# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN CIENCIAS MATEMÁTICAS Y DE LA ESPECIALIZACIÓN EN ESTADÍSTICA APLICADA

## LA SUMA DE CONJUNTOS FINITOS EN $R^2$

TESIS
QUE PARA OPTAR POR EL GRADO DE:
MAESTRO EN CIENCIAS

PRESENTA:
JOSÉ DAVID SUÁREZ GONZALEZ

DIRECTORA:
DRA. AMANDA MONTEJANO CANTORAL, FACULTAD DE CIENCIAS.

CIUDAD DE MÉXICO, 10 DE ENERO DEL 2019.

# Agradecimientos

En este trabajo de tesis quiero agradecer principalmente a mi familia que me ha apoyado siempre en todo, al igual que ha estado conmigo en cualquier decisión y rumbo que he tomado. Soy lo que soy gracias a ellos. También quiero agradecer a mi asesora Amanda Montejano, ya que tuvo la paciencia y la confianza en mí para poder concluir este trabajo. Por último quiero agradecer a CONACyT por apoyarme durante la duración de la maestría y por apoyarme con el proyecto "CONACyT 219727" y a la UNAM por apoyarme con el proyecto "PAPIIT IN114016"

# Índice general

# Capítulo 1

# Introducción

En este trabajo de tesis nuestro principal objetivo es estudiar un teorema de Grynkiewicz y Serra que se relaciona con dos importantes resultados en matemáticas: la *desigualdad de Brunn-Minkowski* y el *teorema* $2^n$ *de Freiman*.

Dados dos conjuntos (no vacíos), $A$ y $B$, de $\mathbb{R}^n$ (el espacio euclideano $n$-dimencional), la *suma de Minkowski* de $A$ y $B$ se define como:

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

La *teoría aditiva de números* estudia, principalmente, propiedades de la suma de Minkowski de subconjuntos finitos de $\mathbb{R}$ (equivalentemente, subconjuntos finitos de $\mathbb{Z}$). Los llamados resultados inversos en esta área establecen que si un conjunto, $A$, satisface que su suma, $A + A$, es pequeña entonces $A$ debe de tener cierta estructura. En este sentido, el *teorema* $2^n$ *de Freiman* es un resultado inverso que nos dice que si $A$ es un subconjunto finito de $\mathbb{R}^n$ y $|A + A|$ es pequeña entonces $A$ tiene cierta estructura geométrica. Más concretamente, el teorema $2^n$ de Freiman nos dice que si $|A + A| \leq c|A|$, donde $c \in \mathbb{R}$ es tal que $1 < c < 2^n$, entonces una fracción positiva de los elementos de $A$ se encuentran contenidos en un hiperplano (sub-espacio afín de dimensión $n - 1$).

En el capítulo 2, daremos el enunciado preciso y una prueba completa del teorema $2^n$ de Freiman. Dicha prueba, está basada en el material presentado en el capítulo 5 del libro *Additive Number Theory: Inverse Problems and the Geometry of Numbers*, [1], además en los artículos [2–5] podemos encontrar más información al respecto. Sin embargo, en esta tesis, con la intención de proporcionar una manera amable para estudiar tal demostración, primero la presentaremos en $\mathbb{R}^2$ y posteriormente en $\mathbb{R}^n$, enfatizando que gran parte de la complejidad de la prueba, y por ende de la profundidad del resultado, se encuentra ya en el caso de dos dimensiones. Para que la prueba sea autocontenida, incluimos un apéndice con las definiciones, notaciones y resultados específicios de algebra lineal que usaremos, por consiguiente es recomendado empezar a leer el apéndice antes de comenzar el capítulo 2.

La *desigualdad de Brunn-Minkowski* [6] es una desigualdad que nace de la geometría y se ha consolidado como una potente herramienta tanto en análisis como en geometría convexa, mostrando, además, conexiones con diversas áreas de la matemática. Dados, $A$ y $B$, dos

cuerpos convexos en $\mathbb{R}^n$, la desigualdad de Brunn-Minkowski establece una cota inferior del volumen de $A + B$ en términos de los volúmenes de $A$ y de $B$; concretamente:

$$\mu(A + B)^{1/n} \geq \mu(A)^{1/n} + \mu(B)^{1/n},$$

donde $\mu$ denota la medida de Lebesgue en $\mathbb{R}^n$. En el capítulo 3, presentaremos tanto la desigualdad de Brunn-Minkowski como una posterior versión de Bonnesen que es más fuerte, y que se asemeja a la versión discreta propuesta por Grynkiewicz y Serra para dos dimensiones.

Finalmente el resultado principal del artículo *Properties of two-dimensional sets with small sumset*, [7] extiende el caso 2-dimensional del teorema $2^n$ de Freiman, considerando la suma de dos conjuntos distintos en vez de uno. Para probar dicho teorema, los autores establecen una cota inferior general de $|A + B|$ (donde $A$ y $B$ son conjuntos finitos de $\mathbb{R}^2$) que, en la actualidad, es considerada la mejor versión discreta de la desigualdad de Brunn-Minkowski en dos dimensiones. En el capítulo 4, presentaremos dicha desigualdad de Grynkiewicz y Serra, y además presentaremos una generalización para más de dos conjuntos.

# Capítulo 2

# El teorema $2^n$ de Freiman

En este capítulo estudiaremos un clásico resultado inverso conocido como el *teorema* $2^n$ *de Freiman*. Dicho teorema fue una de las herramientas principales en la prueba original de uno de los resultados más importantes en teoría aditiva de números: el teorema de Freiman (aquel que establece que cualquier subconjunto $A \subset \mathbb{Z}$ con $|A + A|$ pequeña contiene una fuerte estructura aritmética). En esta tesis no daremos el enunciado preciso del teorema de Freiman, sin embargo, nos concentraremos en estudiar a profundidad el teorema $2^n$ de Freiman que ha mostrado tener interés por sí mismo.

La mayoría del material contenido en este capítulo se encuentra en [1]. Como la demostración del teorema $2^n$ de Freiman es compleja, presentaremos primero, en la Sección 2.2, la prueba completa para el caso de dos dimensiones, proporcionando ejemplos concretos de los conceptos usados. Posteriormente, en la Sección 2.3, daremos la prueba para el caso general. Con el objetivo de que la prueba sea autocontenida, los resultados específicos de álgebra lineal que usamos se encuentran demostrados en el apéndice de esta tesis.

## 2.1. Presentación del teorema

En esta sección enunciaremos las dos versiones más comunes del teorema $2^n$ de Freiman, mostraremos su equivalencia, y demostraremos en qué sentido este resultado es óptimo.

A grandes rasgos, lo que nos dice el teorema $2^n$ de Freiman es que cualquier subconjunto finito $A \subset \mathbb{R}^n$ con $|A|$ "suficientemente grande" y $|A + A|$ "relativamente pequeña", debe de estar contenido en "pocos"hiperplanos paralelos, o bien (equivalentemente) existe un hiperplano que contiene una "buena parte"de $A$. En los enunciados de los teoremas 2.1 y 2.2 quedará claro el significado de todos los términos entre comillas.

Antes de enunciar el teorema $2^n$ de Freiman en su primera versión, recordemos que dado $H$ un subespecio vectorial de $\mathbb{R}^n$, denotamos por $\mathbb{R}^n/H$ al subespacio cociente, por:

$$\phi_H : \mathbb{R}^n \to \mathbb{R}^n/H$$

a la proyección natural módulo $H$, y para un subconjunto finito $S \subset \mathbb{R}^n$,

$$\phi_H(S) = \{\mathbf{v} \in \mathbb{R}^n/H \,|\, \phi_H(\mathbf{s}) = \mathbf{v} \text{ para algún } \mathbf{s} \in S\},$$

de modo que $|\phi_H(S)|$ es en número de hiperplanos paralelos a $H$ que intersectan a $S$.

**Ejemplo 2.1.** *Sea $n = 2$. Sea $\boldsymbol{e}_1 = (1, 0)$, y sea $\langle \boldsymbol{e}_1 \rangle$ el subespacio generado por $\boldsymbol{e}_1$. Y sea:*

$$S = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 2)\}.$$

*Observemos en la figura* 2,1 *que:*

$$\phi_{\langle \boldsymbol{e}_1 \rangle}(S) = \{(0, 1) + \langle \boldsymbol{e}_1 \rangle, (0, 2) + \langle \boldsymbol{e}_1 \rangle, (0, 4) + \langle \boldsymbol{e}_1 \rangle\};$$

*así $|\phi_{\langle \boldsymbol{e}_1 \rangle}(S)| = 3$, que es el número de hiperplanos paralelos a $\langle \boldsymbol{e}_1 \rangle$ que intersectan a $S$.*

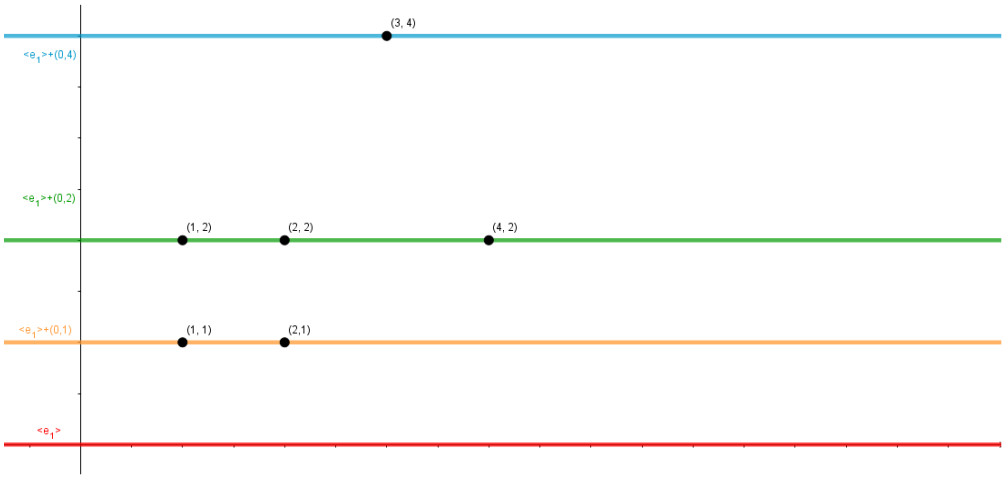



Figura 2.1: Podemos observar al conjunto $S = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 2)\}$ y al conjunto $\phi_{\langle \mathbf{e}_1 \rangle}(S) = \{(0, 1) + \langle \mathbf{e}_1 \rangle, (0, 2) + \langle \mathbf{e}_1 \rangle, (0, 4) + \langle \mathbf{e}_1 \rangle\}$, donde $\langle \mathbf{e}_1 \rangle$ es el hiperplano generado por el vector $\mathbf{e}_1 = (1, 0)$.

**Teorema 2.1** (Teorema $2^n$ de Freiman, versión 1)**.** *Dados $n \geq 2$ entero, y $c$ un número real tal que $1 < c < 2^n$, existen constantes $k = k(n, c)$ y $s = s(n, c)$, tales que si $A$ es un subconjunto finito de $\mathbb{R}^n$ que satisfice:*

1. $|A| \geq k$,
2. $|A + A| \leq c|A|$,

*entonces existe un sub-espacio $H$ de $\mathbb{R}^n$, de dimensión $(n - 1)$, tal que $|\phi_H(A)| < s$.*

**Teorema 2.2** (Teorema $2^n$ de Freiman, versión 2)**.** *Dados $n \geq 2$ entero, y $c$ un número real tal que $1 < c < 2^n$, existen constantes $k^* = k^*(n, c)$ y $\epsilon^* = \epsilon^*(n, c) > 0$, tales que si $A$ es un subconjunto finito de $\mathbb{R}^n$ que satisfice:*

1. $|A| \geq k^*$, *y*

*2.* $|A + A| \leq c|A|$,

*entonces existe un hiperplano* $H'$ *de* $\mathbb{R}^n$ *tal que* $|A \cap H'| > \epsilon^*|A|$.

En la Sección 2,3 probaremos la versión 2 del teorema $2^n$ de Freiman, construyendo explícitamente $k^*$ y $\epsilon^*$ en función de $n$ y $c$. A continuación, mostraremos que la versión 1 (teorema 2.1) y la versión 2 (teorema 2.2) son equivalentes.

**Proposición 2.1.** *Los teoremas 2.1 y 2.2 son equivalentes.*

*Demostración.* Sean $n \geq 2$ entero, y $c$ un número real tal que $1 < c < 2^n$.

$(1 \Rightarrow 2)$ Supongamos que existen $s = s(n, c)$ y $k = k(n, c)$ tales que, si $A$ satisface las hipótesis del teorema 2.1 entonces existe un subespacio, $H$, de dimensión $n-1$ con la propiedad de que $|\phi_H(A)| < s$. Demostraremos que $k^* := k$ y $\epsilon^* := \frac{1}{s}$ cumplen lo que establece el teorema 2.2. Para ello, consideremos un subconjunto finito, $A \subset \mathbb{R}^n$, tal que $|A| \geq k^*$ y $|A+A| \leq c|A|$. Por el teorema 2.1, sabemos que existe un sub-espacio $H$ de $\mathbb{R}^n$, de dimensión $(n-1)$, tal que $|\phi_H(A)| < s$. Equivalentemente, existen menos de $s$ hiperplanos paralelos que cubren al conjunto $A$. Es decir, existen $\mathbf{a}_1, \mathbf{v}_2, \ldots, \mathbf{v}_m \in \mathbb{R}^n$ tales que para $H_i := H + \mathbf{v}_i$ tenemos $A = \bigcup_{i=1}^{m}(H_i \cap A)$ con $m < s$. Por el principio de las casillas, uno de estos hiperplanos debe de contener un número de elementos estrictamente mayor a la fracción $\frac{|A|}{s}$ (de lo contrario tendríamos $|A| = |H_1 \cap A| + \cdots + |H_m \cap A| \leq m\frac{|A|}{s} < |A|$, una contradicción). Luego, existe un hiperplano $H' \in \{H_1, \ldots, H_m\}$ tal que tal que $|A \cap H'| > \frac{1}{s}|A| = \epsilon^*|A|$, que es exactamente lo que se quería demostrar.

$(2 \Rightarrow 1)$ Supongamos que existen $\epsilon^* = \epsilon^*(n, c) > 0$ y $k^* = k^*(n, c)$ tales que, si $A$ satisface las hipótesis del teorema 2.2 entonces existe un hiperplano, $H'$, con la propiedad de que $|A \cap H'| > \epsilon^*|A|$. Demostraremos que $k := k^*$ y $s := \frac{c}{\epsilon^*}$ cumplen lo que establece el teorema 2.1. Para ello, consideremos un subconjunto finito, $A \subset \mathbb{R}^n$, tal que $|A| \geq k$ y $|A+A| \leq c|A|$. Por el teorema 2.2, sabemos que existe un hiperplano $H'$ de $\mathbb{R}^n$ tal que:

$$|A \cap H'| > \epsilon^*|A|. \tag{2.1}$$

Como $A$ es un conjunto finito, existen un número finito de hiperplanos $H_1, H_2, \ldots, H_l$, paralelos a $H'$, tales que $A \cap H_i \neq \emptyset$ y $A \subset \bigcup_{i=1}^{l} H_i$. Para cada $i \in [l]$, elegimos $\mathbf{a}_i \in (A \cap H_i)$. Notemos que $\mathbf{a}_i + (A \cap H') \subseteq A + A$ para toda $1 \leq i \leq l$, de modo que:

$$\bigcup_{i=1}^{l}(\mathbf{a}_i + (A \cap H')) \subseteq A + A,$$

y como $(\mathbf{a}_i + (A \cap H')) \cap (\mathbf{a}_j + (A \cap H')) = \emptyset$ si $i \neq j$, entonces:

$$\sum_{i=1}^{l} |\mathbf{a}_i + (A \cap H')| \leq |A + A| < c|A|. \tag{2.2}$$

Notemos que, como $|\mathbf{a}_i + (A \cap H')| = |A \cap H'|$ para cada $i \in [l]$, de las desigualdades (2.1) y (2.2) obtenemos que $l\epsilon^*|A| < c|A|$, de donde se infiere $l < \frac{c}{\epsilon^*}$. Como, por definición, $l$ es el número de hiperplanos paralelos a $H'$ que cubren $A$, existe un un subespacio, $H$, de dimensión $n-1$ con la propiedad de que $|\phi_H(A)| = l < s$ probando lo que se quería. □

Para finalizar esta sección, veamos que la cota superior de $c$ en el teorema $2^n$ de Freiman es óptima. Es decir, veremos que existen subconjuntos $A$ de $\mathbb{R}^n$ tan grandes como queramos, que satisfacen $|A+A| < 2^n|A|$ pero que no cumplen la conclusión del teorema $2^n$ de Freiman.

**Proposición 2.2.** *Sea $n \geq 2$. Para cualquier par de constantes $k$ y $\epsilon > 0$, existe un subconjunto $A$ finito de $\mathbb{R}^n$ que satisface la siguientes condiciones:*

1. $|A| \geq k$.
2. $|A + A| < 2^n|A|$
3. $|A \cap H| \leq \epsilon|A|$, *para todo hiperplano $H$ de $\mathbb{R}^n$.*

*Demostración.* Sea $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ la base canónica de $\mathbb{R}^n$, sean $k$ y $\epsilon > 0$ constantes y sea $t$ un número entero con la siguiente propiedad:

$$t \geq max\{k^{\frac{1}{n}}, \epsilon^{-1}\}.$$

Sea $A$ un conjunto finito de $\mathbb{R}^n$, definido como:

$$A = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{e}_i \,|\, \lambda_i \in \{0, \ldots, t-1\}, \text{ para cada } i \in \{1, \ldots, n\} \right\},$$

es decir, los elementos de $A$ son todos los vectores de la forma $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ con $\lambda_i \in \{0, \ldots, t-1\}$ para cada $i \in [n]$. Demostraremos que el conjunto $A$ así construido cumple con lo requerido en el lema. Como cada $\lambda_i$ puede tomar $t$ valores distintos, $|A| = t^n$. Por construcción de $t$, tenemos que $t \geq k^{\frac{1}{n}}$ y por lo tanto, $|A| \geq k$ que es la primera condición del lema.

Ahora calcularemos la cardinalidad de $A + A$. Observemos que:

$$A + A = \left\{ \sum_{i=1}^{n} \lambda_i \mathbf{e}_i \,|\, \lambda_i \in \{0, \ldots, 2(t-1)\}, \text{ para cada } i \in \{1, \ldots, n\} \right\}.$$

De lo anterior tenemos que:

$$\begin{aligned} |A + A| &= (2(t-1)+1)^n. \\ &= (2t-1)^n \\ &< (2t)^n \\ &= 2^n t^n \\ &= 2^n |A|, \end{aligned}$$

lo cual nos dice que el conjunto $A$ satisface la segunda condición del lema.

Por último demostraremos que el conjunto $A$ cumple la tercera condición del lema. Sea $H$ un hiperplano de $\mathbb{R}^n$ definido por $H = \{\mathbf{v} \in \mathbb{R}^n \mid (\mathbf{v}, \mathbf{h}) = \gamma\}$ donde $\mathbf{h} = \sum_{i=1}^{n} h_i \mathbf{e}_i$ es un vector en $\mathbb{R}^n$ distinto del vector $\mathbf{0}$ y $\gamma$ un escalar en $\mathbb{R}$. Como $\mathbf{h}$ es distinto del vector $\mathbf{0}$, entonces existe $j \in [n]$ tal que $h_j \neq 0$. Ahora veremos cuantos elementos de $A$ pueden pertenecer a $H$. Si $\mathbf{v} = (v_1, \ldots, v_n)$ es un vector en $A \cap H$, entonces $(\mathbf{h}, \mathbf{v}) = \gamma$ y $v_i \in \{0, \ldots, t-1\}$ para toda $i \in [n]$. Luego $\sum_{i=1}^{n} h_i v_i = \gamma$, entonces:

$$\gamma = h_j v_j + \sum_{i=1}^{j-1} h_i v_i + \sum_{i=j}^{n} h_i v_i,$$

y como $h_j \neq 0$,

$$v_j = \frac{\gamma - \sum_{i=1}^{j-1} h_i v_i - \sum_{i=j}^{n} h_i v_i}{h_j}.$$

De lo anterior tenemos que $v_j$ está unicamente definido por $v_1, \ldots, v_{j-1}, v_{j+1}, ldots, v_n$ entonces en realidad $\mathbf{v}$ está determinado por $n-1$ números a elegir en $\{0, \cdots, t-1\}$ y por lo tanto

$$|A \cap H| \leq t^{n-1} = t^{-1} t^n \leq \epsilon_0 t^n = \epsilon |A|.$$

que es lo que queríamos probar. □

Para entender mejor la construcción del conjunto $A$, veamos el siguiente ejemplo en dos dimensiones.

**Ejemplo 2.2.** *Sea $k = 5$ y $\epsilon = \frac{1}{8}$. Construiremos un conjunto $A$ en $\mathbb{R}^2$ tal que su cardinalidad sea mayor o igual que 5, $|A + A| < 4|A|$ y que cualquier hiperplano en $\mathbb{R}^2$ contenga a lo más $\frac{1}{8}$ de $|A|$. El conjunto $A$ definido en la demostración de la proposición 2,2, consta de los puntos con coordenadas en $\{0, \cdots, t-1\}$ donde $t \geq \text{máx}\{\sqrt{5}, 8\}$. En la figura 2,2 se observa el conjunto $A$ con $t = 8$.*

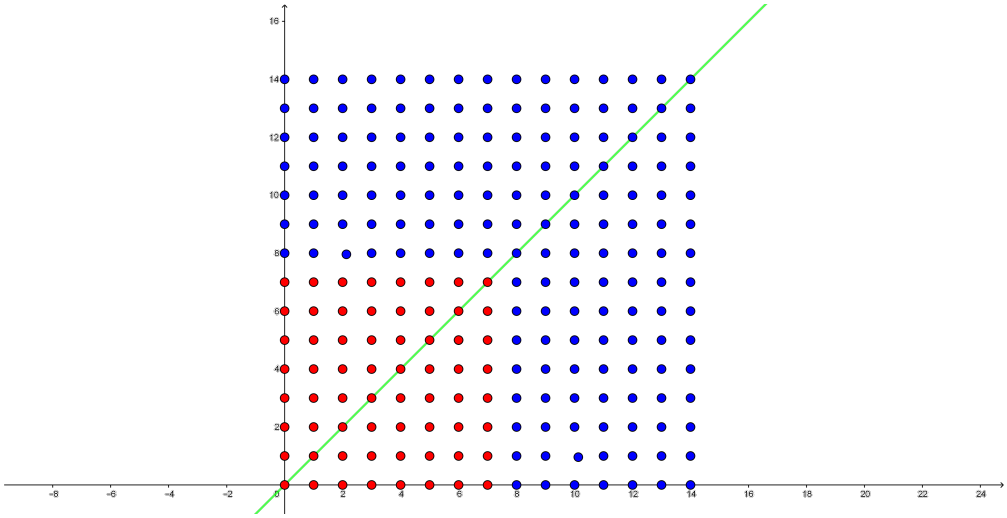


Figura 2.2: El conjunto $A$ está representado por los puntos rojos, mientras que $2A$ es la unión de los puntos rojos con los puntos azules.

*Observemos que* $|A| = (8)^2 = 64 \geq 5$ *y* $|A + A| = (15)^2 = 225 < (4)(64) = 256$. *Además, como en* $\mathbb{R}^2$ *los hiperplanos son rectas, entonces el hiperplano que tiene mayor número de puntos de* $A$ *es la recta que pasa por la diagonal que en este caso contiene* 8 *puntos de* $A$*, luego cualquier recta que intersecta a* $A$ *satisface tener a lo más* $8 = \frac{1}{8}|A|$ *puntos de* $A$*, y por lo tanto* $A$ *cumple con las condiciones.*

## 2.2. Prueba del teorema 2.2 en el caso $n = 2$

Como dijimos al inicio del capítulo, la prueba del teorema $2^n$ *de Freiman* es compleja por lo cual vale la pena presentarla primero para dimensión $n = 2$. De ese modo, podremos visualizar en el plano los conceptos que usaremos y entender las ideas claves de la demostración para después proceder, en la siguiente sección, a demostrar el teorema en el caso general.

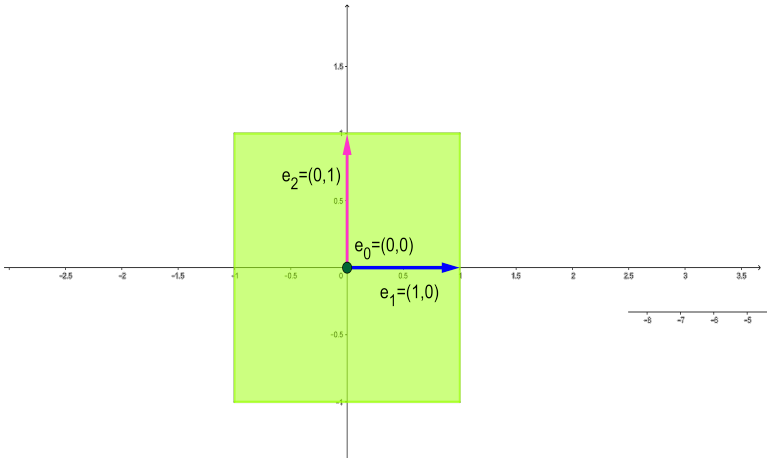
Comenzaremos definiendo lo que es un *bloque*, mostraremos sus propiedades básicas y su relación con los hiperplanos. Estos bloques, como los hiperplanos, serán objetos esenciales en la prueba del teorema $2^n$ de Freiman.

**Definición 2.1.** *Sea* $\boldsymbol{e}_0$ *un vector en* $\mathbb{R}^2$*, y* $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ *una base de* $\mathbb{R}^2$*. El* bloque $B = B(\boldsymbol{e}_0; \boldsymbol{e}_1, \boldsymbol{e}_2)$ *con centro* $\boldsymbol{e}_0$ *y base* $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ *es el conjunto:*

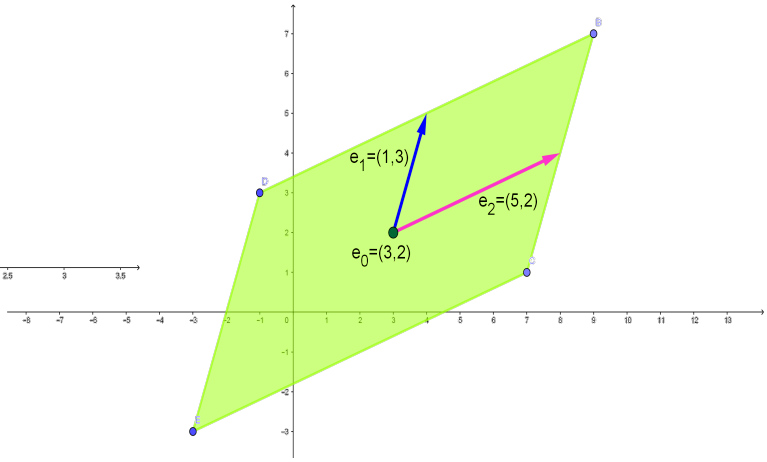
$$B(\boldsymbol{e}_0; \boldsymbol{e}_1, \boldsymbol{e}_2) := \{\boldsymbol{e}_0 + x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 \mid -1 \leq x_1, x_2 \leq 1\}.$$

**Ejemplo 2.3.** *1. En la figura* 2,3*a tenemos un bloque con* $\boldsymbol{e}_0 = (0, 0)$*,* $\boldsymbol{e}_1 = (1, 0)$ *y* $\boldsymbol{e}_2 = (0, 1)$.

*2. En la figura* 2,3*b tenemos un bloque con* $\boldsymbol{e}_0 = (3, 2)$*,* $\boldsymbol{e}_1 = (1, 3)$ *y* $\boldsymbol{e}_2 = (5, 2)$.




(a) Bloque $B(\mathbf{(0,0)};(0,1),(1,0))$




(b) Bloque $B((3,2);(1,3),(5,2))$

Figura 2.3: Ejemplos de bloques.

Dado un bloque $B(\mathbf{e}_0;\mathbf{e}_1,\mathbf{e}_2)$, nos interesa estudiar los siguientes conjuntos.

**Definición 2.2.** *Sea $B = B(\boldsymbol{e}_0;\boldsymbol{e}_1,\boldsymbol{e}_2)$ un bloque en $\mathbb{R}^2$.*

1. *El conjunto de* vértices de $B$ *es:*

$$vert(B) := \{\boldsymbol{e}_0 + \mu_1\boldsymbol{e}_1 + \mu_2\boldsymbol{e}_2 \,|\, (\mu_1,\mu_2) \in \{-1,1\}^2\}.$$

2. *El* interior de $B$ *es:*

$$int(B) := \{\boldsymbol{e}_0 + x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2 \,|\, -1 < x_1, x_2 < 1\}.$$

3. *Sea $j \in \{1,2\}$ y $\mu_j \in \{-1,1\}$, el* hiperplano facial correspondiente a $j$ y $\mu_j$ *es:*

$$F_{j,\mu_j} := \{\boldsymbol{e}_0 + \mu_j\boldsymbol{e}_j + x\boldsymbol{e}_i \,|\, x \in \mathbb{R}, i \neq j\}.$$

Para visualizar los conceptos definidos anteriormente, veamos un ejemplo concreto.

**Ejemplo 2.4.** *Sean $\boldsymbol{e}_0 = (3,5)$, $\boldsymbol{e}_1 = (-2,-5)$ y $\boldsymbol{e}_2 = (-6,3)$. Consideramos el bloque $B = B(\boldsymbol{e}_0;\boldsymbol{e}_1,\boldsymbol{e}_2)$. Así $vert(B) = \{(11,7),(-1,13),(-5,3),(7,-3)\}$, y en la figura 2,4 se muestran el interior de $B$ así como sus cuatro hiperplanos faciales: $F_{1,-1}$, $F_{1,1}$, $F_{2,-1}$ y $F_{2,1}$.*

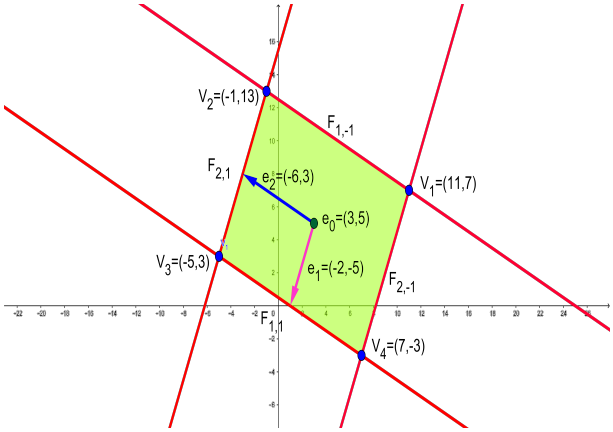



Figura 2.4: En esta figura podemos apreciar los conjuntos definidos en 2,2 para el bloque $B((3,5);(-2,-5),(-6,3))$, donde el $int(B)$ es la parte verde del bloque y $vert(B) = \{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4\}$. Además podemos observar que $F_{1,-1} \cap F_{2,-1} = \{\mathbf{v}_1\}$, $F_{1,-1} \cap F_{2,1} = \{\mathbf{v}_2\}$, $F_{1,+1} \cap F_{2,1} = \{\mathbf{v}_3\}$, $F_{1,+1} \cap F_{2,-1} = \{\mathbf{v}_4\}$

Observemos que $B$ es un rombo cuyas esquinas son los elementos de $vert(B)$, y cuyo interior es $int(B)$. Los hiperplanos faciales de $B$ son los lados de $B$ extendidos a ambas direcciones.

Las siguientes propiedades se infieren directamente de la Definición 2,2.

**Observación 2.1.** *Sea $B = B(\boldsymbol{e}_0; \boldsymbol{e}_1, \boldsymbol{e}_2)$ un bloque en $\mathbb{R}^2$. Entonces:*

1. $|vert(B)| = 4$.
2. *El bloque $B$ es la envolvente convexa de $vert(B)$.*
3. *Existen exactamente 4 hiperplanos faciales.*

Notemos también que los hierplanos faciales dividen el plano $\mathbb{R}^2$ en nueve secciones ajenas. Estas secciones se definen formalmente a continuación.

**Definición 2.3.** *Sea $B = B(\boldsymbol{e}_0; \boldsymbol{e}_1, \boldsymbol{e}_2)$ un bloque en $\mathbb{R}^2$, y sean $\lambda_1, \lambda_2 \in \{-1, 0, 1\}$. Definimos $D(\lambda_1, \lambda_2)$ como el conjunto de vectores de la forma $\boldsymbol{e}_0 + x_1\boldsymbol{e}_1 + x_2\boldsymbol{e}_2$ donde:*

$$\begin{aligned} x_i > 1, \ si\ \lambda_i = 1, \\ -1 < x_i < 1, \ si\ \lambda_i = 0, \\ x_i < -1, \ si\ \lambda_i = -1, \end{aligned}$$

*con $1 \leq i \leq 2$.*

En particular $D(0,0) = int(B)$. Con respecto al bloque dado en el ejemplo 2,4, las 9 secciones se pueden ver en la figura 2,5.

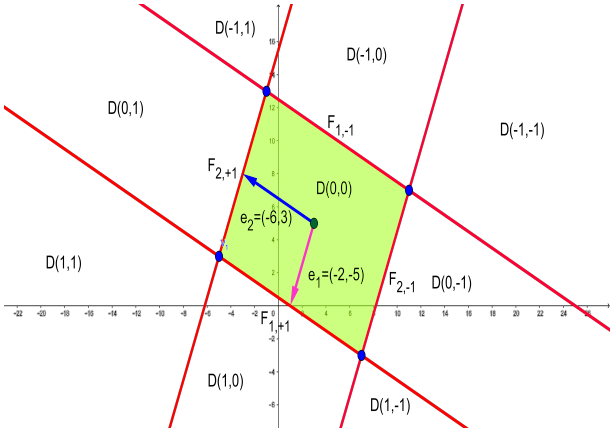



Figura 2.5: Bloque $B((3,5);(-2,-5),(-6,3))$ con sus 4 hiperplanos faciales y sus 9 secciones

La siguiente observación se deduce facilmente de la definición 2,3.

**Observación 2.2.** *Los conjuntos definidos en* 2,3 *son ajenos por pares y además son conjuntos convexos.*

Ahora veremos propiedades útiles de los bloques para la demostración del teoma $2^n$ de Freiman.

**Lema 2.1.** *Sea* $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ *una base de* $\mathbb{R}^2$*, sea* $B = B((0,0); \boldsymbol{e}_1, \boldsymbol{e}_2)$ *y* $\boldsymbol{u}$ *y* $\boldsymbol{v}$ *vectores en* $\mathbb{R}^2$*. Entonces las siguientes afirmaciones se cumplen.*

1. $B(\boldsymbol{u}, \boldsymbol{e}_1, \boldsymbol{e}_2) = B + \{\boldsymbol{u}\}$.
2. *Si* $(0,0) \in B(\boldsymbol{u}; \boldsymbol{e}_1, \boldsymbol{e}_2)$*, entonces* $(0,0) \in B + \{t\boldsymbol{u}\}$ *para todo* $0 \leq t \leq 1$.
3. *Si* $(B + \{\boldsymbol{u}\}) \cap (B + \{\boldsymbol{w}\}) \neq \emptyset$*, entonces* $(ver(B) + \{\boldsymbol{u}\}) \cap (B + \{\boldsymbol{w}\}) \neq \emptyset$.

*Demostración.* 1. Observemos lo siguiente:

$$\begin{aligned} B(\mathbf{u}; \mathbf{e}_1, \mathbf{e}_2) &= \{\mathbf{u} + x_1\mathbf{e}_1 + x_2\mathbf{e}_2 \mid -1 \leq x_1, x_2 \leq 1\} \\ &= \{(0,0) + x_1\mathbf{e}_1 + x_2\mathbf{e}_2 \mid -1 \leq x_1, x_2 \leq 1\} + \{\mathbf{u}\} \\ &= B + \{\mathbf{u}\}. \end{aligned}$$

2. Sea $(0,0) \in B(\mathbf{u}; \mathbf{e}_1, \mathbf{e}_2)$ y sea $0 \leq t \leq 1$. Por el inciso anterior basta probar que $(0,0) \in B(t\mathbf{u}; \mathbf{e}_1, \mathbf{e}_2\}$. Como $(0,0)$ está en $B(\mathbf{u}; \mathbf{e}_1, \mathbf{e}_2)$, entonces existen $-1 \leq x_1, x_2 \leq 1$, tales que:

$$(0,0) = \mathbf{u} + x_1\mathbf{e}_1 + x_2\mathbf{e}_2,$$

luego multiplicando ambos lados de la igualdad por $t$, se concluye que:

$$(0,0) = t\mathbf{u} + tx_1\mathbf{e}_1 + tx_2\mathbf{e}_2.$$

Pero como $-1 \leq x_1, x_2, t \leq 1$, entonces $-1 \leq tx_1, tx_2 \leq 1$ y por lo tanto $(0,0) \in B + \{t\mathbf{u}\}$.

3. Como los vectores $\mathbf{e}_1$ y $\mathbf{e}_2$ forman una base de $\mathbb{R}^2$, entonces tenemos que los vectores $\mathbf{u}$ y $\mathbf{v}$ los podemos escribir como combinación lineal de los vectores $\mathbf{e}_1$ y $\mathbf{e}_2$, es decir, existen $u_1, u_2, v_1$ y $v_2$ en $\mathbb{R}$ tales que:

$$\mathbf{u} = u_1\mathbf{e}_1 + u_2\mathbf{e}_2$$

$$y$$

$$\mathbf{v} = v_1\mathbf{e}_1 + v_2\mathbf{e}_2.$$

Antes de continuar con la demostración observemos lo siguiente. El vector $\mathbf{w} = (w_1\mathbf{e}_1 + w_2\mathbf{e}_2) \in B + \{\mathbf{v}\}$, si y sólo si existen escalares $\alpha_1$ y $\alpha_2$ tales que $-1 \leq \alpha_1, \alpha_2 \leq 1$, y:

$$\mathbf{w} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + \mathbf{v},$$

si y sólo si

$$w_1\mathbf{e}_1 + w_2\mathbf{e}_2 = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + v_1\mathbf{e}_1 + v_2\mathbf{e}_2,$$

si y solo si

$$w_1\mathbf{e}_1 + w_2\mathbf{e}_2 = (\alpha_1 + v_1)\mathbf{e}_1 + (\alpha_2 + v_2)\mathbf{e}_2,$$

si y solo si

$$w_1 = \alpha_1 + v_1 \text{ y } w_2 = \alpha_2 + v_2.$$

Como $-1 \leq \alpha_1, \alpha_2 \leq 1$, tenemos que:

$$v_1 - 1 \leq \alpha_1 + v_1 \leq v_1 + 1 \text{ y } v_2 - 1 \leq \alpha_2 + v_2 \leq v_2 + 1,$$

y por lo tanto:

$$\mathbf{w} \in B + \{\mathbf{v}\} \text{ si y sólo si } v_1 - 1 \leq w_1 \leq v_2 + 1 \text{ y } v_2 - 1 \leq w_2 \leq v_2 + 1. \tag{2.3}$$

Ya que establecimos la observación anterior, procederemos a demostrar lo requerido. Por hipótesis tenemos que $(B + \{\mathbf{u}\}) \cap (B + \{\mathbf{v}\}) \neq \emptyset$, entonces existen escalares $x_1, x_2, y_1$ y $y_2$ tales que $-1 \leq x_1, y_1, x_2, y_2, \leq 1$, y que:

$$x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + \mathbf{u} = y_1\mathbf{e}_1 + y_2\mathbf{e}_2 + \mathbf{v},$$

luego,

$$x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + u_1\mathbf{e}_1 + u_2\mathbf{e}_2 = y_1\mathbf{e}_1 + y_2\mathbf{e}_2 + v_1\mathbf{e}_1 + v_2\mathbf{e}_2,$$

obteniendo,

$$(x_1 + u_1)\mathbf{e}_1 + (x_2 + u_2)\mathbf{e}_2 = (y_1 + v_1)\mathbf{e}_1 + (y_2 + v_2)\mathbf{e}_2,$$

y por lo tanto

$$x_1 + u_1 = y_1 + v_1 \text{ y } x_2 + u_2 = y_2 + v_2.$$

Como $1 \leq x_1, y_1, x_2, y_2 \leq 1$, entonces obtenemo que:

$$u_1 - 1 \leq x_1 + u_1 \leq u_1 + 1 \text{ y } v_1 - 1 \leq y_1 + v_1 \leq v_1 + 1.$$

Como:

$$x_1 + u_1 = y_1 + v_1,$$

entonces obtenemos que:

$$v_1 - 1 \leq x_1 + u_1 \leq v_1 + 1 \tag{2.4}$$

Ahora exhibiremos explícitamente el vértice del bloque $B + \{\mathbf{u}\}$ que está en el bloque $B + \{\mathbf{w}\}$, pero esto depende de los valores de $u_1, u_2, v_1$ y $v_2$. Primero analizaremos los valores de $v_1$ y $u_1$. Si $u_1 \leq v_1$, entonces obtenemos que:

$$u_1 + 1 \leq v_1 + 1. \tag{2.5}$$

Combinando la desigualdad 2,4 con la desigualdad 2,5 y el hecho de que $-1 \leq x_1 \leq 1$, tenemos que:

$$v_1 - 1 \leq x_1 + u_1 \leq u_1 + 1 \leq v_1 + 1,$$

luego:

$$v_1 - 1 \leq u_1 + 1 \leq v_1 + 1. \tag{2.6}$$

Ahora, si $v_1 < u_1$. En este caso obtenemos que:

$$v_1 - 1 < u_1 - 1 \tag{2.7}$$

Nuevamente por la desigualdad 2,4 y ahora por la desigualdad 2,7 y el hecho de que $-1 \leq x_1 \leq 1$, tenemos que:

$$v_1 - 1 \leq u_1 - 1 \leq x_1 + u_1 \leq v_1 + 1,$$

luego

$$v_1 - 1 \leq u_1 - 1 \leq v_1 + 1.$$

Análogamente podemos deducir que:

$$u_2 \leq v_2,$$

entonces:

$$v_2 - 1 \leq u_2 + 1 \leq v_2 + 1 \tag{2.8}$$

$$y$$

$$v_2 < u_2,$$

$$entonces:$$

$$v_2 - 1 \leq u_2 - 1 \leq v_2 + 1.$$

Por último usando la observación 2,3 descrita anteriormente y las desigualdades 2,6 y 2,8, obtenemos que si $u_1 \leq v_1$ y $u_2 \leq v_2$, entonces el vector $(u_1 + 1)\mathbf{e}_1 + (u_2 + 1)\mathbf{e}_2 \in B + \{\mathbf{v}\}$, pero:

$$(u_1 + 1)\mathbf{e}_1 + (u_2 + 1)\mathbf{e}_2 = \mathbf{e}_1 + \mathbf{e}_2 + u_1\mathbf{e}_1 + u_2\mathbf{e}_2 = \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{v},$$

que es un vértice del bloque $B + \{\mathbf{u}\}$, cuando $\mu_1 = \mu_2 = 1$, y por lo tanto:

$$(B + \{\mathbf{v}\}) \cap (ver(B + \{\mathbf{u}\}) \neq \emptyset.$$

Siguiendo el mismo procedimiento llegamos que:

*a)* $u_1 \leq v_1$ y $u_2 \leq v_2$, entonces $\mathbf{u} + \mathbf{e}_1 + \mathbf{e}_2 \in (B + \{\mathbf{v}\}) \cap (ver(B + \{\mathbf{u}\})$

*b)* $u_1 \leq v_1$ y $u_2 > v_2$, entonces $\mathbf{u} + \mathbf{e}_1 - \mathbf{e}_2 \in (B + \{\mathbf{v}\}) \cap (ver(B + \{\mathbf{u}\})$

*c)* $u_1 > v_1$ y $u_2 \leq v_2$, entonces $\mathbf{v} - \mathbf{e}_1 + \mathbf{e}_2 \in (B + \{\mathbf{v}\}) \cap (ver(B + \{\mathbf{u}\})$

*d)* $u_1 > v_1$ y $u_2 > v_2$, entonces $\mathbf{v} - \mathbf{e}_1 - \mathbf{e}_2 \in (B + \{\mathbf{v}\}) \cap (ver(B + \{\mathbf{u}\})$

□

Procederemos ahora a definir una operación en $\mathbb{R}^2$ que, al igual que todo lo definido en este capítulo, nos servirá para la demostración del *teorema* $2^n$ *de Freiman.*

**Definición 2.4.** *Sean* $\boldsymbol{f}$ *y* $\boldsymbol{a}$ *vectores en* $\mathbb{R}^2$*. La* reflexión de $\mathbf{a}$ con respecto a $\mathbf{f}$ *es el vector:*

$$2\boldsymbol{f} - \boldsymbol{a}.$$

En la figura 2,6 se muestra un ejemplo de reflección con $\mathbf{a} = (-3, 2)$ y $\mathbf{f} = (2, 5)$.

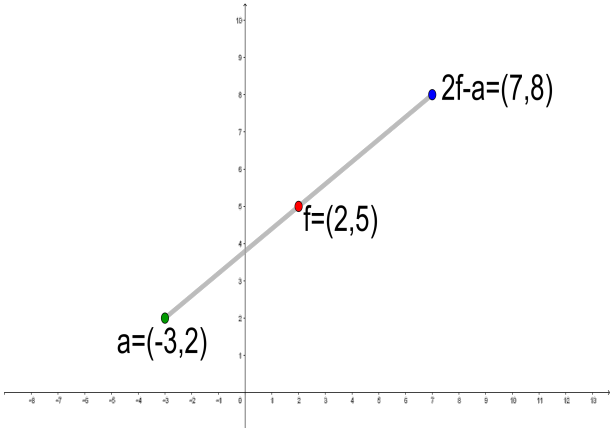



Figura 2.6: En esta figura podemos apreciar la operación de reflejar al vector $\mathbf{a} = (-3, 2)$, respecto al vector $\mathbf{f} = (2, 5)$; dando como resultado el vector $2\mathbf{f} - \mathbf{a} = (7, 8)$.

Podemos observar en la figura 2,6, que $\mathbf{f}$ es el punto medio entre $\mathbf{a}$ y su reflejado $2\mathbf{f} - \mathbf{a}$.
Así como reflejamos vectores, también podemos reflejar conjuntos.

**Definición 2.5.** *Sean* $S$ *un conjunto en* $\mathbb{R}^2$ *y* $\boldsymbol{f}$ *un vector en* $\mathbb{R}^2$*. La* reflexión de $S$ con respecto a $\mathbf{f}$ *es el conjunto:*

$$2\boldsymbol{f} - S := \{2\boldsymbol{f} - \boldsymbol{s} \,|\, \boldsymbol{s} \in S\}.$$

En la figura se muestra un ejemplo de reflexión con $S = \{(-6,3),(-4,4),(8,-3),(3,5)\}$ y $\mathbf{f} = (2,1)$.

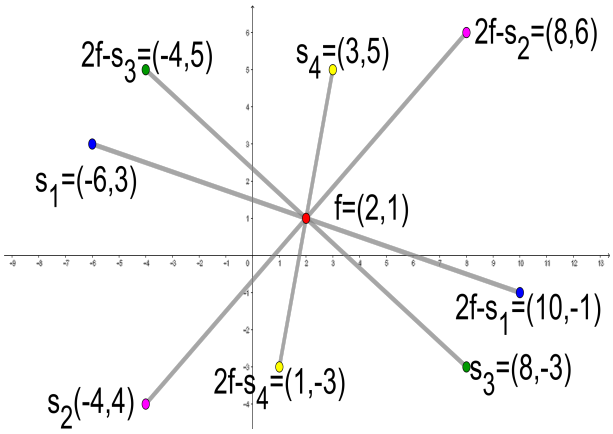



Figura 2.7: Podemos observar al conjunto $S = \{\mathbf{s}_1, \mathbf{s}_2, \mathbf{s}_3, \mathbf{s}_4\}$ y a su reflexión $2\mathbf{f} - S = \{2\mathbf{f} - \mathbf{s}_1, 2\mathbf{f} - \mathbf{s}_2, 2\mathbf{f} - \mathbf{s}_3, 2\mathbf{f} - \mathbf{s}_4\}$ respecto al vector $\mathbf{f} = (2,1)$.

Ya que aprendimos a reflejar conjuntos, podemos dar la siguiente definición.

**Definición 2.6.** *Sean $\boldsymbol{f}_0, \boldsymbol{f}_1$ y $\boldsymbol{f}_2$ vectores en $\mathbb{R}^2$. Definimos los conjuntos $S_0, S_1$ y $S_2$ de la siguiente manera:*

$$\begin{aligned} S_2 &:= \{\boldsymbol{f}_2\} \\ S_1 &:= \{\boldsymbol{f}_2, 2\boldsymbol{f}_1 - \boldsymbol{f}_2\} \\ S_0 &:= \{\boldsymbol{f}_2, 2\boldsymbol{f}_1 - \boldsymbol{f}_2, 2\boldsymbol{f}_0 - \boldsymbol{f}_2, 2\boldsymbol{f}_0 - 2\boldsymbol{f}_1 + \boldsymbol{f}_2\}. \end{aligned}$$

Notemos que $S_2 \subset S_1 \subset S_0$. Lo que estamos haciendo es reflejar $\mathbf{f}_2$ con respecto a $\mathbf{f}_1$, y después reflejar estos dos vectores ($\mathbf{f}_2$ y su reflejado) con respecto a $\mathbf{f}_0$. Para entender mejor estos conjuntos, consideremos el siguiente ejemplo.

**Ejemplo 2.5.** *Sea $\boldsymbol{f}_0 = (0,0)$, $\boldsymbol{f}_1 = (1,1)$ y $\boldsymbol{f}_2 = (5,1)$, entonces:*

$$\begin{gathered} S_2 = \{(5,1)\}, \\ S_1 = \{(5,1),(-3,1)\} \text{ y} \\ S_0 = \{(5,1),(-3,1),(-5,-1),(-3,-1)\}. \end{gathered}$$

*En la figura* 2,8 *podemos apreciar estos conjuntos; además de podemos observar que* $conv(S_0) = B((0,0);(1,1),(4,0))$

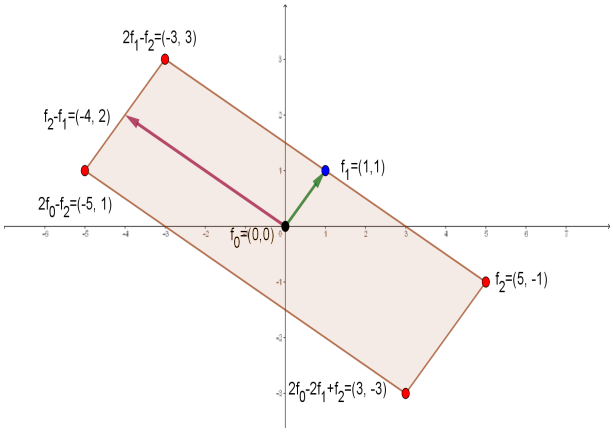



Figura 2.8: En esta figura podemos observar los conjuntos $S_2 = \{(-3,1)\}$, $S_1 = \{(-3,1),(5,1)\}$ y $S_0 = \{(-3,1),(5,1),(-5,1),(3,-1)\}$, construidos apartir de los vectores $\mathbf{f}_0 = \mathbf{0}$, $\mathbf{f}_1 = (1,1)$ y $\mathbf{f}_2 = (-3,1)$. Además de que $conv(S_0) = B(\mathbf{f}_0; \mathbf{f}_1, \mathbf{f}_2 - \mathbf{f}_1)$.

En general, dados $\mathbf{f}_0 = (0,0)$, $\mathbf{f}_1$ y $\mathbf{f}_2$ vectores en $\mathbb{R}^2$, el conjunto $conv(S_0)$ es un bloque cuyo centro y base determinaremos en el siguiente lema.

**Lema 2.2.** *Sean $\boldsymbol{f}_0 = (0,0)$, $\boldsymbol{f}_1$ y $\boldsymbol{f}_2$ vectores en $\mathbb{R}^2$, y sean $S_0$, $S_1$ y $S_2$ los conjuntos dados en la definición 2.6. Si $\boldsymbol{f}_1$ y $\boldsymbol{f}_2$ son linealmente independientes, entonces las siguientes afirmaciones se cumplen.*

1. *Los vectores $\boldsymbol{e}_1 := \boldsymbol{f}_1$ y $\boldsymbol{e}_2 := \boldsymbol{f}_2 - \boldsymbol{f}_1$ son linealmente independientes.*
2. *$S_0 = \{\mu_1 \boldsymbol{e}_1 + \mu_2 \boldsymbol{e}_2 \,|\, \mu_1, \mu_2 \in \{-1, 1\}\}$.*
3. *$B(\boldsymbol{f}_0; \boldsymbol{e}_1, \boldsymbol{e}_2) = conv(S_0)$.*

*Demostración.* 1. Sean $\alpha_1, \alpha_2 \in \mathbb{R}$ tales que:

$$\alpha_1 e_1 + \alpha_2 e_2 = (0,0). \tag{2.9}$$

Demostraremos que $\alpha_1 = \alpha_2 = 0$. Por definición, (2.9) implica:

$$\alpha_1 \mathbf{f}_1 + \alpha_2(\mathbf{f}_2 - \mathbf{f}_1) = (0,0);$$

equivalentemente:

$$(\alpha_1 - \alpha_2)\mathbf{f}_1 + \alpha_2 \mathbf{f}_2 = (0,0).$$

Como $\mathbf{f}_1$ y $\mathbf{f}_2$ son linealmente independientes, entonces $\alpha_1 - \alpha_2 = 0$ y $\alpha_2 = 0$, de donde obtenemos que $\alpha_1 = \alpha_2 = 0$ y por lo tanto $\mathbf{e}_1$ y $\mathbf{e}_2$ son linealmente independientes.

2. Recordemos que $S_0 := \{\mathbf{f}_2, 2\mathbf{f}_1 - \mathbf{f}_2, 2\mathbf{f}_0 - \mathbf{f}_2, 2\mathbf{f}_0 - 2\mathbf{f}_1 + \mathbf{f}_2\}$, y dado que $\mathbf{f}_0 = (0,0)$, entonces $S_0 = \{\mathbf{f}_2, 2\mathbf{f}_1 - \mathbf{f}_2, -\mathbf{f}_2, \mathbf{f}_2 - 2\mathbf{f}_1\}$. Para demostrar que dicho conjunto se puede expresar como $\{\mu_1 e_1 + \mu_2 e_2 \,|\, \mu_1, \mu_2 \in \{1, -1\}\}$ simplemente evaluamos $\mu_1$ y $\mu_2$ en todos sus valores posibles.

Si $\mu_1 = \mu_2 = 1$, entonces:

$$\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{f}_1 + (\mathbf{f}_2 - \mathbf{f}_1) = \mathbf{f}_2.$$

Si $\mu_1 = \mu_2 = -1$, entonces:

$$-\mathbf{e}_1 - \mathbf{e}_2 = -\mathbf{f}_1 + (\mathbf{f}_2 - \mathbf{f}_1) = -\mathbf{f}_2.$$

Si $\mu_1 = 1$ y $\mu_2 = -1$, entonces:

$$\mathbf{e}_1 - \mathbf{e}_2 = \mathbf{f}_1 - (\mathbf{f}_2 - \mathbf{f}_1) = 2\mathbf{f}_1 - \mathbf{f}_2.$$

Por último, si $\mu_1 = -1$ y $\mu_2 = 1$, entonces:

$$-\mathbf{e}_1 + \mathbf{f}_2 = -\mathbf{f}_1 + (\mathbf{f}_2 - \mathbf{f}_1) = \mathbf{f}_2 - 2\mathbf{f}_1,$$

con lo cual concluimos que $S_0 = \{\mu_1 e_1 + \mu_2 e_2 \,|\, \mu_1, \mu_2 \in \{-1, 1\}\}$.

3. Por definición, sabemos que $B = B(\mathbf{f}_0; \mathbf{e}_1, \mathbf{e}_2) := \{\mathbf{f}_0 + x_1\mathbf{e}_1 + x_2\mathbf{e}_2 \,|\, -1 \leq x_1, x_2 \leq 1\}$, y como $\mathbf{f}_0 = (0, 0)$ entonces $B = \{x_1\mathbf{e}_1 + x_2\mathbf{e}_2 \,|\, -1 \leq x_1, x_2 \leq 1\}$, de modo que $vert(B) = \{x_1\mathbf{e}_1 + x_2\mathbf{e}_2 \,|\, x_1, x_2 \in \{-1, 1\}\} = S_0$ (por el punto anterior). Finalmente, por la Observación 2.1 sabemos que $B = conv(vert(B)) = conv(S_0)$.

□

Observemos que el lema anterior nos dice que dado los vectores $\mathbf{f}_0 = (0, 0)$, $\mathbf{f}_1$ y $\mathbf{f}_2$, podemos construir el bloque $B((0, 0); \mathbf{f}_1, \mathbf{f}_2 - \mathbf{f}_1)$, que cumple que es la envolvente convexa de $S_0$. Además el regreso del lema es cierto, es decir, dado un bloque con centro en $f_0 = (0, 0)$ y base $\{\mathbf{e}_1, \mathbf{e}_2\}$ existen vectores $\mathbf{e}_1 = \mathbf{f}_1$ y $\mathbf{f}_2 = \mathbf{e}_2 + \mathbf{e}_1$ tales que $B((0, 0); \mathbf{e}_1, \mathbf{e}_2) = conv(S_0)$.

Procederemos ahora a relacionar los bloques con rectas linealmente independientes; y para esto usaremos fuertemente definiciones y resultados del apéndice, además de la relación, descrita en el lema 2,2, que hay entre los bloques y el conjunto $S_0$. Antes de empezar, recordemos que en $\mathbb{R}^2$ un hiperplano es una recta.

**Lema 2.3.** *Sean $L_1$ y $L_2$ rectas en $\mathbb{R}^2$, y sean $\boldsymbol{f}_0 = (0, 0)$, $\boldsymbol{f}_1$ y $\boldsymbol{f}_2$ vectores en $\mathbb{R}^2$ tales que:*

$$\begin{aligned} \boldsymbol{f}_0 &\in L_1 \cap L_2, \\ \boldsymbol{f}_1 &\in L_2 \cap L_1^{(+1)}, \\ \boldsymbol{f}_2 &\in L_1^{(+1)} \cap L_2^{(+1)}, \end{aligned}$$

*entonces los vectores $\boldsymbol{f}_1$ y $\boldsymbol{f}_2$ son linealmente independientes. Más aún, si $S_0$, $S_1$ y $S_2$ son los conjuntos dados en la definición 2.6, que cumple que:*

$$S_2 \subset L_2^{(+1)} \cap L_1^{(+1)} \text{ y } S_1 \subset L_1^{(+1)},$$

*entonces:*

$$S_0 \cap L(\mu_1, \mu_2) \neq \emptyset,$$

*para todo* $(\mu_1, \mu_2) \in \{-1, +1\}^2$ *y las rectas* $L_1$ *y* $L_2$ *son linealmente independientes.*

*Demostración.* Por contradicción supongamos que existe $\alpha \in \mathbb{R}$ tal que:

$$\mathbf{f}_2 = \alpha \mathbf{f}_1. \tag{2.10}$$

Como $\mathbf{f}_0 = (0,0) \in L_1 \cap L_2$, tenemos que las rectas $L_1$ y $L_2$ son subespacios vectoriales de $\mathbb{R}^2$. De lo anterior y por 2,10, $\mathbf{f}_2 \in L_2$, ya que por hipótesis $\mathbf{f}_1 \in L_2$; lo cual es una contradicción puesto que $\mathbf{f}_2 \in L_2^{+1}$ y $L_2^{+1} \cap L_2 = \emptyset$.

Ahora supongamos que:

$$S_2 \subset L_2^{+1} \cap L_1^{+1}$$

$$y$$

$$S_1 \subset L_1^{+1}.$$

Sea $\mathbf{l}_1$ vector normal a $L_1$ y $\mathbf{l}_2$ vector normal a $L_2$. Como $\mathbf{f}_0 = (0,0)$, entonces $S_0 = \{\mathbf{f}_0, 2\mathbf{f}_1 - \mathbf{f}_2, -\mathbf{f}_2, \mathbf{f}_2 - 2\mathbf{f}_1\}$. Para probar que $S_0 \cap L(\mu_1, \mu_2) \neq \emptyset$, para todo $(\mu_1, \mu_2) \in \{-1, +1\}^2$, probaremos que:

1. $\mathbf{f}_2 \in L(+1, +1)$,
2. $2\mathbf{f}_1 - \mathbf{f}_2 \in L(+1, -1)$,
3. $-\mathbf{f}_2 \in L(-1, -1)$ y
4. $\mathbf{f}_2 - 2\mathbf{f}_1 \in L(-1, +1)$.

1. $\mathbf{f}_2 \in L(+1, +1)$.

   Por hipótesis tenemos que $\mathbf{f}_2 \in L_1^{+1} \cap L_2^{+1}$, es decir, $\mathbf{f}_2 \in L(+1, +1)$.

2. $2\mathbf{f}_1 - \mathbf{f}_2 \in L(+1, -1)$.

   Por hipótesis tenemos que $S_1 \subset L_1^{+1}$ y por construcción de $S_1$ tenemos que $2\mathbf{f}_1 - \mathbf{f}_2 \in S_1$, luego:

   $$2\mathbf{f}_1 - \mathbf{f}_2 \in L_1^{+1}.$$

   Ahora sólo falta demostrar que $2\mathbf{f}_1 - \mathbf{f}_2 \in L_2^{-1}$.

   Observemos lo siguiente:

   $$(2\mathbf{f}_1 - \mathbf{f}_2, \mathbf{l}_2) = 2(\mathbf{f}_1, \mathbf{l}_2) - (\mathbf{f}_2, \mathbf{l}_2).$$

   Como $\mathbf{f}_1 \in L_2$ y $\mathbf{f}_2 \in L_2^{+1}$, entonces $(\mathbf{f}_1, \mathbf{l}_2) = 0$; y $(\mathbf{f}_2, \mathbf{l}_2) > 0$, luego $(\mathbf{l}_2, 2\mathbf{f}_1 - \mathbf{f}_2) < 0$, entonces $2\mathbf{f}_1 - \mathbf{f}_2 \in L_2^{-1}$ y por lo tanto $2\mathbf{f}_1 - \mathbf{f}_2 \in L(+1, -1)$.

3. $-\mathbf{f}_2 \in L(-1,-1)$.

   Como $\mathbf{f}_2 \in L(+1,+1)$, entonces $(\mathbf{f}_2, \mathbf{l}_1) > 0$ y $(\mathbf{f}_2, \mathbf{l}_2) > 0$, luego $(-\mathbf{f}_2, \mathbf{l}_1) < 0$ y $(\mathbf{f}_2, \mathbf{l}_2) < 0$ y por lo tanto $-\mathbf{f}_2 \in L(-1,-1)$.

4. $\mathbf{f}_2 - 2\mathbf{f}_1 \in L(-1,+1)$.

   Como $2\mathbf{f}_1 - \mathbf{f}_2 \in L(+1,-1)$, entonces $(2\mathbf{f}_1 - \mathbf{f}_2, \mathbf{l}_1) > 0$ y $(2\mathbf{f}_1 - \mathbf{f}_2, \mathbf{l}_2) < 0$, luego $(\mathbf{f}_2 - 2\mathbf{f}_1, \mathbf{l}_1) < 0$ y $(\mathbf{f}_2 - 2\mathbf{f}_1, \mathbf{l}_2) > 0$ y por lo tanto $\mathbf{f}_2 - 2\mathbf{f}_1 \in L(-1,+1)$.

Para finalizar la prueba notemos que como $S_0 \cap L(\mu_1,\mu_2) \neq \emptyset, (\mu_1,\mu_2) \in \{-1,+1\}^2$, entonces $L(\mu_1,\mu_2) \neq \emptyset$ para todo $(\mu_1,\mu_2) \in \{-1,+1\}^2$, y por el lema 6,1 tenemos que las rectas $L_1$ y $L_2$ son linealmente independientes. □

En la figura 2,9 podemos observar que las rectas linealmente independientes descritas en el lema 2,3, son las rectas que unen los puntos medios de los lados paralelos del bloque.

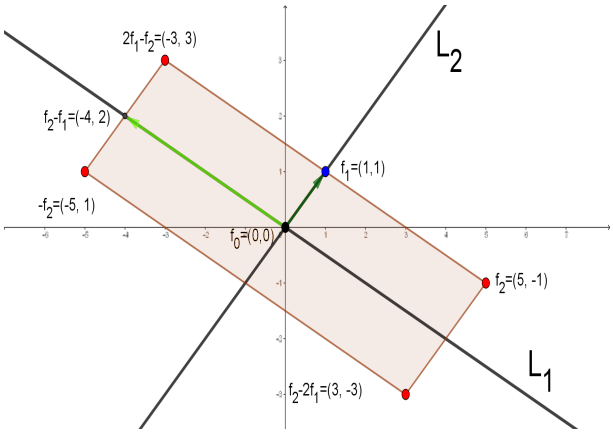



Figura 2.9: En esta figura podemos observar la relación que hay entre bloques, rectas linealmente independientes y el conjunto $S_0$.

De los lemas 2,2 y 2,3 se puede deducir la siguiente observación.

**Observación 2.3.** *Sean $\boldsymbol{f}_0 = (0,0)$, $\boldsymbol{f}_1$ y $\boldsymbol{f}_2$ vectores en $\mathbb{R}^2$; y $L_1$ y $L_2$ rectas que satisfacen las condiciones del lema 2,3. Entonces:*

$$ver(B((0,0); \boldsymbol{f}_1, \boldsymbol{f}_2 - \boldsymbol{f}_1)) = \{\boldsymbol{f}_2, 2\boldsymbol{f}_1 - \boldsymbol{f}_2, -\boldsymbol{f}_2, 2\boldsymbol{f}_2 - \boldsymbol{f}_1\},$$

*además:*

$$\boldsymbol{f}_2 \in L(+1,+1),$$
$$2\boldsymbol{f}_1 - \boldsymbol{f}_2 \in L(+1,-1),$$
$$-\boldsymbol{f}_2 \in L(-1,-1)$$
$$y$$
$$\boldsymbol{f}_2 - 2\boldsymbol{f}_1 \in L(-1,+1).$$

Ahora observemos que dadas dos rectas linealmente independientes $L_1$ y $L_2$ y un vector fijo $\mathbf{f}_1$, no existe un único bloque que satisface la observación 2,3; de hecho depende de la ubicación del vector $\mathbf{f}_2$. Nuestra siguiente definición es la construcción de los bloques que satisfacen la observación 2,3 para rectas linealmente independientes $L_1$ y $L_2$ y vectores fijos $\mathbf{f}_0 = (0,0)$ y $\mathbf{f}_1$. Dichos bloques los definiremos en términos del vector $\mathbf{f}_2$.

**Definición 2.7.** *Sean $L_1$ y $L_2$ rectas en $\mathbb{R}^2$ y $\boldsymbol{f}_0 = (0,0)$ y $\boldsymbol{f}_1$ vectores en $\mathbb{R}^2$ tales que:*

$$\boldsymbol{f}_0 \in L_1 \cap L_2$$

$$y$$

$$\boldsymbol{f}_1 \in L_1^{+1} \cap L_2.$$

*Sea $\boldsymbol{a}$ un vector en $\mathbb{R}^2$ tal que $\boldsymbol{a} \in L(+1,+1)$. Se definen los siguientes conjuntos a partir del vector $\boldsymbol{a}$ :*

$$S_2(\boldsymbol{a}) = \{\boldsymbol{a}\},$$

$$S_1(\boldsymbol{a}) = \{\boldsymbol{a}, 2\boldsymbol{f}_1 - \boldsymbol{a}\}$$

$$y$$

$$S_0(\boldsymbol{a}) = \{\boldsymbol{a}, 2\boldsymbol{f}_1 - \boldsymbol{a}, -\boldsymbol{a}, \boldsymbol{a} - 2\boldsymbol{f}_1\}.$$

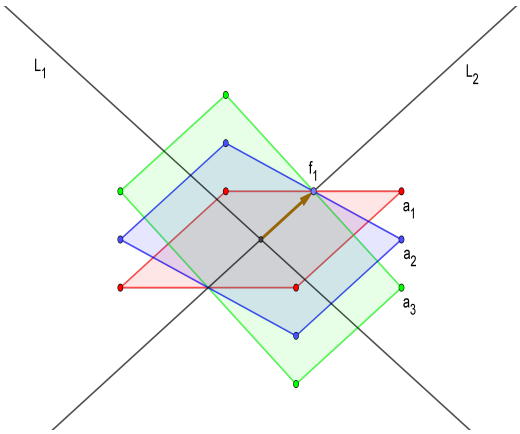



Figura 2.10: En esta figura podemos observar a $S_0(\mathbf{a}_1)$, los vértices del bloque rojo; $S_0(\mathbf{a}_2)$, los vértices del bloque azul; y a $S_0(\mathbf{a}_3)$, los vértices del bloque verde.

En la figura 2,10 podemos observar que para vectores distintos $\mathbf{a}$ y $\mathbf{a}'$ se producen conjuntos $S_0(\mathbf{a})$ y $S_0(\mathbf{a}')$ ajenos.

**Lema 2.4.** *Sean $L_1$ y $L_2$ rectas, y $\boldsymbol{f}_0 = (0,0)$, $\boldsymbol{f}_1$, $\boldsymbol{a}$ y $\boldsymbol{a}'$ vectores como en la definición 2,7. Supongamos que $\boldsymbol{a} \neq \boldsymbol{a}'$, entonces:*

$$S_0(\boldsymbol{a}) \cap S_0(\boldsymbol{a}') = \emptyset.$$

*Demostración.* La observación 2,3, con $\mathbf{a} = \mathbf{f}_2$, nos dice que cada $L(\mu_1, \mu_2)$ contiene un único punto de $S_0(\mathbf{a})$ y además nos dice qué punto es. Por otro lado observemos que cada punto de $S_0(\mathbf{a})$ queda únicamente definido por $a$. Por estas dos observaciones tenemos que $S_0(\mathbf{a}) \neq S_0(\mathbf{a}')$. □

Ya que estudiamos las propiedades de los hiperplanos, de los bloques, de la operación de reflejar un conjunto respecto a un vector y la relación que existe entre estos tres; daremos ahora sí la propiedad que se usará en la prueba del teorema $2^n$ *de Freiman.*

**Teorema 2.3.** *Sean $L_1$ y $L_2$ rectas en $\mathbb{R}^2$ y sean $\boldsymbol{f}_0$, $\boldsymbol{f}_1$ vectores en $\mathbb{R}^2$, tales que:*

$$\boldsymbol{f}_0 = (0,0) \in L_1 \cap L_2,$$

$$\boldsymbol{f}_1 \in L_2 \ y \ \boldsymbol{f}_1 \in L_1^{+1}.$$

*Sea $A_2$ subconjunto finito de $\mathbb{R}^2$ contenido en $L(+1,+1)$. Para cada $\boldsymbol{a} \in A_2$ se construyen los conjuntos $S_2(\boldsymbol{a})$, $S_1(\boldsymbol{a})$, $S_0(\boldsymbol{a})$ y $B(\boldsymbol{a})$ de la siguiente manera:*

$$S_2(\boldsymbol{a}) = \{\boldsymbol{a}\},$$

$$S_1(\boldsymbol{a}) = \{\boldsymbol{a}, 2\boldsymbol{f}_1 - \boldsymbol{a}\},$$

$$S_0(\boldsymbol{a}) = \{\boldsymbol{a}, 2\boldsymbol{f}_1 - \boldsymbol{a}, -\boldsymbol{a}, \boldsymbol{a} - 2\boldsymbol{f}_1\}$$

$$y$$

$$B(\boldsymbol{a}) = conv(S_0(\boldsymbol{a})).$$

*Supongamos que para todo $\boldsymbol{a} \in A_2$, se cumple que:*

$$S_1(\boldsymbol{a}) \subset L^{+1} \ y \ S_2(\boldsymbol{a}) \subset L_1^{+1} \cap L_2^{+1},$$

*entonces existe vector $\boldsymbol{a}^* \in A_2$ tal que:*

$$S_0(\boldsymbol{a}) \cap B(\boldsymbol{a}^*) \neq \emptyset,$$

*para todo $\boldsymbol{a} \in A_2$, y además se cumple que:*

$$\left| \left( \bigcup_{\boldsymbol{a} \in A_2} S_0(\boldsymbol{a}) \right) \bigcap B(\boldsymbol{a}^*) \right| \geq |A_2|.$$

*Demostración.* Sea $\mathbf{a} \in A_2$, empezaremos por analizar las propiedes de $B(\mathbf{a})$. Se definen los siguientes vectores:

$$\mathbf{e}_1 = \mathbf{f}_1$$

$$y$$

$$\mathbf{e}_2(\mathbf{a}) = \mathbf{a} - \mathbf{f}_1.$$

Por el lema 2,3 tenemos que los vectores $\mathbf{f}_1$ y $\mathbf{a}$ son linealmente independientes, además por el lema 2,2 tenemos que los vectores $\mathbf{e}_1$ y $\mathbf{e}_2(\mathbf{a})$ son linealmente independientes. Como $\mathbf{e}_1 \in L_2$, y $\dim(L_2) = 1$, entonces tenemos que $\{\mathbf{e}_1\}$ es una base de $L_2$. Análogamente tenemos que $\{\mathbf{e}_1, \mathbf{e}_2(\mathbf{a})\}$ es una base de $\mathbb{R}^2$, para todo $\mathbf{a} \in A$. A partir de la observación anterior los siguientes conjuntos son bloques en $L_2$ y $\mathbb{R}^2$ respectivamente:

$$B := B((0,0); \mathbf{e}_1)$$

$$y$$

$$B(\mathbf{a}) := B((0,0); \mathbf{e}_1, \mathbf{e}_2(\mathbf{a})).$$

Por el lema 2,2 tenemos que:

$$vert(B(\mathbf{a})) = S_0(\mathbf{a})$$

$$y$$

$$B(\mathbf{a}) = conv(S_0(\mathbf{a})).$$

Ahora definimos los siguientes conjuntos:

$$S_0^{+1}(\mathbf{a}) = \{\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a}), -\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a})\}$$

$$y$$

$$S_0^{-1}(\mathbf{a}) = \{\mathbf{e}_1 - \mathbf{e}_2(\mathbf{a}), -\mathbf{e}_1 - \mathbf{e}_2(\mathbf{a})\}.$$

Veamos lo siguiente:

$$\begin{aligned} vert(B) + \{\mathbf{e}_2(\mathbf{a})\} &= \{\mathbf{e}_1, -\mathbf{e}_1\} + \{\mathbf{e}_2(\mathbf{a})\} \\ &= \{\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a}), -\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a})\} \\ &= S_0^{+1}(\mathbf{a}), \end{aligned}$$

luego

$$\begin{aligned} conv(S_0^{+1}(\mathbf{a})) &= conv(vert(B) + \{\mathbf{e}_2(a)\}) \\ &= conv(vert(B)) + conv(\{\mathbf{e}_2(a)\}), \end{aligned}$$

y por lo tanto

$$conv(S_0^{+1}(\mathbf{a})) = B + \{\mathbf{e}_2(\mathbf{a})\} \subseteq B(\mathbf{a}). \tag{2.11}$$

Análogamente tenemos que:

$$conv(S_0^{-1}(\mathbf{a})) = B - \{\mathbf{e}_2(\mathbf{a})\} \subseteq B(\mathbf{a}). \tag{2.12}$$

Sean $\mathbf{l}_1$ y $\mathbf{l}_2$ vectores normales a $L_1$ y $L_2$ respectivamente. Podemos observar que como $L_1$ y $L_2$ son linealmente independientes y como $\dim(L_1) + \dim(L_2) = 2$, entonces tenemos que:

$$\mathbb{R}^2 = L_1 \oplus L_2.$$

Por teorema de álgebra lineal podemos construir vector $\mathbf{l}_2^*$, tal que $\{\mathbf{l}_2^*\}$ es base de $L_2$ y que satisfaga que:

$$(\mathbf{l}_1, \mathbf{l}_1^*) = 0$$

$$y$$

$$(\mathbf{l}_2, \mathbf{l}_2^*) = 1.$$

Sea:

$$\pi : \mathbb{R}^2 \to L_2$$

la proyección correspondiente a la descomposición de la suma direta de:

$$\mathbb{R}^2 = L_1 \oplus L_2.$$

De lo anterior tenemos que $\mathbf{e}_2(\mathbf{a})$ se puede escribir de manera única con la siguiente forma:

$$\mathbf{e}_2(\mathbf{a}) = \pi(\mathbf{e}_2(\mathbf{a})) + \alpha \mathbf{l}_2^*. \tag{2.13}$$

Por otra parte tenemos que:

$$\mathbf{e}_2(\mathbf{a}) = \mathbf{a} - \mathbf{f}_1. \tag{2.14}$$

Juntando 2,13 y 2,14, y calculando el producto punto de $\mathbf{e}_2(\mathbf{a})$ con $\mathbf{l}_2$, tenemos que:

$$\begin{gathered}\pi(\mathbf{e}_2(\mathbf{a})) + \alpha \mathbf{l}_2^* = \mathbf{a} - \mathbf{f}_1 \\ entonces, \\ (\mathbf{l}_2, \pi(\mathbf{e}_2(\mathbf{a})) + \alpha \mathbf{l}_2^*) = (\mathbf{l}_2, \mathbf{a} - \mathbf{f}_1) \\ luego, \\ (\mathbf{l}_2, \pi(\mathbf{e}_2(\mathbf{a}))) + \alpha(\mathbf{l}_2, \mathbf{l}_2^*) = (\mathbf{l}_2, \mathbf{a}) - (\mathbf{l}_2, \mathbf{f}_1).\end{gathered}$$

Como $\pi(\mathbf{e}_2(\mathbf{a}))$ y $\mathbf{f}_1$ están en $L_2$, $\mathbf{a} \in L_2^{+1}$ y por construcción de $\mathbf{l}_2^*$, lo anterior se reduce a:

$$\alpha = (\mathbf{l}_2, \mathbf{a}) > 0.$$

De lo anterior observamos que $\alpha$ depende del vector $\mathbf{a}$, entonces denotaremos a $\alpha$ como:

$$\alpha = \alpha(\mathbf{a}) > 0.$$

Ahora observemos por construcción de $S_0^{+1}(\mathbf{a})$, por el lema 2,3 y la observación 2,3 tenemos que:

$$\{\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a})\} = S_0(\mathbf{a}) \cap L(+1, +1) = S_0^{+1}(\mathbf{a}) \cap L_1^{+1}$$

$$y$$

$$\{-\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a})\} = S_0(\mathbf{a}) \cap L(-1, +1) = S_0^{+1}(\mathbf{a}) \cap L_1^{-1},$$

implican que:

$$S_0^{+1}(\mathbf{a}) \cap L_1^{\mu_1} \neq \emptyset,$$

para todo $\mu_1 \in \{-1, +1\}$. Por el lema 6,6 y por la ecuación 2,11, tenemos que:

$$(0,0) \in \pi(conv(S_0^{+1}(\mathbf{a}))) = \pi(B + \mathbf{e}_2(\mathbf{a})).$$

Como $\pi$ es una función lineal, llegamos a que:

$$(0,0) \in \pi(B) + \pi(\mathbf{e}_2(\mathbf{a})).$$

Como $B$ es subconjunto de $L_1$, tenemos que:

$$(0,0) \in B + \pi(\mathbf{e}_2(\mathbf{a})), \tag{2.15}$$

para todo $\mathbf{a} \in A_2$.

Ahora procederemos a construir el vector $\mathbf{a}^*$, que satisface el teorema. Como $A_2$ es un conjunto finito podemos escoger $\mathbf{a}^*$ en $A_2$, tal que:

$$\alpha(\mathbf{a}^*) = \text{máx}\{\alpha(\mathbf{a}) \,|\, \mathbf{a} \in A_2\}.$$

Sea $\mathbf{a} \in A_2$ distinto de $\mathbf{a}^*$ y definimos a $t(\mathbf{a})$ como:

$$t(\mathbf{a}) = \frac{\alpha(\mathbf{a})}{\alpha(\mathbf{a}^*)}.$$

Como $\alpha(\mathbf{a}) > 0$ para todo $\mathbf{a} \in A_2$, tenemos que $t(\mathbf{a}) > 0$ y además por elección de $\mathbf{a}^*$ tenemos que $t(\mathbf{a}) \leq 1$. Por la ecuación 2,15 y por el lema 2,1, obtenemos lo siguiente:

1. $(0,0) \in B + \pi(\mathbf{e}_2(\mathbf{a}))$.
2. $(0,0) \in B + \pi(\mathbf{e}_2(\mathbf{a}^*))$.
3. $(0,0) \in B + t(\mathbf{a})\pi(\mathbf{e}_2(\mathbf{a}))$
4. $(vert(B) + \pi(\mathbf{e}_2(\mathbf{a}))) \bigcap (B + t(\mathbf{a})\pi(\mathbf{e}_2(\mathbf{a}^*))) \neq \emptyset$.

De lo anterior tenemos que existen $\mu_1 \in \{-1, 1\}$ y $-1 \leq x_1 \leq 1$ tales que:

$$\begin{aligned}
\mu_1\mathbf{e}_1 + \pi(\mathbf{e}_2(\mathbf{a})) &= x_1\mathbf{e}_1 + t(\mathbf{a})\pi(\mathbf{e}_2(\mathbf{a}^*)) \\
&= x_1\mathbf{e}_1 + t(\mathbf{a})(\mathbf{e}_2(\mathbf{a}^*) - \alpha(\mathbf{a}^*)\mathbf{l}_2^*) \\
&\textit{entonces}, \\
\mu_1\mathbf{e}_1 + \pi(\mathbf{e}_2(\mathbf{a})) &= x_1\mathbf{e}_1 + t(\mathbf{a})\mathbf{e}_2(\mathbf{a}^*)) - t(\mathbf{a})\alpha(\mathbf{a}^*)\mathbf{l}_2^* \\
&\textit{luego}, \\
\mu_1\mathbf{e}_1 + \pi(\mathbf{e}_2(\mathbf{a})) + t(\mathbf{a})\alpha(\mathbf{a}^*)\mathbf{l}_2^* &= x_1\mathbf{e}_1 + t(\mathbf{a})\mathbf{e}_2(\mathbf{a}^*) \\
&\textit{obteniendo}, \\
\mu_1\mathbf{e}_1 + \pi(\mathbf{e}_2(\mathbf{a})) + \frac{\alpha(\mathbf{a})}{\alpha(\mathbf{a}^*)}\alpha(\mathbf{a}^*)\mathbf{l}_2^* &= x_1\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a}^*) \\
&\text{se sigue que}, \\
\mu_1\mathbf{e}_1 + \pi(\mathbf{e}_2(\mathbf{a})) + \alpha(\mathbf{a})\mathbf{l}_2^* &= x_1\mathbf{e}_1 + t(\mathbf{a})\mathbf{e}_2(\mathbf{a}^*) \\
&\textit{entonces}, \\
\mu_1\mathbf{e}_1 + \mathbf{e}_2(\mathbf{a}) &= x_1\mathbf{e}_1 + t(\mathbf{a}) + \mathbf{e}_2(\mathbf{a}^*).
\end{aligned}$$

Pero $\mu_1\mathbf{e}_2 + \mathbf{e}_2(\mathbf{a})$ está en $S_0^{+1}(\mathbf{a}) \subset S_0(\mathbf{a})$ y $x_1\mathbf{e}_1 + t(\mathbf{a})\mathbf{e}_2(\mathbf{a}^*)$ está en $B(\mathbf{a}^*)$, entonces:

$$S_0(\mathbf{a}) \cap B(\mathbf{a}^*) \neq \emptyset,$$

pero esto se cumple para toda $\mathbf{a}$ en $A_2$. Para finalizar la prueba observemos que por el lema 2,4, tenemos que si $\mathbf{a}, \mathbf{a}' \in A_2$, con $\mathbf{a} \neq \mathbf{a}'$, entonces $S_0(\mathbf{a}) \cap S_0(\mathbf{a}') = \emptyset$. Lo anterior nos dice que:

$$(S_0(\mathbf{a}) \cap B(\mathbf{a}^*)) \bigcap (S_0(\mathbf{a}') \cap B(\mathbf{a}^*)) = \emptyset,$$

para $\mathbf{a}$ distinto de $\mathbf{a}'$, y por lo tanto:

$$\left| \left( \bigcup_{\mathbf{a} \in A_2} S_0(\mathbf{a}) \right) \bigcap B(\mathbf{a}^*) \right| \geq |A_2|.$$

□

En la demostración del teorema 2,3, tenemos que el vector $\mathbf{a}^*$, que satisface la conclusión, es el vector cuyo producto punto con el vector normal a la recta $L_2$ es mayor, pero sabemos que el producto punto entre dos vectores nos describe el ángulo que hay entre ellos, por lo tanto el vector $\mathbf{a}^*$ es aquel que tiene un ángulo con la recta $L_2$ mayor; y esto se puede apreciar en la figura 2,11.

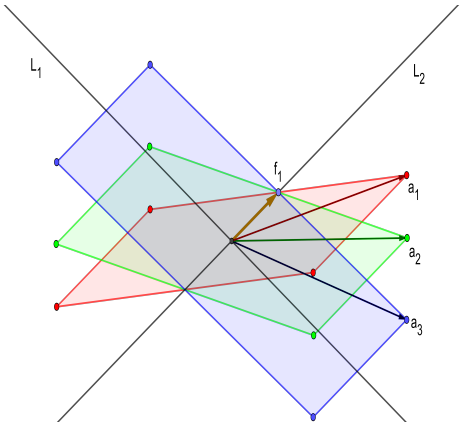



Figura 2.11: En esta figura podemos observa que $\mathbf{a}_3$ es el elemento de $A_2 = \{\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3\}$ que satisface la conclusión del teorema 2,3, además de ser $\mathbf{a}_3$ el vector de $A_2$ cuyo ángulo con la recta $L_2$ es mayor.

Ahora definiremos un conjunto que nos servirá de herramienta.

**Definición 2.8.** *Sea $A_1$ y $A_2$ subconjuntos de $\mathbb{R}^2$, se define el* conjunto de puntos medios *de $A_1$ y $A_2$ como:*

$$mid(A_1, A_2) = \left\{ \frac{\boldsymbol{a}_1 + \boldsymbol{a}_2}{2} \mid \boldsymbol{a}_1 \in A_1, \boldsymbol{a}_2 \in A_2 \right\}$$

*Si $A = A_1 = A_2$, entonces el conjunto de puntos medios de $A_1$ y $A_2$ se denotará como:*

$$mid(A_1, A_2) = mid(A).$$

Las siguientes propiedades se deducen de la definición 2,8.

**Observación 2.4.** *Sean $A_1$, $A_2$ y $A$ subconjuntos de $\mathbb{R}^2$.Las siguientes afirmaciones se cumplen:*

1. $A \subset mid(A)$.
2. $|mid(A)| = |2A|$.
3. *Si* $A \subset A_1 \cap A_2$, *entonces* $mid(A) \subset (mid(A_1) \cap mid(A_2))$.
4. *Si* $A_1$ *y* $A_2$ *son subconjuntos de* $K$ *y* $K$ *es convexo, entonces:*

$$mid(A_1, A_2) \subset K.$$

5. *Sea* $\boldsymbol{v} \in mid(A)$, *y* $\boldsymbol{v}_1$ *y* $\boldsymbol{v}_2$ *en* $A$ *tales que*

$$\frac{\boldsymbol{v}_1 + \boldsymbol{v}_2}{2} = \boldsymbol{v},$$

*entonces* $\boldsymbol{v}_2$ *es el reflejado de* $\boldsymbol{v}_1$ *respecto a* $\boldsymbol{v}$.

Como casi todos las proposiciones expuestas en este capítulo, el siguiente lema es una relación que existe entre el conjunto $mid(A)$ con los bloques.

**Lema 2.5.** *Sea* $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ *una base de* $\mathbb{R}^2$, $B = B((0,0); \boldsymbol{e}_1, \boldsymbol{e}_2)$ *un bloque en* $\mathbb{R}^2$ *y* $W$ *subconjunto de* $int(B)$. *Entonces:*

1. $|mid(W, vert(B))| = 4|W|$.
2. $mid(W, vert(B)) \subset int(B)$.

*Demostración.*

1. Si $\mathbf{x} \in mid(W, vert(B))$, entonces existen $\mathbf{w} \in W$ y $\mathbf{b} \in vert(B)$, tales que:

$$\mathbf{x} = \frac{\mathbf{w} + \mathbf{b}}{2}.$$

De lo anterior y por el principio del producto, tenemos que:

$$|mid(W, vert(B)| \leq |W||vert(B)|,$$

pero como $B$ es un bloque de $\mathbb{R}^2$, tenemos que $|vert(B)| = 4$ y por lo tanto:

$$|mid(W, vert(B))| \leq 4|W|. \tag{2.16}$$

Ahora demostraremos que la igualdad en la ecuación 2,16 siempre se satisface y para esto basta demostrar que cada elemento $\mathbf{x} \in mid(W, vert(B))$ se escribe de manera

única. Supongamos por contradicción que existen $\mathbf{w}_1, \mathbf{w}_2 \in W$ distintos y $\mathbf{b}_1, \mathbf{b}_2 \in vert(B)$ distintos, tales que:

$$\frac{\mathbf{w}_1 + \mathbf{b}_1}{2} = \frac{\mathbf{w}_2 + \mathbf{b}_2}{2},$$

y por lo tanto:

$$\mathbf{w}_1 + \mathbf{b}_1 = \mathbf{w}_2 + \mathbf{b}_2. \tag{2.17}$$

Como $\mathbf{w}_1, \mathbf{w}_2$ están en $W$ y $W$ es subconjunto de $int(B)$, entonces existen $-1 < \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} < 1$ tales que:

$$\mathbf{w}_1 = \alpha_{11}\mathbf{e}_1 + \alpha_{12}\mathbf{e}_2$$

$$y$$

$$\mathbf{w}_2 = \alpha_{21}\mathbf{e}_1 + \alpha_{22}\mathbf{e}_2.$$

Análogamente existen $\mu_{11}, \mu_{12}, \mu_{21}\mu_{22} \in \{-1, 1\}$, tales que:

$$\mathbf{b}_1 = \mu_{11}\mathbf{e}_1 + \mu_{12}\mathbf{e}_2$$

$$y$$

$$\mathbf{b}_2 = \mu_{21}\mathbf{e}_1 + \mu_{22}\mathbf{e}_2.$$

Sustituyendo lo anterior en la ecuación 2,17, obtenemos:

$$\alpha_{11}\mathbf{e}_1 + \alpha_{12}\mathbf{e}_2 + \mu_{11}\mathbf{e}_1 + \mu_{12}\mathbf{e}_2 = \alpha_{21}\mathbf{e}_1 + \alpha_{22}\mathbf{e}_2 + \mu_{21}\mathbf{e}_1 + \mu_{22}\mathbf{e}_2,$$

luego,

$$(\alpha_{11} + \mu_{11})\mathbf{e}_1 + (\alpha_{12} + \mu_{12})\mathbf{e}_2 = (\alpha_{21} + \mu_{21})\mathbf{e}_1 + (\alpha_{22} + \mu_{22})\mathbf{e}_2,$$

entonces,

$$\alpha_{11} + \mu_{11} = \alpha_{21} + \mu_{21}$$

$$y$$

$$\alpha_{12} + \mu_{12} = \alpha_{22} + \mu_{22},$$

obteniendo,

$$\alpha_{11} - \alpha_{21} = \mu_{21} - \mu_{11}$$

$$y$$

$$\alpha_{12} - \alpha_{22} = \mu_{22} - \mu_{12}.$$

Observemos que como $-1 < \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22} < 1$, entonces $-2 < \alpha_{11} - \alpha_{21} < 2$ y $-2 < \alpha_{12} - \alpha_{22} < 2$; además de que como $\mu_{11}, \mu_{12}, \mu_{21}, \mu_{22} \in \{-1, 1\}$, entonces obtenemos que $\mu_{21} - \mu_{11} \in \{-2, 0, 2\}$ y $\mu_{22} - \mu_{12} \in \{-2, 0, 2\}$. Notemos que $\{-2, 0, 2\}$ sólo intersecta al intervalo $(-2, 2)$ de números reales en el 0, entonces no queda más que:

$$\alpha_{11} - \alpha_{21} = \mu_{21} - \mu_{11} = 0$$

$$y$$

$$\alpha_{12} - \alpha_{22} = \mu_{22} - \mu_{12} = 0.$$

Luego $\alpha_{11} = \alpha_{21}$, $\mu_{21} = \mu_{11}$, $\alpha_{12} = \alpha_{22}$ y $\mu_{22} = \mu_{12}$, luego $\mathbf{w}_1 = \mathbf{w}_2$ y $\mathbf{b}_1 = \mathbf{b}_2$, lo cual nos indica que todo elemento de $mid(W, vert(B))$ se escribe de manera única y por lo tanto $|mid(W, vert(B)| = 4|W|$.

2. Sea $\mathbf{x} \in mid(W, vert(B))$, entonces existen $\mathbf{w}$ en $W$ y $\mathbf{b}$ en $B$, tales que:

$$\mathbf{x} = \frac{\mathbf{w} + \mathbf{b}}{2}$$

Como $\mathbf{w} \in W \subset int(B)$ y $\mathbf{b} \in vert(B)$, entonces existen $-1 < \alpha_1, \alpha_2 < 1$ y $\mu_1$ y $\mu_2$ en $\{-1, 1\}$, tales que:

$$\mathbf{w} = \alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2$$

$$y$$

$$\mathbf{b} = \mu_1\mathbf{e}_1 + \mu_2\mathbf{e}_2.$$

De lo anterior tenemos que:

$$\begin{aligned}\frac{\mathbf{w} + \mathbf{b}}{2} &= \frac{\alpha_1\mathbf{e}_1 + \alpha_2\mathbf{e}_2 + \mu_1\mathbf{e}_1 + \mu_2\mathbf{e}_2}{2} \\ &= \frac{(\alpha_1 + \mu_1)\mathbf{e}_1 + (\alpha_2 + \mu_2)\mathbf{e}_2}{2} \\ &= \frac{\alpha_1 + \mu_1}{2}\mathbf{e}_1 + \frac{\alpha_2 + \mu_2}{2}\mathbf{e}_2\end{aligned}$$

Como $-1 < \alpha_1 < 1$ y $\mu_1 \in \{-1, 1\}$, tenemos que: $-2 < \alpha_1 + \mu_1 < 2$, luego $-1 < \frac{\alpha_1+\mu_1}{2} < 1$; análogamente tenemos que $-1 < \frac{\alpha_2+\mu_2}{2} < 1$, lo cual nos implica que $\mathbf{x} \in int(B)$ y por lo tanto $mid(W, vert(B)) \subset int(B)$.

□

**Definición 2.9.** *Sea $A$ subconjunto finito de $\mathbb{R}^2$ con $|A| = n$ y sea $\boldsymbol{v}$ en $mid(A)$. Se define $r_A(\boldsymbol{v})$ como el número de parejas $(\boldsymbol{v}_1, \boldsymbol{v}_2) \subset A^2$ tales que:*

$$\frac{\boldsymbol{v}_1 + \boldsymbol{v}_2}{2} = \boldsymbol{v}.$$

**Lema 2.6.** *Sea $A$ un conjunto finito, entonces las siguientes afirmaciones se cumplen:*

1. $\frac{|A||(|A|+1)}{2} = \sum_{\boldsymbol{v} \in mid(A)} r_A(\boldsymbol{v})$

2. *Si $\boldsymbol{v}$ es un vector en $mid(A)$ tal que $r_A(\boldsymbol{v}) = max\{r_A(\boldsymbol{u}) \mid \boldsymbol{u} \in mid(A)\}$, entonces $r_{A-\boldsymbol{v}}((0,0)) = max\{r_{A-\boldsymbol{v}}(\boldsymbol{u}) \mid \boldsymbol{u} \in mid(A - \boldsymbol{v})\}$.*

*Demostración.* 1. Observemos que si $\mathbf{v}_1, \mathbf{v}_2 \in A$, entonces $\frac{\mathbf{v}_1+\mathbf{v}_2}{2}$ pertenece a $mid(A)$, entonces existe $\mathbf{v} \in mid(A)$, tal que $r_A(\mathbf{v})$ está contando a la pareja $(\mathbf{v}_1, \mathbf{v}_2)$ y a su vez esta pareja sólo está siendo contada en este $r_A(\mathbf{v})$. Entonces toda pareja de elementos de $A$, es contado en algún $r_A(\mathbf{v})$, por consiguiente $\sum_{\mathbf{v}\in mid(A)} r_A(\mathbf{v})$ equivale a calcular el número de parejas distintas con elementos de $A$.

Como $A$ es finito, entonces $A = \{\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_n\}$. Observemos que el elemento $\mathbf{a}_1$ está en $n$ parejas, ya que hay $n-1$ elementos restantes en $A$ y además $\mathbf{a}_1$ puede formar pareja consigo mismo. Como la pareja $(\mathbf{a}_i, \mathbf{a}_j)$ la estamos considerando como igual a la pareja $(\mathbf{a}_j, \mathbf{a}_i)$, entonces el elemento $\mathbf{a}_i$ puede formar $n-i+1$ parejas con los elementos restantes de $A$. De lo anterior tenemos que hay $n + (n-1) + (n-2) + \cdots + 1$ parejas distintas con los elementos de $A$, y la anterior suma es $\frac{n(n+1)}{2} = \frac{|A|(|A|+1)}{2}$ y por lo tanto:

$$\sum_{\mathbf{v}\in mid(A)} r_A(\mathbf{v}) = \frac{|A|(|A|-1)}{2}.$$

2. Sea $\mathbf{v}$ un vector en $A$, tal que $r_A(\mathbf{v}) = \text{máx}\{r_A(\mathbf{u}) \,|\, \mathbf{u} \in mid(A)\}$ y sea $\mathbf{w}$ en $mid(A)$ distinto de $\mathbf{v}$. Como $\mathbf{w} \in mid(A)$, existen $\mathbf{w}_1$ y $\mathbf{w}_2$ en $A$, tales que:

$$\frac{\mathbf{w}_1 + \mathbf{w}_2}{2} = \mathbf{w},$$

entonces,

$$\frac{\mathbf{w}_1 + \mathbf{w}_2}{2} - \mathbf{v} = \mathbf{w} - \mathbf{v},$$

luego,

$$\frac{(\mathbf{w}_1 - \mathbf{v}) + (\mathbf{w}_2 - \mathbf{v})}{2} = \mathbf{w} - \mathbf{v}.$$

Pero $\mathbf{w}_1 - \mathbf{v} \in A - \mathbf{v}$ y $\mathbf{w}_2 - \mathbf{v} \in A - \mathbf{v}$, luego $(\mathbf{w} - \mathbf{v}) \in mid(A - \mathbf{v})$. Observemos que de lo anterior tenemos dos cosas:

*a)* $\mathbf{w} \in mid(A)$ si y sólo si $\mathbf{w} - \mathbf{v} \in mid(A - \mathbf{v})$

*b)* Dada una pareja de vectores $\mathbf{w}_1, \mathbf{w}_2$ tales que $\frac{\mathbf{w}_1+\mathbf{w}_2}{2} = \mathbf{w}$ puedo construir una pareja de vectores $\mathbf{w}'_1, \mathbf{w}'_2$ tales que $\frac{\mathbf{w}'_1+\mathbf{w}'_2}{2} = \mathbf{w} - \mathbf{v}$ y viceversa.

Entonces de lo anterior tenemos que $r_A(\mathbf{w}) = r_{A-\mathbf{v}}(\mathbf{w} - \mathbf{v})$ y además de que si $\mathbf{w}$ es un vector en $mid(A)$ tal que $r_A(\mathbf{w}) = \text{máx}\{r_A(\mathbf{u}) \,|\, \mathbf{u} \in mid(A)\}$, entonces $r_{A-\mathbf{v}}(\mathbf{w}\text{-}\mathbf{v}) = \text{máx}\{r_{A-\mathbf{v}}(\mathbf{u}) \,|\, \mathbf{u} \in mid(A - \mathbf{v})\}$. Y como $\mathbf{v}$ cumple que $r_A(\mathbf{v}) = \text{máx}\{r_A(\mathbf{u}) \,|\, \mathbf{u} \in mid(A)\}$, entonces:

$$r_{A-\mathbf{v}}((0,0)) = \text{máx}\{r_{A-\mathbf{v}}(\mathbf{u}) \,|\, \mathbf{u} \in mid(A - \mathbf{v})\}$$

que es lo que se quería demostrar.

□

El siguiente lema es el paso importante en la demostración del *teorema* $2^n$ *de Freiman*, por lo cual hemos decidido exponerlo fuera de la prueba. Además de demostrarlo, posteriormente procederemos a dar un ejemplo de lo que se expone en la prueba para que así sea entendido.

**Lema 2.7.** *Sea* $1 < c < 4$ *y sean* $\epsilon_0 = \epsilon_0(2, c) > 0$ *y* $k_0 = k_0(2, c)$ *definidos como:*

$$\epsilon_0 = \frac{4 - c}{8(13c + 1)(4c)^3}$$

$$y$$

$$k_0 = (4c)^3.$$

*Sea* $A \subset \mathbb{R}^2$ *finito tal que:*

$$|A| \geq k_0,$$

$$|2A| \leq c|A|$$

$$y$$

$$|A \cap L| \leq \epsilon_0|A|$$

*para toda recta* $L$ *en* $\mathbb{R}^2$*, entonces existe* $W$ *subconjunto de* $A$ *tal que:*

$$|W| \geq \epsilon_0|A|$$

$$y$$

$$|2W| \leq (c - \epsilon_0)|W|.$$

*Demostración.* Sea $A$ subconjunto de $\mathbb{R}^2$ que satisface las tres condiciones del lema. Se demostrará primero que existen rectas $L_1, L_2$ en $\mathbb{R}^2$, vectores $\mathbf{f}_0, \mathbf{f}_1$ en $\mathbb{R}^2$, con $\mathbf{f}_0 = (0, 0)$, y conjuntos $A_0$, $A_1$ y $A_2$ tales que:

1. $\mathbf{f}_0 \in L_1 \cap L_2$ y $\mathbf{f}_1 \in L_2$.
2. $\mathbf{f}_1 \in L_1^{+1}$
3. $A_2 \subset A_1 \subset A_0$.
4. $|A_1| = k_1 > \frac{|A_0|}{4c}$ y $|A_2| = k_2 > \frac{|A_0|}{(4c)^3}$.
5. $A_1 \subset L_1^{+1}$ y $A_2 \subset L_1^{+1} \cap L_2^{+1}$.
6. $A_1 \cup (2\mathbf{f}_0 - A_1) \subset A_0$ y $A_2 \cup (2\mathbf{f}_1 - A_2) \subset A_1$.

Sea $A = A_0$. Como $A$ es finito existe $\mathbf{v} \in A$, tal que $r_A(\mathbf{v}) = \text{máx}\{r_A(\mathbf{u}) \,|\, \mathbf{u} \in mid(A)\}$ y por el lema 2,6, podemos suponer que $\mathbf{v} = \mathbf{f}_0 = (0,0)$. Sea $L_1$ una recta de $\mathbb{R}^2$ tal que $\mathbf{f}_0 \in L_1$ y sea $\mathbf{l}_1$ su vector normal. Para construir el conjunto $A_1$ primero observemos lo siguiente. Si $\mathbf{v}_1$ y $\mathbf{v}_2$ es una pareja de vectores tales que $\frac{\mathbf{v}_1+\mathbf{v}_2}{2} = \mathbf{f}_0$, entonces:

$$\begin{aligned} 0 &= (\mathbf{l}_1, \mathbf{f}_0) \\ &= (\mathbf{l}_1, \frac{\mathbf{v}_1 + \mathbf{v}_2}{2}) \\ &= \frac{1}{2}(\mathbf{l}_1, \mathbf{v}_1) + \frac{1}{2}(\mathbf{l}_1, \mathbf{v}_2), \end{aligned}$$

luego:

$$(\mathbf{l}_1, \mathbf{v}_1) = -(\mathbf{l}_1, \mathbf{v}_2).$$

De lo anterior obtenemos 3 casos:

- $(\mathbf{f}_1, \mathbf{v}_1) = 0$, entonces $(\mathbf{l}_1, \mathbf{v}_2) = 0$ y por lo tanto $\mathbf{v}_1, \mathbf{v}_2 \in L_1$.
- $(\mathbf{l}_1, \mathbf{v}_1) > 0$, entonces $(\mathbf{l}_1, \mathbf{v}_2) < 0$ y por lo tanto $\mathbf{v}_1 \in L_1^{+1}$ y $\mathbf{v}_2 \in L_1^{-1}$
- $(\mathbf{l}_1, \mathbf{v}_1) < 0$, entonces $(\mathbf{l}_1, \mathbf{v}_2) > 0$ y por lo tanto $\mathbf{v}_1 \in L_1^{-1}$ y $\mathbf{v}_2 \in L_1^{+1}$,

Además de que $\mathbf{v}_1 = 2\mathbf{f}_0 - \mathbf{v}_2$, es decir $\mathbf{v}_1$ es el reflejado de $\mathbf{v}_2$ respecto $\mathbf{f}_0$. Ya hecha esta observación procederemos a construir $A_1$. Sea $A_1$ definido de la siguiente manera:

$$A_1 = \{\mathbf{w} \in A \,|\, \mathbf{w} \in L_1^{+1} \text{ y } 2\mathbf{f}_0 - \mathbf{w} \in A\}.$$

Por construcción de $L_1$. $A_0$ y $A_1$ tenemos que las condiciones $1, 3, 5$ y $6$ se satisfacen para $L_1$, $A_1$ y $A_0$, entonces sólo queda por demostrar la condición 4. Observemos lo siguiente:

$$\begin{aligned} \frac{|A_0|^2}{2} &< \frac{|A_0|(|A_0|+1)}{2} \\ &= \sum_{\mathbf{v} \in mid(A)} r_{A_0}(\mathbf{v}) \\ &< r_{A_0}(\mathbf{f}_0)|mid(A_0)| \\ &= r_{A_0}(\mathbf{f}_0)|2A_0|, \\ &< r_{A_0}(\mathbf{f}_0)c|A_0|, \end{aligned}$$

y por lo tanto:

$$r_{A_0}(\mathbf{f}_0) > \frac{|A_0|}{2c}. \tag{2.18}$$

Por otro lado, por construcción de $A_1$ y por la desigualdad 2,18, tenemos que:

$$\begin{aligned}
|A_1| &\geq r_{A_0}(\mathbf{f}_0) - |A_0 \cap L_1| \\
&\geq r_{A_0}(\mathbf{f}_0) - \epsilon_0 |A_0| \\
&\geq |A_0| \left( \frac{1}{2c} - \frac{4-c}{8(13c+1)(4c)^3} \right) \\
&\geq |A_0| \left( \frac{1}{2c} - \frac{4}{8(13c+1)(4c)^3} \right) \\
&\geq |A_0| \left( \frac{1}{2c} - \frac{4}{(4c)^3} \right) \\
&\geq |A_0| \left( \frac{1}{2c} - \frac{1}{4c} \right),
\end{aligned}$$

y por lo tanto:

$$|A_1| \geq \frac{|A_0|}{2c}, \tag{2.19}$$

que es lo que se quería demostrar. Ahora procederemos a construir $A_2$, $\mathbf{f}_1$ y $L_2$. Sea $\mathbf{f}_1$ un vector en $A_1$ con la siguiente propiedad:

$$r_{A_1}(\mathbf{f}_1) = \text{máx}\{r_{A_1}(\mathbf{v}) \,|\, \mathbf{v} \in A_1\}$$

y sea $L_2$ la recta que pasa por $\mathbf{f}_0$ y $\mathbf{f}_1$ y $\mathbf{l}_2$ su vector normal. Nuevamente obtenemos que si $\mathbf{v}_1$ y $\mathbf{v}_2$ son una pareja de vectores tales que $\frac{\mathbf{v}_1+\mathbf{v}_2}{2} = \mathbf{f}_1$, entonces o ambos vectores están en $L_2$ o uno está en $L_2^{+1}$ y el otro está en $L_2^{-1}$; además de que $\mathbf{v}_2 = 2\mathbf{f}_2 - \mathbf{v}_1$, es decir, el vector $\mathbf{v}_2$ es el reflejado del vector $\mathbf{v}_1$, especto a $\mathbf{f}_1$. Análogamente construimos $A_2$ de la siguiente manera:

$$A_2 := \{\mathbf{w} \in A_1 \,|\, \mathbf{w} \in L_2^{+1} \text{ y } 2\mathbf{f}_1 - \mathbf{w} \in A\}.$$

Por contrucción de $L_2$ y $A_2$ tenemos que las condiciones $1, 2, 3, 5$ y $6$ se satisfacen para $L_2$, $A_2$ y $\mathbf{f}_1$, entonces sólo queda por demostrar la condición 4. Notemos lo siguiente:

$$\begin{aligned}
\frac{|A_1|^2}{2} &< \frac{|A_1|(|A_1|+1)}{2} \\
&< r_{A_1}(\mathbf{f}_1)|mid(A_1)| \\
&< r_{A_1}(\mathbf{f}_1)|mid(A_0)| \\
&< r_{A_1}(\mathbf{f}_1)c|A_0|,
\end{aligned}$$

luego:

$$r_{A_1}(\mathbf{f}_1) > \frac{|A_1|^2}{2c|A_0|}.$$

Ahora por la desigualdad 2,19, tenemos que:

$$\begin{aligned} r_{A_1}(\mathbf{f}_1) &> \frac{\frac{|A_0|^2}{(4c)^2}}{2c|A_0|} \\ &> \frac{|A_0|}{2c(4c)^2}, \end{aligned}$$

y por lo tanto:

$$r_{A_1}(\mathbf{f}_1) > \frac{2|A_0|}{(4c)^3}. \tag{2.20}$$

Por otro lado, por construcción de $A_2$ y por la desigualdad 2,20, tenemos que:

$$\begin{aligned} |A_2| &\geq r_{A_1}(\mathbf{f}_1) - |A_1 \cap L_2| \\ &\geq |A_0| \left( \frac{2}{(4c)^3} - \frac{4-c}{8(13c+1)(4c)^3} \right) \\ &\geq |A_0| \left( \frac{2}{(4c)^3} - \frac{4}{(4c)^3} \right) \\ &\geq |A_0| \left( \frac{2}{(4c)^3} - \frac{1}{(4c)^3} \right). \end{aligned}$$

Y por lo tanto:

$$|A_2| \geq \frac{|A_0|}{(4c)^3}, \tag{2.21}$$

que es lo que se quería demostrar. Ahora sea $\mathbf{a}$ un vector en $A_2$. A partir de $\mathbf{a}$ se construyen los conjuntos definidos en 2,7. Probaremos que:

$$S_m(\mathbf{a}) \subset \bigcap_{i=1}^{m} L_i^{+1},$$

para todo $0 \leq m \leq 2$. Observemos que por construcción de $A_m$, tenemos que $A_m \subset \bigcap_{i=1}^{m} L_i^{+1}$, entonces para demostrar lo anterior basta demostrar que $S_m(\mathbf{a}) \subset A_m$. Por elección de $\mathbf{a}$, tenemos que $\mathbf{a} \in A_2$ y además por construcción de $S_2(\mathbf{a})$, obtenemos que:

$$S_2(\mathbf{a}) = \{\mathbf{a}\} \in A_2,$$

luego:

$$S_2(\mathbf{a}) \subset A_2.$$

Ahora demostraremos que $S_1(\mathbf{a}) \subset A_1$. Recordemos que $S_1(\mathbf{a}) = S_2(\mathbf{a}) \cup (\{2\mathbf{f}_1\} - S_2(\mathbf{a}))$, y como $A_2 \subset A_1$ y $S_2(\mathbf{a}) \subset A_2$, entonces basta demostrar que $\{2\mathbf{f}_1\} - S_2(\mathbf{a}) \subset A_1$. Observemos lo siguiente:

$$\{2\mathbf{f}_1\} - S_2(\mathbf{a}) \subset \{2\mathbf{f}_1\} - A_2,$$

y por construcción de $A_1$, tenemos que $2\{\mathbf{f}_1\} - A_2 \subset A_1$, luego $\{2\mathbf{f}_1\} - S_2(\mathbf{a}) \subset A_1$ y por lo tanto $S_1(\mathbf{a}) \subset A_1$. Análogamente tenemos que $S_0(\mathbf{a}) \subset A$.

Observemos que las rectas $L_1$ y $L_2$; los vectores $\mathbf{f}_0, \mathbf{f}_1$ y $\mathbf{f}_2$; el conjunto $A_2$; y los bloques $S_0(\mathbf{a})$, $S_1(\mathbf{a})$ y $S_2(\mathbf{a})$ satisfacen las hipótesis del teorema 2,3, por lo tanto existe $\mathbf{a}^* \in A_2$, tal que:

$$\left| \left( \bigcup_{\mathbf{a} \in A_2} S_0(\mathbf{a}) \right) \cap B(\mathbf{a}^*) \right| \geq |A_2|.$$

Pero sabemos que $S_0(\mathbf{a}) \in A$, para todo $\mathbf{a} \in A_2$, entonces:

$$\begin{aligned} |A \cap B(\mathbf{a}^*)| &\geq \left| \left( \bigcup_{\mathbf{a} \in A_2} S_0(\mathbf{a}) \right) \cap B(\mathbf{a}^*) \right| \\ &\geq |A_2| \\ &\geq \frac{|A|}{(4c)^3}, \end{aligned}$$

y por lo tanto:

$$|A \cap B(\mathbf{a}^*)| \geq \frac{|A|}{(4c)^3}. \tag{2.22}$$

Por otra parte sabemos que todo bloque en $\mathbb{R}^2$ nos produce 4 hiperplanos faciales. Sean $F_{1,+1}$, $F_{1,-1}$, $F_{2,-1}$ y $F_{2,+1}$ los hiperplanos faciales producidos por el bloque $B(\mathbf{a}^*)$ y sea:

$$F^* := F_{1,+1} \cup F_{1,-1} \cup F_{2,+1} \cup F_{2,-1}.$$

De la construcción de $F^*$ tenemos que:

$$|F^*| \leq |F_{1,+1}| + |F_{1,-1}| + |F_{2,+1}| + |F_{2,-1}|,$$

lueg0:

$$|A \cap F^*| \leq |F_{1,+1}| + |F_{1,-1}| + |F_{2,+1}| + |F_{2,-1}|.$$

Como cada $F_{j,\mu}$ son hiperplanos, entonces por elección del conjunto $A$, tenemos que:

$$|A \cap F_{j,\mu}| \leq \epsilon_0 |A|,$$

y por lo tanto:

$$|A \cap F^*| \leq 4\epsilon_0 |A|. \tag{2.23}$$

Además sabemos que:

$$int(B(\mathbf{a}^*)) = B(\mathbf{a}^*) \setminus F^*.$$

Sea $W_0 := A \cap int(B(\mathbf{a}^*))$. Ahora acotaremos la cardinalidad de $W_0$ y para esto usaremos las ecuaciones 2,22 y 2,23

$$\begin{aligned}
|W_0| =& |A \cap int(B(\mathbf{a}^*))| \\
&= |A \cap (B(\mathbf{a}^*) \setminus F^*)| \\
&= |(A \cap B(\mathbf{a}^*)) \setminus (A \cap F^*)| \\
&\geq |A \cap B(\mathbf{a}^*))| - |A \cap F^*| \\
&> \frac{|A|}{(4c)^3} - 4\epsilon_0|A| \\
&> \frac{|A|}{(4c)^3} - \frac{4(4-c)(4c)^3}{8(13c+1)(4c)^3} \\
&> \frac{|A|}{(4c)^3} - \frac{1}{2} \\
&> \frac{2|A| - (4c)^3}{2(4c)^3} \\
&> \frac{|A|}{2(4c)^3},
\end{aligned}$$

luego:

$$|W_0| > \frac{|A|}{2(4c)^3} \tag{2.24}$$

Ahora, como:

$$vert(B(\mathbf{a}^*)) = S_0(\mathbf{a}^*) \subset A$$

$$y$$

$$W_0 = int(B(\mathbf{a}^*)) \cap A,$$

tenemos que:

$$mid(W_0, S_0(\mathbf{a}^*)) = mid(W_0, vert(B(\mathbf{a}^*))) \subset mid(A). \tag{2.25}$$

Además por el lema 2,5, también tenemos que:

$$mid(W_0, S_0(\mathbf{a}^*)) = mid(W_0, vert(B(\mathbf{a}^*)) \subset int(B(\mathbf{a}^*)). \tag{2.26}$$

y que:

$$|mid(W_0, S_0(\mathbf{a}^*)) = |4||W_0|. \tag{2.27}$$

Juntando 2,25 y 2,27, obtenemos que:

$$mid(W_0, S_0(\mathbf{a}^*)) \subset int(B(\mathbf{a}^*)) \cap mid(A). \tag{2.28}$$

Por otra parte sean $D(\lambda_1, \lambda_2)$, con $\lambda_1, \lambda_2 \in \{-1, 0, +1\}$, los conjuntos definidos en 2,3 correspondientes al bloque $B(\mathbf{a}^*)$. Se definen los conjuntos $W(\lambda_1, \lambda_2)$ de la siguiente manera:

$$W(\lambda_1, \lambda_2) = A \cap D(\lambda_1, \lambda_2).$$

Sabemos que $D(0,0) = int(B(\mathbf{a}^*))$, entonces $W_0 = W(0,0)$. Por la observación 2,2, tenemos que los conjuntos $D(\lambda_1, \lambda_2)$ son disjuntos por pares y convexos, entonces los conjuntos $W(\lambda_1, \lambda_2)$ son disjuntos por pares y además por la observación 2,4, tenemos que los conjuntos $mid(W(\lambda_1, \lambda_2)) \subset D(\lambda_1, \lambda_2)$ y por lo tanto:

$$mid(W(\lambda_1, \lambda_2)) \cap mid(W((\lambda_3, \lambda_4))) = \emptyset, \tag{2.29}$$

para todo $\lambda_1 \neq \lambda_3$ o $\lambda_2 \neq \lambda_4$. Como tenemos 9 conjuntos $W_{(\lambda_1,\lambda_2)}$, entonces para no trabajar con índice de dos entradas podemos numerarlos del 0 al 8, de tal manera que $W_0 = W_{(0,0)}$.

Observemos que por la ecuación 2,28 obtenemos que:

$$mid(W_0, S_0(\mathbf{a}^*)) \cap mid(W_i) = \emptyset, \tag{2.30}$$

para todo $1 \leq i \leq 8$. Para terminar la prueba demostraremos que existe $W_i$, con $1 \leq i \leq 8$, que satisface la conclusión del lema, es decir, que existe $W_i$, tal que:

$$|W_i| \geq \epsilon_0 |A|$$

$$y$$

$$|2W_i| \leq (c - \epsilon_0)|W_i|,$$

para algún $1 \leq i \leq 8$. Lo anterior se demostrará por contradicción, es decir, supondremos que si $W_i$ satisface que:

$$|W_i| \geq \epsilon_0 |A|,$$

entonces se cumple que:

$$|2W_i| = |mid(W_i| > (c - \epsilon_0)|W_i|.$$

Denotamos a $\mathcal{W}$ al conjunto de los $W_i$ que cumplen con que $|W_i| \geq \epsilon_0 |A|$. Como $mid(W_i) \subset mid(A)$ y como los $mid(W_i)$ son ajenos por pares, entonces:

$$\sum_{i=1}^{8} |mid(W_i)| \leq |mid(A)|. \tag{2.31}$$

Juntando la ecuación 2,30 y la desigualdad 2,31, obtenemos que:

$$\begin{aligned} ck_0 &\geq |2A| \\ &= mid(A) \\ &\geq |mid(W_0, S(\mathbf{a}^*))| + \sum_{i=1}^{8} |mid(W_i)| \end{aligned}$$

Ahora por la desigualdad 2,27, tenemos que:

$$\begin{aligned}
c|A| &\geq 4|W_0| + \sum_{i=1}^{8} |mid(W_i)| \\
&\geq 4|W_0| + \sum_{W_i \in \mathcal{W}} |mid(W_i)| \\
&\geq 4|W_0| + \sum_{W_i \in \mathcal{W}} (c - \epsilon_0)|W_i| \\
&= 4|W_0| + c \sum_{W_i \in \mathcal{W}} |W_i| - \epsilon_0 \sum_{W_i \in \mathcal{W}} |W_i| \\
&\geq 4|W_0| + c \sum_{W_i \in \mathcal{W}} |W_i| - \epsilon_0 |A| \\
&= 4|W_0| + c \left( \sum_{i=1}^{8} |W_i| - \sum_{W_j \notin \mathcal{W}} |W_j| \right) - \epsilon_0 |A| \\
&\geq 4|W_0| + c \sum_{i=1}^{8} |W_i| - c(9\epsilon_0 |A|) - \epsilon_0 |A| \\
&> (4-c)|W_0| + c \sum_{i=0}^{8} |W_i| - c(9\epsilon_0 |A|) - \epsilon_0 |A| \\
&= (4-c)|W_0| + c(|A| - |A \cap F^*) - c(9\epsilon_0 |A|) - \epsilon_0 |A| \\
&= (4-c)|W_0| + c(|A| - 4|A|\epsilon_0) - c(9\epsilon_0 |A|) - \epsilon_0 |A| \\
&= (4-c)|W_0| + c|A| - (9c + 4c + 1)\epsilon_0 |A| \\
&= (4-c)|W_0| + c|A| - (13c + 1)\epsilon_0 |A|,
\end{aligned}$$

luego:

$$|A| + (13c+1)\epsilon_0 |A| > (4-c)|W_0| + c|A|,$$

y por lo tanto:

$$(13c + 1\epsilon_0 |A| > (4-c)|W_0|,$$

pero por la desigualdad 2,24, obtenemos que:

$$(13c+1)\epsilon_0 |A| > \frac{(4-c)|A|}{2(4c)^3},$$

entonces:

$$\epsilon_0 > \frac{(4-c)}{2(4c)^3(13c+1)}.$$

Pero por definición de $\epsilon_0$, tenemos que:

$$\frac{4-c}{8(13c+1)(4c)^3} > \frac{(4-c)}{2(4c)^3(13c+1)},$$

luego:

$$\frac{1}{8} > \frac{1}{2},$$

lo cual es una contradicción y por lo tanto existe $W = W_i \subset A$, tal que:

$$|W| \geq \epsilon_0 |A|$$

$$y$$

$$|2W| \leq (c - \epsilon_0)|W|.$$

□

Ahora sí estamos listos para demostrar el *teorema* $2^n$ *de Freiman en el caso para* $n = 2$.

**Teorema 2.4** (Teorema de $2^n$ Freiman, para $n = 2$)**.** *Dado* $c$ *un número real tal que* $1 < c < 2^n$*, existen constantes* $k^* = k^*(2, c)$ *y* $\epsilon^* = \epsilon^*(2, c) > 0$*, tales que si* $A$ *es un subconjunto finito de* $\mathbb{R}^2$ *que satisfice:*

1. $|A| \geq k^*$*, y*
2. $|A + A| \leq c|A|$*,*

*entonces existe una recta* $L$ *de* $\mathbb{R}^2$ *tal que* $|A \cap L| > \epsilon^*|A|$.

*Demostración.* Sean $\epsilon_0(2, c) = \epsilon_0$ y $k_0(2, c) = k_0$ números reales definidos como:

$$\epsilon_0 := \frac{4 - c}{8(13c + 1)(4c)^3},$$

$$y$$

$$k_0 := (4c)^3.$$

Definimos al entero $t$ y los reales $\epsilon^*(2, c) = \epsilon^*$ y $k^*(2, c) = k^*$ de la siguiente manera:

$$t = \lceil \frac{c - 1}{\epsilon_0} \rceil,$$

$$\epsilon^* = \epsilon_0^{*t}$$

$$y$$

$$k^* = \epsilon_0^{-t} k_0.$$

Antes de continuar con la demostración observemos las siguientes propiedades de $k_0$ y de $\epsilon_0$. Si $1 \leq c_1 \leq c_2$, entonces tenemos que:

$$\frac{4 - c_1}{8(13c_1 + 1)(4c)^3} \leq \frac{4 - c_2}{8(13c_2 + 1)(4c_2)^3},$$

es decir si $1 \leq c_1 \leq c_2$, entonces:

$$\epsilon_0(2, c_1) \leq \epsilon_0(2, c_1). \tag{2.32}$$

Análogamente tenemos que si $1 \leq c_1 \leq c_2$, entonces:

$$k_0(2, c_1) \geq k_0(2, c_2). \tag{2.33}$$

Además de que:

$$|A| \geq k^* \geq k_0, \tag{2.34}$$

y,

$$\epsilon^* \leq \epsilon_0 \tag{2.35}$$

para toda $c$.

Por contradicción demostraremos que $\epsilon^*$ y $k^*$ son los requeridos en el teorema, es decir, supondremos si $A$ es un conjunto de $\mathbb{R}^2$ que satisface que:

1. $|A| \geq k^*$,
2. $|A + A| \leq c|A|$,
3. pero $|A \cap L| \leq \epsilon^*|A|$, para toda recta $L$ en $\mathbb{R}^2$,

llegaremos a una contradicción Definimos a los reales $c_0, \ldots, c_{t-1}$ de la siguiente manera:

$$c_0 = c$$

$$y$$

$$c_j := (c - j\epsilon_0(2, c)),$$

para todo $1 \leq j \leq t-1$, claramente $c_i \leq c_j$ si $i \leq j$. Por inducción construiremos conjuntos $A_0, \ldots, A_{t-1}$, tales que:

1. $|A_j| \geq k_0(2, c_j)$
2. $|A_j + A_j| \leq c_j|A_j|$
3. $|A_j \cap L| \leq \epsilon_0(2, c_j)|A|$, para toda recta $L$ en $\mathbb{R}^2$,

es decir, los conjuntos $A_j$ satisfacen las hipótesis del lema 2,7. Definimos a $A_0 = A$, por construcción de $A$ y por las ecuaciones 2,35 y 2,34, tenemos que $A_0$ cumple con los requisitos. Al satisfacer $A_0$ las hipótesis del 2,7, tenemos que existe $A_1 \subset A$, tal que:

$$|A_1| \geq \epsilon_0(2, c_0)|A_0| \text{ y } |A_1 + A_1| \leq (c - \epsilon_0(2, c_0))|A_1|$$

Como $|A_1| \geq \epsilon_0(2, c_0)|A_0|$, por la ecuación 2,34 y como $0 < \epsilon_0(2, c) \leq 1$, obtenemos:

$$\begin{aligned} |A_1| &\geq \epsilon_0(2, c_0)|A_0| \\ &\geq \epsilon_0(2, c_0)k^*(2, c_0) \\ &\geq k_0(2, c_1) \end{aligned}$$

Por otra parte como $|A_1 + A_1| \leq (c - \epsilon_0(2, c_0))|A_1|$, es decir:

$$|A_1 + A_1| \leq c_1|A_1|.$$

Por último por las ecuaciones 2,35 y 2,32, y el hecho de que $|A_0 \cap L| \leq \epsilon^*(c, 2)|A_0|$, para toda recta $L \subset \mathbb{R}^2$, tenemos que:

$$\begin{aligned} |A_1 \cap L| &\leq |A_0 \cap L| \\ &\leq \epsilon^*(2, c)|A_0| \\ &\leq \epsilon_0(2, c)|A| \\ &\leq \epsilon_0(2, c_1)|A|. \end{aligned}$$

Luego $A_1$ cumple las tres propiedades requeridas y por lo tanto podemos aplicar nuevamente el lema 2,7 para construir el conjunto $A_3$. Recursivamente construimos los conjuntos $A_4, \ldots, A_{t-1}$ que satisfacen las propiedades requeridas.

Al cumplir $A_{t-1}$ las tres propiedades obtenemos que existe $A_t$ subconjunto de $A_{t-1}$, tal que:

$$|A_t| \geq \epsilon_0(2, c_{t-1})|A_{t-1}| \text{ y } |A_t + A_t| \leq c_t|A_t|,$$

es decir, que $|A_t| > 1$ y que:

$$\begin{aligned} |A_t + A_t| &\leq c_t|A_t| \\ &\leq \left(c - \frac{c-1}{\epsilon(2, c_0)}\right)\epsilon(2, c_0)|A_t| \\ &\leq |A_t| \end{aligned}$$

Lo cual es imposible si $|A_t| > 1$ y por lo tanto existe una recta $L$ tal que $|A \cap L| \geq \epsilon^*$. □

## 2.3. Prueba del teorema 2.2 en el caso general

Como dijimos al inicio del capítulo, en esta sección demostraremos el teorema $2^n$ *de Freiman* en su versión general. Para esto, generalizaremos los conceptos vistos en la sección pasada. Además como mencionamos también al inicio del capítulo, la sección anterior fue hecha para entender la demostración del teorema objetivo. Por este motivo lo enunciado aquí no será ejemplificado. Por último, cabe destacar al vector neutro de $\mathbb{R}^n$ lo denotaremos como $\mathbf{0}$.

Iniciaremos la sección definiendo lo que es un *bloque* en $\mathbb{R}^n$ y sus elementos principales.

**Definición 2.10.** *Sea* $\boldsymbol{e}_0$ *un vector en* $\mathbb{R}^n$*, y* $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ *una base de* $\mathbb{R}^n$*. El* bloque $B = B(\boldsymbol{e}_0; \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ *con centro en* $\boldsymbol{e}_0$ *y base* $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ *es el conjunto:*

$$B(\boldsymbol{e}_0; \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) := \{\boldsymbol{e}_0 + \sum_{i=1}^{n} x_i \boldsymbol{e}_i \mid -1 \leq x_i \leq 1 \text{ para todo } 1 \leq i \leq n\}.$$

*Además definimos los siguientes conjuntos a partir del bloque* $B$*.*

1. *El conjunto de* vértices de $B$ *es:*

$$vert(B) := \{\boldsymbol{e}_0 + \sum_{i=1}^{n} \mu_i \boldsymbol{e}_i \mid \mu_i \in \{-1, 1\}^n, \text{ para toda } 1 \leq i \leq n\}.$$

2. *El* interior de $B$ *es:*

$$int(B) := \{\{\boldsymbol{e}_0 + \sum_{i=1}^{n} x_i \boldsymbol{e}_i \mid -1 < x_i < 1, \text{ para toda } 1 \leq i \leq n\}.$$

3. *Sea* $j \in \{1, 2, \ldots, n\}$ *y* $\mu_j \in \{-1, 1\}$*, el* hiperplano facial correspondiente a $j$ y $\mu_j$ *es:*

$$F_{j,\mu_j} := \{\boldsymbol{e}_0 + \mu_j \boldsymbol{e}_j + x\boldsymbol{e}_i \mid x \in \mathbb{R}, i \neq j\}.$$

4. *Definimos* $D(\lambda_1, \ldots, \lambda_n)$ *con* $\lambda_i \in \{-1, 0, 1\}$*, para toda* $1 \leq i \leq n$*; como el conjunto de vectores de la forma* $\boldsymbol{e}_0 + \sum_{i=1}^{n} x_i \boldsymbol{e}_i$*, donde:*

$$\begin{aligned} x_i > 1, &\text{ si } \lambda_i = 1, \\ -1 < x_i < 1, &\text{ si } \lambda_i = 0, \\ x_i < -1, &\text{ si } \lambda_i = -1, \end{aligned}$$

   *con* $1 \leq i \leq n$*.*

Observemos que para un bloque $B$ tanto la cardinalidad $vert(B)$ como el número de hiperplanos faciales es $2^n$. También observemos que tenemos $3^n$ conjuntos $D(\lambda_1, \ldots, \lambda_n)$ y además de que estos son ajenos por pares y son conjuntos convexos.

Procederemos ahora a generalizar la propiedad útil de los bloques.

**Lema 2.8.** *Sea* $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n\}$ *una base de* $\mathbb{R}^n$*, sea* $B = B(\boldsymbol{0}; \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$ *y* $\boldsymbol{u}$ *y* $\boldsymbol{v}$ *vectores en* $\mathbb{R}^n$*. Entonces las siguientes afirmaciones se cumplen.*

1. $B(\boldsymbol{u}, \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) = B + \{\boldsymbol{u}\}$.
2. *Si* $\boldsymbol{0} \in B(\boldsymbol{u}; \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n)$*, entonces* $\boldsymbol{0} \in B + \{t\boldsymbol{u}\}$ *para todo* $0 \leq t \leq 1$*.*
3. *Si* $(B + \{\boldsymbol{u}\}) \cap (B + \{\boldsymbol{w}\}) \neq \emptyset$*, entonces* $(ver(B) + \{\boldsymbol{u}\}) \cap (B + \{\boldsymbol{w}\}) \neq \emptyset$*.*

*Demostración.* Las demostraciones del los puntos 1 y 2 son totalmente análogas a las demostraciones de los puntos 1 y 2 del lema 2,1, entonces procederemos a demostrar el punto 3. Sea $\mathbf{u} = \sum_{i=1}^{n} u_i \mathbf{e}_i$ y sea $\mathbf{v} = \sum_{i=1}^{n} v_i \mathbf{e}_i$. Si $(B + \{\mathbf{u}\})) \cap (B + \mathbf{v}) \neq \emptyset$, entonces existen escalares $-1 \leq x_i, y_i \leq 1$, para todo $1 \leq i \leq n$, tales que $\sum_{i=1}^{n} x_i \mathbf{e}_i \in B$ y $\sum_{i=1}^{n} y_i \mathbf{e}_i \in B$. Además de que:

$$\sum_{i=1}^{n} (u_i + x_i)\mathbf{e}_i = \sum_{i=1}^{n} (v_i + y_i)\mathbf{e}_i,$$

luego obtenemos que:

$$u_i + x_i = v_i + y_i,$$

para todo $1 \leq i \leq n$. Como $-1 \leq x_i, y_i \leq 1$, de lo anterior obtenemos que:

$$v_i - 1 \leq v_i + y_i = u_i + x_i \leq u_1 + 1 \tag{2.36}$$

La ecuación anterior la analizaremos para diferentes valores que pueden tener los escalares $v_i$ y $u_i$.

1. Si $u_i \leq v_i$. De la ecuación 2,36 obtenemos que:

   $$v_i - 1 \leq u_i + 1 \leq v_i + 1, \tag{2.37}$$

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

2. Si $v_i < u_i$. De la ecuación 2,36, obtenemos que:

   $$v_i - 1 < u_i - 1 \leq u_i + x_i = v_i + y_i \leq v_i + 1,$$

   luego:

   $$v_i - 1 < u_i - 1 \leq v_i + 1, \tag{2.38}$$

   $1 \leq i \leq n$.

Si en la ecuación 2,37 sustituimos a $1 = \mu_i$ y a $-1 = \mu_i$ en 2,38, en ambas ecuaciones obtenemos que:

$$v_i - 1 \leq u_i + \mu_i \leq v_i + 1$$

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

$$\sum_{i=1}^{n} (u_i + \mu_i)\mathbf{e}_i = \mathbf{u} + \sum_{i=1}^{n} \mu_i \mathbf{e}_i \in (vert(B) + \{\mathbf{u}\}) \cap (B + \{\mathbf{v}\}).$$

□

Ahora generalizaremos el concepto de reflexión respecto a un vector.

**Definición 2.11.** *Sean $\boldsymbol{f}$ y $\boldsymbol{a}$ vectores en $\mathbb{R}^n$. La* reflexión de **a** con respecto a **f** *es el vector:*

$$2\boldsymbol{f} - \boldsymbol{a}.$$

*Además si $S$ es un conjunto en $\mathbb{R}^n$, la* reflexión de $S$ con respecto a **f** *es el conjunto:*

$$2\boldsymbol{f} - S := \{2\boldsymbol{f} - \boldsymbol{s} \,|\, \boldsymbol{s} \in S\}.$$

Continuaremos definiendo unos conjuntos fundamentales para la demostración de teorema $2^n$ *de Freiman.*

**Definición 2.12.** *Sean $\boldsymbol{f}_0, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$ vectores en $\mathbb{R}^n$. Definimos los conjuntos $S_0, S_1, \ldots, S_n$ de manera recursiva, como:*

$$\begin{aligned} S_n &= \{\boldsymbol{f}_n\} \\ S_{k-1} &= S_k \cup (\{2f_{k-1}\} - S_k), \end{aligned}$$

*con $1 \leq k \leq n$.*

Observemos que por construcción de $S_k$, tenemos que $|S_k| = 2^{n-k}$. Ahora generalizaremos el lema que nos relaciona bloques con la operación reflexión.

**Lema 2.9.** *Sean $\boldsymbol{f}_0 = \boldsymbol{0}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$ vectores en $\mathbb{R}^n$, y sean $S_0, \ldots, S_n$ los conjuntos dados en la definición 2.12. Si $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$ son linealmente independientes, entonces las siguientes afirmaciones se cumplen.*

1. *Los vectores $\boldsymbol{e}_i := \boldsymbol{f}_i - \boldsymbol{f}_{i-1}$, para toda $1 \leq i \leq n$, son linealmente independientes.*
2. *$S_0 = \{\sum_{i=1}^{n} \mu_i \boldsymbol{e}_i \,|\, \mu_i \in \{-1, 1\}$ para toda $1 \leq i \leq n\}$.*
3. *$B(\boldsymbol{0}; \boldsymbol{e}_1, \ldots, \boldsymbol{e}_n) = conv(S_0)$.*

*Demostración.* 1. Sean $\alpha_1, \ldots \alpha_n \in \mathbb{R}$ tales que:

$$\sum_{i=1}^{n} \alpha_i \mathbf{e}_i = \mathbf{0}.$$

Por la definición de los vectores $\mathbf{e}_i$, tenemos que:

$$\begin{aligned} \mathbf{0} &= \sum_{i=1}^{n} \alpha_i \mathbf{e}_i \\ &= \sum_{i=1}^{n} \alpha_i (\mathbf{f}_i - \mathbf{f}_{i-1}) \\ &= \sum_{i=1}^{n} \left( \sum_{j=i}^{n} (-1)^{j+1} \alpha_j \right) \mathbf{f}_i. \end{aligned}$$

Pero como los vectores $\mathbf{f}_1, \ldots, \mathbf{f}_n$ son linealmente independientes, obtenemos que:

$$\sum_{i=j}^{n}(-1)^{j+1}\alpha_j = 0,$$

para todo $1 \leq i \leq n$, y por lo tanto $\alpha_1 = \ldots = \alpha_n = 0$.

2. Se probará inductivamente que:

$$S_k = \{\mathbf{f}_k\} + \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i \,|\, \mu_1 \in \{1, -1\}, \text{para toda } k+1 \leq i \leq n\}, \tag{2.39}$$

para toda $0 \leq k \leq n$. Si $k = n$, claramente se cumple que $S_n = \{\mathbf{f}_n\}$. Supongamos que la ecuación 2,39 se cumple para $k$. Por definición de $S_{k-1}$, tenemos que:

$$\begin{aligned} S_{k-1} &= S_k \bigcup (\{2\mathbf{f}_{k-1}\} - S_k) \\ &= \left(\{\mathbf{f}_k\} + \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i\}\right) \bigcup \left(\{2\mathbf{f}_{k-1} - \mathbf{f}_k\} - \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i\}\right) \end{aligned}$$

Como $\mathbf{e}_k = \mathbf{f}_k - \mathbf{f}_{k-1}$, tenemos que:

$$\begin{aligned} S_{k-1} &= \left(\{\mathbf{f}_{k-1} + \mathbf{e}_k\} + \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i\}\right) \cup \left(\{\mathbf{f}_{k-1} - \mathbf{e}_k\} - \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i\}\right) \\ &= \left(\{\mathbf{f}_k\} + \{\mathbf{e}_k\} + \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i\}\right) \cup \left(\{\mathbf{f}_{k-1}\} + \{-\mathbf{e}_k\} + \{\sum_{i=k+1}^{n} \mu_i \mathbf{e}_i\}\right) \end{aligned}$$

y por lo tanto:

$$S_{k-1} = \{\mathbf{f}_{k-1}\} + \{\sum_{i=k}^{n} \mu_i \mathbf{e}_i \,|\, \mu_1 \in \{1, -1\}, \text{para toda } k \leq i \leq n\}$$

Para $k = 0$, obtenemos que:

$$S_0 = \{\sum_{i=1}^{n} \mu_i \mathbf{e}_i \,|\, \mu_i \in \{1, -1\} \text{ para toda } 1 \leq i \leq n\}.$$

3. Como $B = B(\mathbf{0}; \mathbf{e}_1, \ldots, \mathbf{e}_n) = conv(vert(B))$, y por el punto anterior se sigue que $B = conv(S_0))$.

□

Nuevamente a partir de aquí usaremos fuertemente conceptos y resultados del apéndice.

**Lema 2.10.** *Sean $H_1, \ldots, H_n$ hiperplanos en $\mathbb{R}^n$, y sean $\boldsymbol{f}_0 = \boldsymbol{0}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_n$ vectores en $\mathbb{R}^n$ tales que:*

$$\boldsymbol{f}_i \in H_j, \text{ para todo } 0 \leq i < j \leq n$$
$$\boldsymbol{f}_i \in H_j^{(+1)}, \text{ para todo } 0 \leq j \leq i \leq n,$$

*entonces los vectores $\boldsymbol{f}_1 \ldots, \boldsymbol{f}_n$ son linealmente independientes. Más aún, si $S_0, S_1 \ldots, S_n$ son los conjuntos dados en la definición 2.12, que cumplen que:*

$$S_k \subset \bigcap_{j=1}^{k} H_j^{(+1)},$$

*entonces:*

$$S_0 \bigcap H(\mu_1, \ldots, \mu_n) \neq \emptyset,$$

*para todo $(\mu_1, \ldots, \mu_n) \in \{-1, +1\}^n$, y los hiperplanos $H_1, \ldots, H_n$ son linealmente independientes. Además si $\boldsymbol{s} \in S_0 \bigcap H(\mu_1, \ldots, \mu_n)$ y $S_{n+1} = \emptyset$; entonces $\boldsymbol{s} \in S_k \setminus S_{k+1}$ si y sólo si $\mu_i = 1$ para $1 \leq i \leq k$ y $\mu_{k+1} = -1$.*

*Demostración.* Sean $H_1 \ldots, H_n$ hiperplanos en $\mathbb{R}^n$ y $\mathbf{f}_0 = \mathbf{0}, \mathbf{f}_1, \ldots, \mathbf{f}_n$ vectores en $\mathbb{R}^n$ que satisfacen las condiciones del lema. Primero demostraremos que los vectores $\mathbf{f}_1 \ldots, \mathbf{f}_n$, son linealmente independiente y esto se efectuará por contradicción. Sean $x_1, \ldots, x_n$ escalares en $\mathbb{R}$, no todos 0, tales que:

$$\sum_{i=1}^{n} x_i \mathbf{f}_n = \mathbf{0}.$$

Sin pérdida de generalidad supongamos que $x_n \neq 0$. De lo anterior tenemos que:

$$\mathbf{f}_n = \sum_{i=1}^{n-1} \frac{x_i}{-x_n} \mathbf{f}_i,$$

es decir, el vector $\mathbf{f}_n$ es combinación lineal de los vectores $\mathbf{f}_1, \ldots, \mathbf{f}_n$. Por construcción de los vectores $\mathbf{f}_1, \ldots \mathbf{f}_{n-1}$ y del hiperplano $H_n$, tenemos que $\mathbf{f}_1, \ldots \mathbf{f}_{n-1} \in H_n$ y $\mathbf{0} \in H_n$ y por lo tanto $\mathbf{f}_n \in H_n$, lo cual es una contradicción ya que por construcción de $\mathbf{f}_n$, tenemos que $\mathbf{f}_n \in H_n^{(+1)}$ y $H_n \cap H_n^{(+1)} = \emptyset$, y por lo tanto los vectores $\mathbf{f}_1, \ldots, \mathbf{f}_n$ son linealmente independientes. Ahora procederemos a demostrar que $S_0 \bigcap H(\mu_1 \ldots, \mu_n) \neq \emptyset$, para todo $(\mu_1, \ldots, \mu_n) \in \{-1, 1\}^n$. Primero demostraremos inductivamente que:

$$S_k \bigcap H(1, \ldots, \mu_{k+1}, \ldots, \mu_n) \neq \emptyset,$$

para todo $1 \leq k \leq n$. Observemos que si $n = k$, por construcción de $S_n$ y de $\mathbf{f}_n$, tenemos que $S_n = \{\mathbf{f}_n\}$ y $\mathbf{f}_n \in H_i^{(+1)}$, para todo $1 \leq i \leq n$. De lo anterior obtenemos que:

$$\mathbf{f}_n \in S_n \bigcap H(\underbrace{1, \ldots, 1}_{n}).$$

Supongamos que lo anterior se cumple para todo $k$. Por hipótesis de inducción, para todo $(\mu_{k+1}, \ldots, \mu_n) \in \{-1, 1\}^{n-k}$, existe vector $\mathbf{s}$, tal que:

$$S_k \cap H(1, \ldots, \mu_{k+1}, \ldots, \mu_n).$$

Como, por hipótesis, tenemos que $S_{k-1} \subset \left( \bigcap_{i=1}^{k-1} H_i^{(+1)} \right)$, entonces para demostrar que $S_{k-1} \cap H(1, \ldots, 1, \mu_k, \ldots, \mu_n) \neq \emptyset$, basta demostrar que $S_{k-1} \cap \left( \bigcap_{i=k}^{n} H_i^{(\mu_i)} \right) \neq \emptyset$, para todo $(\mu_k, \ldots, \mu_n) \in \{-1, +1\}^{n-k+1}$.
Por construcción de $S_{k-1}$, tenemos que $S_k \subset S_{k-1}$ y además por hipótesis de inducción tenemos:

$$S_{k-1} \cap \left[ \left( H_k^{(+1)} \right) \cap \left( \bigcap_{i=k+1}^{n} H_i^{(\mu_i)} \right) \right] \neq \emptyset. \tag{2.40}$$

Por otro lado, nuevamente por hipótesis de inducción, tenemos que existe vector $\mathbf{s}$, tal que:

$$\mathbf{s} \in S_k \cap \left[ \left( H_k^{(+1)} \right) \cap \left( \bigcap_{i=k+1}^{n} H_i^{(\mu_i)} \right) \right]$$

, para todo $(\mu_k, \ldots, \mu_n) \in \{-1, +1\}^{n-k+1}$. Por construcción de $S_{k+1}$ tenemos que $2\mathbf{f}_{k-1} - \mathbf{s} \in S_{k-1}$. Además por hipótesis tenemos que $\mathbf{f}_{k-1} \in H_i$, para todo $k \leq \ i \leq n$. De lo anterior se sigue que $2\mathbf{f}_{k-1} - \mathbf{s} \in H_k^{(-1)}$ y $2\mathbf{f}_{k-1} - \mathbf{s} \in H_i^{(-\mu_i)}$, para todo $k+1 \leq i \leq n$ y para todo $(\mu_{k+1}, \ldots, \mu_n) \in \{-1, +1\}^{n-k}$; luego:

$$S_{k-1} \cap \left[ \left( H_k^{(-1)} \right) \cap \left( \bigcap_{i=k+1}^{n} H_i^{(\mu_i)} \right) \right] \neq \emptyset. \tag{2.41}$$

Juntando las ecuaciones 2,40 y 2,41, obtenemos que:

$$S_{k-1} \cap \left( \bigcap_{i=k}^{n} H_i^{(\mu_i)} \right) \neq \emptyset$$

, para todo $(\mu_k, \ldots, \mu_n) \in \{-1, +1\}^{n-k+1}$, y por lo tanto $S_{k-1} \cap H(1, \ldots, \mu_k, \ldots, \mu_n)$. Tomando a $k = 0$ obtenemos que:

$$S_0 \cap H(\mu_1, \ldots, \mu_n) \neq \emptyset,$$

para todo $(\mu_1, \ldots, \mu_n) \in \{-1, +1\}^n$, que es lo que se quería demostrar. Además por el lema 6,1, tenemos que los hiperplanos $H_1, \ldots, H_n$ son linealmente independientes.
Como $|S_k| = 2^{n-k}$ y $S_k \cap H(1, \ldots, 1, \mu_{k+1}, \ldots, \mu_n) \neq \emptyset$, para todo $1 \leq k \leq n$ y para todo $(\mu_{k+1}, \ldots, \mu_n) \in \{-1, +1\}^n$; obtenemos que:

$$|S_k \cap H(1, \ldots 1, \mu_{k+1}, \ldots, \mu_n)| = 1$$

. De lo anterior obtenemos que cada uno de los $2^n$ conjuntos $H(\mu_1, \ldots, \mu_n)$ contiene exactamente un elemento de $S_0$. Luego obtenemos que si:

$$\mathbf{s} \in S_0 \cap H(\mu_1, \ldots, \mu_n),$$

y $\mu_i = 1$ para todo $1 \leq i \leq k$, entonces $\mathbf{s} \in S_k$. Por otra parte si $\mu_{k+1} = -1$, entonces $\mathbf{s} \notin S_{k+1}$. Luego:

$$S_0 \cap H(1, \ldots, 1, -1, \mu_{k+2}, \ldots, \mu_n) \subset S_k \setminus S_{k+1}.$$

Además como:

$$|S_0 \cap H(1, \ldots, 1, -1, \mu_{k+2}, \ldots, \mu_n)| = |S_k \setminus S_{k+1}| = 2^{n-k-1},$$

obtenemos que:

$$S_0 \cap H(1, \ldots, 1, -1, \mu_{k+2}, \ldots, \mu_n) = S_k \setminus S_{k+1},$$

que es lo que se quería demostrar □

Ahora defefiniremos a los conjuntos $S_n, \ldots, S_n$ cuando el vector $\mathbf{f}_n$ no es fijo y además daremos una propiedad muy importante de dichos conjuntos.

**Lema 2.11.** *Sean $H_1, \ldots, H_n$ hiperplanos en $\mathbb{R}^n$, y sean $\boldsymbol{f}_0 = \boldsymbol{0}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_{n-1}$ vectores en $\mathbb{R}^n$ tales que:*

$$\boldsymbol{f}_i \in H_j, \text{ para todo } 0 \leq i < j \leq n-1$$
$$\boldsymbol{f}_i \in H_j^{(+1)}, \text{ para todo } 0 \leq j \leq i \leq n-1,$$

*Sea $\boldsymbol{a}$ un vector en $H(\underbrace{1, \ldots, 1}_{n})$. Se definen los conjuntos $S_n(\boldsymbol{a}), \ldots, S_0(\boldsymbol{a})$, de manera recursiva, como sigue:*

$$S_n(\boldsymbol{a}) = \{\boldsymbol{a}\}$$
$$S_{k-1} = S_k(\boldsymbol{a}) \cup (\{2f_{k-1}\} - S_k(\boldsymbol{a})),$$

*con $1 \leq k \leq n$. Si $\boldsymbol{a}, \boldsymbol{a}'$ son vectores en $H(\underbrace{1, \ldots, 1}_{n})$, tales que $\boldsymbol{a} \neq \boldsymbol{a}'$, entonces $S_0(\boldsymbol{a}) \cap S_0(\boldsymbol{a}') \neq \emptyset$.*

*Demostración.* Sean $\mathbf{a}$ y $\mathbf{a}'$ vectores en $H(\underbrace{1, \ldots, 1}_{n})$, distintos. Como $S_n(\mathbf{a}) = \{\mathbf{a}\}$ y $S_n(\mathbf{a}') = \{\mathbf{a}'\}$, entonces $S_n(\mathbf{a}) \cap S_n(\mathbf{a}') = \emptyset$. Por contradicción supongamos que $S_0(\mathbf{a}) \cap S_0(\mathbf{a}') \neq \emptyset$. Sea $k$ el mayor entero tal que $S_k(\mathbf{a}) \cap S_k(\mathbf{a}') \neq \emptyset$, luego $0 \leq k \leq n-1$. Sea $\mathbf{s}$ un vector en $S_k(\mathbf{a}) \cap S_k(\mathbf{a}')$, luego $\mathbf{s} \notin S_{k+1}(\mathbf{a}) \cap S_{k+1}(\mathbf{a}')$. Si $\mathbf{s} \notin S_{k+1}(\mathbf{a})$, tenemos que:

$$\mathbf{s} \in S_k(\mathbf{a}) \setminus S_{k+1} = \{2\mathbf{f}_k\} - S_{k+1}(\mathbf{a}).$$

Por el lema 2,10 obtenemos que:

$$\mathbf{s} \in H(1, \ldots, 1, -1, \mu_{k+2}, \ldots, \mu_n).$$

Nuevamente por el lema 2,10, tenemos que:

$$\mathbf{s} \in S_k(\mathbf{a}') \setminus S_{k+1}(\mathbf{a}') = \{2\mathbf{f}_k\} - S_{k+1}(\mathbf{a}').$$

De lo anterior tenemos que existe un $\mathbf{v} \in S_{k+1}(\mathbf{a})$ y un vector $\mathbf{v}' \in S_{k+1}(\mathbf{a}')$, tal que:

$$\mathbf{s} = 2\mathbf{f}_k - \mathbf{v} = 2\mathbf{f}_k - \mathbf{v}'.$$

Lo anterior nos dice que $\mathbf{v} = \mathbf{v}' \in S_{k+1}(\mathbf{a}) \cap S_{k+1}(\mathbf{a}')$, lo cual contradice la elección de $k$ y por lo tanto:

$$S_0(\mathbf{a}) \cap S_0(\mathbf{a}') = \emptyset$$

□

Destaquemos que las demostraciones de los lemas y teoremas que vienen a continuación son muy similares a las demostraciones de sus versiones de $\mathbb{R}^2$, por ello algunos pasos los obviaremos. Ahora procederemos a demostrar un teorema que nos envuelve todo lo visto hasta el momento.

**Teorema 2.5.** *Sean $H_1, \ldots, H_n$ hiperplanos en $\mathbb{R}^n$, y sean $\boldsymbol{f}_0 = \boldsymbol{0}, \boldsymbol{f}_1, \ldots, \boldsymbol{f}_{n-1}$ vectores en $\mathbb{R}^n$ tales que:*

$$\boldsymbol{f}_i \in H_j, \text{ para todo } 0 \leq i < j \leq n-1$$
$$\boldsymbol{f}_i \in H_j^{(+1)}, \text{ para todo } 0 \leq j \leq i \leq n-1,$$

*Sea $A_n$ un subconjunto finito de $H(\underbrace{1, \ldots, 1}_{n})$. Para cada vector $\boldsymbol{a} \in A_n$ se definen los conjuntos $S_n(\boldsymbol{a}), \ldots, S_0(\boldsymbol{a})$, y el bloque $B(\boldsymbol{a})$ como sigue:*

$$\begin{aligned} S_n(\boldsymbol{a}) &= \{\boldsymbol{a}\} \\ S_{k-1} &= S_k(\boldsymbol{a}) \cup (\{2f_{k-1}\} - S_k(\boldsymbol{a})), \\ B(\boldsymbol{a}) &= conv(S_0(\boldsymbol{a})), \end{aligned}$$

*con $1 \leq k \leq n$.*
*Además supongamos que para todo $\boldsymbol{a} \in A_n$ se cumple que:*

$$S_k(\boldsymbol{a}) \subset \bigcap_{i=1}^{k} H_i^{(+1)},$$

*para todo $1 \leq k \leq n$. Entonces existe $\boldsymbol{a}^* \in A_n$ tal que para todo $\boldsymbol{a} \in A_n$ se cumple que:*

$$S_0(\boldsymbol{a}) \cap B(\boldsymbol{a}^*) \neq \emptyset$$

*y*

$$\left| \left( \bigcup_{\boldsymbol{a} \in A_n} S_0(\boldsymbol{a}) \right) \cap B(\boldsymbol{a}^*) \right| \geq |A_n|.$$

*Demostración.* Sea $\mathbf{a} \in A_n$, definimos los siguientes vectores:

$$\mathbf{e}_i = \mathbf{f}_i - \mathbf{f}_{i-1},$$

para todo $1 \leq i \leq n-1$ y

$$\mathbf{e}_n(\mathbf{a}) = \mathbf{a} - \mathbf{f}_{n-1}.$$

Por el lema 2,10 tenemos que los vectores $\mathbf{f}_1, \ldots, \mathbf{f}_{n-1}$ son linealmente independientes, además por el lema 2,9 tenemos que los vectores $\mathbf{e}_1, \ldots \mathbf{e}_n(\mathbf{a})$ son linealmente independientes también. Como $\mathbf{e}_1, \ldots, \mathbf{e}_{n-1} \in H_n$, y $\dim(H_n) = n-1$, entonces tenemos que $\{\mathbf{e}_1, \ldots, \mathbf{e}_{n-1}\}$ es una base de $H_n$. Análogamente tenemos que $\{\mathbf{e}_1, \ldots, \mathbf{e}_n(\mathbf{a})\}$ es una base de $\mathbb{R}^n$, para todo $\mathbf{a} \in A_n$. A partir de la observación anterior los siguientes conjuntos son bloques en $H_n$ y $\mathbb{R}^n$ respectivamente:

$$B := B(\mathbf{0}; \mathbf{e}_1, \ldots, \mathbf{e}_{n-1})$$

$$y$$

$$B(\mathbf{a}) := B(\mathbf{0}; \mathbf{e}_1, \ldots, \mathbf{e}_n(\mathbf{a})).$$

Por el lema 2,9 tenemos que:

$$vert(B(\mathbf{a})) = S_0(\mathbf{a})$$

$$y$$

$$B(\mathbf{a}) = conv(S_0(\mathbf{a})).$$

Para $\mu_n \in \{-1, +1\}$ definimos los siguientes conjuntos:

$$S_0^{(\mu_n)}(\mathbf{a}) = \{\sum_{i=1}^{n-1} \mu_i \mathbf{e}_i + \mu_n \mathbf{e}_n(\mathbf{a}) \mid (\mu_1, \ldots, \mu_{n-1}) \in \{-1, +1\}^{n-1}\}.$$

Veamos lo siguiente:

$$vert(B) + \{\mathbf{e}_n(\mathbf{a})\} = S_0^{(+1)}(\mathbf{a}),$$

luego:

$$conv(S_0^(+1)(\mathbf{a})) = B + \{\mathbf{e}_n(\mathbf{a})\} \subseteq B(\mathbf{a}). \tag{2.42}$$

Análogamente tenemos que:

$$conv(S_0^{-1}(\mathbf{a})) = B - \{\mathbf{e}_n(\mathbf{a})\} \subseteq B(\mathbf{a}). \tag{2.43}$$

Sean $\mathbf{h}_1, \ldots, \mathbf{h}_n$ vectores normales a los hiperplanos $H_1 \ldots, H_n$ respectivamente. Sea $L_n = \bigcap_{i=1}^{n-1} H_n$. Por teorema de álgebra lineal podemos construir vector $\mathbf{h}_n^*$, tal que $\{\mathbf{h}_n^*\}$ es base de $H_n$ y que satisfaga que:

$$(\mathbf{h}_i, \mathbf{h}_n^*) = 0,$$

si $i \neq n$ y

$$(\mathbf{h}_n, \mathbf{h}_n^*) = 1.$$

Sea:

$$\pi : \mathbb{R}^n \to L_n$$

la proyección correspondiente a la descomposición de la suma direta de:

$$\mathbb{R}^n = H_n \oplus L_n.$$

Como $\mathbf{f}_{n-1} \in H_n$ y $\mathbf{a} \in H_n^{(+1)}$, tenemos que $\mathbf{e}_n(\mathbf{a}) = \mathbf{a} - \mathbf{f}_{n-1} \in H_n^{(+1)}$, y por lo tanto $\mathbf{e}_n(\mathbf{a})$ puede ser escrito de manera única como:

$$\mathbf{e}_n(\mathbf{a}) = \pi(\mathbf{e}_n(\mathbf{a})) + \phi(\mathbf{a})\mathbf{h}^*,$$

donde:

$$(\mathbf{h}_n, \mathbf{e}_n(\mathbf{a})) = (\mathbf{h}_n, \pi(\mathbf{e}_n(\mathbf{a}))) + \phi(\mathbf{a})(\mathbf{h}_n, \mathbf{h}_n^*) = \phi(\mathbf{a}) > 0.$$

De lo anterior y por el lema 2,10, tenemos que:

$$S_0(\mathbf{a}) \cap H(\mu_1, \ldots, \mu_{n-1}, +1) = S_0^{(+1)}(\mathbf{a} \cap \left( \bigcap_{i=1}^{n-1} H_i^{(\mu_i)} \right) \neq \emptyset,$$

para todo $(\mu_1, \ldots, \mu_{n-1}, +1) \in \{-1, +1\}^{n-1}$. De la observación anterior y por el lema 6,6, tenemos que:

$$\begin{aligned} \mathbf{0} \in conv\left(\pi(S_0^{(+1)}(\mathbf{a}))\right) &= \pi\left(conv(S_0^{(+1)}(\mathbf{a}))\right) \\ &= \pi\left(B + \mathbf{e}_n(\mathbf{a})\right) \\ &= B + \pi(\mathbf{e}_n(\mathbf{a})) \end{aligned}$$

Por otro lado como $A_n$ es un conjunto finito, podemos escoger $\mathbf{a}^* \in A_n$ tal que:

$$\pi(\mathbf{a}^*) = \max\{\phi(\mathbf{a}) \,|\, \mathbf{a} \in A_n\}.$$

Observemos que si $\mathbf{a}$ es un vector distinto de $\mathbf{a}^*$ en $A_n$, y si definimos a $t = \frac{\phi(\mathbf{a})}{\phi(\mathbf{a}^*)}$, entonces $0 \leq t \leq 1$ y además:

$$t\mathbf{e}_n(\mathbf{a}^*) = \pi(t\mathbf{e}_n(\mathbf{a}^*)) + t\phi(\mathbf{a}^*)\mathbf{h}_n^* = \phi(t\mathbf{e}_n(\mathbf{a}^*)) + \phi(\mathbf{a})\mathbf{h}^*.$$

Además como $\mathbf{0} \in B + \pi(\mathbf{e}_n(\mathbf{a}^*))$, obtenemos por el lema 2,8 que:

$$\mathbf{0} \in (B + \phi(\mathbf{e}_n(\mathbf{a}))) \cap (B + t\pi(\mathbf{e}_n(\mathbf{a}^*))) \neq \emptyset.$$

y nuevamente por el lema 2,8, obtenemos que:

$$(vert(B) + \pi(\mathbf{e}_n(\mathbf{a}))) \cap (B + \pi(t\mathbf{e}_n(\mathbf{a}^*))) \neq \emptyset.$$

Y por lo tanto existe $(\mu_1, \ldots, \mu_{n-1}) \in \{-1, +1\}^{n-1}$ tal que:

$$\sum_{i=1}^{n-1} \mu_i \mathbf{e}_i + \pi(\mathbf{e}_n(\mathbf{a})) \in B + \pi(t\mathbf{e}_n(\mathbf{a}^*)),$$

luego:

$$\sum_{i=1}^{n-1} \mu_i \mathbf{e}_i + \pi(\mathbf{e}_n(\mathbf{a})) + \phi(\mathbf{a})\mathbf{h}_n^* = \sum_{i=1}^{n-1} \mu_i \mathbf{e}_i + \mathbf{e}_n(\mathbf{a}) \in S_0^{(+1)}(\mathbf{a}),$$

y además:

$$\sum_{i=1}^{n-1} \mu_i \mathbf{e}_i + \mathbf{e}_n(\mathbf{a}) \in B + t\pi(\mathbf{e}_n(\mathbf{a}^*)) + \phi(\mathbf{a})\mathbf{h}_n^* = B + t\mathbf{e}_n(\mathbf{a}^*) \subset B(\mathbf{a}^*).$$

De lo anterior tenemos que para toda $\mathbf{a} \in A_n$ se tiene que:

$$S_0^{(+1)}(\mathbf{a}) \cap B(\mathbf{a}^*) \neq \emptyset,$$

y por lo tanto

$$S_0(\mathbf{a}) \cap B(\mathbf{a}^*) \neq \emptyset.$$

Para terminar observemos que por el lema 2,11, si $\mathbf{a}$ y $\mathbf{a}'$ son vectores en $A_n$, con $\mathbf{a} \neq \mathbf{a}'$, entonces $S_0(\mathbf{a}) \cap S_0(\mathbf{a}') = \emptyset$, y por lo tanto:

$$\left| \left( \bigcup_{\mathbf{a} \in A_n} S_0(\mathbf{a}) \right) \cap B(\mathbf{a}^*) \right| \geq |A_n|.$$

□

Ahora procederemos a generalizar el último concepto definido en la sección anterior.

**Definición 2.13.** *Sean $A_1$, $A_2$ y subconjuntos de $\mathbb{R}^n$. El conjunto de los puntos medios de $A_1$ y $A_2$ se define como:*

$$mid(A_1, A_2) = \left\{ \frac{\boldsymbol{a}_1 + \boldsymbol{a}_2}{2} \mid \boldsymbol{a}_1 \in A_1 \text{ y } \boldsymbol{a}_2 \in A_2 \right\}.$$

*Si $A_1 = A_2 = A$, entonces:*

$$mid(A) = \left\{ \frac{\boldsymbol{a} + \boldsymbol{a}'}{2} \| \mid \boldsymbol{a}, \boldsymbol{a}1 \in A \right\}$$

De la definición se puntos medios se infieren las siguientes porpiedades:

**Observación 2.5.** *1. Si $K$ es un conjunto convexo de $\mathbb{R}^n$ y $A_1, A_2 \subset K$, entonces $mid(A_1, A_2) \subset K$.*

*2. $A \subset mid(A)$ y $|mid(A)| = |2A|$.*

**Lema 2.12.** *Sea $B$ un bloque en $\mathbb{R}^n$, y sea $W \subset int(B)$. Entonces:*

$$mid(W, vert(B)) \subset int(B)$$

*y*

$$|mid(w, vert(B))| = 2^n |W|.$$

*Demostración.* Sea $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ una base de $\mathbb{R}^n$ y $\mathbf{e}_0$ un vector en $\mathbb{R}^n$. Sea $B = B(\mathbf{e}_0; \mathbf{e}_1, \ldots, \mathbf{e}_n)$ Para todo $j \in \{1, 2\}$, sea

$$\mathbf{w}_j = \mathbf{e}_0 + \sum_{i=1}^{n} x_{ij}\mathbf{e}_i \in W \subset int(B)$$

y sea

$$\mathbf{b}_j = \mathbf{e}_0 + \sum_{i=1}^{n} \mu_{ij}\mathbf{e}_i \in vert(B).$$

Entonces $-1 < x_{ij} < 1$ y $\mu_{ij} \in \{-1, 1\}$, para todo $1 \leq i \leq n$ y $1 \leq j \leq 2$. Si:

$$\frac{\mathbf{w}_1 + \mathbf{b}_1}{2} = \frac{\mathbf{w}_2 + \mathbf{b}_2}{2}$$

, entonces

$$\sum_{i=1}^{n}(x_{i1} + \mu_{i1}\mathbf{e}_i = \sum_{i=1}^{n}(x_{i2} + \mu_{i2}\mathbf{e}_i,$$

luego:

$$x_{i1} - x_{i2} = \mu_{i2} - \mu_{i1},$$

para todo $1 \leq i \leq n$. Como $-2 < x_{i1} - x_{i2} < 2, y \mu_{i2} - \mu_{i1} \in \{-2, 0, 2\}, tenemos que : x_{i1} - xi2 = \mu_{i2} - \mu_l i1 = 0, luego : \mathbf{w}_1 = \mathbf{w}_2$ y

$$\mathbf{b}_1 = \mathbf{b}_2,$$

y por lo tanto

$$|mid(W, vert(B))| = |W||vert(b)| = 2^n|W|.$$

Además de que

$$\frac{x_{ij} + \mu_{ij}}{2} \in (-1, 1)$$

, para todo $1 \leq i \leq n$, luego $\frac{\mathbf{w}_j + \mathbf{b}_j}{2} \in int(W)$; y por lo tanto $mid(W, vert(B)) \in int(B)$. □

**Lema 2.13.** *Sea $W$ un conjunto finito de $\mathbb{R}^n$, con $|W| = k$ y sea $\boldsymbol{v}$ un vector en $mid(W)$. Definimos $r_w(\boldsymbol{v})$ como el número de conjuntos $\{\boldsymbol{w}_1, \boldsymbol{w}_2\}$ de $W$ tales que:*

$$\frac{\boldsymbol{w}_1 + \boldsymbol{w}_2}{2} = \boldsymbol{v},$$

*entonces las siguientes propiedades se cumplen:*

1. $\frac{|W|(|W|+1}{2} = \sum_{\boldsymbol{v} \in mid(W)} r_W(\boldsymbol{v})$.
2. *Si $\boldsymbol{v}$ es un vector en $mid(W)$, tal que $r_W(\boldsymbol{v} = máx\,\{r_W(\boldsymbol{u} \mid \boldsymbol{u} \in mid(W)\}$, entonces $r_{A-\boldsymbol{v}(\boldsymbol{0}) = máx\,\{r_{A-v}(\boldsymbol{u}) \mid \boldsymbol{u} \in mid(A-\boldsymbol{v})}$.*

La demostración del lema es totalmente igual a la demostración de su versión en $R^2$. Ahora procederemos a generalizar el lema clave de la demostración del teorema $2^n$ de Freiman.

**Lema 2.14.** *Sea $n \geq 2$ y $1 < c < 2^n$. Definimos $\epsilon_0 = \epsilon_0(n,c) > 0$ y $k^* = k^*(n,c)$, como:*

$$\epsilon_0 = \frac{2^n - c}{4n(3^n c + 2nc + 1)(4c)^{2n-1}},$$

*y*

$$k^* = (4c)^{2n-1}.$$

*Sea $A$ un sunconjunto finito de $\mathbb{R}^n$ que satisface lo siguiente:*

$$|A| \geq k_0,$$

$$|2A| \geq c|A|$$

*y*

$$|A \cap H| \leq \epsilon_0 |A|,$$

*para todo hiperplano $H$ en $\mathbb{R}^n$, entonces existe un subconjunto $W$ de $A$, tal que:*

$$|W| \geq \epsilon_0 |A|$$

*y*

$$|2W| \leq (c - \epsilon_0)|W|.$$

*Demostración.* Sea $A$ un subconjunto finito de $\mathbb{R}^n$ que satisface las tres condiciones del lema. Probaremos por inducción que existen hiperplanos $H_1, \ldots, H_n$ en $\mathbb{R}^n$, y vectores $\mathbf{f}_0, \ldots, \mathbf{f}_{n-1}$ en $\mathbb{R}^n$, con $\mathbf{f}_0 = \mathbf{0}$, y conjuntos $A_1, \ldots, A_n$; tales que:

1. $\mathbf{f}_i \in H_j$, para todo $0 \leq i < j \leq n$.
2. $\mathbf{f}_i \in H_j^{(+1)}$ para todo $1 \leq j \leq i \leq n-1$.
3. $A_n \subset A_{n-1} \subset \ldots \subset A_1 \subset A_0 = A$.
4. $k_j = |A_j| > \frac{k_0}{(4c)^{2^j - 1}}$ para todo $1 \leq j \leq n$.
5. $A_j \subset \bigcap_{i=1}^{j} H_i^{(+1)}$, para todo $1 \leq j \leq n$.
6. $A_{j+1} \cup (\{2\mathbf{f}_j\} - A_{j+1}) \subset A_j$ para todo $0 \leq j \leq n-1$.

Sea $A_0 = A$ y $k_0 = |A_0|$. Sea $\mathbf{f}_0 \in A_0$ tal que

$$r_{A_0}(\mathbf{f}_0) = \text{máx } \{r_{A_0}(\mathbf{v}) \,|\, \mathbf{v} \in mid(A_0)\}.$$

Por el lema 2,13, tenemos que:

$$\begin{aligned} \frac{k_0^2}{2} &< \sum_{\mathbf{v} \in mid(A_0)} r_{A_0}(\mathbf{v}) \\ &\leq r_{A_0}(\mathbf{f}_0)|mid(A_0)| \\ &= r_{A_0}(\mathbf{f}_0)|2A_0| \\ &\leq r_{A_0}(\mathbf{f}_0)ck_0, \end{aligned}$$

luego:

$$r_{A_0}(\mathbf{f}_0) > \frac{k_0}{2c}.$$

Por el lema 2,13, podemos suponer que $\mathbf{f}_0 = \mathbf{0}$. Sea $H_1$ un hiperplano en $\mathbb{R}^n$ tal que $\mathbf{0} \in H_1$. Si $\frac{(\mathbf{w}_1+\mathbf{w}_2}{2} = \mathbf{0}$, entonces tenemos que $\{\mathbf{w}_1, \mathbf{w}_2\} \subset H_1$ o:

$$|\{\mathbf{w}_1, \mathbf{w}_2\} \cap H_1^{(+1)}| = |\{\mathbf{w}_1, \mathbf{w}_2\} \Cap H_1^{(-1)}| = 1.$$

Sea

$$A_1 = \{\mathbf{w} \in A_0 \,|\, \mathbf{w} \in H_1^{(-1)} \text{ y } 2\mathbf{0} - \mathbf{w} \in A_0\}.$$

Entonces:

$$A_1 \subset A_0 \Cap H_1^{(+1)} \subset H_1^{(+1)}$$

y

$$A_1 \cup (\{2\mathbf{0}\} - A_1) \subset A_0.$$

Como $|A_0 \cap H_1| \leq \epsilon_0 k_0$ y

$$\epsilon_0 < \frac{1}{(4c)^{4^n-1}} \leq \frac{1}{4c},$$

entonces:

$$\begin{aligned} k_1 = |A_1| &\geq r_{A_0}(\mathbf{0} - |A_0 \cap H_1| \\ &> \frac{k_0}{2c} - \epsilon_0 k_0 \\ &> \frac{k_0}{4c}. \end{aligned}$$

De lo anterior se infiere que $H_1, \mathbf{f}_0$ y $A_1$ satisfacen las 5 condiciones a demostrar.
Por hipótesis de inducción supongamos que, para todo $1 \leq m \leq n-1$, construimos los hiperplanos $H_1, \ldots, H_m$; los vectores $\mathbf{f}_0, \ldots, \mathbf{f}_{m-1}$ y los conjuntos $A_1, \ldots, A_m$ de manera recursiva; y además satisfacen las 5 condiciones requeridas. Como $A_m \subset \bigcap_{i=1}^{m} H_i^{(+1)}$ y como $\bigcap_{i=1}^{m} H_i^{(+1)}$ es convexo, tenemos por el la observación 2,5 que:

$$mid(A_m) \subset \bigcap_{i=1}^{m} H_i^{(+1)}.$$

De lo anterior, podemos escoger un vector
$textbf f_m \in mid(A_m)$, tal que:

$$r_{A_m}(\mathbf{f}_m) = \text{máx } \{r_{A_m}(\mathbf{v}) \,|\, \mathbf{v} \in mid(A_m)\}.$$

Luego obtenemos que:

$$\begin{aligned}\frac{1}{2}\left(\frac{k_0}{(4c)^{2^m-1}}\right)^2 &< \frac{k_m^2}{2}\\ &< r_{A_m}(\mathbf{f}_m)|mid(A_m)|\\ &\leq r_{A_m}(\mathbf{f}_m)|mid(A_0)|\\ &\leq r_{A_m}(\mathbf{f}_m)ck_0.\end{aligned}$$

luego obtenemos que:

$$r_{A_m}(\mathbf{f}_m) > \frac{2k_0}{(4c)^{2^{m+1}-1}}.$$

Sea $H_{m+1}$ un hiperplano en $\mathbb{R}^n$ tal que:

$$\{\mathbf{0}, \ldots, \mathbf{f}_m\} \subset H_{m+1}$$

Además sea:

$$A_{m+1} = \{\mathbf{w} \in A_m \,|\, \mathbf{w} \in H_{m+1}^{(+1)} \text{ y } 2\mathbf{f}_m - \mathbf{w} \in A_m\},$$

entonces:

$$A_{m+1} \subset A_m \cap H_{m+1}^{(+1)} \subset \bigcap_{i=1}^{m+1} H_i^{(+1)},$$

y

$$A_{m+1} \cup (\{2\mathbf{f}_m\} - A_{m+1}) \subset A_m.$$

Como

$$|A_m \cap H_{m+1}| \leq |A_0 \cap H_{m+1}| \leq \epsilon_0 k_0$$

y

$$\epsilon_0 < \frac{1}{(4c)^{4^n-1}} \leq \frac{1}{4c},$$

obtenemos que:

$$\begin{aligned}k_{m+1} &= |A_{m+1}|\\ &\geq r_{A_m}(\mathbf{f}_m) - |A_m \cap H_{m+1}|\\ &> \frac{2k_0}{(4c)^{2^{m+1}-1}} - \epsilon_0 k_0\\ &> \frac{k_0}{(4c)^{2^{m+1}-1}}\end{aligned}$$

Y por lo tanto los hiperplanos $H_1, \ldots, H_{m+1}$; los vectores $\mathbf{0}, \ldots, \mathbf{f}_m$ y los conjuntos $A_1, \ldots, A_{m+1}$ satisfacen las 5 propiedades requeridas. Y esto completa la inducción. Por otra parte sea $\mathbf{a} \in A_n$. Construimos los conjuntos:

$$S_n(\mathbf{a}) \subset S_{n-1}(\mathbf{a}) \ldots \subset S_0(\mathbf{a}) \subset A.$$

como en la definición 2,11 Nuevamente por inducción, probaremos que:

$$S_m(\mathbf{a}) \subset A_m \subset \bigcap_{i=1}^{m} H_i^{(+1)},$$

para toda $1 \leq m \leq n$. Claramente tenemos que:

$$S_n(\mathbf{a}) = \{\mathbf{a}\} \subset A_n \subset \bigcap_{i=1}^{n} H_i^{(+1)}.$$

Por hipótesis de inducción supongamos que:

$$S_{m+1}(\mathbf{a} \subset A_{m+1} \subset \bigcap_{i=1}^{m+1} H_i^{(+1)}$$

donde $0 \leq m \leq n-1$. Entonces:

$$\{2\mathbf{f}_m\} - S_{m+1}(\mathbf{a}) \subset \{2\mathbf{f}_m\} - A_{m+1} \subset A_m \subset \bigcap_{i=1}^{m} H_i^{(+1)},$$

luego obtenemos que:

$$S_m(\mathbf{a}) = S_{m+1}(\mathbf{a}) \cup (\{2\mathbf{f}_m\} - s_{m+1}(\mathbf{a})) \subset A_m \subset \bigcap_{i=1}^{m} H_i^{(+1)},$$

lo cual completa la inducción. De todo lo anterior, hemos demostrado que los hiperplanos $H_1, \ldots H_n$; los vectores $\mathbf{0}, \ldots, \mathbf{f}_{n-1}$; el conjunto $A_n \subset H(\underbrace{1, \ldots, 1}_{n})$ y los conjuntos:

$$\{S_k(\mathbf{a}) \,|\, \mathbf{a} \in A_n \text{ y } 0 \leq k \leq n\},$$

satisfacen las hipótesis del teorema 2,5 y por lo tanto existe vector $\mathbf{a}^* \in A_n$ tal que el bloque:

$$B(\mathbf{a}^*) = conv\left(S_0(\mathbf{a}^*)\right),$$

tiene la propiedad que:

$$\begin{aligned} |A \cap B(\mathbf{a}^*)| &\geq |\left(\bigcup_{\mathbf{a} \in A_n} S_0(\mathbf{a})\right) \cap B(\mathbf{a}^*)| \\ &\geq |A_n| \\ &= k_n \\ &> \frac{k_0}{(4c)^{2^n-1}} \end{aligned}$$

Por otra parte tenemos que el bloque $B(\mathbf{a}^*)$ determina los $2n$ hiperplanos faciales $F_{j,\mu_j}$, donde $1 \leq j \leq n$ y $\mu_j \in \{-1, 1\}$. Sea

$$F^* = \bigcup_{j=1}^{n} \bigcup_{\mu_j=1,-1} F_{j,\mu_j}.$$

Sea $W_0 = A \cap int\,(B(\mathbf{a}^*))$. Como $|A \cap H| \leq \epsilon_0 k_0$ para todo hiperplano $H$ y

$$\epsilon_0 < \frac{1}{4n(4c)^{2^n-1}},$$

obtenemos que:

$$|A \cap F^*| \leq 2n\epsilon_0 k_0,$$

luego:

$$\begin{aligned} |W_0| &= |A \cap int\,(B(a^*))\,| \\ &\geq |A \cap B(\mathbf{a}^*| - |A \cap F^*| \\ &> \frac{k_0}{(4c)^{2^n-1}} - 2n\epsilon_0 k_0 \\ > \frac{k_0}{2(4c)^{2^n-1}} \end{aligned}$$

Además como:

$$vert\,(B(\mathbf{a}^*)) = S_0(\mathbf{a}^*) \subset A,$$

y por del lema 2,12 tenemos que:

$$mid\,(W_0, S_0(\mathbf{a}^*)) = \{\frac{\mathbf{w}+\mathbf{s}}{2} \,|\, \mathbf{w} \in W_0, \mathbf{s} \in S_0(\mathbf{a}^*)\} \subset int\,(B(\mathbf{a}^*)) \cap mid(A)$$

y

$$|mid(W_0, S_0(\mathbf{a}^*))| = 2^n |W_0|.$$

Por otro lado los $2n$ hiperplanos faciales hacen una partición de $\mathbb{R}^n \setminus F^*$ en $3^n$ conjuntos convexos disjuntos por pares, llamemos $D(\lambda_1, \ldots, \lambda_n)$ a estos conjuntos, donde $(\lambda_1, \ldots, \lambda_n) \in \{-1, 0, 1\}^n$ y

$$D(0, \ldots, 0) = int(B(\mathbf{a}^*)).$$

Luego obtenemos que:

$$W_0 = A \cap int\,(B(\mathbf{a}^*)) = A \cap D(0, \ldots, 0)$$

y

$$mid(W_0, S_0(\mathbf{a}*)) \subset int\,(B(\mathbf{a}^*)) \cap mid(A) = D(0, \ldots, 0) \cap mid(A).$$

Sean $W_1, \ldots, W_{3^n-1}$ los conjuntos:

$$A \cap D(\lambda_1, \ldots, \lambda_n),$$

donde $(\lambda_1, \ldots, \lambda_n) \in \{-1, 0, 1\}^n$ y $(\lambda_1, \ldots, \lambda_n) \neq (0, \ldots, 0)$. Como los conjuntos $D(\lambda_1, \ldots, \lambda_n)$ son convexos, obtenemos que:

$$mid(W_i) \cap mid(W_j) = \emptyset$$

para todo $1 \leq i < j \leq 3^n - 1$ y

$$mid(W_0, S_0(\mathbf{a}^*)) \cap mid(W_i) = \emptyset,$$

para todo $1 \leq i \leq 3^n - 1$. Para terminar probaremos que existe $W_i$ tal que

$$|W_i| \geq \epsilon |A| = \epsilon_0 k_0,$$

y

$$|2W_i| = |mid(w_i)| \leq (c - \epsilon_0)|W_i|.$$

Por contradicción supongamos que $|mid(w_i)| > (c - \epsilon)|W_i|$ para todo $W_i$ que satisface que $|W_i| \geq \epsilon_0 k_0$. Sea $\Gamma$ la suma sobre todos los $i \in [1, 3^n - 1]$ tal que $|W_i| \geq \epsilon_0 k_0|$. Entonces:

$$\begin{aligned}
ck_0 \geq |2A| & = |mid(A)| \\
\geq |mid(w_0, S(\mathbf{a}^*))| + \sum_{i=1}^{3^n-1} |mid(w_i)| & \geq 2^n |W_0| + \Gamma |mid(W_i)| \\
\geq 2^n |W_0| + (c - \epsilon_0)\Gamma |W_i| & \\
> 2^n |W_0| + c\Gamma |W_i| - \epsilon_0 k_0 & \\
> (2^n - c)|W_0| + c \sum_{1=0}^{3^n-1} |W_i| - 3^n c \epsilon_0 k_0 - \epsilon_0 k_0 & \\
= (2^n - c)|W_0| + c(k_0 - |A \cap F^*|) - 3^n c \epsilon_0 k_0 - \epsilon_0 k_0 & \\
\geq (2^n - c)|W_0| + ck_0 - (3^n c + 2nc + 1)\epsilon_0 k_0 &
\end{aligned}$$

Lo anterior nos implica que:

$$(3^n c + 2nc + 1)\epsilon_0 k_0 > (2^n - c)|W_0| > \frac{(2^n - c)k_0}{2(4c)^{2^n - 1}},$$

luego obtenemos que:

$$\epsilon_0 > \frac{2^n - c}{2(3^n c + 2nc + 1)(4c)^{2^n - 1}} = 2n\epsilon_0 > \epsilon_0$$

lo cual es una contradicción y por lo tanto existe $W$ que satisface las condiciones del lema. $\square$

Ya para terminar la sección procederemos a demostrar el teorema objetivo en su forma general.

**Teorema 2.6** (Teorema $2^n$ de Freiman)**.** *Dados $n \geq 2$ entero, y $c$ un número real tal que $1 < c < 2^n$, existen constantes $k^* = k^*(n,c)$ y $\epsilon^* = \epsilon^*(n,c) > 0$, tales que si $A$ es un subconjunto finito de $\mathbb{R}^n$ que satisfice:*

1. $|A| \geq k^*$, *y*
2. $|A + A| \leq c|A|$,

*entonces existe un hiperplano $H'$ de $\mathbb{R}^n$ tal que $|A \cap H'| > \epsilon^*|A|$.*

*Demostración.* Para $1 < c < 2^n$, sea:

$$\epsilon_0 = \epsilon_0(n,c) = \frac{2^n - c}{4n(3^n c + 2nc + 1)(4c)^{2^n - 1)}}$$

El entero positivo definido en el lema 2,14. Sea $t = t(n,c)$ el único entero positivo tal que:

$$t - 1 < \frac{c-1}{\epsilon_0} \leq t.$$

Sea

$$\epsilon_0^* = \epsilon_0^t,$$
$$k^* = k^*(n,c) = (4c)^{2^n - 1}$$

y sea

$$k_0^* = k_0^*(n,c) = \epsilon_0^{-t} k^*.$$

Si $1 < c' < c$, entonces tenemos que:

$$\epsilon_0(n,c) < \epsilon(n,c')$$

y

$$k^*(n,c) > k^*(n,c').$$

Sea $A$ un subconjunto finito de $\mathbb{R}^n$ tal que:

$$|A| \geq k_0^* \geq k_0$$

y

$$|2A| \leq c|A|.$$

Supongamos por contradicción que:

$$|A \cap H| \leq \epsilon_0^*|A| \leq \epsilon_0|A|,$$

para todo hiperplano $H$ en $\mathbb{R}^n$. Por el lema 2,14, tenemos que existe un subconjuto $W$ de $A$, tal que

$$|W| \geq \epsilon_0|A| \geq \epsilon_0 k_0^* = \epsilon_0^{-1(t-1)} k^* \geq k^*$$

y

$$|2W| \leq (c - \epsilon_0)|W|.$$

Más aún, para todo hiperplano $H$ en $\mathbb{R}^n$, se tiene que:

$$|W \cap H| \leq |A \cap H| \leq \epsilon_0^t |A| \leq \epsilon_0^{t-1}|W| \leq \epsilon_0 |W|.$$

Definimos los conjuntos $A'_1 = W$ and $A'_0 = A$. Sea $i \leq j \leq t-1$ y sea $c' = c - j\epsilon_0$. Entonces si $j \leq t-1$, implica que $1 < c' = c - j\epsilon_0 < c$. Por las propiedades antes descritas podemos construir recursivamente, por el lema 2,14, conjuntos:

$$A'_j \subset A'_{j-1} \subset \ldots \subset A'_1 \subset A'_0 = A$$

tales que

$$|A'_j| \geq \epsilon_0^j |A| \geq \epsilon_0^j k_0^* \geq k^*$$

y

$$|2A'_j| \leq (c - j\epsilon_0)|A_j| = c'|A_j|.$$

Más aún, dichos conjuntos satisfacen que para todo hiperplano $H$ en $\mathbb{R}^n$, se tiene que:

$$\begin{aligned} |A'_j \cap H| &\leq |A \cap H| \\ &\leq \epsilon_0^* |A| \\ &\leq \epsilon_0^{t-j} |A'_j| \\ &\leq \epsilon_0 |A'_j| \\ &= \epsilon_0(n, c)|A'_j| \\ &< \epsilon_0(n, c')|A'_j|. \end{aligned}$$

Como

$$|A'_j| \geq k^* = k^*(n, c) > k^*(n, c'),$$

y

$$|2A'_j| \leq (c - j\epsilon_0)|A'_j| = c'|A'_j|.$$

Por lo anterior descrito, tenemos que $A'_j$ satisface las condiciones del lema 2,14, entonces existe $A'_{j+1}$ subconjunto de $A'_j$ tal que:

$$\begin{aligned} |A'_{j+1}| &\geq \epsilon_0(n, c')|A'_j| \\ &\epsilon_0(n, c)|A'_j| \\ &\epsilon_0^{j+1}|A| \\ &\epsilon_0^{j+1} k_0^* \\ &= \epsilon_0^{-(t-j-1)} k^* \qquad\qquad \geq k^* \end{aligned}$$

y además:

$$\begin{aligned} |2A'_{j+1} &\leq (c' - \epsilon_0(n, c'))|A_{j+1}| \\ &\leq (c' - \epsilon_0(n, c))|A'_{j+1}| \\ &= (c - (j+1)\epsilon)|A'_{j+1}|. \end{aligned}$$

Y así sucesivamente hasta llegar que $j = t$. Cuando $j = t$, obtenemos un conjunto $A'_t$ tal que:

$$|A'_t| \geq k^* > 1$$

y

$$|2A'_t| \leq (c - t\epsilon_0)|A'_t| \leq |A'_t|,$$

lo cual es una contradicción ya que si $|A'_t| > 1$, implica que

$$|2A'_t| > |A'_t|,$$

y por lo tanto existe un hiperplano $H$ de $\mathbb{R}^n$ tal que $|A \cap H| > \epsilon_0^*|A|$. □

# Capítulo 3

# Desigualdad de Brunn-Minkowski

En 1896 Hermann Minkowski demostró una desigualdad que relaciona el volumen de la suma de dos cuerpos convexos, en $\mathbb{R}^n$, con la suma del volumen de cada uno de ellos. Tal desigualdad había sido descubierta anteriormente (en 1887) por Hermann Brunn para el caso de $n = 3$, y es ahora conocida como la desigualdad de Brunn-Minkowski. La desigualdad es importante porque ha probado ser una herramienta poderosa tanto en análisis como en geometría convexa, y porque se relaciona con muchas otras desigualdades interesantes en matemáticas, [6].

## 3.1. Presentación de la desigualdad

Asumiremos en este capítulo que se conocen la definición y las propiedades básicas, tanto topológicas como de análisis, de la *medida de Lesbergue*; en el espacio euclidiano $n$-dimencional, la cual, denotaremos por $\mu$, es decir, $\mu$ es la función que asigna de manera estándar una medida a un subconjunto de $\mathbb{R}^n$ (por ejemplo, para $n = 1, 2$ o 3 dimensiones, $\mu$ determina la longitud, el área y el volumen, respectivamente). Además recordemos que un conjunto *compacto* es simplemente un conjunto cerrado y acotado.

**Definición 3.1.** *Sea $S$ un subconjunto de $\mathbb{R}^n$. Se dice que $S$ es un* cuerpo convexo *si $S$ es compacto, convexo, y tiene interior no vacío.*

**Ejemplo 3.1.** *En la figura* 3,1 *podemos observar:*

1. *Puntos y rectas no son cuerpos convexos ya que tienen interior vacío.*
2. *Semi-planos no son cuerpos por convexos por no ser acotados.*
3. *Un conjunto que no se cumple el ser convexo y por lo tanto no es un cuerpo convexo.*
4. *Un conjunto que sí es cuerpo convexo.*

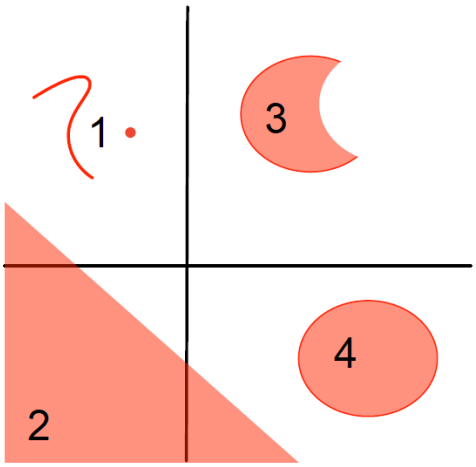



Figura 3.1: En estas figura podemos observar un conjunto que es un cuerpo convexo, (4), y conjuntos que no son cuerpos convexos, (1), (2), (3).

Ya que establecimos los elementos necesarios para la desigualdad de Brunn-Minkowski, procederemos a enunciarla.

**Teorema 3.1** (Desigualdad de Brunn-Minkowski)**.** *Si* $A, B \subset \mathbb{R}^n$ *son cuerpos convexos, entonces:*

$$\mu(A+B)^{1/n} \geq \mu(A)^{1/n} + \mu(B)^{1/n}.$$

En el caso de una dimensión, $n = 1$, los conjuntos $A$ y $B$ son intervalos cerrados en $\mathbb{R}$, con $\mu(A)$ y $\mu(B)$ sus respectivas longitudes. La desigualdad de Brunn-Minkowski, entonces, nos dice que:

$$\mu(A+B) \geq \mu(A) + \mu(B),$$

lo cual es claramente cierto y, de hecho, siempre se da la igualdad pues, dados $A = [a_1, a_2]$ y $B = [b_1, b_2]$, tenemos que:

$$\begin{aligned} \mu([a_1,a_2]+[b_1,b_2]) &= \mu([a_1+b_1, a_2+b_2]) \\ &= (a_2+b_2)-(a_1+b_1) \\ &= (a_2-a_1)+(b_2-b_1) \\ &= \mu([a_1,a_2]) + \mu([b_1,b_2]) \end{aligned}$$

En el caso de dos dimensiones, $n = 2$, los conjuntos $A$ y $B$ son conjuntos convexos, cerrados y acotados con interior no vacío (es decir, con área) en $\mathbb{R}^2$; de modo que, $\mu(A)$ y $\mu(B)$ son precisamente el área de $A$ y el área de $B$, respectivamente. La desigualdad de Brunn-Minkowski, entonces, es:

$$\mu(A+B) \geq \left(\sqrt{\mu(A)} + \sqrt{\mu(B)}\right)^2.$$

**Ejemplo 3.2.** *Consideremos dos rectangulos en* $\mathbb{R}^2$*: Un rectángulo* $A$ *cuya base y altura sean* $a_1$ *y* $a_2$ *respectivamente; y otro rectángulo* $B$ *cuya base y altura sean* $b_1$ *y* $b_2$ *respectivamente. Observemos que* $A+B$ *es un rectángulo cuya base es* $a_1+b_1$ *y altura es* $a_2+b_2$*. Calculando la medida de Lesbegue de los* 3 *rectángulos tenemos que:*

$$\begin{gathered}\mu(A)=a_1a_2;\\ \mu(B)=b_1b_2;\\ y\\ \mu(A+B)=(a_1+b_1)(a_2+b_2).\end{gathered}$$

*Observemos lo siguiente:*

$$\begin{gathered}\left(\sqrt{a_1b_2}-\sqrt{b_1a_2}\right)^2\geq 0\\ entonces,\\ a_1b_2+b_1a_2\geq 2\sqrt{a_1b_2b_1a_2}\\ luego,\\ a_1a_2+a_1b_2+b_1a_2+b_1b_2\geq a_1a_2+2\sqrt{a_1b_2b_1a_2}+b_1b_2\\ obteniendo,\\ (a_1+b_1)(a_2+b_2)\geq(\sqrt{a_1a_2}+\sqrt{b_1b_2})^2\end{gathered}$$

*De lo anterior tenemos que:*

$$\mu(A+B)\geq\left(\sqrt{\mu(A)}+\sqrt{\mu(B)}\right)^2.$$

*Además observemos que la igualdad se da si y sólo si:*

$$\begin{gathered}(\sqrt{a_1b_2}-\sqrt{b_1a_2})^2=0\\ entonces,\\ \sqrt{a_1b_2}=\sqrt{b_1a_2}\\ luego,\\ \frac{a_1}{b_1}=\frac{a_2}{b_2}\end{gathered}$$

*es decir, los lados del rectángulo* $B$ *son múltiplos escalares de los lados de* $A$*.*

En el ejemplo anterior vimos que la igualdad en la desigualdad de Brunn-Minkowski se da si y sólo si el rectángulo $A$ es una .ªmpliación.º reducción"del rectángulo $B$; de hecho esto siempre cumple para todo cuerpo convexo $A$ y $B$ y para todo $\mathbb{R}^n$. Formalmente cuando $A$ es una ampliación o reducción de $B$ decimos que $A$ y $B$ son dos cuerpos convexos homotéticos.

**Definición 3.2.** *Sean* $A$ *y* $B$ *dos cuerpos convexos en* $\mathbb{R}^n$*. Decimos que* $A$ *es homotético a* $B$*, si existe vector* $\boldsymbol{C}\in\mathbb{R}^n$ *y escalar* $k$*; tales que para todo* $\boldsymbol{a}\in A$ *existe un único* $\boldsymbol{b}\in B$ *tal que:*

$$\boldsymbol{b}-\boldsymbol{C}=k(\boldsymbol{a}-\boldsymbol{C}).$$

**Lema 3.1.** *Sean $A$ y $B$ dos cuerpos convexos en $\mathbb{R}^n$. La igualdad en el teorema* 3,1 *se cumple si y sólo si $A$ y $B$ son dos cuerpos convexos homotéticos.*

## 3.2. La desigualdad de Bonnesen

En 1929 Bonnesen demuestra una desigualdad que es mejor a la de Brunn-Minkowski.

**Teorema 3.2** (Desigualdad de Bonnesen)**.** *Si $A, B \subset \mathbb{R}^n$ son cuerpos convexos, y $H$ es un subespacio de dimensión $n-1$, entonces:*

$$\mu(A+B) \geq \left(m^{\frac{1}{n-1}} + n^{\frac{1}{n-1}}\right)^{n-1} \left(\frac{\mu(A)}{m} + \frac{\mu(B)}{n}\right),$$

*donde $m = \mu\left(\phi_H(A)\right)$ y $n = \mu\left(\phi_H(B)\right)$.*

Notemos que como $H$ es un subespacio de dimensión $n-1$, entonces $\mathbb{R}^n/H$ es un espacio de dimensión uno (una recta); y como $A$ y $B$ son cuerpos convexos, entonces $\phi_H(A)$ y $\phi_H(B)$ son intervalos cerrados con $\mu\left(\phi_H(A)\right)$ y $\mu\left(\phi_H(B)\right)$ sus longitudes respectivamente.

En el caso de una dimensión, $n = 1$, la desigualdad de Bonnesen se interpreta tomando el límite de los coeficientes de $\mu(A)$ y $\mu(B)$, obteniendose: $\mu(A+B) \geq \mu(A) + \mu(B)$, que es exactamente la desigualdad de Brunn-Minkowski (y que, como ya vimos, en este caso se da siempre la igualdad).

En el caso de dos dimensiones, $n = 2$, la desigualdad de Bonnesen nos dice que

$$\mu(A+B) \geq (m+n)\left(\frac{\mu(A)}{m} + \frac{\mu(B)}{n}\right), \tag{3.1}$$

donde $m$ y $n$ son las longitudes de las respectivas proyecciones de $A$ y $B$ a alguna recta en $\mathbb{R}^2$ que pase por el origen.

# Capítulo 4

# La suma de conjuntos finitos en $\mathbb{R}^2$

En el artículo *Properties of two-dimensional sets with small sumset*,[7], los autores estudian la cardinalidad del conjunto suma de dos conjuntos finitos, en términos del mínimo número de lineas paralelas que cubren a cada uno; concretamente, entre otros resultados, se prueba la siguiente desigualdad. Denotamos por $h_1(A, B)$ al mínimo $s$ tal que existe $\mathbf{u} \in \mathbb{R}^2$ con $|\phi_{\langle \mathbf{u} \rangle}(A)| \leq s$ y $|\phi_{\langle \mathbf{u} \rangle}(B)| \leq s$.

**Teorema 4.1.** *[Grynkiewicz, Serra, 2010] Sea $s \geq 2$ un entero, y sean $A$ y $B$ conjuntos finitos en $\mathbb{R}^2$ tales que $|A| \geq |B| \geq 2s^2 - 3s + 2$. Si $h_1(A, B) \geq s$ entonces*

$$|A + B| \geq |A| + \left(3 - \frac{2}{s}\right)|B| - 2s + 1.$$

Este resultado extiende el caso 2-dimensional del teorema $2^n$ de Freiman, considerando la suma de dos conjuntos distintos en vez de uno.

Para probar el teorema 4.1, los autores establecen otra cota inferior general de $|A + B|$ (donde $A$ y $B$ son conjuntos finitos de $\mathbb{R}^2$) que, en la actualidad, es considerada la mejor versión discreta de la desigualdad de Brunn-Minkowski en dos dimensiones. En este capítulo presentaremos dicha desigualdad (teorema 4.4) y daremos su prueba. También presentaremos, en la sección 4.3, una generalización al teorema 4.4, lo cual es trabajo original.

## 4.1. Compresión de conjuntos

Antes de presentar la desigualdad de Grynkiewicz-Serra, veremos una técnica bastante usada en el área, llamada *compresión de conjuntos*[8]. Dados dos conjuntos finitos $A$ y $B$ en $\mathbb{R}^n$, queremos determinar conjuntos $\mathbf{C}(A)$ y $\mathbf{C}(B)$ de modo que $|A| = |\mathbf{C}(A)|$, $|B| = |\mathbf{C}(B)|$ y $|A + B| \geq |\mathbf{C}(A) + \mathbf{C}(B)|$, con la condición adicional de que sea más fácil calcular $|\mathbf{C}(A) + \mathbf{C}(B)|$ que $|A + B|$.

En general, se define la compresión de un conjunto en $\mathbb{R}^n$ con respecto a una base ordenada $(\mathbf{v}_1, \cdots, \mathbf{v}_n)$. Sin embargo, en este trabajo de tesis estudiaremos la compresión de conjuntos unicamente en $\mathbb{R}^2$. Antes de ver la definición de compresión con respecto a cualquier base

ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ de $\mathbb{R}^2$, daremos la definición para el caso particular en que la base sea la base canónica, $(\mathbf{e}_1, \mathbf{e}_2)$. Notemos que, en tal caso, siendo $S$ un subconjunto finito de $\mathbb{R}^2$, $|\phi_{\langle \mathbf{e}_1 \rangle}(S)|$ es el número de rectas paralelas al eje $x$ que intersectan a $S$, y $|\phi_{\langle \mathbf{e}_2 \rangle}(S)|$ es el número de rectas paralelas al eje $y$ que intersectan a $S$. Definiremos primero la compresión lineal de un conjunto finito $S$ con respecto a $\mathbf{e}_i$ para cada $i \in \{1, 2\}$.

**Definición 4.1.** *Sea $S$ un subconjunto finito de $\mathbb{R}^2$, y sea $\boldsymbol{e}_1 = (1, 0)$. Sea $q = |\phi_{\langle \boldsymbol{e}_1 \rangle}(S)|$, y sean $y_1, y_2, \ldots, y_q \in \mathbb{R}$ precisamente los valores tales que $S \cap ((0, y_j) + \langle \boldsymbol{e}_1 \rangle) \neq \emptyset$. Entonces la* compresión lineal de $S$ con respecto a $\mathbf{e}_1$*, denotada por $\boldsymbol{C}_{\boldsymbol{e}_1}(S)$, se define como:*

$$\boldsymbol{C}_{\boldsymbol{e}_1}(S) = \bigcup_{j=1}^{q} \{(k, y_j) \,|\, 0 \leq k \leq r_j - 1\},$$

*donde $r_j = |S \cap ((0, y_j) + \langle \boldsymbol{e}_1 \rangle)|$ para cada $1 \leq j \leq q$.*

**Ejemplo 4.1.** *Sea $S = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,2)\}$ como en el ejemplo* 2,1*. Notemos que para este conjunto $S$, tenemos que $q = 3$ y además que $y_1 = 1$, $y_2 = 2$ y $y_3 = 4$. De modo que $r_1 = 2$, $r_2 = 3$ y $r_3 = 1$ y por lo tanto:*

$$\boldsymbol{C}_{\langle \boldsymbol{e}_1 \rangle}(S) = \{(0,1), (1,1), (0,2), (1,2), (2,2), (0,4)\};$$

*como se puede apreciar en la figura* 4,1

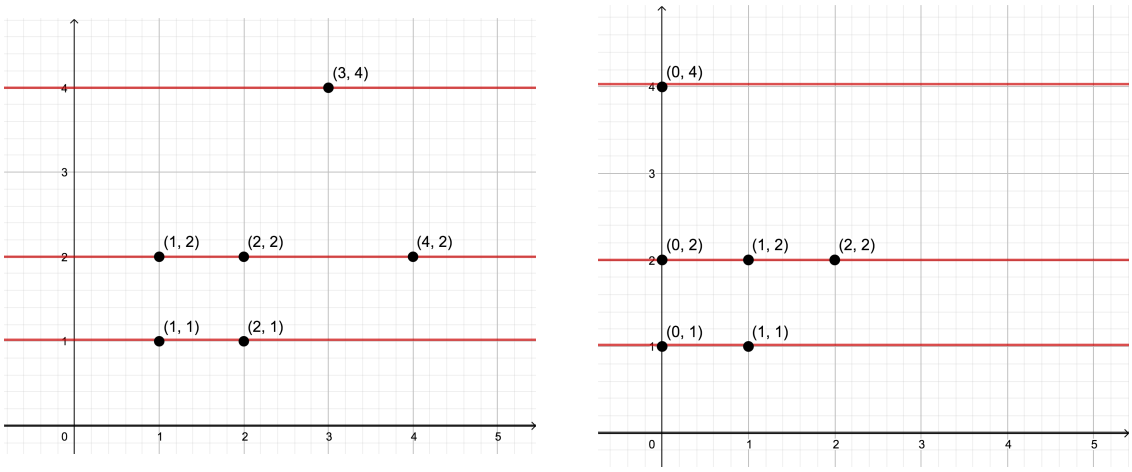



Figura 4.1: Conjuntos $S$ y $\mathbf{C}_{\langle \mathbf{e}_1 \rangle}(S)$.

En el ejemplo anterior, todos los puntos de $S$ tienen coordenadas enteras y por lo tanto los escalares $y_1, y_2, \ldots, y_q$ también resultaron ser números enteros, lo cual no necesariamente es así. Sin embargo, es importante notar que aunque $S$ contenga puntos con coordenadas no enteras, la compresión $\mathbf{C}_{\langle \mathbf{e}_1 \rangle}(S)$ siempre será un conjunto con coordenadas enteras.

**Definición 4.2.** *Sea $S$ un subconjunto finito de $\mathbb{R}^2$, y sea $\boldsymbol{e}_2 = (0,2)$. Sea $p = |\phi_{\langle \boldsymbol{e}_2 \rangle}(S)|$, y sean $x_1, x_2, \ldots, x_p$ precisamente los valeres tales que $S \cap (\langle \boldsymbol{e}_2 \rangle + (x_j, 0)) \neq \emptyset$. Entonces la* compresión lineal de $S$ con respecto a $\mathbf{e}_2$, *denotada por $\boldsymbol{C}_{\boldsymbol{e}_2}(S)$, se define como:*

$$\boldsymbol{C}_{\boldsymbol{e}_2}(S) = \bigcup_{j=1}^{p} \{(x_j, k) \,|\, 0 \leq k \leq r_j - 1\},$$

*donde $r_j = |S \cap (\langle \boldsymbol{e}_2 \rangle + (x_j, 0))\,|$ para cada $1 \leq j \leq p$.*

**Ejemplo 4.2.** *Sea $S = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,2)\}$ como en el ejemplo* 2,1. *Notemos que para este conjunto $S$, tenemos que $p = 4$ y además que $x_1 = 1$, $x_2 = 2$, $y_3 = 3$ y $x_4 = 4$. De modo que $r_1 = 2$, $r_2 = 2$, $r_3 = 1$ y $r_4 = 1$, y por lo tanto:*

$$\boldsymbol{C}_{\langle \boldsymbol{e}_1 \rangle}(S) = \{(1,0), (2,1), (2,0), (2,1), (3,0), (4,0)\};$$

*como se puede apreciar en la figura* 4,2

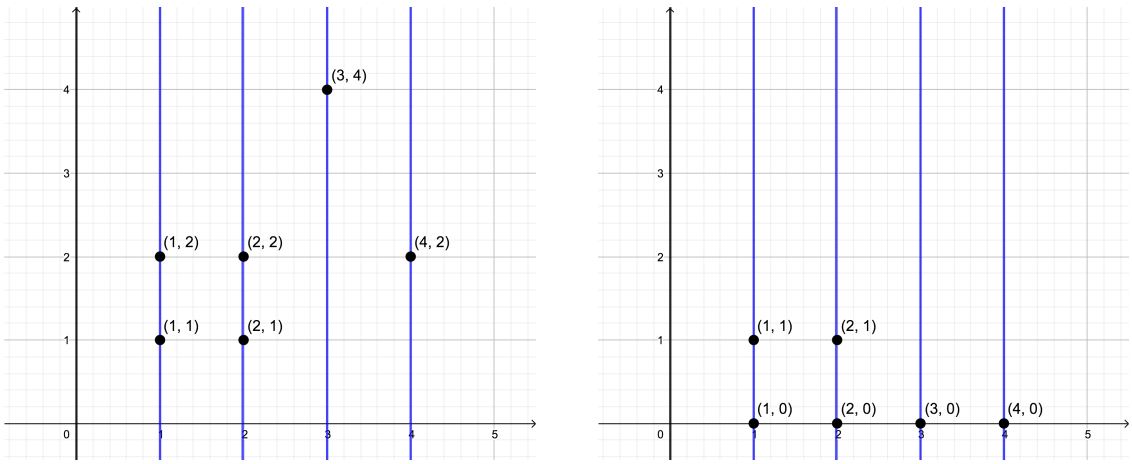



Figura 4.2: Conjuntos $S$ y $\mathbf{C}_{\langle \mathbf{e}_2 \rangle}(S)$.

Ahora, definimos la compresión de un conjunto finito $S$ con respecto a la base ordenada $(\mathbf{e}_1, \mathbf{e}_2)$ como sigue.

**Definición 4.3.** *Sea $S$ un subconjunto finito de $\mathbb{R}^2$. La* compresión de $S$ con respecto a la base canónica ordenada $(\mathbf{e}_1, \mathbf{e}_2)$, *denotada por $\boldsymbol{C}(S) = \boldsymbol{C}_{(\boldsymbol{e}_1, \boldsymbol{e}_2)}(S)$, se define como:*

$$\boldsymbol{C}(S) = \boldsymbol{C}_{\boldsymbol{e}_2}(\boldsymbol{C}_{\boldsymbol{e}_1}(S)).$$

**Ejemplo 4.3.** *Sea $S = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,2)\}$ como en los ejemplos anteriores, y sea $(\boldsymbol{e}_1, \boldsymbol{e}_2)$ la base canónica ordenada. Entonces tenemos que:*

$$\boldsymbol{C}(S) = \{(0,0), (0,1), (0,2), (1,0), (1,1), (2,0)\}.$$

*Notemos que es importante que la base sea ordenada, ya que si tomamos ahora la base ordenada* $(\boldsymbol{e}_2, \boldsymbol{e}_1)$*, entonces:*

$$\boldsymbol{C}(S) = \{(0,0), (0,1), (1,0), (1,1), (2,0), (3,0)\},$$

*y por lo tanto ambas compresiones son distintas como se puede observar en la figura* 4,3

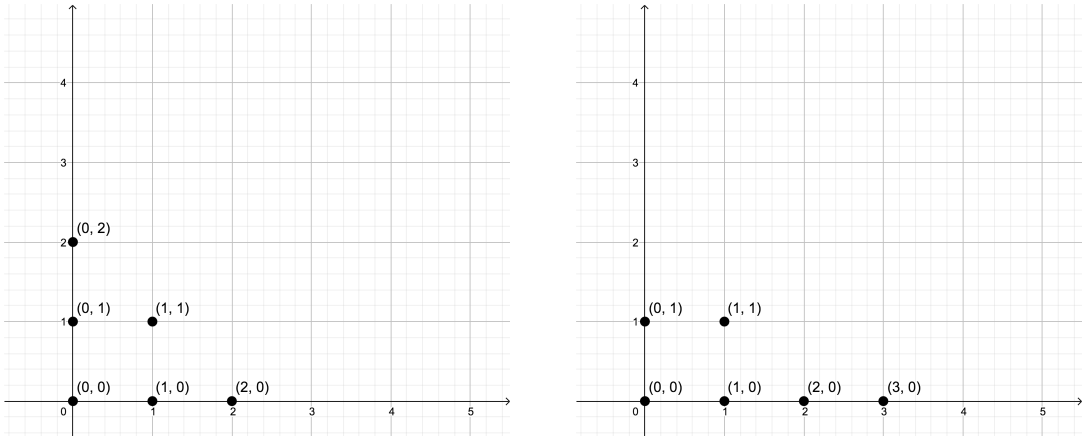



Figura 4.3: Compresiones del conjunto $S$ con respecto a las bases ordenadas $(\mathbf{e}_1, \mathbf{e}_2)$ y $(\mathbf{e}_2, \mathbf{e}_1)$ respectivamente.

Finalmente, definimos la compresión de un conjunto finito $S$ con respecto a cualquier base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ de $\mathbb{R}^2$, como sigue.

**Definición 4.4.** *Sea* $S$ *un subconjunto finito de* $\mathbb{R}^2$*, y sea* $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ *una base ordenada de* $\mathbb{R}^2$*. Para* $i \in \{1, 2\}$ *definimos primero, por pedazos, la* compresión lineal de $S$ con respecto a $\mathbf{v}_i$*. Sea* $j \in \{1, 2\}$*,* $j \neq i$*, entonces* $\boldsymbol{C}_i(S)$ *es el conjunto que satisface, para cada* $\boldsymbol{u} \in \langle \boldsymbol{v}_j \rangle$*, lo siguiente*

$$\boldsymbol{C}_i(S) \cap (\langle \boldsymbol{v}_i \rangle + \boldsymbol{u}) = \{0, \boldsymbol{v}_i, 2\boldsymbol{v}_i, \cdots, (r-1)\boldsymbol{v}_i\} + \boldsymbol{u},$$

*donde* $r = |S \cap (\langle \boldsymbol{v}_i \rangle + \boldsymbol{u})|$*, y en caso de que* $r = 0$ *consideramos* $\boldsymbol{C}_i(S) \cap (\langle \boldsymbol{v}_i \rangle + \boldsymbol{u}) = \emptyset$*. La* compresión de $S$ con respecto a la base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ *se define entonces como:*

$$\boldsymbol{C}(S) = \boldsymbol{C}_2(\boldsymbol{C}_1(S)).$$

**Ejemplo 4.4.** *Sea* $S = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,2)\}$ *como en los demás ejemplos, y sean* $\boldsymbol{v}_1 = (2,1)$ *y* $\boldsymbol{v}_2 = (1,1)$ *dos vectores en* $\mathbb{R}^2$*. Calcularemos la compresión de* $S$ *respecto a la base* $(\boldsymbol{v}_1, \boldsymbol{v}_2)$*. Observemos primero que:*

$$\boldsymbol{C}_1(S) = \{(0,0), (1,1), (2,2), (3,3), (5,5), (2,1)\},$$

*y por lo tanto:*

$$\boldsymbol{C}(S) = \boldsymbol{C}_2(\boldsymbol{C}_1(S)) = \{(0,0), (1,1), (2,2), (3,3), (4,4), (2,1)\}.$$

*En la figura* 4,5 *podemos observar estos conjuntos.*

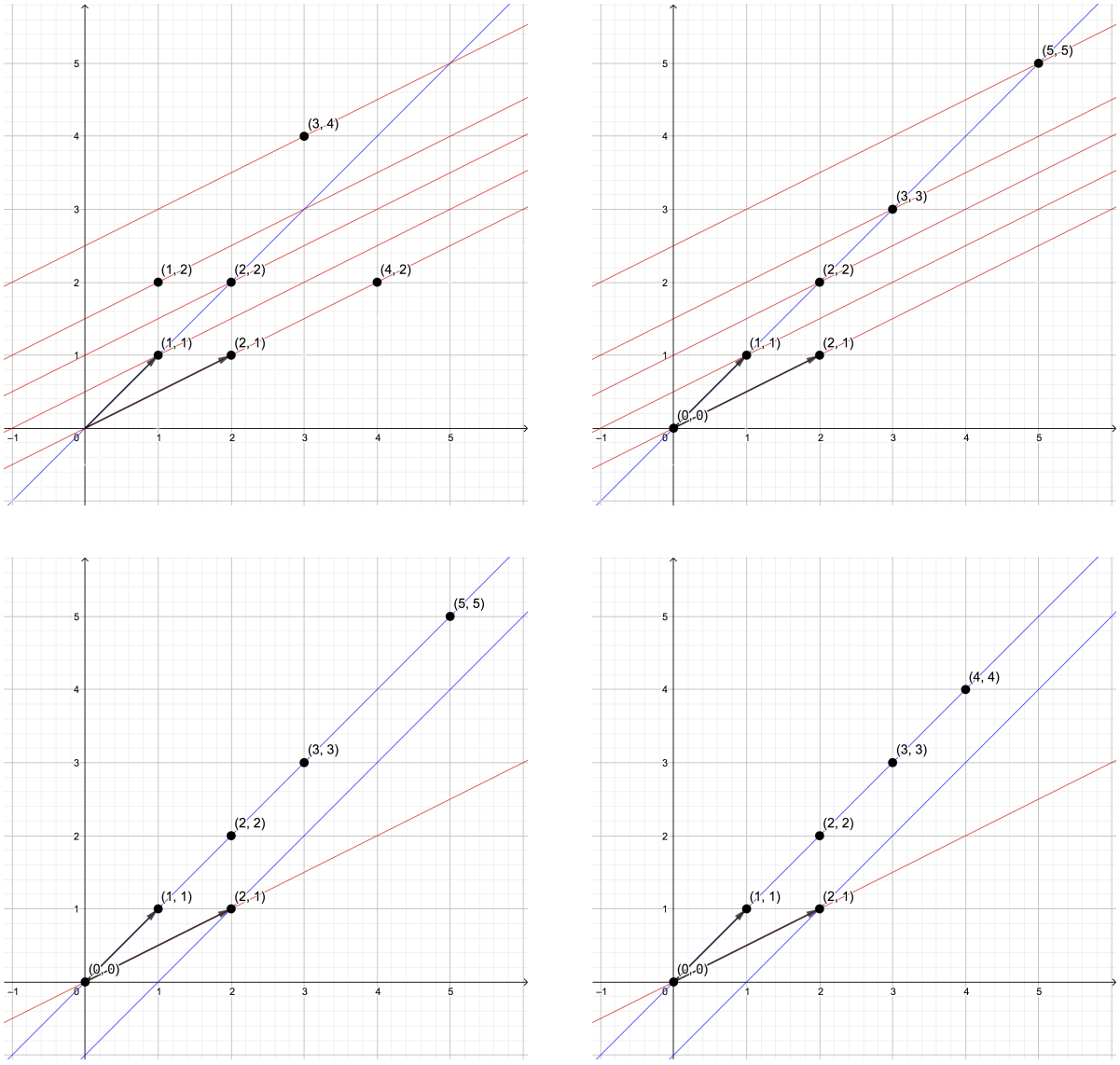



Figura 4.5: Compresión del conjunto $S$ respecto a la base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ donde $\mathbf{v}_1 = (2, 1)$ y $\mathbf{v}_2 = (1, 1)$; primero se muestra se muestra $\mathbf{C}_1(S)$ y después $\mathbf{C}(S) = \mathbf{C}_2(\mathbf{C}_1(S))$.

No es difícil ver que si $(\mathbf{v}_1, \mathbf{v}_2) = (\mathbf{e}_1, \mathbf{e}_2)$, entonces la definición 4.4 coincide con la definición 4.3. De modo que, tal como vimos en el ejemplo 4.3, la compresión de un conjunto $S$ con respecto a una base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ no necesariamente es igual a compresión del mismo conjunto con respecto a la base ordenada $(\mathbf{v}_2, \mathbf{v}_1)$. Sin embargo, para cualquier conjunto finito $S \subset \mathbb{R}^2$ y para cualquier base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ tenemos que

$$|S| = |\mathbf{C}(S)|. \tag{4.1}$$

También es importante notar que si $\mathbf{C}(S)$ es la compresión de un conjunto $S$ con respecto a la base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$, entonces:

$$|\phi_{\mathbf{v}_1}(S)| = |\phi_{\mathbf{v}_1}(\mathbf{C}(S))|, \tag{4.2}$$

lo cual no es necesariamente cierto con respecto a $\mathbf{v}_2$; es decir, cuando hacemos la proyección con respecto a la base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$ el número de rectas paralelas a $\langle \mathbf{v}_1 \rangle$ que intersectan al conjunto $S$ es igual al número de rectas paralelas a $\langle \mathbf{v}_1 \rangle$ que intersectan al conjunto $\mathbf{C}(S)$, mientras que el número de rectas paralelas a $\langle \mathbf{v}_2 \rangle$ que intersectan al conjunto $S$ no es necesariamente igual al número de rectas paralelas a $\langle \mathbf{v}_2 \rangle$ que intersectan al conjunto $\mathbf{C}(S)$.

A continuación demostraremos los dos teoremas básicos que justifican la utilidad de la compresión de conjuntos, y para ello necesitaremos dos teoremas importantes en la literatura. EL primero es el que sigue

**Teorema 4.2** (Folklore 1)**.** *Sean $A$ y $B$ subconjuntos finitos (no vacíos) de un grupo abeliano sin torsión. Entonces,*

$$|A + B| \geq |A| + |B| - 1,$$

*Demostración.* La demostración será por inducción sobre mín $\{$máx $A -$ mín $A,$ máx $B -$ mín $B\}$. Sin pérdida de generalidad asumiremos que máx $A -$ mín $A \leq$ máx $B -$ mín $B$. Si máx $A -$ mín $A = 0$, entonces $A + B$ es una traslación de $B$ y la igualdad es trivial en este caso. De lo anterior podemos asumir que $0 <$ máx $A -$ mín $A \leq$ máx $B -$ mín $B$ y que la afirmación es cierta para cualquier par de subconjuntos $(A', B')$ de $G$ no vacíos y finitos con mín $\{$máx $A' -$ mín $A',$ máx $B' -$ mín $B'\} <$ máx $A -$ mín $A$. Definimos los siguientes conjuntos:

$$A' = A \cap (B + \{\text{máx } A - \text{mín } B\})$$

$$y$$

$$B' = (A + \{\text{mín } B - \text{máx } A\}) \cup B.$$

Primero notemos que:

$$A' = \{\text{máx } A\} \tag{4.3}$$

Además de que:

$$|A'| + |B'| = |A| + |B|. \tag{4.4}$$

Dado que $(A + \{\text{mín } B - \text{máx } A\}) + (B + \{\text{máx } A - \text{mín } B\}) \subset A + B$, obtenemos que:

$$A' + B' \subset A + B. \tag{4.5}$$

Por las ecuaciones 4,3, 4,4 u 4,5, podemos aplicar la hipótesis de inducción, llegando a que:

$$\begin{aligned} |A| + |B| - 1 &= |A'| + |B'| - 1 \\ &\leq |A' + B'| \\ &\leq |A + B| \end{aligned}$$

Que es lo que se quería demostrar. □

Antes de enunciar y demostrar el segundo teorema, demostraremos un caso especial de él.

**Lema 4.1.** *Sean $A$ y $B$ subconjuntos finitos (no vacíos) de un grupo abeliano sin torsión, tales que $2 \leq |A| = |B|$. Si*

$$|A + B| = |A| + |B| - 1,$$

*entonces $A$ y $B$ son progresiones aritméticas de la misma diferencia.*

*Demostración.* Sea $A = \{a_1 \ldots, a_k\}$ y $B = \{b_1, \ldots, b_k\}$, con $a_1 < \ldots < a_k$ y $b_1 < \ldots < b_k$. Observemos que $A + B$ contiene los siguientes $2k - 1$ enteros distintos:

$$a_1 + b_1, a_1 + b_2, a_2 + b_2, a_2 + b_3, \ldots, a_{i-1} + b_i, a_i + b_i, a_i + b_{i+1}, a_{i+1} + b_{i+1} \ldots, a_k + b_k.$$

Como $|A+B| = 2k-1$m entonces tenemos que todos los elementos de $A+B$ están incluidos en la lista anterior. Observemos lo siguiente:

$$a_{i-1} + b_i < a_i + b_i < a_i + b_{i+1},$$

y

$$a_{i-1} + b_i < a_{i-1} + b_{i+1} < a_i + b_{i+1},$$

de lo anterior tenemos que:

$$a_{i-1} + b_{i+1} = a_i + b_i$$

, es decir:

$$a_i - a_{i-1} = b_{i+1} - b_i,$$

para todo $2 \leq i \leq k$. Análogamente con las desigualdades:

$$a_{i-1} + b_{i-1} < a_{i-1} + b_i < a_i + b_i,$$

y

$$a_{i-1} + b_{i-1} < a_i + b_{i-1} < a_i + b_i,$$

obtenemos que:

$$a_i - a_{i-1} = b_i - b_{i-1},$$

para todo $2 \leq i \leq k$ y por lo tanto $A$ y $B$ son progresiones aritméticas de la misma diferencia. □

Ahora sí procederemos a demostrar el segundo teorema básico.

**Teorema 4.3** (Folklore 2)**.** *Sean $A$ y $B$ dos subconjuntos finitos (no vacíos) de un grupo abeliano sin torsión. Entonces:*

$$|A + B| = |A| + |B| - 1$$

*si y sólo si $A$ y $B$ son progresiones aritméticas de la misma diferencia, o bien, mín $\{|A|, |B|\} = 1$.*

*Demostración.* Podemos observar que si mín $\{|A|, |B|\} = 1$, la igualdad en el teorema se da facilmente. Sea $|A| = n$ y $|B| = m$. Si $A$ y $B$ son progresiones aritméticas de la misma distancia podemos escribir tanto a $A$ como a $B$ de la siguiente manera:

$$A = \{a_0 + id \,|\, 0 \leq i \leq n-1\}$$

$$y$$

$$B = \{b_0 + jd \,|\, 0 \leq i \leq m-1\}.$$

Observemos que, entonces $A + B$ se puede escribir como:

$$\begin{aligned} A + B &= \{a_0 + b_0 + (i+j)d \,|\, 0 \leq i \leq n-1 \text{ y } 0 \leq j \leq m-1\} \\ &= \{a_0 + b_0 + kd \,|\, 0 \leq k \leq m+n-2\}. \end{aligned}$$

De lo anterior obtenemos que $|A + B| = m + n - 1$, es decir:

$$|A + B| = |A| + |B| - 1.$$

Ahora supongamos que $|A + B| = |A| + |B| - 1$. Sea $A = \{a_1, \ldots, a_n\}$ y $B = \{b_1, \ldots, b_m\}$, con $a_1 < \ldots < a_n$ y $b_1 < \ldots < b_m$. Sin pérdida de generalidad supongamos que $2 \leq n \leq m$. Sea $0 \leq t \leq m - n$. Definimos los conjuntos:

$$\begin{aligned} B_0^{(t)} &= \{b_1, \ldots, b_t\}, \\ B_1^{(t)} &= \{b_{t+1}, \ldots, b_{t+n}\} \\ B_2^{(t)} &= \{b_{t+n+1}, \ldots, b_m\} \end{aligned}$$

Observemos que $B = B_0^{(t)} \cup B_1^{(t)} \cup B_2^{(t)}$. De dichos conjuntos tenemos que:

$$\left(a_0 + B_0^{(t)}\right) \cup \left(A + B_1^{(t)}\right) \cup \left(a_n + B_2^{(t)}\right) \subset A + B \tag{4.6}$$

además de que los conjuntos $\left(a_0 + B_0^{(t)}\right), \left(A + B_1^{(t)}\right), \left(a_n + B_2^{(t)}\right)$ son ajenos por pares. Ahora observemos que:

$$\begin{aligned} a_0 + B_0^{(t)} &\subset [a_1 + b_1, a_1 + b_t], \\ A + B_1^{(t)} &\subset [a_1 + b_{t+1}, a_n + b_{t+n}] \\ a_n + B_2^{(t)} &\subset [a_n + b_{t+n+1}, a_n + b_m], \end{aligned}$$

Más aún:

$$\begin{aligned} |a_1 + B_0^{(t)}| &= t, \\ |A + B_1^{(t)} &\geq |A| + |B_1^{(t)}| - 1 = 2k - 1, \\ |a_n + B_2^{(t)}| &= m - t + n. \end{aligned}$$

De lo anterior tenemos que:

$$\begin{aligned} m+n-1 &= |A+B| \\ &\geq |a_1 + B_0^{(t)}| + |A + B_1^{(t)}| + |a_n + B_2^{(t)}| \\ &\geq t + (2k-1) + (m-t-n) \\ &= m+n-1, \end{aligned}$$

luego:

$$|A + B_1^{(t)}| = 2k-1,$$

para toda $0 \leq t \leq m-n$. Por el lema 4,1 tanto $A$ como $B_1^{(t)}$ son progresiones aritméticas de la misma diferencia, para toda $0 \leq t \leq m-n$. Y por lo tanto $B$ también es una progresión aritmética de la misma diferencia que $A$. □

Antes de continuar requerimos establecer la siguiente notación. Dado un conjunto finito $S \subset \mathbb{R}^2$ y una base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$, para cada $\mathbf{u} \in \langle \mathbf{v}_2 \rangle$ definimos $S_{\mathbf{u}} = S \cap (\langle \mathbf{v}_1 \rangle + \mathbf{u})$. Observemos que

$$|S| = \sum_{\mathbf{u} \in \langle \mathbf{v}_2 \rangle} |S_{\mathbf{u}}|. \tag{4.7}$$

**Lema 4.2.** *Sean $A$ y $B$ dos conjuntos finitos de $\mathbb{R}^2$, y sean $\boldsymbol{C}(A)$ y $\boldsymbol{C}(B)$ sus respectivas compresiones con respecto a una base ordenada $(\boldsymbol{v}_1, \boldsymbol{v}_2)$. Entonces,*

$$|A+B| \geq |\boldsymbol{C}(A) + \boldsymbol{C}(B)|.$$

*Demostración.* Consideremos $A, B \subset \mathbb{R}^2$ finitos, y su conjunto suma $A+B$. Notemos que si $\mathbf{c} \in (A+B)_{\mathbf{u}}$ para algún $\mathbf{u} \in \langle \mathbf{v}_2 \rangle$, entonces $\mathbf{c} = \mathbf{a} + \mathbf{b}$ donde $\mathbf{a} \in A \cap (\langle \mathbf{v}_1 \rangle + \mathbf{w})$ y $\mathbf{b} \in B \cap (\langle \mathbf{v}_1 \rangle + \mathbf{w'})$ con $\mathbf{w} + \mathbf{w'} = \mathbf{u}$. De este modo, para cada $\mathbf{u} \in \langle \mathbf{v}_2 \rangle$ tal que $(A+B)_{\mathbf{u}} \neq \emptyset$ tenemos:

$$(A+B)_{\mathbf{u}} = \bigcup_{A_{\mathbf{w}} \neq \emptyset, B_{\mathbf{u}-\mathbf{w}} \neq \emptyset} (A_{\mathbf{w}} + B_{\mathbf{u}-\mathbf{w}}),$$

de modo que:

$$|(A+B)_{\mathbf{u}}| \geq \text{máx}\{|A_{\mathbf{w}} + B_{\mathbf{u}-\mathbf{w}}| : A_{\mathbf{w}} \neq \emptyset, B_{\mathbf{u}-\mathbf{w}} \neq \emptyset\}. \tag{4.8}$$

De la ecuación (4.7) tenemos que:

$$\begin{aligned} |A+B| &= \sum_{\mathbf{u} \in \langle \mathbf{v}_2 \rangle} |(A+B)_{\mathbf{u}}| \\ &\geq \sum_{\mathbf{u} \in \langle \mathbf{v}_2 \rangle} \text{máx}\{|A_{\mathbf{w}} + B_{\mathbf{u}-\mathbf{w}}| : A_{\mathbf{w}} \neq \emptyset, B_{\mathbf{u}-\mathbf{w}} \neq \emptyset\} \\ &\geq \sum_{\mathbf{u} \in \langle \mathbf{v}_2 \rangle} \text{máx}\{|A_{\mathbf{w}}| + |B_{\mathbf{u}-\mathbf{w}}| - 1 : A_{\mathbf{w}} \neq \emptyset, B_{\mathbf{u}-\mathbf{w}} \neq \emptyset\}, \end{aligned} \tag{4.9}$$

donde la primera desigualdad se implica de (4.8) y la segunda desigualdad se obtiene por el teorema 4.2.

Consideremos ahora los conjuntos $\mathbf{C}_1(A)$ y $\mathbf{C}_1(B)$ con respecto a la base ordenada $(\mathbf{v}_1, \mathbf{v}_2)$. Por definición, para cada $\mathbf{u} \in \langle \mathbf{v}_2 \rangle$, tenemos que:

$$(\mathbf{C}_1(A))_{\mathbf{u}} = \mathbf{C}_1(A) \cap (\langle \mathbf{v}_1 \rangle + \mathbf{u}) = \{0, \mathbf{v}_1, 2\mathbf{v}_1, \cdots, (|A_{\mathbf{u}}| - 1)\mathbf{v}_1\} + \mathbf{u}$$

y

$$(\mathbf{C}_1(B))_{\mathbf{u}} = \mathbf{C}_1(B) \cap (\langle \mathbf{v}_1 \rangle + \mathbf{u}) = \{0, \mathbf{v}_1, 2\mathbf{v}_1, \cdots, (|B_{\mathbf{u}}| - 1)\mathbf{v}_1\} + \mathbf{u}.$$

En consecuencia, para todo $\mathbf{u} \in \langle \mathbf{v}_2 \rangle$, ambos conjuntos $(\mathbf{C}_1(A))_{\mathbf{u}}$ y $(\mathbf{C}_1(B))_{\mathbf{u}}$ son progresiones aritméticas con la misma diferencia tales que $|(\mathbf{C}_1(A))_{\mathbf{u}}| = |A_{\mathbf{u}}|$ y $|(\mathbf{C}_1(B))_{\mathbf{u}}| = |B_{\mathbf{u}}|$, de lo cual se infiere que:

$$|(\mathbf{C}_1(A) + \mathbf{C}_1(B))_{\mathbf{u}}| = \text{máx}\{|A_{\mathbf{w}}| + |B_{\mathbf{u}-\mathbf{w}}| - 1 : A_{\mathbf{w}} \neq \emptyset, B_{\mathbf{u}-\mathbf{w}} \neq \emptyset\}. \tag{4.10}$$

Entonces, de (4.7) y (4.10) tenemos que:

$$\begin{aligned} |\mathbf{C}_1(A) + \mathbf{C}_1(B)| &= \sum_{\mathbf{u} \in \langle \mathbf{v}_2 \rangle} |(\mathbf{C}_1(A) + \mathbf{C}_1(B))_{\mathbf{u}}| \\ &= \sum_{\mathbf{u} \in \langle \mathbf{v}_2 \rangle} \text{máx}\{|A_{\mathbf{w}}| + |B_{\mathbf{u}-\mathbf{w}}| - 1 : A_{\mathbf{w}} \neq \emptyset, B_{\mathbf{u}-\mathbf{w}} \neq \emptyset\}, \end{aligned} \tag{4.11}$$

y finalmente, de (4.11) y (4.9) obtenemos:

$$|A + B| \geq |\mathbf{C}_1(A) + \mathbf{C}_1(B)|.$$

Para concluir la demostración del lema, basta observar que podemos repetir los argumentos anteriores comenzando con los conjuntos $\mathbf{C}_1(A)$ y $\mathbf{C}_1(B)$ (en vez de $A$ y $B$), y tomando en cuenta la base ordenada $(\mathbf{v}_2, \mathbf{v}_1)$ (en vez de $(\mathbf{v}_1, \mathbf{v}_2)$), obteniendo:

$$|\mathbf{C}_1(A) + \mathbf{C}_1(B)| \geq |\mathbf{C}_2(\mathbf{C}_1(A)) + \mathbf{C}_2(\mathbf{C}_1(B))| = |\mathbf{C}(A) + \mathbf{C}(B)|$$

y por lo tanto:

$$|A + B| \geq |\mathbf{C}(A) + \mathbf{C}(B)|.$$

□

Para ejemplificar algunos aspectos de la prueba anterior, veremos un ejemplo.

**Ejemplo 4.5.** *Consideremos los conjuntos* $A = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,2)\}$ *y* $B = \{(0,0), (0,3), (2,1), (3,0)\}$ *ilustrados en la figura 4.6, donde se muestra también el conjunto suma* $A + B$. *Consideremos la base ordenada* $(\boldsymbol{e}_1, \boldsymbol{e}_2)$ *y las primeras compresiones* $\boldsymbol{C}_1(A)$ *y* $\boldsymbol{C}_1(B)$ *así como la suma* $\boldsymbol{C}_1(A) + \boldsymbol{C}_1(B)$ *mostradas en la figura 4.7. Concentremos*

*nuestra atención en los subconjuntos* $(A+B)_{2\boldsymbol{e}_1}$ *y* $(\boldsymbol{C}_1(A)+\boldsymbol{C}_1(B))_{2\boldsymbol{e}_1}$ *marcados en las figuras correspondientes. Notemos que:*

$$\begin{aligned}(A+B)_{2\boldsymbol{e}_1} &= (A_{\boldsymbol{e}_1}+B_{\boldsymbol{e}_1})\cup(A_{2\boldsymbol{e}_1}+B_{0\boldsymbol{e}_1})\\ &= \{(3,2),(4,2)\}\cup\{(1,2),(2,2),(4,2),(5,2),(7,2)\}\\ &= \{(1,2),(2,2),(3,2),(4,2),(5,2),(7,2)\}\end{aligned}$$

*satisfaciendo, en efecto,*

$$6 = |(A+B)_{2\boldsymbol{e}_1}| \geq \text{máx}\{|(A_{\boldsymbol{e}_1}+B_{\boldsymbol{e}_1})|, |(A_{2\boldsymbol{e}_1}+B_{0\boldsymbol{e}_1})|\} = \text{máx}\{2,5\} = 5.$$

*Mientras que:*

$$\begin{aligned}(\boldsymbol{C}_1(A)+\boldsymbol{C}_1(B))_{2\boldsymbol{e}_1} &= (\boldsymbol{C}_1(A)_{\boldsymbol{e}_1}+\boldsymbol{C}_1(B)_{\boldsymbol{e}_1})\cup(\boldsymbol{C}_1(A)_{2\boldsymbol{e}_1}+\boldsymbol{C}_1(B)_{0\boldsymbol{e}_1})\\ &= \{(0,2),(1,2)\}\cup\{(0,2),(1,2),(2,2),(3,2)\}\\ &= \{(0,2),(1,2),(2,2),(3,2)\},\end{aligned}$$

*de modo que, efectivamente,*

$$\begin{aligned}4 = |(\boldsymbol{C}_1(A)+\boldsymbol{C}_1(B))_{2\boldsymbol{e}_1}| &= \text{máx}\{|\boldsymbol{C}_1(A)_{\boldsymbol{e}_1}|+|\boldsymbol{C}_1(B)_{\boldsymbol{e}_1})|-1, |\boldsymbol{C}_1(A)_{2\boldsymbol{e}_1}|+|\boldsymbol{C}_1(B)_{0\boldsymbol{e}_1}|-1)|\}\\ &= \text{máx}\{2+1-1, 3+2-1)|\} = 4.\end{aligned}$$

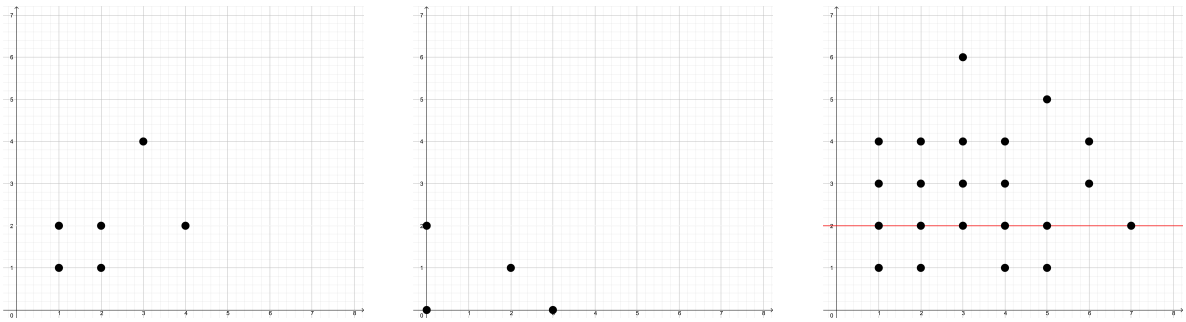


Figura 4.6: Conjuntos $A$, $B$, y conjunto suma $A+B$.

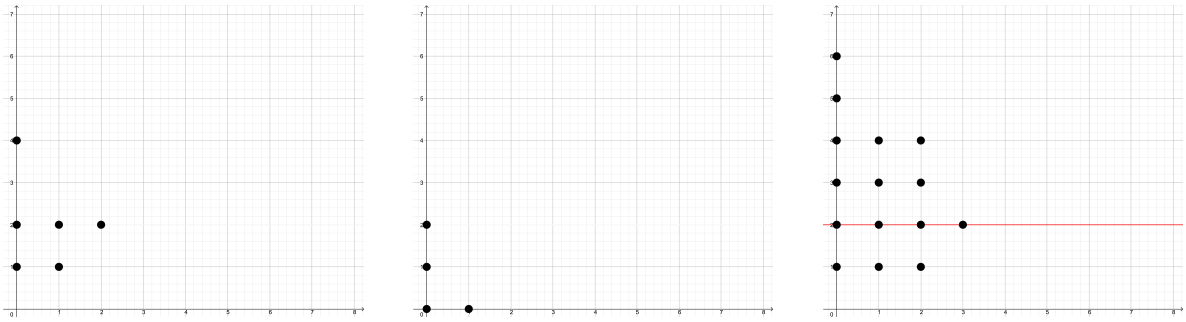


Figura 4.7: Conjuntos $\mathbf{C}_1(A)$, $\mathbf{C}_1(B)$, y conjunto suma $\mathbf{C}_1(A)+\mathbf{C}_1(B)$.

Sabemos entonces que dados dos conjuntos finitos $A$ y $B$ de $\mathbb{R}^2$ podemos acotar inferiormente la cardinalidad de su conjunto suma, $A+B$, acotando inferiormente la cardinalidad de $\mathbf{C}(A)+\mathbf{C}(B)$. Como las compresiones, $\mathbf{C}(A)$ y $\mathbf{C}(B)$ son conjuntos particularmente especiales podemos, de hecho, determinar de manera exacta $|\mathbf{C}(A)+\mathbf{C}(B)|$. Para ello requerimos establecer un poco más de notación. Sean $m = |\phi_{\langle \mathbf{v}_1\rangle}(A)|$ y $n = |\phi_{\langle \mathbf{v}_1\rangle}(B)|$. Por construcción, $\mathbf{C}(A)$ es la union de $m$ progresiones aritméticas paralelas a $\langle \mathbf{v}_1\rangle$, y $\mathbf{C}(B)$ es la union de $n$ progresiones aritméticas paralelas a $\langle \mathbf{v}_1\rangle$. En concreto, para cada $1 \leq i \leq m$, consideramos:

$$A_i = \mathbf{C}(A) \cap (\langle \mathbf{v}_1\rangle + (i-1)\mathbf{v}_2) = \{0, \mathbf{v}_1, 2\mathbf{v}_1, \cdots, (a_i-1)\mathbf{v}_1\} + (i-1)\mathbf{v}_2,$$

donde:

$$a_i = |A_i|; \tag{4.12}$$

y para cada $1 \leq i \leq n$, consideramos:

$$B_i = \mathbf{C}(B) \cap (\langle \mathbf{v}_1\rangle + (i-1)\mathbf{v}_2) = \{0, \mathbf{v}_1, 2\mathbf{v}_1, \cdots, (b_i-1)\mathbf{v}_1\} + (i-1)\mathbf{v}_2,$$

donde:

$$b_i = |B_i|. \tag{4.13}$$

De este modo,

$$\mathbf{C}(A) = \bigcup_{i=1}^{n} A_i \quad \text{y} \quad \mathbf{C}(B) = \bigcup_{i=1}^{m} B_i. \tag{4.14}$$

Obsérvese que $a_1 \geq a_2 \geq \cdots \geq a_m \geq 1$, y

$$\sum_{i=1}^{m} a_i = |\mathbf{C}(A)| = |A|, \tag{4.15}$$

igualmente, $b_1 \geq b_2 \geq \cdots \geq b_n \geq 1$, y

$$\sum_{i=1}^{n} b_j = |\mathbf{C}(B)| = |B|. \tag{4.16}$$

**Lema 4.3.** *Sean $A$ y $B$ dos conjuntos finitos de $\mathbb{R}^2$, y sean $\boldsymbol{C}(A)$ y $\boldsymbol{C}(B)$ sus respectivas compresiones con respecto a una base ordenada $(\boldsymbol{v}_1, \boldsymbol{v}_2)$. Sean $m = |\phi_{\langle \boldsymbol{v}_1\rangle}(A)|$, $n = |\phi_{\langle \boldsymbol{v}_1\rangle}(B)|$, los conjuntos $A_1, \ldots, A_m, B_1, \ldots, B_n$ y los enteros $a_1, \ldots, a_m$; $b_1, \ldots, b_n$ como se definieron arriba. Entonces,*

$$|\boldsymbol{C}(A) + \boldsymbol{C}(B)| = \sum_{t=2}^{m+n} \text{máx}\,\{a_i + b_{t-i} \,|\, 1 \leq i \leq m\,,\, 1 \leq t-i \leq n\} - (m+n-1).$$

*Demostración.* Por la ecuación (4.7) sabemos que:

$$|\mathbf{C}(A) + \mathbf{C}(B)| = \sum_{\mathbf{u} \in \langle \mathbf{v}_2\rangle} |(\mathbf{C}(A) + \mathbf{C}(B))_{\mathbf{u}}|.$$

Por definición, $\{\mathbf{u} \in \langle \mathbf{v}_2 \rangle \,:\, (\mathbf{C}(A) + \mathbf{C}(B))_{\mathbf{u}} \neq \emptyset\} = \{t\,\mathbf{v}_2 \,:\, 2 \leq t \leq n+m\}$, de modo que:

$$|\mathbf{C}(A) + \mathbf{C}(B)| = \sum_{t=2}^{n+m} |(\mathbf{C}(A) + \mathbf{C}(B))_{t\,\mathbf{v}_2}|. \tag{4.17}$$

Además, sabemos que:

$$(\mathbf{C}(A) + \mathbf{C}(B))_{t\,\mathbf{v}_2} = \bigcup_{1 \leq i \leq m\,,\, 1 \leq t-i \leq n} (A_i + B_{t-i}).$$

Pero, dado que $A_i$ y $B_{t-i}$ son progresiones aritméticas con la misma diferencia, el teorema 4.2 nos dice que:

$$|(\mathbf{C}(A) + \mathbf{C}(B))_{t\,\mathbf{v}_2}| = \text{máx}\{|A_i| + |B_{t-i}| - 1 :\, 1 \leq i \leq m\,,\, 1 \leq t-i \leq n\}. \tag{4.18}$$

Juntando (4.17) y (4.18), y sustituyendo $a_i = |A_i|$ para $1 \leq i \leq m$, y $b_j = |B_j|$ para $1 \leq i \leq n$ obtenemos:

$$|\mathbf{C}(A) + \mathbf{C}(B)| = \sum_{t=2}^{m+n} \text{máx}\left\{a_i + b_{t-i} - 1 \,|\, 1 \leq i \leq m\,,\, 1 \leq t-i \leq n\right\}.$$

Factorizando un $(-1)$ en cada uno de los $m+n-2+1 = m+n-1$ sumando obtenemos lo que se buscaba.

□

**Ejemplo 4.6.** *Sean $A$ y $B$ como en el ejemplo 4.5. Los conjuntos comprimidos, $\boldsymbol{C}(A)$ y $\boldsymbol{C}(B)$, con respecto a la base ordenada $(\boldsymbol{e}_1, \boldsymbol{e}_2)$ así como la suma $\boldsymbol{C}(A) + \boldsymbol{C}(B)$ se muestran en la figura 4.8, donde se puede ver que $a_1 = 3 \geq a_2 = 2 \geq a_3 = 1$, $b_1 = 2 \geq b_2 = 1 \geq b_3 = 1$, y*

$$\begin{aligned}
13 &= |\boldsymbol{C}(A) + \boldsymbol{C}(B)| \\
&= \sum_{t=2}^{6} \text{máx}\left\{a_i + b_{t-i} \,|\, 1 \leq i \leq 3\,,\, 1 \leq t-i \leq 3\right\} - 5 \\
&= \text{máx}\{a_1 + b_1\} + \text{máx}\{a_1 + b_2, a_2 + b_1\} + \text{máx}\{a_1 + b_3, a_2 + b_2, a_3 + b_1\} \\
&\quad + \text{máx}\{a_2 + b_3, a_3 + b_2\} + \text{máx}\{a_3 + b_3\} - 5 \\
&= \text{máx}\{5\} + \text{máx}\{4, 3\} + \text{máx}\{4, 3, 3\} + \text{máx}\{3, 3\} + \text{máx}\{2\} - 5 \\
&= 5 + 4 + 4 + 3 + 2 - 5 = 13
\end{aligned}$$

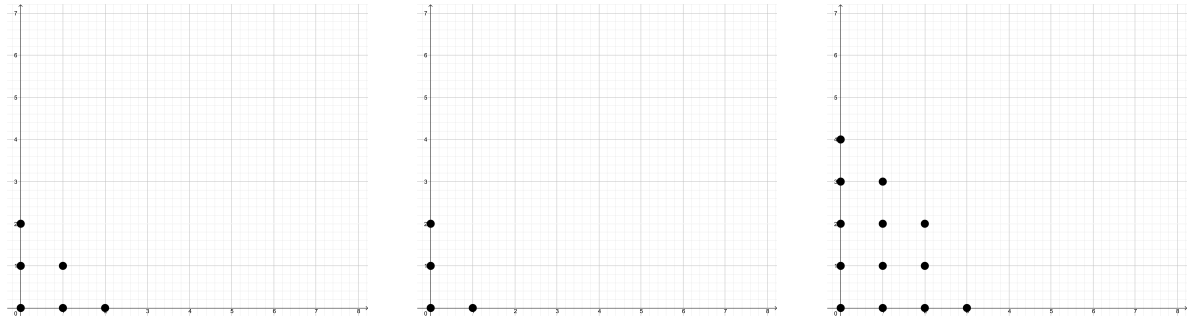


Figura 4.8: Conjuntos $\mathbf{C}(A)$, $\mathbf{C}(B)$, y conjunto suma $\mathbf{C}(A) + \mathbf{C}(B)$.

## 4.2. La desigualdad de Grynkiewicz-Serra

La desigualdad de Grynkiewicz-Serra es una cota inferior a la cardinalidad de la suma de dos conjuntos finitos en $\mathbb{R}^2$ en términos del numero de lineas paralelas que intersectan a cada uno de ellos.

**Teorema 4.4.** *[Grynkiewicz, Serra, 2010] Sean $A$ y $B$ conjuntos finitos en $\mathbb{R}^2$. Para cualquier $\boldsymbol{v} \in \mathbb{R}^2$, $\boldsymbol{v} \neq \boldsymbol{0}$, se cumple*

$$|A + B| \geq \left( \frac{|A|}{m} + \frac{|B|}{n} - 1 \right) (m + n - 1),$$

*donde $m = |\phi_{\langle \boldsymbol{v} \rangle}(A)|$ y $n = |\phi_{\langle \boldsymbol{v} \rangle}(B)|$.*

Para probar el teorema 4.4 tenemos casi todos los ingredientes: usaremos la compresión de conjuntos con respecto a la base ordenada $(\mathbf{v}, \mathbf{v}^{\perp})$. Así, en vista de los lemas 4.2 y 4.3, nos hace falta la siguiente desigualdad para poder completar la prueba.

**Lema 4.4.** *Sean $a_1, \ldots, a_m, b_1, \ldots, b_n \in \mathbb{R}$, entonces:*

$$\sum_{t=2}^{m+n} \text{máx}\{a_i + b_{t-i} \mid 1 \leq i \leq m, 1 \leq i - j \leq n\} \geq \left( \frac{1}{m} \sum_{i=1}^{m} a_i + \frac{1}{n} \sum_{i=1}^{n} b_i \right) (m + n - 1). \quad (4.19)$$

*Demostración.* La prueba se realizará por inducción sobre $m + n$. Observemos que si $n = 1$, entonces:

$$\sum_{t=2}^{m+1} \text{máx}\{a_i + b_1 \mid 1 \leq i \leq m\} = \left( \frac{1}{m} \sum_{i=1}^{m} a_i + b_1 \right) (m),$$

que es lo que se quería demostrar. Análogamente el lema se cumple si $n = 1$. De lo anterior podemos suponer que $n, m \geq 2$.

Para un vector $\mathbf{x} = (x_1, \ldots, x_k) \in \mathbb{R}^k$, definimos el escalar $\bar{x}$, como sigue:

$$\bar{x} = \frac{1}{k} \sum_{i=1}^{k} x_i. \quad (4.20)$$

Además definimos la operación escalar $u(\mathbf{x},\mathbf{y})$ para dos vectores $\mathbf{x} = (x_1,\ldots,x_k) \in \mathbb{R}^k$ y $\mathbf{y} = (y_1,\ldots,y_l) \in \mathbb{R}^l$ como sigue:

$$u(\mathbf{x},\mathbf{y}) = \sum_{t=2}^{k+l} \text{máx}\{x_i + y_{t-i} \mid 1 \leq i \leq k, 1 \leq t-j \leq l\} \tag{4.21}$$

De lo anterior tenemos que, demostrar el lema es equivalente a demostrar:

$$u(\mathbf{a},\mathbf{b}) \geq (m+n-1)(\bar{a}+\bar{b}), \tag{4.22}$$

donde $\mathbf{a} = (a_1,\ldots,a_m)$ y $\mathbf{b} = (b_1,\ldots,b_n)$. Sean $\mathbf{a}' = (a_2,\ldots,a_m)$ y $\mathbf{b}' = (b_2,\ldots,b_n)$. Observemos lo siguientes:

$$u(\mathbf{a},\mathbf{b}) \geq \sum_{t=3}^{m+n} \text{máx}\{a_i + b_{t-i} \mid 2 \leq i \leq m, 1 \leq t-j \leq n\} + (a_1+b_1),$$

es decir,

$$u(\mathbf{a},\mathbf{b}) \geq u(\mathbf{a}',\mathbf{b}) + a_1 + b_1. \tag{4.23}$$

Por otra parte, por hipótesis de inducción tenemos que:

$$u(\mathbf{a}',\mathbf{b}) \geq (m+n-2)(\bar{a}'+\bar{b}). \tag{4.24}$$

Sin pérdida de generalidad podemos suponer que $\bar{a}-\bar{a}' \leq \bar{b}-\bar{b}'$. Juntando las ecuaciones 4,23 y 4,24, tenemos que:

$$\begin{aligned}
u(\mathbf{a},\mathbf{b}) \geq & (m+n-2)(\bar{a}'+\bar{b}) + a_1 + b_1 \\
= & m\bar{a}' + m\bar{b} + n\bar{a}' + n\bar{b} - 2\bar{a}' - 2\bar{b} + \left(\sum_{i=1}^{m} a_i - \sum_{i=2}^{m} a_i\right) + \left(\sum_{i=1}^{n} b_i - \sum_{i=2}^{n} b_i\right) \\
= & m\bar{a}' + m\bar{b} + n\bar{a}' + n\bar{b} - 2\bar{a}' - 2\bar{b} + m\bar{a} - (m-1)\bar{a}' + n\bar{b} - (n-1)\bar{b}' \\
= & m\bar{a}' + m\bar{b} + n\bar{a}' + n\bar{b} - 2\bar{a}' - 2\bar{b} + m\bar{a} - m\bar{a} + \bar{a}' + n\bar{b} - n\bar{b}' + \bar{b}' \\
= & m(\bar{a}+\bar{b}) + n(\bar{a}+\bar{b}) - n\bar{a} - (\bar{a}+\bar{b}) + \bar{a} + n\bar{a}' + n\bar{b} - \bar{a}' - n\bar{b}' + \bar{b}' \\
= & (m+n-1)(\bar{a}+\bar{b}) + n(\bar{a}'-\bar{a}) - (\bar{a}'-\bar{a}) + n(\bar{b}-\bar{b}') - (\bar{b}-\bar{b}') \\
= & (m+n-1)(\bar{a}+\bar{b}) + (n-1)(\bar{b}-\bar{b}') - (n-1)(\bar{a}+\bar{a}'),
\end{aligned}$$

pero como $\bar{a}-\bar{a}' \leq \bar{b}-\bar{b}'$, obtenemos que:

$$u(\mathbf{a},\mathbf{b}) \geq (m+n-1)(\bar{a}+\bar{b}),$$

que es lo que se quería demostrar. □

Ya demostrado el lema 4,4, procederemos a demostrar el teorema 4,4.

**Teorema 4.5.** *Sean $A$ y $B$ conjuntos finitos en $\mathbb{R}^2$. Para cualquier $\boldsymbol{v} \in \mathbb{R}^2$, $\boldsymbol{v} \neq \boldsymbol{0}$, se cumple*

$$|A+B| \geq \left(\frac{|A|}{m} + \frac{|B|}{n} - 1\right)(m+n-1),$$

*donde $m = |\phi_{\langle \boldsymbol{v} \rangle}(A)|$ y $n = |\phi_{\langle \boldsymbol{v} \rangle}(B)|$.*

*Demostración.* Sea $\mathbf{v} \neq \mathbf{0}$ un vector en $\mathbb{R}^2$, consideremos la base ordenada $(\mathbf{v}, \mathbf{v}^{\perp})$; y sean $\mathbf{C}(A)$ y $\mathbf{C}(B)$ las compresiones de $A$ y de $B$ respecto a esta base ordenada. Por el lema 4,2, tenemos que:

$$|A+B| \geq |\mathbf{C}(A) + \mathbf{C}(B)|.$$

Ahora, por el lema 4,3, tenemos que:

$$|A+B| \geq \sum_{t=2}^{m+n} \max\{a_i + b_{t-i} \,|\, 1 \leq i \leq m\,,\, 1 \leq t-i \leq n\} - (m+n-1).$$

Pero por el lema 4,4, tenemos que:

$$|A+B| \geq \left(\frac{1}{m}\sum_{i=1}^{m} a_i + \frac{1}{n}\sum_{i=1}^{n} b_i\right)(m+n-1) - (m+n-1).$$

Recordemos que $\displaystyle\sum_{i=1}^{m} a_i = |A|$ y $\displaystyle\sum_{i=1}^{n} b_i = |B|$, luego:

$$|A+B| \geq \left(\frac{1}{m}|A| + \frac{1}{n}|B|\right)(m+n-1) - (m+n-1),$$

y por lo tanto:

$$|A+B| \geq \left(\frac{|A|}{m} + \frac{|B|}{n} - 1\right)(m+n-1).$$

□

## 4.3. Una generalización del teorema 4.4

El teorema 4.2 se puede generalizar, por inducción, para obtener la siguiente desigualdad correspondiente a la suma de $h \geq 2$ subconjuntos en vez de solo dos. Naturalmente, dados conjuntos finitos $A_1, \ldots, A_h$ en un grupo aditivo sin torsión,

$$A_1 + \cdots + A_h = \{\mathbf{a}_1 + \ldots + \mathbf{a}_h \mid \mathbf{a}_i \in A_i, 1 \leq i \leq h\}.$$

**Teorema 4.6** (Folklore)**.** *Sean $A_1, \ldots, A_h$ subconjuntos finitos (no vacíos) de un grupo abeliano sin torsión. Entonces,*

$$|A_1 + \cdots + A_h| \geq \left(\sum_{i=1}^{h} |A_i|\right) - (h-1).$$

*Demostración.* La prueba se realizará por inducción sobre $h$. Si $h = 2$, obtenemos el teorema 4,2. Supongamos que el teorema se cumple para $h$. Por demostrar para $h + 1$. Observemos que por el teorema 4,2, tenemos que:

$$|A_1 + \cdots + A_{h+1}| \geq |A_1 + \cdots + A_h| + |A_{h+1}| - 1.$$

Por hipótesis de inducción obtenemos ahora que:

$$\begin{aligned} |A_1 + \cdots + A_{h+1}| &\geq |A_1 + \cdots + A_h| + |A_{h+1}| - 1. \\ &\geq \left(\sum_{i=1}^{h} |A_i|\right) - (h-1) + |A_{h+1}| - 1 \\ &\geq \left(\sum_{i=1}^{h+1} |A_i|\right) - h \end{aligned}$$

Que es lo que se quería demostrar. □

Con el uso del teorema 4.6 podemos dar una generalización del teorema 4.4.

**Teorema 4.7.** *Sea $h \geq 2$ un entero, y sean $A_1, \ldots A_h$ subconjuntos finitos (no vacíos) de $\mathbb{R}^2$. Para cualquier $\boldsymbol{v} \in \mathbb{R}^2$, $\boldsymbol{v} \neq \boldsymbol{0}$, se cumple*

$$|A_1 + \ldots + A_h| \geq \left(\left(\sum_{i=1}^{h} \frac{|A_i|}{m_i}\right) - (h-1)\right)\left(\left(\sum_{i=1}^{h} m_i\right) - (h-1)\right),$$

*donde $m_i = |\phi_{\langle \boldsymbol{u} \rangle}(A_i)|$, $1 \leq i \leq h$.*

Para probar el teorema 4.8 usaremos inducción, además de los siguientes lemas que se demuestran usando el teorema 4.6. El siguiente lema generaliza al lema 4,2 y por lo tanto usaremos fuertemente su demostración para demostrar el de interés.

**Lema 4.5.** *Sean $A_1, \ldots, A_h$ subconjuntos finitos de $\mathbb{R}^2$ y, para cada $1 \leq i \leq h$, sea $\boldsymbol{C}(A_i)$ la compresión de $A_i$ respecto a la base ordenada $(\boldsymbol{v}_1, \boldsymbol{v}_2)$. Entonces,*

$$|A_1 + \ldots + A_h| \geq |\boldsymbol{C}(A_1) + \ldots + \boldsymbol{C}(A_h)|. \tag{4.25}$$

*Demostración.* Primero demostraremos que $|A_1 + \ldots + A_h| \geq |\mathbf{C}_1(A_1) + \ldots + \mathbf{C}_1(A_h)|$ y la prueba se efectuará por inducción sobre $h$. Observemos que en la demostración del lema 4,2 tenemos que lo anterior se cumple para $h = 2$, es decir, $|A_1 + A_2| \geq |\mathbf{C}_1(A_1) + \mathbf{C}_1(A_2)|$. Por el teorema 4,2, tenemos que:

$$|A_1 + \ldots + A_h| \geq |A_1 + A_2| + |A_3 + \ldots + A_h| - 1.$$

Por hipotésis de inducción, tenemos además que:

$$|A_1 + \ldots + A_h| \geq |\mathbf{C}_1(A_1) + \mathbf{C}_1(A_2)| + |\mathbf{C}_1(A_3) + \ldots + \mathbf{C}_1(A_h)|.$$

Por el teorema 4,6, obtenemos:

$$|A_1 + \ldots + A_h| \geq |\mathbf{C}_1(A)_1| + \ldots + |\mathbf{C}_1(A_h)| - (h-1);$$

ahora como $\mathbf{C}_1(A_1), \ldots, \mathbf{C}_1(A_h)$ son progresiones aritméticas de la misma diferencia, y nuevamente por el teorema 4,6, tenemos que:

$$|A_1 + \ldots + A_h| \geq |\mathbf{C}_1(A_1) + \ldots \mathbf{C}_1(A_h)|.$$

Para concluir la demostración del lema, basta observar que podemos repetir los argumentos anteriores comenzando con los conjuntos $\mathbf{C}_1(A_1), \ldots, \mathbf{C}_1(A_h)$ (en vez de los conjuntos $A_1, \ldots, A_h$), y tomando en cuenta la base ordenada $(\mathbf{v}_2, \mathbf{v}_1)$ (en vez de $(\mathbf{v}_1, \mathbf{v}_2)$), obteniendo:

$$|\mathbf{C}_1(A_1) + \ldots + \mathbf{C}_1(A_h)| \geq |\mathbf{C}_2(\mathbf{C}_1(A_1)) + \ldots + \mathbf{C}_2(\mathbf{C}_1(A_h))| = |\mathbf{C}(A) + \mathbf{C}(B)|$$

y por lo tanto:

$$|A_1 + \ldots + A_h| \geq |\mathbf{C}(A_1) + \ldots + \mathbf{C}(A_h)|.$$

□

Antes de enunciar y demostrar el segundo lema importante, definiremo los siguientes conjuntos que serán de gran utilidad en la demostración del lema y veremos sus propiedades básicas que se infieren rápidamente de la construcción de .$\mathbf{C}(A)$.

**Definición 4.5.** *Sea $A$ un conjunto $\mathbb{R}^2$, $(\boldsymbol{v}_1, \boldsymbol{v}_2)$; y sea $\boldsymbol{C}(A)$ la compresión de $A$ respecto a la base $(\boldsymbol{v}_1, \boldsymbol{v}_2)$ para cada $1 \leq i \leq \phi_{\langle \boldsymbol{v}_2 \rangle}(\boldsymbol{C}(A))$ definimos:*

$$A'_i = \boldsymbol{C}(A) \cap (\langle \boldsymbol{v}_2 \rangle + (i-1)\boldsymbol{v}_1) = \{\boldsymbol{0}, \boldsymbol{v}_2 \ldots, (a'_1 - 1)\boldsymbol{v}_2\} + (i-1)\boldsymbol{v}_1,$$

*donde $a'_i = |A'_i|$*

**Observación 4.1.** *Los conjuntos definidos en* 4,5*, satisfacen lo siguiente:*

1. $\boldsymbol{C}(A) = \bigcup_{i=1}^{\phi_{\langle \boldsymbol{v}_2 \rangle}(\boldsymbol{C}(A))} A'_i$.
2. $a'_i \leq a'_j$ *si* $i \leq j$.
3. $a'_1 = \phi_{\langle \boldsymbol{v}_1 \rangle} |\boldsymbol{C}(A)|$.

**Lema 4.6.** *Sean $A_1, \ldots, A_h$ subconjuntos finitos (no vacíos) de $\mathbb{R}^2$ y, para cada $1 \leq i \leq h$, sea $\boldsymbol{C}(A_i)$ la compresión de $A_i$ con respecto a la base ordenada $(\boldsymbol{v}_1, \boldsymbol{v}_2)$. Entonces,*

$$\left|\phi_{\langle \boldsymbol{v}_1 \rangle}\left(\boldsymbol{C}(A_1) + \cdots + \boldsymbol{C}(A_h)\right)\right| = \left(\sum_{i=1}^{h} \left|\phi_{\langle \boldsymbol{v}_1 \rangle}\left(\boldsymbol{C}(A_i)\right)\right|\right) - (h-1). \tag{4.26}$$

*Demostración.* Por la observación 4,1, tenemos que basta demostrar que:

$$|\phi_{\langle \mathbf{v}_1 \rangle}(\mathbf{C}(A_1) + \cdots, \mathbf{C}A_h)| = a'_1 + \cdots + a'_h - (h-1).$$

Observemos que:

$$\mathbf{C}(A_1) + \cdots + \mathbf{C}(A_h) = \bigcup \left( \sum_{j_h=1}^{\phi_{\langle \mathbf{v}_2 \rangle}(\mathbf{C}(A_h))} \ldots \right) \tag{4.27}$$

Además observemos que:

$$A'_{1_{j_1}} + \cdots + A'_{h_{j_h}} = \{\mathbf{0}, \ldots, (a'_{1_{j_1}} + \cdots + a'_{h_{j_h}} - h)\mathbf{v}_2\} + (i + j - h)\mathbf{v}_1 \tag{4.28}$$

Por la observación 4,1 tenemos que:

$$|A'_{1_1} + \cdots + A'_{h_1}| > |A'_{1_{j_1}} + \cdots + A'_{h_{j_h}}| \tag{4.29}$$

para todo $1 \leq i_{j_1} \leq \phi_{\langle \mathbf{v}_2 \rangle}(\mathbf{C}(A_i)$ y para todo $1 \leq i \leq h$. Por las ecuaciones 4,27, 4,28 y 4,29; y por la observación 4,1, tenemos que:

$$|\phi_{\langle \mathbf{v}_1 \rangle}(\mathbf{C}(A_1) + \cdots, \mathbf{C}A_h)| = a'_1 + \cdots + a'_h - (h-1),$$

que es lo que se quería demostrar. □

**Teorema 4.8.** *Sea $h \geq 2$ un entero, y sean $A_1, \ldots A_h$ subconjuntos finitos (no vacíos) de $\mathbb{R}^2$. Para cualquier $\boldsymbol{v} \in \mathbb{R}^2$, $\boldsymbol{v} \neq \boldsymbol{0}$, se cumple*

$$|A_1 + \ldots + A_h| \geq \left( \left( \sum_{i=1}^{h} \frac{|A_i|}{m_i} \right) - (h-1) \right) \left( \left( \sum_{i=1}^{h} m_i \right) - (h-1) \right),$$

*donde $m_i = |\phi_{\langle \mathbf{u} \rangle}(A_i)|$, $1 \leq i \leq h$.*

*Demostración.* La demostración se efectuará por inducción sobre $h$. Si $h = 2$, el teorema se cumple por el teorema 4,4. Definimos los conjuntos $A = \mathbf{C}_1(A_1) + \ldots + \mathbf{C}_1(A_{h-1})$ y $B = \mathbf{C}(A_h)$, donde $\mathbf{C}(A_i)$ es la compresión de $A_i$ respecto a la base ordenada $(\mathbf{v}, \mathbf{v}^{\perp})$, para todo $1 \leq i \leq h$. Por el lema 4,5, tenemos que:

$$|A_1 + \ldots + A_h| \geq |\mathbf{C}(A_1) + \ldots + \mathbf{C}(A_h)| = |A + B|.$$

Por el teorema 4,4, obtenemos ahora que:

$$|A_1 + \ldots + A_h| \geq \left( \frac{|A|}{m} + \frac{|B|}{n} - 1 \right)(m + n - 1), \tag{4.30}$$

donde $m = |\phi_{\langle \mathbf{v} \rangle}(A)|$ y $n = |\phi_{\langle \mathbf{v} \rangle}(B)|$. Sabemos que $|\mathbf{C}(A_i)| = |A_i|$ y $|\phi_{\langle \mathbf{v} \rangle}(\mathbf{C}(A_i))| = |\phi_{\langle \mathbf{v} \rangle}((A_i)| = m_i$, para todo $1 \leq i \leq h$, entonces:

$$n = m_h. \tag{4.31}$$

Análogamente tenemos que:

$$m = |\phi_{\langle \mathbf{v} \rangle}(\mathbf{C}(A_1) + \ldots + \mathbf{C}(A_{h-1}))|.$$

Por el lema 4,6, obtenemos ahora que:

$$\begin{aligned} m &= \left( \sum_{i=1}^{h-1} \left| \phi_{\langle \mathbf{v}_1 \rangle} \left( \mathbf{C}(A_i) \right) \right| \right) - (h-2) \\ &= \left( \sum_{i=1}^{h-1} \left| \phi_{\langle \mathbf{v}_1 \rangle} \left( A_i \right) \right| \right) - (h-2), \end{aligned}$$

luego:

$$m = \left( \sum_{i=1}^{h-1} m_i \right) - (h-2) \tag{4.32}$$

Por las ecuaciones 4,31 y 4,32, obtenemos que:

$$m + n - 1 = \left( \sum_{i=1}^{h-1} m_i \right) - (h-2) + m_h - 1,$$

luego,

$$m + n - 1 = \left( \sum_{i=1}^{h} m_i \right) - (h-1). \tag{4.33}$$

Por otra parte, tenemos que:

$$\frac{B}{n} = \frac{|A_h|}{m_h}. \tag{4.34}$$

Por hipótesis de inducción tenemos que:

$$|A| \geq \left( \left( \sum_{i=1}^{h-1} \frac{|A_i|}{m_i} \right) - (h-2) \right) \left( \left( \sum_{i=1}^{h-1} m_i \right) - (h-2) \right). \tag{4.35}$$

Por las ecuaciones 4,32 y 4,35, obtenemos que:

$$\frac{|A|}{m} \geq \left( \left( \sum_{i=1}^{h-1} \frac{|A_i|}{m_i} \right) - (h-2) \right) \tag{4.36}$$

Para terminar, sustituimos las ecuaciones 4,33, 4,34 y 4,36 en la ecuación 4,30, obteniendo:

$$\begin{aligned} |A_1 + \ldots + A_h| &\geq \left( \frac{|A|}{m} + \frac{|B|}{n} - 1 \right) (m + n - 1) \\ &\geq \left( \left( \sum_{i=1}^{h-1} \frac{|A_i|}{m_i} \right) - (h-2) + \frac{|A_h|}{m_h} - 1 \right) \left( \left( \sum_{i=1}^{h} m_i \right) - (h-1) \right) \\ &\geq \left( \left( \sum_{i=1}^{h} \frac{|A_i|}{m_i} \right) - (h-1) \right) \left( \left( \sum_{i=1}^{h} m_i \right) - (h-1) \right). \end{aligned}$$

□

# Capítulo 5

# Conclusiones y trabajo a futuro

Después de estudiar a profundidad el *teorema* $2^n$ *de Freiman* podemos concluir que la complejidad de la demostración no radica en la dimensión en la que se está trabajando. Es por ello que, en este trabajo de tesis, se estudió primero la prueba para el caso bidimensional; para así aterrizar de manera más fácil, preciso y con ejemplos las ideas usadas en dicha demostración para después, una vez ya entendida la técnica de la prueba, proceder a demostrar el teorema en su forma general. Por otra parte, el resultado de Bonnesen (teorema 3,2), un resultado muy importante pero poco conocido, establece una conexión, además de abrir la posibilidad de estudiar un sin fin de problemas interesantes, entre la desigualdad de Brunn-Minkowski (teorema 3,1), importante resultado dentro del área de geometría convexa que nos acota la medida de la suma de conjuntos en $\mathbb{R}^n$) y la teoría de números aditiva, área que se encarga de estudiar la forma de acotar la suma de conjuntos finitos: ya sea usando la cardinalidad de los conjuntos que se están sumando; o en el caso de esta tesis, usando las proyecciones que tienen los conjuntos que se están sumando sobre hiperplanos. El resultado de Grynkiewicz y Serra (teorema 4,1) es un ejemplo de dicha conexión, ya que recordemos que una medida para conjuntos finitos es su cardinalidad, y es por ello que dicho resultado nos proporciona una versión discreta a la desigualdad Brunn-Minkowski pero unicamente para dos dimensiones. Como los autores Grynkiewicz y Serra sólo nos dieron el caso bidimensional para la desigualdad de Brunn-Minkowski, resulta natural y atractivo encontrar la versión discreta de la desigualdad pero para cualquier dimensión. Sin embargo, este salto no se ha podido dar, ni siquiera para tres dimensiones. Como vimos que la dificultad de la prueba del *teorema* $2^n$ *de Freiman* no radica en la dimensión, se decidió estudiarla de manera profunda y exhaustiva tanto el caso bidimensional como el caso general para así entender en donde radica su complejidad, y con ello poder entender de manera certera la complejidad del resultado de Grynkiewicz y Serra y en un futuro poder dar la versión del teorema para cualquier dimensión.

Aunque en este trabajo de tesis no se pudo encontrar la generalización del resultado de Grynkiewicz y Serra para cualquier dimensión, sí pudimos generalizarlo desde otra perspectiva: dar un resultado para cuando se sumen más de dos conjuntos que también es otra forma muy intersante de abordar el problema; dicha generalización que es la parte original de este trabajo.

# Capítulo 6

# Apéndice

En este apéndice se enunciarán y se probarán resultados de álgebra lineal sobre hiperplanos en $\mathbb{R}^n$ y algunas relaciones de estos con conjuntos convexos. Estos resultados fueron usados en la prueba del *Teorema* $2^n$ *de Freiman* en el capítulo 2

## 6.1. Álgebra lineal de hiperplanos

Recordemos que $\mathbb{R}^n$ es el espacio euclidiano de dimensión $n$, cuyos elementos (vectores) son las $n$-tuplas ordenadas $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ con $u_i \in \mathbb{R}$, para $1 \leq i \leq n$.

**Definición 6.1.** *Dado un vector* $\mathbf{h}$ *distinto de* $\mathbf{0}$ *en* $\mathbb{R}^n$*, para todo escalar* $\gamma \in \mathbb{R}$*, decimos que:*

$$H = \{\boldsymbol{v} \in \mathbb{R}^n \,|\, (\boldsymbol{h}, \boldsymbol{v}) = \gamma\}$$

*es un* hiperplano *de* $\mathbb{R}^n$ *con* vector normal $\mathbf{h}$*, donde* $(\ ,\ )$ *es el producto interno canónico.*

Notemos que el hiperplano $H = \{\mathbf{v} \in \mathbb{R}^n \,|\, (\mathbf{h}, \mathbf{v}) = \gamma\}$ definido arriba es es un subespacio vectorial de $\mathbb{R}^n$ si y solo si el vector $\mathbf{0}$ está en $H$ (equivalentemente, si y solo si el escalar $\gamma$ es 0). Más aún, la dimensión de un subespacio vectorial, $H = \{\mathbf{v} \in \mathbb{R}^n \,|\, (\mathbf{h}, \mathbf{v}) = 0\}$, es $\dim(H) = n - 1$.

**Ejemplo 6.1.** *Sea* $\boldsymbol{h} = (h_1, h_2)$ *un vector en* $\mathbb{R}^2$*, y sea* $\gamma \in \mathbb{R}$*. El hiperplano:*

$$H = \{\boldsymbol{v} \in \mathbb{R}^2 \,|\, (\boldsymbol{h}, \boldsymbol{v}) = \gamma\}$$

*es el conjunto de vectores* $(x, y) \in \mathbb{R}^2$ *que satisfacen:*

$$((h_1, h_2), (x, y)) = \gamma \text{ luego, } h_1 x + h_2 y = \gamma,$$

*que es la ecuación de una recta en* $\mathbb{R}^2$*. Observemos que para un vector fijo* $\boldsymbol{h} = (h_1, h_2)$ *y distintos valores de* $\gamma \in \mathbb{R}$*, obtenemos rectas paralelas, y si* $\gamma = 0$*, la recta pasa por el origen; en cuyo caso, el hiperplano es un sub-espacio vectorial. De lo anterior tenemos que todo hiperplano en* $\mathbb{R}^2$ *es una recta, y que toda recta en* $\mathbb{R}^2$ *es un hiperplano. Además, todas las rectas que pasan por el origen, es decir, cuya ecuación es* $u_1 x + u_2 y = 0$*, son subespecios vectoriales de dimensión* 1*.*

Dado un hiperplano $H$ en $\mathbb{R}^n$ definimos los siguientes conjuntos.

**Definición 6.2.** *Sea* $\boldsymbol{h}$ *un vector en* $\mathbb{R}^n$, $\gamma$ *un escalar en* $\mathbb{R}$ *y* $H = \{\mathbf{v} \in \mathbb{R}^n \,|\, (\boldsymbol{h}, \boldsymbol{v}) = \gamma\}$ *un hiperplano en* $\mathbb{R}^n$. *Se define el* semi-espacio superior de $H$ *y el* semi-espacio inferior de $H$, *respectivamente, como:*

$$H^{(+1)} := \{\mathbf{v} \in \mathbb{R}^n \,|\, (\mathbf{h}, \mathbf{v}) > \gamma\},$$
$$H^{(-1)} := \{\mathbf{v} \in \mathbb{R}^n \,|\, (\mathbf{h}, \mathbf{v}) < \gamma\}.$$

Podemos observar que por la ley de la tricotomía de los números los conjuntos $H$, $H^{(+1)}$ y $H^{(-1)}$ forman una partición de $\mathbb{R}^n$, es decir, son ajenos dos a dos, y además su unión es $\mathbb{R}^n$. Un ejemplo de estos tres conjuntos se muestra en la figura 6,1.

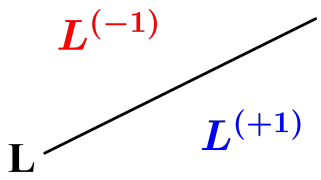



Figura 6.1: Semi-espacios superior e inferior de $L$ en $\mathbb{R}^2$.

Una vez definidos los conjuntos $H^{(+1)}$ y $H^{(-1)}$, procedemos a definir otros conjuntos más generales. Para un entero positivo $m$, denotamos por $\{-1, +1\}^m$ al conjunto de $m$-tuplas $(\mu_1, \ldots, \mu_m)$ con $\mu_i \in \{-1, +1\}$ para todo $1 \leq i \leq m$.

**Definición 6.3.** *Sean* $H_1, \ldots, H_m$ *hiperplanos en* $\mathbb{R}^n$, *y* $(\mu_1, \ldots, \mu_m) \in \{-1, +1\}^m$. *Se define:*

$$H(\mu_1, \ldots, \mu_m) := \bigcap_{i=1}^{m} H^{(\mu_i)}.$$

Las siguientes propiedades elementales se infieren directamente de la definición.

**Observación 6.1.** *Sean* $H_1, \ldots, H_m$ *hiperplanos en* $\mathbb{R}^n$.

1. *Si* $m = 1$, *entonces* $H(+1) = H^{(+1)}$ *y* $H(-1) = H^{(-1)}$.
2. *Los* $2^m$ *conjuntos* $H(\mu_1, \ldots, \mu_m)$ *son disjuntos dos a dos.*

Para entender mejor lo visto anteriormente, obsérvese el ejemplo en $\mathbb{R}^2$ con tres hiperplanos, $L_1$, $L_2$ y $L_3$, ilustrado en la figura 6,2. En dicho ejemplo podemos ver que algunos de los conjuntos $L(\mu_1, \ldots, \mu_m)$ pueden ser vacíos.

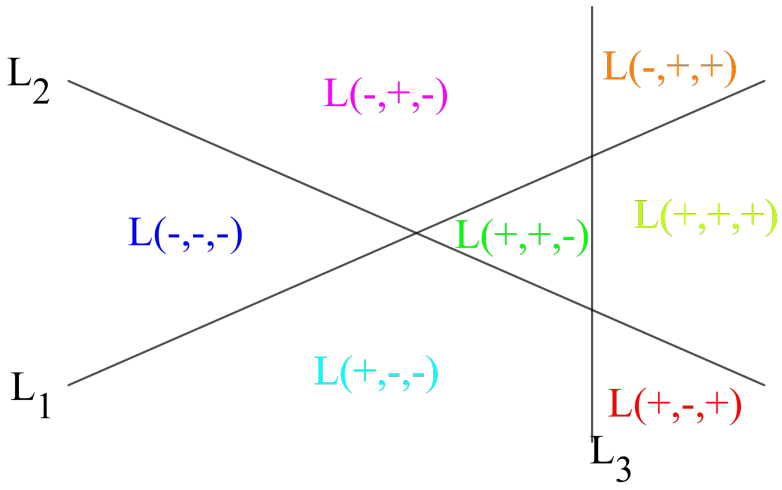



Figura 6.2: Podemos observar que el conjunto $L(-1,-1,+1) = L_1^{-1} \cap L_2^{-1} \cap L_3^{+1} = \emptyset$

Ahora, extenderemos el concepto de *independencia lineal* de vectores a hiperplanos.

**Definición 6.4.** *Sean $H_1, \dots H_m$ hiperplanos de $\mathbb{R}^n$ con vectores normales $\boldsymbol{h}_1, \dots, \boldsymbol{h}_m$ respectivamente. Se dice que los hiperplanos $H_1, \dots, H_m$ son* linealmente independientes *si los vectores $\boldsymbol{h}_1, \dots, \boldsymbol{h}_m$ son linealmente independientes.*

El siguiente lema es una condición suficiente y necesaria para que un conjunto de hiperplanos sea linealmente independiente.

**Lema 6.1.** *Sean $H_1, \dots, H_m$ hiperplanos tales que el vector $\boldsymbol{0} \in H_i$ para todo $1 \leq i \leq m$. Los hiperplanos $H_1, \dots, H_m$ son linealmente independientes si y sólo si $H(\mu_1, \dots, \mu_m) \neq \emptyset$ para todo $(\mu_1, \dots, \mu_m) \in \{-1, +1\}^m$.*

*Demostración.*
Para cada $1 \leq i \leq m$, sea $\mathbf{h}_i \neq \mathbf{0}$ vector normal al hiperplano $H_i$. Recordemos que:

$$H(\mu_1, \dots, \mu_m) = \bigcap_{i=1}^{m} H^{(\mu_i)}.$$

($\Rightarrow$) Supongamos que los hiperplanos $H_1, \dots, H_m$ son linealmente independientes, entonces los vectores $\mathbf{h}_1, \dots, \mathbf{h}_m$ son linealmente independientes. Entonces, podemos construir vectores duales $\mathbf{h}_1^*, \dots, \mathbf{h}_m^*$ tales que $(\mathbf{h}_i, \mathbf{h}_j^*) = \delta_{ij}$, donde:

$$\delta_{ij} = \begin{cases} 1 & si \quad i = j \\ 0 & si \quad i \neq j. \end{cases}$$

Los cuales en la demostración del lema 6,3, demostraremos su existencia. Sea $(\mu_1, \dots, \mu_m) \in$

$\{-1,+1\}^m$, y sea $\mathbf{v} = \sum_{i=1}^{m} \mu_i \mathbf{h}_i^*$. Notemos que:

$$(\mathbf{h}_i, \mathbf{v}) = (\mathbf{h}_i, \sum_{j=1}^{m} \mu_j \mathbf{h}_j^*) = \sum_{j=1}^{m} \mu_j (\mathbf{h}_i, \mathbf{h}_j^*) = \sum_{j=1}^{m} \mu_j \delta_{ij} = \mu_i,$$

entonces, $\mathbf{v} \in H_i^{(\mu_i)}$ para todo $1 \leq i \leq m$, y por lo tanto $H(\mu_1, \ldots, \mu_m) \neq \emptyset$, que es lo que queríamos demostrar.
($\Leftarrow$) Ahora demostraremos que si $H(\mu_1, \ldots, \mu_m) \neq \emptyset$, para todo $(\mu_1, \ldots, \mu_m) \in \{-1,+1\}^m$, entonces los hiperplanos $H_1, \ldots, H_m$ son linealmente independientes, y esto se efectuará por contrapositiva, es decir, demostraremos que si los hiperplanos $H_1, \ldots, H_m$ son linealmente dependientes, entonces existe $(\mu_1, \ldots, \mu_m) \in \{-1,+1\}^m$ tal que $H(\mu_1, \ldots, \mu_m) = \emptyset$. Sean $H_1, \ldots, H_m$ linealmente dependientes. Entonces, los vectores $\mathbf{h}_1 \ldots, \mathbf{h}_m$ son linealmente dependientes, es decir, existen $\alpha_1, \ldots, \alpha_m \in \mathbb{R}$, no todos cero, tales que:

$$\sum_{i=1}^{m} \alpha_i \mathbf{h}_i = 0.$$

Sin pérdida de generalidad supongamos que $\alpha_1 \neq 0$. Definamos $\mu_i$, para $1 \leq i \leq m$, de la siguiente manera:

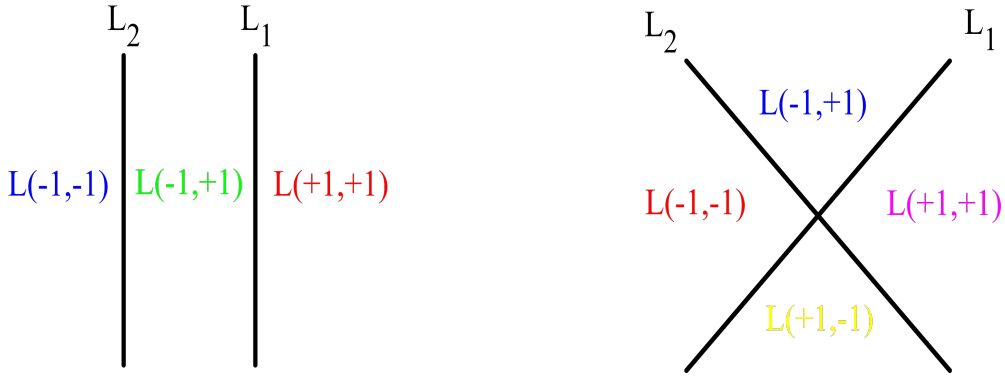
$$\mu_i = \begin{cases} 1 & si \quad \alpha_i > 0 \\ -1 & si \quad \alpha_i \leq 0. \end{cases}$$

Observemos que $\mu_i \alpha_i \geq 0$ para toda $1 \leq i \leq m$, y en particular $\mu_1 \alpha_1 > 0$. Probaremos que $H(\mu_1, \ldots, \mu_m) = \emptyset$. Supongamos lo contrario, es decir, supongamos que existe $\mathbf{v} \in \mathbb{R}^n$ tal que $\mathbf{v} \in H^{(\mu_i)}$ para todo $1 \leq i \leq m$. Entonces, si $\mu_i = 1$ tenemos que $(\mathbf{h}_i, \mathbf{v}) > 0$, y como $\alpha_i > 0$, se implica que $\alpha_i(\mathbf{h}_i, \mathbf{v}) \geq 0$. Análogamente, si $\mu_i = -1$, tenemos que $(\mathbf{h}_i, \mathbf{v}) < 0$, y como $\alpha_i \leq 0$, se implica que $\alpha_i(\mathbf{h}_i, \mathbf{v}) \geq 0$. De lo anterior tenemos que para todo $1 \leq i \leq m$, $\alpha_i(\mathbf{h}_i, \mathbf{v}) \geq 0$, y en especial $\alpha_1(\mathbf{h}_1, \mathbf{v}) > 0$. Ahora veamos lo siguiente:

$$0 = (\mathbf{v}, 0) = (\mathbf{v}, \sum_{i=1}^{m} \alpha_i \mathbf{h}_i) = \sum_{i=1}^{m} \alpha_i (\mathbf{v}, \mathbf{h}_i) > 0,$$

lo cual es una contradicción. Por lo tanto, $H(\mu_1, \ldots, \mu_m) = \emptyset$ que era lo que queríamos probar. □

Para entender mejor el lema anterior pensemos en dos dimensiones. Dos rectas, $L_1$ y $L_2$, en $\mathbb{R}^2$ pueden ser linealmente dependientes (si son paralelas), o linealmente independientes (si no son paralelas). En el primer caso, tenemos que, o bien $L(+1,-1) = \emptyset$, o bien $L(-1,+1) = \emptyset$ (ver figura 6.3a). En el segundo caso tenemos las cuatro regiones no vacías (ver figura 6.3b). Para $m \geq 3$, naturalmente, un conjunto de $L_1, \ldots, L_m$ rectas será linealmente dependiente, como en la figura 6.2; pues $m \geq 3$ vectores normales no pueden ser linealmente independientes. En tal caso, podemos observar que, en el plano, es imposible que $m \geq 3$ rectas determinen $2^m$ regiones.




(a) Como $L_1$ y $L_2$ son dos rectas paralelas, $L(+1,-1) = L_1^{+1} \cap L_2^{-1} = \emptyset$

(b) Como $L_1$ y $L_2$ no son rectas paralelas, tenemos que las 4 regiones son no vacías.

Figura 6.3: Las rectas de la derecha son dos rectas linealmente dependientes, mientras que las rectas de la izquierda son linealmente independientes.

El siguiente lema es un resultado básico de álgebra lineal que usaremos en repetidas ocasiones a lo largo de la tesis, por lo cual vale la pena demostrarlo.

**Lema 6.2.** *Sean $H_1, \ldots, H_m$ hiperplanos linealmente independientes en $\mathbb{R}^n$ tales que el vector $\boldsymbol{0} \in H_i$ para todo $1 \leq i \leq m$. Entonces:*

$$\dim(\bigcap_{i=1}^{m} H_i) = n - m.$$

*En particular, si $m = n$, entonces:*

$$\bigcap_{i=1}^{m} H_i = \{0\}.$$

*Demostración.* Para demostrar esto, demostraremos que $\dim(\bigcap_{i=1}^{m} H_i) \leq n - m$ y que $\dim(\bigcap_{i=1}^{m} H_i) \geq n - m$; empezando por demostrar lo primero.

Sea $\mathbf{h}_i$ el vector normal al hiperplano $H_i$ y sea $W = \bigcap_{i=1}^{m} H_i$. Como los hiperplanos $H_1, \ldots, H_m$ son linealmente independientes, entonces los vectores $\mathbf{h}_1, \ldots, \mathbf{h}_m$ son linealmente independientes. Consideremos:

$$W^{\perp} = \{\mathbf{v} \in \mathbb{R}^n \mid (\mathbf{v}, \mathbf{w}) = 0 \text{ para todo } \mathbf{w} \in W\}.$$

Como $(\mathbf{h}_i, \mathbf{w}) = 0$ para todo $\mathbf{w} \in H_i$, entonces $(\mathbf{h}_i, \mathbf{w}) = 0$ para todo $\mathbf{w} \in W$, luego $\mathbf{h}_i \in W^{\perp}$ para todo $1 \leq i \leq m$. Como los vectores $\mathbf{h}_1, \ldots, \mathbf{h}_m$ son linealmente independientes, entonces $\dim(W^{\perp}) \geq m$, y dado que $\dim(W) + \dim(W^{\perp}) = n$, entonces $\dim(W) \leq n - m$.

Ahora demostraremos que $\dim(W) \geq n-m$ y la demostración se efectuará por inducción sobre $m$. Si $m = 1$, entonces $W = H_1$ y como $H_1$ es un hiperplano con $\mathbf{0} \in H_1$, sabemos que $H_1$ es un subespacio de dimensión $n-1$. Definimos $W' = \bigcap_{i=1}^{m-1} H_i$. Por hipótesis de inducción tenemos que $\dim(W') \geq n-m+1$. Luego:

$$\dim(W' \cap H_m) = \dim(W') + \dim(H_m) - \dim(W' + H_m),$$

y como $W = W' \cap H_m$, entonces:

$$\begin{aligned}\dim(W) &= \dim(W') + \dim(H_m) - \dim(W' + H_m) \\ &\geq \dim(W') + \dim(H_m) - \dim(\mathbb{R}^n) \\ &\geq (n-m+1) + (n-1) - n \\ &= n - m.\end{aligned}$$

Como $\dim(\bigcap_{i=1}^{m} H_i) \leq n-m$ y $\dim(\bigcap_{i=1}^{m} H_i) \geq n-m$, entonces $\dim(\bigcap_{i=1}^{m} H_i) = n-m$ que es lo que se quería demostrar.

Finalmente, observemos que $n = m$ implica $\dim(\bigcap_{i=1}^{m} H_i) = n-n = 0$, luego $\bigcap_{i=1}^{m} H_i = \{0\}$. □

Antes de continuar requerimos ver la definición de conjunto convexo y envolvente o cubierta convexa.

**Definición 6.5.** *Sea $S$ un subconjunto de $\mathbb{R}^n$. Se dice que $S$ es* convexo *si para todo $\boldsymbol{s}_1$ y $\boldsymbol{s}_2$ en $S$, y para todo $\alpha \in \mathbb{R}$ con $0 \leq \alpha \leq 1$, se tiene que:*

$$\alpha \boldsymbol{s}_1 + (1-\alpha)\boldsymbol{s}_2 \in S.$$

*Además si $S$ no es convexo se define su* envolvente convexa*, denotada por $conv(S)$ al convexo más pequeño de $\mathbb{R}^n$ que contiene a $S$, es decir, si $T$ es un convexo tal que $S \subset T$, entonces $conv(S) \subset T$.*

En la figura 6,4 se puede apreciar a un conjunto y a su envolvente conexa.

Las siguientes son propiedades elementales que tienen los conjunto convexos.

**Observación 6.2.** *Sean $S$ y $T$ subconjuntos de $\mathbb{R}^n$. Las siguientes propiedades se cumplen:*

1. *$S$ es convexo si y sólo si $conv(S) = S$.*
2. *Si $S$ y $T$ son convexos, entonces $S \cap T$ es convexo.*
3. *Si $S \subset T$, entonces $conv(S) \subset conv(T)$.*
4. *Si $\boldsymbol{s}_1, \ldots, \boldsymbol{s}_k \in S$, con $k \in \mathbb{Z}^+$, entonces $\alpha_1 \boldsymbol{s}_1 + \cdots + \alpha_k \boldsymbol{s}_k \in S$ para todo $\alpha_1, \ldots, \alpha_k \geq 0$, tales que $\alpha_1 + \cdots + \alpha_k = 1$.*

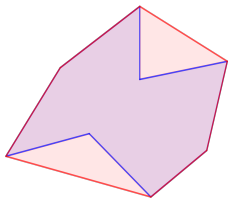


Figura 6.4: En esta figura podemos observar a un conjunto delimitado por el contorno azul y a su envolvente convexa, delimitada por el contorno rojo.

5. $conv(S+T) = conv(S) + conv(T)$.

Observemos que por inducción podemos demostrar que para todo $k \geq 0$, si $S_1, \ldots, S_k$ son conjuntos convexos, entonces $\bigcap_{i=1}^{k} S_k$ es un conjunto convexo. En seguida demostraremos la convexidad de los conjuntos definidos anteriormente.

**Proposición 6.1.** *Sean $H, H_1, \ldots H_m$ hiperplanos de $\mathbb{R}^n$, entonces los siguientes conjuntos son convexos:*

1. $H$
2. $H^{(+1)}$ *y* $H^{(-1)}$.
3. $H(\mu_1, \ldots, \mu_m)$ *para todo* $(\mu_1, \ldots, \mu_m) \in \{-1, +1\}^m$.

*Demostración.*

1. Sea $\mathbf{h}_1, \mathbf{h}_2$ vectores en $H$ y sea $\mathbf{h}$ vector normal de $H$. Como $\mathbf{h}$ es vector normal de $H$, entonces existe escalar $\gamma$ tal que $(\mathbf{h}, \mathbf{v}) = \gamma$ para todo $\mathbf{v} \in H$. Para probar que $H$ es convexo basta probar que si $0 \leq \alpha \leq 1$, entonces $(\alpha\mathbf{h}_1 + (1-\alpha)\mathbf{h}_2, \mathbf{h}) = \gamma$. Observemos que:

$$\begin{aligned}(\alpha\mathbf{h}_1 + (1-\alpha)\mathbf{h}_2, \mathbf{h}) &= (\alpha\mathbf{h}_1, \mathbf{h}) + ((1-\alpha)\mathbf{h}_2, \mathbf{h}) \\ &= \alpha(\mathbf{h}_1, \mathbf{h}) + (1-\alpha)(\mathbf{h}_2, \mathbf{h}) \\ &= \alpha\gamma + (1-\alpha)\gamma \\ &= (\alpha + 1 - \alpha)\gamma \\ \textit{luego,}& \\ (\alpha\mathbf{h}_1 + (1-\alpha)\mathbf{h}_2, \mathbf{h}) &= \gamma.\end{aligned}$$

   Por lo tanto $H$ es convexo.

2. Sean $\mathbf{h}_1, \mathbf{h}_2$ vectores en $H^{(+1)}$ y $\mathbf{h}$ vector normal de $H$. Como $\mathbf{h}$ es vector normal de $H$, entonces existe escalar $\gamma$ tal que $(\mathbf{h}, \mathbf{v}) = \gamma$ para todo $\mathbf{v} \in H$. Para probar que $H^{(+1)}$ es convexo basta probar que si $0 \leq \alpha \leq 1$, entonces $(\alpha\mathbf{h}_1 + (1-\alpha)\mathbf{h}_2, \mathbf{h}) > \gamma$. Observemos que:

$$\begin{aligned}(\alpha\mathbf{h}_1 + (1-\alpha)\mathbf{h}_2, \mathbf{h}) &= (\alpha\mathbf{h}_1, \mathbf{h}) + ((1-\alpha)\mathbf{h}_2, \mathbf{h}) \\ &= \alpha(\mathbf{h}_1, \mathbf{h}) + (1-\alpha)(\mathbf{h}_2, \mathbf{h}) \\ &> \alpha\gamma + (1-\alpha)\gamma \\ &= (\alpha + 1 - \alpha)\gamma\end{aligned}$$

Por lo tanto $H^{+1}$ es convexo. La demostración de que $H^{(-1)}$ es convexo es análoga a la anterior.

3. Recordemos que:

$$H(\mu_1, \ldots, \mu_m) = \bigcap_{i=1}^{m} H^{(\mu_i)}.$$

Por el inciso anterior tenemos que cada $H^{(\mu_i)}$ es un conjunto convexo y además sabemos que la intersección de conjuntos convexos es convexa, por lo tanto $H(\mu_1, \ldots, \mu_m)$ es un conjunto convexo.

□

**Proposición 6.2.** *Sean $H_1, \ldots, H_m$ hiperplanos en $\mathbb{R}^n$ tales que el vector $\mathbf{0} \in H_i$ para todo $1 \leq i \leq m$. Sea $S$ un subconjunto de $\mathbb{R}^n$ tal que:*

$$S \cap H(\mu_1, \ldots, \mu_m) \neq \emptyset$$

*para todo $\mu_1, \ldots, \mu_m \in \{-1, 1\}$. Entonces:*

$$conv\,(S) \cap \left(\bigcap_{i=1}^{m} H_i\right) \neq \emptyset.$$

*Demostración.* La demostración se efectuará por inducción sobre $m$.

Sea $m = 1$ y sea $\mathbf{h}_1$ vector normal a $H_1$. Por hipótesis tenemos que $H^{(+1)} \cap S$ y $H^{(-1)} \cap S$ son no vacíos, entonces existen $\mathbf{s}_1, \mathbf{s}_2 \in S$, tales que:

$$\begin{aligned}(\mathbf{h}_1, \mathbf{s}_1) =& \alpha_1 > 0 \\ & y \\ (\mathbf{h}_1, \mathbf{s}_2) =& \alpha_2 < 0.\end{aligned}$$

Observemos que:

$$\frac{\alpha_1}{\alpha_1 - \alpha_2} + \frac{-\alpha_2}{\alpha_1 - \alpha_2} = \frac{\alpha_1 - \alpha_2}{\alpha_1 - \alpha_2} = 1.$$

Además que $\frac{-\alpha_2}{\alpha_1-\alpha_2}, \frac{\alpha_1}{\alpha_1-\alpha_2} \in [0,1]$.

Definimos $\mathbf{s}$ de la siguiente manera:

$$\mathbf{s} = \frac{-\alpha_2}{\alpha_1-\alpha_2}\mathbf{s}_1 + \frac{\alpha_1}{\alpha_1-\alpha_2}\mathbf{s}_2.$$

Como $conv(S)$ es el convexo más pequeño que contiene a $S$, entonces $\mathbf{s}_1, \mathbf{s}_2 \in conv(S)$ y por lo tanto $\mathbf{s} \in conv(S)$. Ahora calculemos $(\mathbf{s}, \mathbf{h}_1)$:

$$\begin{aligned}(\mathbf{s},\mathbf{h}_1) =& (\frac{-\alpha_2}{\alpha_1-\alpha_2}\mathbf{s}_1 + \frac{\alpha_1}{\alpha_1-\alpha_2}\mathbf{s}_2, \mathbf{h}_1)\\ =& \frac{-\alpha_2}{\alpha_1-\alpha_2}(\mathbf{s}_1,\mathbf{h}_1) + \frac{\alpha_1}{\alpha_1-\alpha_2}(\mathbf{s}_2,\mathbf{h}_1)\\ =& \frac{-\alpha_2\alpha_1}{\alpha_1-\alpha_2} + \frac{\alpha_1\alpha_2}{\alpha_1-\alpha_2}\\ =& 0\end{aligned}$$

$$\begin{aligned}&luego,\\ (\mathbf{s},\mathbf{h}_1) =& 0.\end{aligned}$$

Luego $\mathbf{s} \in H_1$ y por lo tanto $conv(S) \cap H_1 \neq \emptyset$.

Sea $m \geq 2$ y supongamos que el lema se cumple para todo $0 \leq k < m$. Definamos $S^{(+1)}$ y $S^{(-1)}$ de la siguiente manera:

$$\begin{aligned}S^{(+1)} =& S \cap H_m^{(+1)}\\ &y\\ S^{(-1)} =& S \cap H_m^{(-1)}\end{aligned}$$

Para todo $\mu_1, \ldots, \mu_n \in \{-1, +1\}$, como $S \cap H(\mu_1, \ldots, \mu_m) \neq \emptyset$, entonces:

$$S \cap H(\mu_1, \ldots, \mu_{m-1}, +1) \neq \emptyset$$

entonces,

$$\left(S \cap \left(\bigcap_{i=1}^{m-1} H_i^{(\mu_i)}\right)\right) \cap H_m^{(+1)} \neq \emptyset$$

luego,

$$\left(S \cap H_m^{(+1)}\right) \cap \left(\bigcap_{i=1}^{m-1} H_i^{(\mu_i)}\right) \neq \emptyset$$

y por lo tanto,

$$S^{(+1)} \cap \left(\bigcap_{i=1}^{m-1} H_i^{(\mu_i)}\right) \neq \emptyset.$$

De lo anterior tenemos que $S^{(+1)}$ cumple las hipótesis del lema y por hipótesis de inducción y por el inciso 4 de la proposición 6,2, se tiene que para todo conjunto de vectores $\mathbf{s}_1, \ldots, \mathbf{s}_k \in$

$S^{(+1)}$ y escalares $\alpha_1, \ldots, \alpha_k \in \mathbb{R}$ con $\alpha_i \geq 0$ para todo $1 \leq i \leq k$ y $\alpha_1 + \cdots + \alpha_k = 1$; se cumple que:

$$\mathbf{s}^{(+1)} := \sum_{i=1}^{k} \alpha_i \mathbf{s}_i \in (conv(S^{(+1)})) \cap (\bigcap_{i=1}^{m-1} H_i).$$

Como cada $\mathbf{s}_i \in S^{(+1)}$ y $S^{(+1)} = S \cap H^{(+1)}$, entonces $\mathbf{s}_i \in H^{(+1)}$ y además como $H^{(+1)}$ es un conjunto convexo, obtenemos también que $\mathbf{s}^{(+1)} \in H^{(+1)}$.

Ahora observemos que como $S^{(+1)} \subset S$, entonces $conv(S^{(+1)}) \subset conv(S)$, lo cual nos dice que $\mathbf{s}^{(+1)} \in conv(S)$, luego:

$$\mathbf{s}^{(+1)} \in conv(S) \cap (\bigcap_{i=1}^{m-1} H_i).$$

Usando los mismos argumentos tenemos que existe $\mathbf{s}^{(-1)} \in H^{(-1)}$ tal que:

$$\mathbf{s}^{(-1)} \in (conv(S^{-1})) \cap (\bigcap_{i=1}^{m-1} H_i) \subset conv(S) \cap (\bigcap_{i=1}^{m-1} H_i).$$

Definamos $T = \{\mathbf{s}^{(+1)}, \mathbf{s}^{(-1)}\}$. Como $\mathbf{s}^{(+1)}, \mathbf{s}^{(-1)} \in conv(S) \cap (\bigcap_{i=1}^{m-1} H_i)$, entonces tenemos que:

$$T \subset conv(S) \cap (\bigcap_{i=1}^{m-1} H_i).$$

Sabemos que un conjunto es $X$ es convexo si y sólo si $X = conv(X)$ y que la intersección de conjuntos convexos es convexa. Aplicando lo anterior tenemos que:

$$T \subset conv(S) \cap (\bigcap_{i=1}^{m-1} H_i),$$

entonces,

$$conv(T) \subset conv(conv(S) \cap (\bigcap_{i=1}^{m-1} H_i))$$

luego,

$$conv(T) \subset conv(S) \cap (\bigcap_{i=1}^{m-1} H_i)$$

Como $T \cap H_m^{(\mu_m)} \neq \emptyset$, para todo $\mu_m \in \{-1, 1\}$, entonces por hipótesis de inducción aplicada a $T$, tenemos que:

$$conv(T) \cap H_m \neq \emptyset,$$

es decir, existe $\mathbf{s}$ tal que:

$$\mathbf{s} \in conv(T) \cap H_m \subset conv(T) \subset conv(S) \cap (\bigcap_{i=1}^{m-1} H_i).$$

De lo anterior tenemos que $\mathbf{s} \in H_m$, $\mathbf{s} \in conv(S)$ y $\mathbf{s} \in \bigcap_{i=1}^{m-1} H_i$ y por lo tanto:

$$\mathbf{s} \in conv(S) \cap (\bigcap_{i=1}^{m} H_i).$$

Que es lo que se quería demostrar. □

Para entender mejor esta proposición, observemos la figura 6,5.

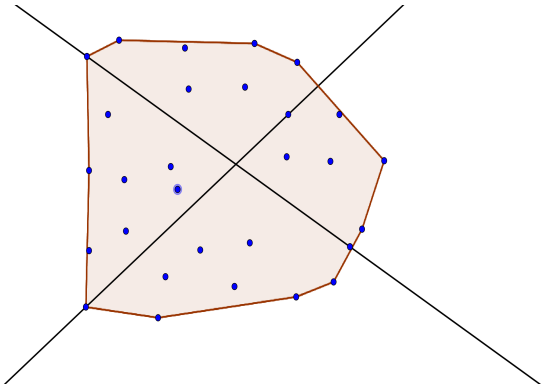


Figura 6.5: Ejemplo de la proposición 6,2, donde los puntos azules pertenecen a nuestro conjunto $S$ y la sección rosa a su envolvente convexa.

Para finalizar la sección se demostrará un colorario de lo que relaciona todo lo expuesta en esta sección.

**Corolario 6.1.** *Sean $H_1, \ldots, H_n$ hiperplanos en $\mathbb{R}^n$ tales que $\boldsymbol{0} \in H_i$ para todo $i = 1, \ldots, n$, y sea $S \subset \mathbb{R}^n$ tal que:*

$$S \cap H(\mu_1, \ldots, \mu_n) \neq \emptyset,$$

*para todo $\mu_1, \ldots, \mu_m \in \{-1, 1\}$. Entonces:*

$$\boldsymbol{0} \in conv(S).$$

*Demostración.*
Como $S \cap H(\mu_1, \ldots, \mu_n) \neq \emptyset$, entonces tenemos que:

$$H(\mu_1, \ldots, \mu_n) = \bigcap_{i=1}^{n} H_i^{(\mu_i)} \neq \emptyset$$

y por el lema 6,1 los hiperplanos $H_1, \ldots, H_n$ son linealmente independientes. Además como $S \cap H(\mu_1, \ldots, \mu_n) \neq \emptyset$, entonces por la proposición 6,2 tenemos que:

$$conv(S) \cap (\bigcap_{i=1}^{n} H_i) \neq \emptyset.$$

Como los hiperplanos $H_1, \ldots, H_n$ son linealmente independientes por el lema 6,2 tenemos que:

$$\bigcap_{i=1}^{n} H_i = \{0\},$$

luego:

$$conv(S) \cap (\bigcap_{i=1}^{n} H_i) \neq \emptyset$$

entonces,

$$conv(S) \cap \{0\} \neq \emptyset$$

y por lo tanto:

$$0 \in conv(S)$$

que es lo que se quería demostrar. □

## 6.2. Resultados específicos

**Lema 6.3.** *Sean $H_1, \ldots, H_n$ hiperplanos linealmente independientes en $\mathbb{R}^n$ tales que $\boldsymbol{0} \in H_i$ para todo $1 \leq i \leq n$ y con vectores normales $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_n$ respectivamente. Definamos la recta $L_j$, para todo $1 \leq j \leq n$, de la siguiente manera:*

$$L_j = \bigcap_{i \neq j} H_i.$$

*Entonces:*

$$\mathbb{R}^n = H_j \oplus L_j.$$

*Además existe una base dual $\{\boldsymbol{h}_1^*, \ldots, \boldsymbol{h}_n^*\}$ de $\mathbb{R}^n$ tal que:*

$$(\boldsymbol{h}_i, \boldsymbol{h}_j^*) = \delta_{ij} = \begin{cases} 1 & si \quad i = j \\ \\ 0 & si \quad i \neq j \end{cases}$$

*El conjunto $\{\boldsymbol{h}_1^*, \ldots, \boldsymbol{h}_{j-1}^*, \boldsymbol{h}_{j+1}^*, \ldots, \boldsymbol{h}_n^*\}$ es base del hiperplano $H_j$ y el vector $\boldsymbol{h}_j^*$ es base de la recta $L_j$.*

*Demostración.*
Primero procederemos a construir los vectores duales $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$.

Como $L_j$ es la intersección de $n-1$ hiperplanos linealmente independientes, entonces por el lema 6,2 tenemos que $L_j$ es un subespacio de $\mathbb{R}^n$ de dimensión 1. Sea $\mathbf{l}_j$ base de la recta $L_j$ .

Como $\mathbf{l}_j$ es base de la recta $L_j$ y $L_j = \bigcap_{i \neq j}^{n} H_i$, entonces $\mathbf{l}_j \in H_i$ para todo $1 \leq i \leq n$ e $i \neq j$. Al estar el vector $\mathbf{l}_j$ en el hiperplano $H_i$, entonces tenemos que:

$$(\mathbf{l}_j, \mathbf{h}_i) = 0.$$

Podemos observar que si $(\mathbf{l}_j, \mathbf{h}_j) = 0$ tendríamos que $\mathbf{l}_j$ está también en el hiperplano $H_j$, lo cual nos implicaría que $\mathbf{l}_j \in \bigcap_{i=1}^{n} H_i$, pero por el lema 6,2 tenemos que $\bigcap_{i=1}^{n} H_i = \{\mathbf{0}\}$, luego el vector $\mathbf{l}_j$ resultaría ser el vector $\mathbf{0}$, lo cual es una contradicción y por lo tanto $(\mathbf{h}_j, \mathbf{l}_j) \neq 0$.

De lo anterior podemos definir el vector $\mathbf{h}_j^*$ de la siguiente manera:

$$\mathbf{h}_j^* =: \frac{\mathbf{l}_j}{(\mathbf{h}_j, \mathbf{l}_j)}.$$

Ya construido el conjunto $\{\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*\}$, continuaremos por demostrar que:

$$(\mathbf{h}_i, \mathbf{h}_j^*) = \delta_{ij} = \begin{cases} 1 & si \quad i = j \\ \\ 0 & si \quad i \neq j \end{cases}$$

Primero calculemos $(\mathbf{h}_i, \mathbf{h}_j^*)$, para $i \neq j$:

$$\begin{aligned} (\mathbf{h}_i, \mathbf{h}_j^*) &= (\mathbf{h}_i, \frac{\mathbf{l}_j}{(\mathbf{h}_j, \mathbf{l}_j)}) \\ &= \frac{(\mathbf{h}_i, \mathbf{l}_j)}{(\mathbf{h}_j, \mathbf{l}_j)} \\ &= \frac{0}{(\mathbf{h}_j, \mathbf{l}_j)} \\ \textit{luego}, & \\ (\mathbf{h}_i, \mathbf{h}_j^*) &= 0. \end{aligned}$$

Ahora calculemos $(\mathbf{h}_j, \mathbf{h}_j^*)$:

$$\begin{aligned} (\mathbf{h}_j, \mathbf{h}_j^*) &= (\mathbf{h}_j, \frac{\mathbf{l}_j}{(\mathbf{h}_j, \mathbf{l}_j)}) \\ &= \frac{(\mathbf{h}_j, \mathbf{l}_j)}{(\mathbf{h}_j, \mathbf{l}_j)} \\ \textit{entonces}, & \\ (\mathbf{h}_i, \mathbf{h}_j^*) &= 1. \end{aligned}$$

Procederemos ahora por demostrar que los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_{j-1}^*, \ldots, \mathbf{h}_{j+1}^*, \ldots, \mathbf{h}_n^*$ forman una base de $H_j$ y que el vector $\mathbf{h}_j^*$ es base de la recta $L_j$. Observemos que la recta $L_j$ es un subespacio de dimensión 1 entonces para demostrar que el vector $\mathbf{h}_j^*$ es base, basta demostrar que $\mathbf{h}_j^* \in L_j$. Además observemos que el hiperplano $H_j$ es un subespacio de dimensión $n-1$ y los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_{j-1}^*, \ldots, \mathbf{h}_{j+1}^*, \ldots, \mathbf{h}_n^*$ son $n-1$ vectores, entonces para demostrar que los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_{j-1}^*, \ldots, \mathbf{h}_{j+1}^*, \ldots, \mathbf{h}_n^*$ forman una base de $H_j$ basta demostrar que son vectores en $H_j$ y que son linealmente independientes.

Como $(\mathbf{h}_i, \mathbf{h}_j^*) = 0$, para todo $i \neq j$, entonces el vector $\mathbf{h}_j^*$ está en el hiperplano $H_i$. De lo anterior tenemos que los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_{j-1}^*, \ldots, \mathbf{h}_{j+1}^*, \ldots, \mathbf{h}_n^* \in H_j$; además como el vector $\mathbf{h}_j^*$ es múliplo escalar del vector $\mathbf{l}_j$, entonces el vector $\mathbf{h}_j^*$ está en la recta $L_j$.

Ahora demostraremos que los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ son linealmente independientes. Sean $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ tales que:

$$\sum_{j=1}^{n} \alpha_j \mathbf{h}_j^* = 0.$$

Observemos lo siguiente:

$$\begin{aligned} 0 &= (\mathbf{h}_i, \mathbf{0}) \\ &= (\mathbf{h}_i, \sum_{j=1}^{n} \alpha_j \mathbf{h}_j^*) \\ &= \sum_{j=1}^{n} \alpha_j (\mathbf{h}_i, \mathbf{h}_j^*) \\ &= \alpha_j (\mathbf{h}_i, \mathbf{h}_i^*) \\ &= \alpha_i \end{aligned}$$

*entonces*,

$$\alpha_i = 0.$$

Pero lo anterior se vale para todo $1 \leq i \leq n$, entonces tenemos que $\alpha_i = 0$ para todo $1 \leq i \leq n$, y por lo tanto los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ son linealmente independientes.

Para finalizar demostraremos que los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ forman una base de $\mathbb{R}^n$ y que $\mathbb{R}^n = H_j \oplus L_j$.

Como los vectores $\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*$ son $n$ vectores linealmente independientes, entonces forman una base de $\mathbb{R}^n$.

Por último como $\{\mathbf{h}_1^*, \ldots, \mathbf{h}_n^*\}$ es una base de $\mathbb{R}^n$, tales que $\{\mathbf{h}_1^*, \ldots, \mathbf{h}_{j-1}^*, \ldots, \mathbf{h}_{j+1}^*, \ldots, \mathbf{h}_n^*\}$ es una base de $H_j$ y $\{\mathbf{h}_j^*\}$ es una base de $L_j$, entonces el álgebra lineal nos dice que:

$$\mathbb{R}^n = L_j \oplus H_j.$$

Por lo tanto queda demostrado el lema. □

Para finalizar la sección demostraremos el resultado principal de estas tres secciones que usaremos en la demostración del *teorema* $2^n$ *de Freiman*, para enterlo mejor estará distribuido en los siguientes 3 lemas.

**Lema 6.4.** *Sean $H_1$,..., $H_n$ hiperplanos linealmente independientes en $\mathbb{R}^n$ tales que el vector $\boldsymbol{0} \in H_i$, para toda $1 \leq i \leq n$. Se definen los subespacio $Q_1, \ldots, Q_n$, como:*

$$Q_i = H_i \cap H_n,$$

*para todo $1 \leq i \leq n-1$. Entonces, $\dim(Q_i) = n-2$ y más aún los subespacios $Q_1$,...,$Q_{n-1}$ son linealmente independientes, vistos como hiperplanos en $H_n$.*

*Demostración.*

Como cada $Q_i$ es intersección de dos subespacios de $\mathbb{R}^n$, entonces cada $Q_i$ es subespacio de $\mathbb{R}^n$, y además como están contenidos en $H_n$, en especial son subespacios de $H_n$. Por el lema 6.2 tenemos que $\dim(Q_i) = n - 2$.

Ahora probaremos que $Q_1, \ldots, Q_{n-1}$ son linealmente independientes en $H_n$. Sean $\mathbf{h}_1, \ldots, \mathbf{h}_n$ vectores normales a $H_1, \ldots, H_n$ respectivamente. Se define el vector $\mathbf{q}_i$ de la siguiente manera:

$$\mathbf{q}_i = \mathbf{h}_i - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n,$$

para todo $1 \leq i \leq n-1$. Para probar que los los subespacios $Q_1, \ldots, Q_{n-1}$ son linealmente independientes, se probará que los vectores $\mathbf{q}_i$ son linealmente independientes y además que son vectores normales a los subespacios $Q_i$. Supongamos que existen $\alpha_1, \ldots, \alpha_{n-1}$ elementos en $\mathbb{R}$, tales que:

$$\sum_{i=1}^{n-1} \alpha_i \mathbf{q}_i = \mathbf{0}.$$

De lo anterior tenemos que:

$$\begin{aligned}
\mathbf{0} &= \sum_{i=1}^{n-1} \alpha_i \mathbf{q}_i \\
&= \sum_{i=1}^{n-1} \alpha_i (\mathbf{h}_i - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n) \\
&= \sum_{i=1}^{n-1} (\alpha_i \mathbf{h}_i - \frac{\alpha_i(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n) \\
&= \sum_{i=1}^{n-1} \alpha_i \mathbf{h}_i - (\sum_{i=1}^{n-1} \frac{\alpha_i(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)})\mathbf{h}_n.
\end{aligned}$$

Definiendo a $\alpha_n$ como $\alpha_n := -\sum_{i=1}^{n-1} \frac{\alpha_i(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}$ y sustituyendo en lo anterior, obtenemos que:

$$\sum_{i=1}^{n-1} \alpha_i \mathbf{h}_i + \alpha_n \mathbf{h}_n = \sum_{i=1}^{n} \alpha_i \mathbf{h}_i = 0$$

Como los vectores $\mathbf{h}_1 \ldots, \mathbf{h}_n$ son linealmente independientes, obtenemos que $\alpha_i = 0$ para todo $1 \leq i \leq n$, en especial los escalares $\alpha_1, \ldots, \alpha_{n-1}$ son 0 y por lo tanto los vectores $\mathbf{q}_1 \ldots, \mathbf{q}_{n-1}$ son linealmente independientes.

Por último se probará que los subespacios $Q_1, \ldots, Q_{n-1}$ son linealmente independientes en $H_n$, es decir, que para todo $1 \leq i \leq n-1$, $\mathbf{q}_i$ está en $H_n$ y que $(\mathbf{v}, \mathbf{q}_i) = 0$ para todo $\mathbf{v} \in Q_i$.

Observemos lo siguiente:

$$\begin{aligned}(\mathbf{q}_i, \mathbf{h}_n) &= (\mathbf{h}_i - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n, \mathbf{h}_n) \\ &= (\mathbf{h}_i, \mathbf{h}_n) - (\frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n, \mathbf{h}_n) \\ &= (\mathbf{h}_i, \mathbf{h}_n) - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}(\mathbf{h}_n, \mathbf{h}_n) \\ &= (\mathbf{h}_i, \mathbf{h}_n) - (\mathbf{h}_n, \mathbf{h}_i)\end{aligned}$$

*luego,*

$$(\mathbf{q}_i, \mathbf{h}_n) = 0.$$

De lo anterior y por definición de $H_n$, tenemos que $\mathbf{q}_i$ está en $H_n$, para todo $1 \leq i \leq n-1$. Sea $\mathbf{v} \in Q_i$, entonces obtenemos lo siguiente:

$$\begin{aligned}(\mathbf{v}, \mathbf{q}_i) &= (\mathbf{v}, \mathbf{h}_i - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n) \\ &= (\mathbf{v}, \mathbf{h}_i) - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}(\mathbf{v}, \mathbf{h}_n)\end{aligned}$$

Como $\mathbf{v} \in H_i$ y $\mathbf{h}_i$ es vector normal a $\mathbf{h}_i$, tenemos que $(\mathbf{v}, \mathbf{h}_i) = 0$. Análogamente tenemos que $(\mathbf{v}, \mathbf{h}_n) = 0$, luego $(\mathbf{v}, \mathbf{q}_i) = 0$ y por lo tanto el vector $\mathbf{q}_i$ es vector normal a $Q_i$, para todo $1 \leq i \leq n-1$. De lo anterior se sigue que los subespacios $Q_i, \ldots, Q_{n-1}$ son espacios linealmente independientes en $H_n$, que es lo que se quería demostrar. □

**Lema 6.5.** *Sean $H_1, \ldots, H_n$ hiperplanos linealmente independientes tales que el vector $\boldsymbol{0} \in H_i$ para todo $1 \leq i \leq n$; sean $Q_1, \ldots, Q_n$ definidos como en el lema 6,4. Sea la recta $L_n$ definida como en el lema 6,3. Se definen la función $\pi : \mathbb{R}^n \to H_n$ como la proyección correspondiente a la descomposición de la suma directa de:*

$$\mathbb{R}^n = H_n \oplus L_n,$$

*es decir, si $\boldsymbol{v} = \boldsymbol{k} \oplus \boldsymbol{r}$ con $\boldsymbol{v} \in \mathbb{R}^n$, $\boldsymbol{k} \in H_n$ y $\boldsymbol{r} \in L_n$; entonces $\pi(\boldsymbol{v}) = \boldsymbol{k}$. Sea $(\mu_1, \ldots, \mu_{n-1}) \in \{+1, -1\}^{n-1}$ y sea $\boldsymbol{v} \in \mathbb{R}^n$. Si:*

$$\boldsymbol{v} \in H(\mu_1, \ldots, \mu_{n-1}),$$

*entonces:*

$$\pi_n(\boldsymbol{v}) \in \bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}.$$

*Demostración.*
Primero observemos que por el lema 6,3 la función $\pi$ está bien definida. Sean $\mathbf{h}_1, \ldots, \mathbf{h}_n$ vectores normales a los hiperplanos $H_1, \ldots, H_n$. Por el lema 6,3 sabemos que existe vector $\mathbf{h}_n^*$ base de $L_n$ tal que:

$$(\mathbf{h}_i, \mathbf{h}_n^*) = \delta_{in} = \begin{cases} 1 & si \quad i = n \\ \\ 0 & si \quad i \neq n \end{cases}$$

para todo $1 \leq i \leq n$. Sea $\mathbf{v} \in \mathbb{R}^n$; por le lema 6,3 sabemos que $\mathbf{v} = \mathbf{k} + \mathbf{r}$ con $\mathbf{k} \in H_n$ y $\mathbf{r} \in L_n$. Por definición de la función $\pi$, tenemos que $\pi(\mathbf{v}) = \mathbf{k}$ y además como el vector $\mathbf{h}_n^*$ es base de $L_n$, podemos escribir a $\mathbf{r}$ como $\alpha\mathbf{h}_n^*$, con $\alpha \in \mathbb{R}$. De lo anterior tenemos que para todo $\mathbf{v} \in \mathbb{R}^n$, $\mathbf{v} = \pi(\mathbf{v}) + \alpha\mathbf{h}_n^*$.

Para probar que si $\mathbf{v} \in H(\mu_1, \ldots, \mu_{n-1})$, entonces $\pi_n(\mathbf{v}) \in \bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}$; basta probar que $(\mathbf{v}, \mathbf{h}_i) = (\mathbf{q}_i, \pi(\mathbf{v}))$, para todo $1 \leq i \leq n-1$, donde el vector $\mathbf{q}_i$ es el vector normal de $Q_i$ definido en el lema 6,4. Lo anterior es cierto ya que si $(\mathbf{v}, \mathbf{h}_i) > 0$, entonces $(\pi(\mathbf{v}), \mathbf{q}_i) > 0$, es decir, si $\mathbf{v} \in H^{(+1)}$, entonces $\pi(\mathbf{v}) \in Q^{(+1)}$, para todo $1 \leq i \leq n-1$. Análogamente si $\mathbf{v} \in H_i^{(-1)}$, entonces $Q_i^{(-1)}$. De ahí se sigue que si $\mathbf{v} \in \bigcap_{i=1}^{n-1} H_i^{\mu_i} = H(\mu_1, \ldots, \mu_{n-1})$, entonces $\pi_n(\mathbf{v}) \in \bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}$.

Para demostrar que $(\mathbf{h}_i, \mathbf{v}) = (\mathbf{q}_i, \pi(\mathbf{v}))$, para todo $1 \leq i \leq n-1$, calcularemos $(\mathbf{q}_i, \pi(\mathbf{v}))$ y llegaremos a que es igual a $(\mathbf{h}_i, \mathbf{v})$.

$$\begin{aligned}
(\mathbf{q}_i, \pi(\mathbf{v})) =& (\mathbf{h}_i - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}\mathbf{h}_n, \pi(\mathbf{v})) \\
=& (\mathbf{h}_i, \pi(\mathbf{v})) - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}(\mathbf{h}_n, \pi(\mathbf{v})) \\
=& (\mathbf{h}_i, \mathbf{v} - \alpha\mathbf{h}_n^*) - \frac{(\mathbf{h}_n, \mathbf{h}_i)}{(\mathbf{h}_n, \mathbf{h}_n)}(0) \\
=& (\mathbf{h}_i, \mathbf{v}) - \alpha(\mathbf{h}_i, \mathbf{h}_n^*) \\
=& (\mathbf{h}_i, \mathbf{v}) - \alpha\delta_{i,n} \\
\textit{entonces}&, \\
(\mathbf{q}_i, \pi(\mathbf{v})) =& (\mathbf{h}_i, \mathbf{v})
\end{aligned}$$

Por lo tanto si $\mathbf{v} \in \bigcap_{i=1}^{n-1} H_i^{(\mu_i)}$, entonces $\pi_n(\mathbf{v}) \in \bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}$. □

**Lema 6.6.** *Sean $H_1, \ldots, H_n$ hiperplanos linealmente con el vector $\boldsymbol{0} \in H_i$ para todo $1 \leq i \leq n$ y sea $L_n$ definido como en el lema 6,3. Sea $S \subseteq \mathbb{R}^n$, sea la función $\pi$ como en el lema 6,5 y se define $\pi(S) = \{\pi(\boldsymbol{s}) | \boldsymbol{s} \in S\} \subseteq H_n$. Si para todo $(\mu_1, \ldots, \mu_{n-1}) \in \{1, -1\}^n$ se tiene que:*

$$S \cap (\bigcap_{i=1}^{n-1} H_i^{(\mu_i)}) \neq \emptyset,$$

*entonces:*

$$\boldsymbol{0} \in conv(\pi(S)).$$

*Más aún existe un vector base $\boldsymbol{h}_n^*$ de $L_n$ tal que si $S \subseteq H_n^{(+1)}$, entonces:*

$$\alpha\boldsymbol{h}_n^* \in conv(S),$$

*para algún* $\alpha > 0$.

*Demostración.*

Como $S \cap (\bigcap_{i=1}^{n-1} H_i^{(\mu_i)}) \neq \emptyset$, para todo $(\mu_1, \ldots, \mu_n) \in \{1, -1\}^n$, entonces existe $\mathbf{v} \in S$ tal que $\mathbf{v} \in \bigcap_{i=1}^{n-1} H_i^{(\mu_i)}$. Sean $Q_1, \ldots, Q_n$ definidos como en el lema 6,4. Por el lema 6,5, tenemos que $\pi(\mathbf{v}) \in \bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}$, y por lo tanto $\pi(S) \cap (\bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}) \neq \emptyset$. Observemos que como $Q_i = H_i \cap H_n$ y $\mathbf{0} \in H_i$ para todo $1 \leq i \leq n$, entonces $\mathbf{0} \in Q_i$ para todo $1 \leq i \leq n-1$. Ahora como $\pi(S) \cap (\bigcap_{i=1}^{n-1} Q_i^{(\mu_i)}) \neq \emptyset$, entonces por el corolario 6,1 tenemos que $\mathbf{0} \in conv(\pi(S))$. Como $\mathbf{0} \in conv(\pi(S))$ por el lema 6,2, tenemos que existen $\mathbf{s}_1, \ldots, \mathbf{s}_k$ vectores en $S$ y escalares $\alpha_1, \ldots, \alpha_k$ en $\mathbb{R}$ tales que:

$$\sum_{i=1}^{k} \alpha_i \pi(\mathbf{s}_i) = \mathbf{0},$$

con $\alpha_1 + \cdots + \alpha_k = 1$ y $\alpha_i \geq 0$ para todo $1 \leq i \leq k$. Sabemos que podemos escribir a cada $\mathbf{s}_i$ de la siguiente manera:

$$\mathbf{s}_i = \pi(\mathbf{s}_i) + \beta_i \mathbf{h}_n^*,$$

donde $\mathbf{h}_n^*$ es el vector base de $L_n$ definido en el lema 6,5. Definimos a:

$$\alpha = \sum_{i=1}^{k} \alpha_i \beta_i.$$

De lo anterior tenemos que:

$$\sum_{i=1}^{k} \alpha_i \mathbf{s}_i \in conv(S)$$

*entonces*,

$$\begin{aligned} \sum_{i=1}^{k} \alpha_i \mathbf{s}_i &= \sum_{i=1}^{k} \alpha_i (\pi(\mathbf{s}_i) + \beta_i \mathbf{h}_n^*) \\ &= \sum_{i=1}^{k} \alpha_i \pi(\mathbf{s}_i) + \sum_{i=1}^{k} \alpha_i \beta_i \mathbf{h}_n^* \\ &= \sum_{i=1}^{k} \alpha_i \pi(\mathbf{s}_i) + \alpha \mathbf{h}_n^* \\ &= 0 + \alpha \mathbf{h}_n^* \end{aligned}$$

*luego*,

$$\alpha \mathbf{h}_n^* \in conv(S)$$

Ahora si $S \subseteq H_n^{(+1)}$, entonces:

$$(\mathbf{h}_n, \mathbf{s}_i) = (\mathbf{h}_n, \pi(\mathbf{s}_i)) + \beta_i(\mathbf{h}_n, \mathbf{h}_n^*) = 0 + \beta_i \delta_{n,n} = \beta_i,$$

para todo $1 \leq i \leq k$. Pero como $(\mathbf{h}_n, \mathbf{s}_i) > 0$, entonces $\beta_i > 0$. Por último observemos que por definición de $\alpha_i$, tenemos que $\alpha_i \geq 0$, entonces $\alpha > 0$, ya que al menos un $\alpha_i \neq 0$, y esto es lo último que se quería probar. □

# Bibliografía


[1] M. B. Nathanson, *Additive number theory: inverse problems and the geometry of sumsets.* Springer-Verlag New York, 1996.

[2] M.-C. Chang, "A polynomial bound in freimans theorem," *Duke Mathematical Journal*, vol. 113, no. 3, p. 399–419, 2002.

[3] P. C. Fishburn, "On a contribution of freiman to additive number theory," *Journal of Number Theory*, vol. 35, no. 3, p. 325–334, 1990.

[4] G. Freiman, "Foundations of a structural theory of set addition," *Translations of Mathematical Monographs*, 2007.

[5] Y. V. Stanchescu, "The structure of d-dimensional sets with small sumset," *Journal of Number Theory*, vol. 130, no. 2, p. 289–303, 2010.

[6] R. J. Gardner and P. Gronchi, "A brunn-minkowski inequality for the integer lattice," *Trans. Amer. Math. Soc*, Jun 2001.

[7] D. Grynkiewicz and O. Serra, "Properties of two-dimensional sets with small sumset," *Journal of Combinatorial Theory, Series A*, vol. 117, no. 2, p. 164–188, 2010.

[8] B. Green and T. Tao, "Compressions, convex geometry and the freiman–bilu theorem," *The Quarterly Journal of Mathematics*, vol. 57, no. 4, p. 495–504, 2006.