \mathbb{Z}_+^n$ con $w_B(x) < w_B(a)$ debe pertenecer al B-segmento inicial F ya que $a \in F$, así que todo $x \in \mathbb{Z}_+^n$ con $w_B(x) < w_B(a)+1 = w_B(y)$ se encuentra en $F + B$, dado que los puntos $x \in \mathbb{Z}_+^n$ con $w_B(x) \leq 1$ son los puntos de B (por ser $B = D^B_{|B|}$).

Entonces tenemos a la fuerza que $w_B(z) = w_B(y)$. Si $v = z - y$, el lema 3.4.14 nos asegura que $v \in \mathbb{Z}^B$. Además, $w_B(v) = 0$ y, dado que $y \in F$ y $z \notin F$, $F + B$ no es v-compreso. Por el lema 3.4.15, entonces existe un $m \in \mathbb{N}$ (de hecho $m = (|B| - n)w_B(y)$) tal que $(F + B)[1, m]$ no es un B_1-segmento inicial.

Por otro lado, usando el lema 3.4.12, $h_B(X_1(F)) \leq h_B(F)$. Como F es un B-segmento inicial, la altura $h_B(F)$ mínima de entre los conjuntos de igual cardinal, por lo que $h_B(X_1(F)) = h_B(F)$, y usando la caracterización de la igualdad del lema 3.4.12 esto implica que $X_1(F) = F$. Por otro lado, usando la fórmula (3.7) tenemos

$$\begin{aligned}(F + B)[1, m] = F[1, m] \cup F[1, m - 1] \cup \cdots \cup F[1, m - |B| + n + 1] \\ \cup (F[1, m - |B| + n] + B_1).\end{aligned}$$

Ahora bien, dado que los conjuntos

$$F[1, l] = X_1(F)[1, l] = D^{B_1}_{|F[1,l]|}$$

son B_1-segmentos iniciales para todo $l \in \mathbb{N}$.

Finalmente, usando la hipótesis de inducción, $F[1, m-|B|+n]+B_1 \subset \mathbb{Z}_+^{n-1}$ es también un B_1-segmento inicial, lo que permite concluir que $(F + B)[1, m]$ es un B_1-segmento inicial por ser suma finita de B_1-segmentos iniciales. Esta contradicción completa la prueba. □

3.4.4. La demostración del teorema 3.4.3

Todo el trabajo realizado hasta el momento va a permitir probar el teorema 3.4.3 de forma sencilla.

Demostración del teorema 3.4.3. La prueba se realiza por inducción sobre n. Para $n = 1$, el teorema 3.4.3 es consecuencia directa de (3.1) y el lema 3.4.9 demuestra el caso $n = 2$.

Supongamos entonces que $n > 2$ y que el teorema 3.4.3 está probado para todas las dimensiones menores que n.

Si $m \in \mathbb{N}$, consideramos la familia

$$\mathcal{F}_m := \{F \subset \mathbb{Z}_+^n : |F| = m \text{ y } |F + B| \text{ es minimal}\}.$$

Sea $F \in \mathcal{F}_{|A|}$ el conjunto de B-altura minimal dentro de la familia $\mathcal{F}_{|A|}$. Nuestro objetivo será probar que $F = D^B_{|A|}$, lo que concluirá la demostración puesto que entonces tendremos

$$|A + B| \geq |F + B| = |D^B_{|A|} + B| = |D^B_{|A|} + D^B_{|B|}|.$$

(recordemos que estamos suponiendo que $B = D^B_{|B|}$ por el lema 3.4.8).

Vamos a ver que para $1 < i \leq n$, tenemos

$$|F + B| \geq |X_i(F) + B|. \tag{3.9}$$

Para demostrar esto, sea $m \in \mathbb{N}$. Usando (3.6), el lema 3.4.17, la hipótesis de inducción, y (3.6) otra vez, obtenemos que

$$\begin{aligned}
|(X_i(F) + B)[i, m]| &= |X_i(F)[i, m-1] \cup (X_i(F)[i, m] + B_i)| \\
&= \text{máx}\left\{|X_i(F)[i, m-1]|, |X_i(F)[i, m] + B_i|\right\} \\
&\leq \text{máx}\left\{|F[i, m-1]|, |F[i, m] + B_i|\right\} \\
&\leq |F[i, m-1] \cup (F[i, m] + B_i)| \\
&= |(F + B)[i, m]|,
\end{aligned}$$

lo que prueba 3.9.

Por nuestras condiciones sobre F, tenemos que $h_B(X_i(F)) = h_B(F)$ para $1 < i \leq n$, ya que F daba el mínimo en la B-altura dentro de la familia $\mathcal{F}_{|A|}$ y además $X_i(F) \in \mathcal{F}_{|A|}$ por (3.9). Análogamente, usando (3.7) en vez de (3.6), concluimos que $h_B(X_1(F)) = h_B(F)$. Entonces el lema 3.4.12 implica que $X_i(F) = F$ para $1 \leq i \leq n$. Por el lema 3.4.16, F es un B-segmento inicial, así que $F = D^B_{|A|}$. □

3.4.5. Observaciones finales

Cabe destacar que, en principio, podría parecer que el teorema 3.4.3 no es muy útil, dado que al usarlo únicamente pasamos de tener el problema de calcular el cardinal $|A + B|$ a calcular el cardinal de otra suma $|D^B_{|A|} + D^B_{|B|}|$. Si bien es cierto que los conjuntos $D^B_{|A|}$ y $D^B_{|B|}$ son a priori buenos conjuntos: son B-segmentos iniciales y sólo dependen en su definición de los cardinales $|A|$ y $|B|$.

Sin embargo, la utilidad del teorema 3.4.3 aparece cuando aplicamos el lema 3.4.17. Este lema, al margen de servir para demostrar el teorema 3.4.3, sirve para probar que el conjunto $D^B_{|A|} + D^B_{|B|}$ es un B-segmento inicial. Por tanto, para calcular su cardinal, bastará con conocer el punto $p = a + b \in D^B_{|A|} + D^B_{|B|}$ de mayor posición en el B-orden, puesto que en estas condiciones tendremos que

$$x \in D^B_{|A|} + D^B_{|B|} \Leftrightarrow x <_B p,$$

es decir, que $|D^B_{|A|} + D^B_{|B|}|$ coincide con la posición en el B-orden de p.

Remarcamos el hecho de que $p = a + b$ es el punto de posición máxima en el B-orden de $D^B_{|A|} + D^B_{|B|}$ si, y sólo si $a \in D^B_{|A|}$ y $b \in D^B_{|B|}$ son los puntos de máxima posición en el B-orden (en sus respectivos conjuntos). Dado que sabemos que los puntos de $D^B_{|B|}$ (ordenados según el B-orden) son

$$o <_B e_1 <_B 2e_1 <_B 3e_1 <_B \ldots <_B (|B| - n)e_1 <_B e_2 <_B e_3 <_B \ldots <_B e_n,$$

resulta claro que el punto en B de mayor posición en el B-orden es $b = e_n$.

Ejemplo. Sea $B \subset \mathbb{Z}^n$ con $|B| = 6$. En este caso, sabemos que el punto de mayor posición de B en el B-orden es e_2. Gracias a lo visto anteriormente, garantizamos que la cota del teorema 3.4.3 para el cardinal $|A + B|$ cuando $|A| = 54$ es

$$|A + B| \geq 77,$$

esto se debe a que, en el B-orden, el punto de posición 54-ésima es $a = (6, 3)$ y por tanto, la cota del teorema 3.4.3 viene dada por la posición del punto $a + e_2 = (6, 4)$, que es 77 (véase figura 3.13).

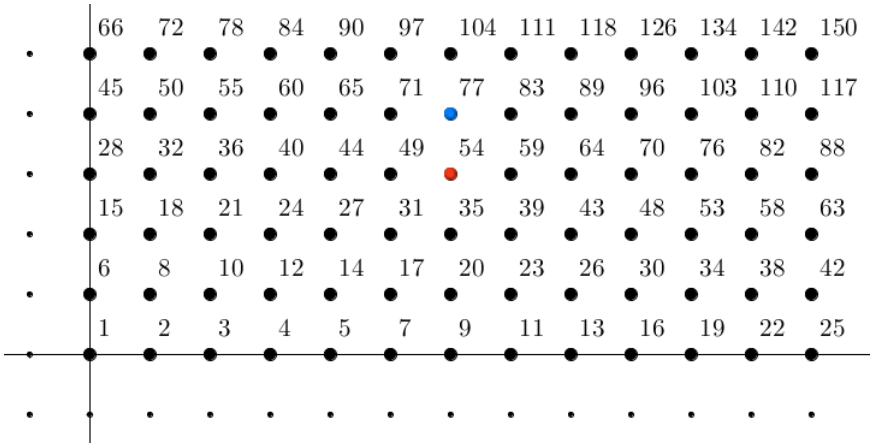


Figura 3.13: Los puntos de $\mathbb{Z}^2_+$ junto a su posición en el B-orden, con los puntos a y $a+e_2$ marcados, respectivamente, en rojo y azul.

Todo este análisis de la desigualdad hace que mostremos más interés si cabe en los B-órdenes, pues calcular la cota del teorema 3.4.3 es un problema equivalente a determinar qué punto ocupa una posición dada en el B-orden.

Otra observación interesante es que es posible calcular de forma precisa el número de puntos que contiene el conjunto P_m. Recogemos este resultado en la siguiente proposición.

Proposición 3.4.18. *Sean $m \in \mathbb{N}$ y $B \in \mathbb{Z}_+^n$ un conjunto finito. Entonces*

$$|P_m| = \binom{n + \left[\frac{m}{|B|-n}\right] - 1}{\left[\frac{m}{|B|-n}\right]}, \tag{3.10}$$

donde $[\,\cdot\,]$ representa la función parte entera.

Demostración. En primer lugar, destacamos que el cardinal de P_m no depende de m, sino de $\left[\frac{m}{|B|-n}\right]$. Esto se debe a que $|P_{m_1}| = |P_{m_2}|$ siempre que $\left[\frac{m_1}{|B|-n}\right] = \left[\frac{m_2}{|B|-n}\right]$: en efecto, sean $k, m \in \mathbb{Z}$ con $0 \leq k < |B| - n$ y

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

Siempre tenemos que si $x \in P_m$, entonces $x + ke_1 \in P_{m+k}$, de donde $P_m + ke_1 \subset P_{m+k}$. Por otro lado, si $y \in P_{m+k}$, entonces

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

por tanto $\frac{y_1-k}{|B|-n} \in \mathbb{Z}$ y, dado que $0 \leq \frac{k}{|B|-n} < 1$, deducimos que $\frac{k}{|B|-n}$ es la parte fraccionaria de $\frac{y_1}{|B|-n}$. Tenemos entonces $y_1 - k \geq 0$ y podemos garantizar que

$$y' = y - ke_1 = (y_1 - k, y_2, \ldots, y_n) \in \mathbb{Z}_+^n.$$

Al tener $w_B(y') = \frac{m}{|B|-n}$, sabemos que $y' \in P_m$ y, por tanto, que $P_{m+k} - ke_1 \subset P_m$ o, lo que es lo mismo, $P_{m+k} \subset P_m + ke_1$. Esto prueba $P_m + ke_1 = P_{m+k}$ y, consecuentemente, que $|P_m| = |P_{m+k}|$ como queríamos.

Por tanto, es suficiente con probar (3.10) cuando $\frac{m}{|B|-n} \in \mathbb{Z}$. Sea $r = \frac{m}{|B|-n}$. En estas condiciones, podemos definir una aplicación

$$f : P_m \to \{0,1\}^{n+r-1}$$

como sigue: dado $x \in P_m$, al ser $r \in \mathbb{Z}$, se tiene que

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

Definimos entonces $f(x)$ como la "palabra" de $\{0,1\}^{n+r-1}$ que tiene $\frac{x_1}{|B|-n}$ veces la letra "0", a la derecha un "1", seguidamente a la derecha x_2 veces la letra "0", y a su derecha un "1" y así siguiendo hasta escribir a la derecha de la $(n-1)$-ésima letra "1", x_n letras "0". Quedan por tanto escritas r letras "0" y $n-1$ letras "1", luego esta palabra pertenece a $\{0,1\}^{n+r-1}$. Esta aplicación es una biyección al conjunto de palabras con r veces la letra "0" de $\{0,1\}^{n+r-1}$ por la condición de que $x \in P_m$.

Por tanto, contar los puntos de P_m corresponde a contar las combinaciones que podemos hacer tomando r elementos de entre $n+r-1$, es decir,

$$|P_m| = \binom{n+r-1}{r}. \qquad \square$$

En consecuencia, dado $k \in \mathbb{Z}$, sabemos calcular a qué P_m pertenece el punto de posición k con respecto al B-orden. Basta con calcular el primer $m \in \mathbb{Z}$ tal que

$$\sum_{i=0}^{m} |P_i| = \sum_{i=0}^{m} \binom{n + \left[\frac{i}{|B|-n}\right] - 1}{\left[\frac{i}{|B|-n}\right]} \geq k.$$

Índice de figuras

Índice alfabético

Bibliografía

[1] B. Bollobás and I. Leader: Compressions and isoperimetric inequalities, *J. Comb. Theory A*, **56**, 47-62, 1991.

[2] R. J. Gardner and P. Gronchi: A Brunn-Minkowski inequality for the integer lattice. *Trans. Amer. Math. Soc.*, **353**, no. 10, 3995-4024, 2001.

[3] R. J. Gardner: The Brunn-Minkowski inequality, *Bull. Amer. Math. Soc.*, **39**, no. 3, 355-405, 2002.

[4] P. M. Gruber: *Convex and Discrete Geometry*. Springer, Berlin Heidelberg, 2007.

[5] M. B. Nathanson: *Additive number theory. Inverse problems and the geometry of sumsets*. Graduate Texts in Mathematics, 165. Springer-Verlag, New York, 1996.

[6] I. Z. Ruzsa: Sum of sets in several dimensions. *Combinatorica*, **14**, 485-490, 1994.

[7] R. Schneider: *Convex bodies: The Brunn-Minkowski Theory*. Cambridge University Press, 2nd expanded edition, 2014.