

CORPOS CONVEXOS, FUNÇÕES DE DISTÂNCIA E  
PROPRIEDADES

## 1 Motivação

Dado um conjunto  $K \subset \mathbb{R}^n$ , sob quais condições podemos garantir que exista um ponto de  $K$  com todas as suas coordenadas inteiras? Quantos pontos inteiros existem num círculo centrado na origem de raio  $r$ ? Qual a melhor maneira de dispormos cópias disjuntas de um conjunto  $K \subset \mathbb{R}^n$  de modo a minimizarmos a proporção de espaços vazios entre elas? Estas perguntas e conceitos relacionados são tópicos de estudos da Geometria dos Números.

Podemos dizer que a primeira formalização da Geometria dos Números é devida a Hermann Minkowski, no seu seminal *Geometrie der Zahlen* [Min10], em que é observado que conjuntos convexos podem ser analiticamente descritos através de um funcional, conhecido hoje como função de gauge (ou de distância). A partir desta aparentemente simples ideia, Minkowski estabelece diversas conexões entre propriedades geométricas de corpos convexos e Teoria dos Números, exploradas mais tarde por diversos autores como Cassels, Mahler e Gruber. Uma das mais fascinantes destas conexões é talvez a demonstração dos teoremas dos dois quadrados e dos quatro quadrados a partir de propriedades de pontos inteiros no interior de corpos convexos. Atualmente, conceitos de Geometria dos Números podem ser vistos aplicados em contextos como formas quadráticas e Teoria Algébrica dos Números, aproximações diofantinas simultâneas, Programação Linear Inteira, Criptografia, Teoria da Informação, entre muitos outros. O objetivo destas notas é estabelecer as bases teóricas para a Geometria dos Números.

## 2 Propriedades Iniciais

Esta primeira seção apresenta um compilado de resultados preliminares sobre corpos convexos, a serem utilizados no decorrer destas notas. Cada resultado

é acompanhado de uma referência apropriada, onde o leitor pode encontrar sua demonstração.

A principal propriedade geométrica que exigimos dos conjuntos os quais lidamos nestas notas é a convexidade. Seja  $K \subset \mathbb{R}^n$ . Dizemos que  $K$  é *convexo* se para quaisquer  $\mathbf{x}, \mathbf{y} \in K$ , o segmento unindo  $\mathbf{x}$  a  $\mathbf{y}$  está inteiramente contido em  $K$ . Mais analiticamente, dizemos que  $K$  é convexo se

$$\mathbf{x}, \mathbf{y} \in K \implies \lambda \mathbf{x} + (1 - \lambda)\mathbf{y} \in K, \forall \lambda \in [0, 1].$$

Como veremos mais para frente, a convexidade de um conjunto implica uma gama de outras propriedades desejáveis à Geometria dos Números e a outras áreas, como a Otimização Linear/Não-Linear. Exemplos simples de conjuntos convexos incluem:

- (i)  $K = \mathbb{R}^n$  ou  $K =$  qualquer subespaço do  $\mathbb{R}^n$ ;
- (ii)  $K = \{\mathbf{x}\}$ ,  $\mathbf{x} \in \mathbb{R}^n$ ;
- (iii) Esferas euclidianas ( $K = \{\mathbf{x} \in \mathbb{R}^n : (x_1 - c_1)^2 + \dots + (x_n - c_n)^2 \leq R^2\}$ , em que  $c_1, c_2, \dots, c_n \in \mathbb{R}$ );
- (iv) Cubos ( $K = \{\mathbf{x} \in \mathbb{R}^n : |x_i| \leq R\}$ );
- (v) O conjunto vazio (por vacuidade).

Um *corpo convexo* é um conjunto convexo limitado cujo interior é não-vazio<sup>1</sup>. Se  $K$  é um conjunto com a propriedade de que  $\mathbf{x} \in K \iff -\mathbf{x} \in K$ , dizemos que  $K$  é *centralmente simétrico*. Dos conjuntos listados acima, apenas os itens (iii) e (iv) são corpos convexos. Apenas (iii), no caso em que  $c_i = 0, i = 1, \dots, n$ , e (iv) são corpos convexos centralmente simétricos. Corpos convexos fechados centralmente simétricos são tão importantes na teoria que Minkowski os denotava por uma só palavra: *Eichkörper* (corpo padrão).

Para nossas aplicações, necessitamos da noção de volume de um conjunto. Seja  $\chi$  a função característica de  $K \subset \mathbb{R}^n$ , dada por

$$\chi(\mathbf{x}) = \begin{cases} 1 & \text{se } \mathbf{x} \in K \\ 0 & \text{caso contrário.} \end{cases}$$

Definimos o *volume* de  $K$  como a integral de Riemman de  $\chi(\mathbf{x})$ , isto é

$$\text{vol } K = \int_{\mathbb{R}^n} \chi(\mathbf{x}) d\mathbf{x} = \int_K d\mathbf{x}.$$

---

<sup>1</sup>Algumas definições de corpo convexo necessitam também que  $K$  seja fechado. Para nossos propósitos, essa exigência não é conveniente.

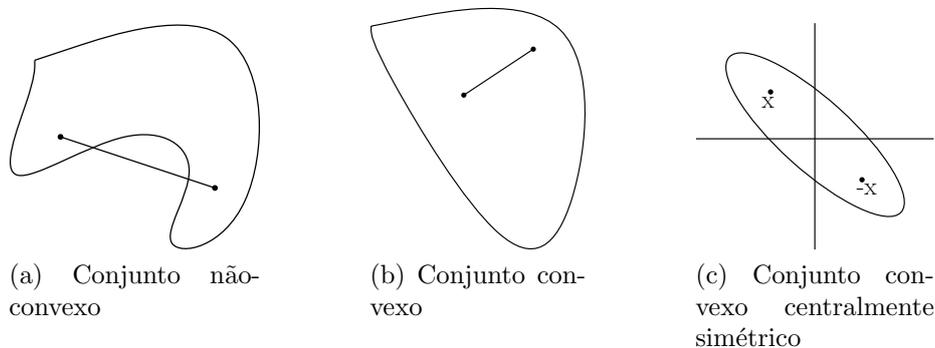


Figura 1: Exemplos de conjuntos convexos e não-convexos

Dizemos que um conjunto possui volume finito quando a integral de  $\chi(\mathbf{x})$  for finita. Todo corpo convexo possui volume finito (a demonstração disso foge ao escopo do curso e encontra-se em [GL87, p. 9], utilizando a noção de função de distância, a qual trataremos a seguir). Desta maneira, o volume definido através da integral de Riemman (também conhecido como medida de Jordan) será suficiente quando tratarmos de corpos convexos. As seguintes propriedades de volume serão usadas exhaustivamente durante do curso e decorrem imediatamente de propriedades básicas da integral de Riemman.

**Proposição 2.1.** *Sejam  $K, M \subset \mathbb{R}^n$  conjuntos com volume finito*

- (i) *Se  $M \subset K$ , então  $\text{vol } K \geq \text{vol } M$ .*
- (ii)  *$\text{vol } (M \cup K) \leq \text{vol } M + \text{vol } K$ .*
- (iii) *Se  $A$  é uma matriz não-singular e  $AK = \{A\mathbf{x} : \mathbf{x} \in K\}$ , então*

$$\text{vol } AK = |\det A| \text{vol } K.$$

*Em particular, para um número real positivo  $\lambda$ ,  $\text{vol } \lambda K = \lambda^n \text{vol } K$ .*

Dados dois conjuntos  $M, N \subset \mathbb{R}^n$ , a soma (de Minkowski)  $M + N$  é definida como  $M + N = \{m + n : m \in M, n \in N\}$ . A soma de Minkowski de dois corpos (conjuntos) convexos é novamente um corpo (conjunto) convexo. De maneira geral, não há uma relação simples como a da Proposição 2.1(ii) para a soma de Minkowski. Para ver isso, tome

$$M = \{\mathbf{x} \in \mathbb{R}^2 : |x_1| \leq 1, |x_2| \leq 1\}.$$

Claramente  $M + M = \{\mathbf{x} \in \mathbb{R}^2 : |x_1| \leq 2, |x_2| \leq 2\} = 2M$  (ver Exercício 1). Deste modo,  $\text{vol } (M + M) > \text{vol } M + \text{vol } M$ . Mais ainda, a soma de

Minkowski de dois conjuntos com volume zero pode resultar em um conjunto com volume não-nulo.

A relação entre o volume da soma de Minkowski de conjuntos se dá através da Desigualdade de Brunn-Minkowski, a saber:

$$\text{vol}(M + N)^{1/n} \geq (\text{vol } M)^{1/n} + (\text{vol } N)^{1/n}, \quad (1)$$

em que  $M$ ,  $N$  e  $M + N$  são conjuntos em  $\mathbb{R}^n$  com volume finito.

## 2.1 Classes de Conjuntos Convexos

O fecho convexo dos pontos  $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbb{R}^n$  é definido como

$$\text{ConvHull}(\mathbf{x}_1, \dots, \mathbf{x}_m) = \left\{ \lambda_1 \mathbf{x}_1 + \dots + \lambda_m \mathbf{x}_m : 0 \leq \lambda_i \leq 1 \text{ e } \sum_{i=1}^m \lambda_i = 1 \right\}.$$

O fecho convexo é sempre um corpo convexo e, mais do que isso, ele é o menor conjunto convexo que contém os pontos  $\mathbf{x}_1, \dots, \mathbf{x}_m$  (Exercício 2). Um politopo (ou poliedro) é o fecho convexo de algum conjunto de pontos do  $\mathbb{R}^n$ . Uma outra maneira de caracterizar politopos é através de intersecções de semi-espacos do  $\mathbb{R}^n$ , ou seja, conjuntos do tipo

$$\{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leq \mathbf{b}\},$$

em que  $A$  é uma matriz  $n \times m$ ,  $\mathbf{b} \in \mathbb{R}^m$ , e o símbolo  $\leq$  deve ser lido em cada coordenada. É fácil ver que tais conjuntos são sempre convexos. O seguinte Teorema de Minkowski-Weyl estabelece a equivalência entre as duas caracterizações. Para uma demonstração, sugerimos [Zie95, Sec. 1.2].

**Teorema 1** (de Minkowski-Weyl). *Seja  $K$  um corpo convexo. As seguintes afirmativas são equivalentes:*

- (i) *Existem pontos  $\mathbf{x}_1, \dots, \mathbf{x}_m$  tais que  $K = \text{ConvHull}(\mathbf{x}_1, \dots, \mathbf{x}_m)$ .*
- (ii) *Existe uma matriz  $A$  e um vetor  $\mathbf{b}$  tais que  $K = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leq \mathbf{b}\}$ .*

O fecho convexo de um conjunto  $S \subset \mathbb{R}^n$  é o conjunto de todas as combinações convexas de pontos em  $S$ , isto é:

$$\text{ConvHull}(S) = \left\{ \lambda_1 \mathbf{x}_1 + \dots + \lambda_m \mathbf{x}_m : \mathbf{x}_i \in S, 0 \leq \lambda_i \leq 1 \text{ e } \sum_{i=1}^m \lambda_i = 1 \right\}.$$

Outra classe de corpos convexos importantes para nós serão bolas com respeito a alguma norma de  $\mathbb{R}^n$ . Dada uma norma  $\|\cdot\| : \mathbb{R}^n \rightarrow [0, \infty)$ , a bola fechada centrada na origem é definida como

$$B(\mathbf{0}, r) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\| \leq r\}.$$

O fato de que  $B(\mathbf{0}, r)$  é um conjunto convexo decorre imediatamente da desigualdade triangular. Com efeito, se  $\mathbf{x}, \mathbf{y} \in B(\mathbf{0}, r)$ , então

$$\|\lambda\mathbf{x} + (1 - \lambda)\mathbf{y}\| \leq \lambda\|\mathbf{x}\| + (1 - \lambda)\|\mathbf{y}\| \leq r.$$

Sabendo que bolas em uma dada norma  $\|\cdot\|$  são corpos convexos, é natural perguntar se a recíproca deste fato é verdadeira, isto é, se dado um corpo convexo  $K$ , existe uma norma do  $\mathbb{R}^n$  tal que as bolas possuem a mesma “forma” que  $K$ . Essa pergunta é respondida mais precisamente utilizando a noção de função de distância (ou de gauge) de um conjunto.

### 3 Funções de Distância

É devida a Minkowski, a fecunda observação de que um conjunto convexo pode ser descrito analiticamente através da sua chamada função de distância (ou *gauge*). Tal função captura todas as propriedades essenciais de um corpo convexo e permite estudar conexões com Teoria dos Números em um alto grau de generalidade.

Seja  $K \subset \mathbb{R}^n$  um conjunto que contém a origem. A *função de distância* (ou *gauge*) de  $K$  é definida como:

$$F_K(\mathbf{x}) = \inf \{\lambda > 0 : \mathbf{x} \in \lambda K\}. \quad (2)$$

Intuitivamente, dado um ponto  $\mathbf{x} \in \mathbb{R}^n$  contraímos/dilatamos o conjunto  $K$  até que  $\mathbf{x}$  pertença à fronteira de  $K$ , e então definimos o fator pelo qual precisamos contrair/dilatar como a função de distância de  $\mathbf{x}$  com respeito a  $K$ .

Está claro que a depender do conjunto  $K$ , a função  $F_K(\mathbf{x})$  pode não estar bem definida. No caso de corpos convexos, entretanto, é fácil ver que  $0 \leq F_K(\mathbf{x}) < \infty$ . O próximo teorema justifica, de uma certa forma, a definição de  $F_K(\mathbf{x})$ .

**Teorema 2.** *Se  $K$  é um corpo convexo centralmente simétrico, a função de gauge de  $K$  define uma norma em  $\mathbb{R}^n$ . Mais especificamente, valem:*

- (i) (*Positividade*):  $F_K(\mathbf{x}) > 0$  se  $\mathbf{x} \neq \mathbf{0}$  e  $F_K(\mathbf{x}) = 0$  se  $\mathbf{x} = \mathbf{0}$ .

(ii) (Homogeneidade):  $F_K(\alpha \mathbf{x}) = |\alpha| F_K(\mathbf{x})$ .

(iii) (Desigualdade Triangular):  $F_K(\mathbf{x} + \mathbf{y}) \leq F_K(\mathbf{x}) + F_K(\mathbf{y})$ .

Se  $K$  é fechado, a bola na norma  $F_K(x)$  centrada na origem, de raio  $r$ , é dada por  $rK$ .

*Demonstração.* Vamos verificar os axiomas de norma.

(i) (Positividade): É claro que  $F_K(\mathbf{x}) \geq 0$ . Se  $F_K(\mathbf{x}) = 0$ , para qualquer  $\varepsilon > 0$  suficientemente pequeno  $\mathbf{x} \in \varepsilon K$ , ou seja  $\mathbf{x} = \varepsilon \mathbf{k}_\varepsilon$ ,  $\mathbf{k}_\varepsilon \in K$ . Como  $K$  é limitado, existe uma constante  $M$  tal que  $\|\mathbf{k}_\varepsilon\| \leq M$ , e portanto  $\|\mathbf{x}\| \leq \varepsilon M$ . Fazendo  $\varepsilon \rightarrow 0^+$ , temos que  $\mathbf{x} = 0$ .

(ii) (Homogeneidade) Como  $K$  é centralmente simétrico,

$$\begin{aligned} F_K(\alpha \mathbf{x}) &= F_K(-\alpha \mathbf{x}) = \inf \{ \lambda > 0 : |\alpha| \mathbf{x} \in \lambda K \} = \inf \left\{ \lambda > 0 : \mathbf{x} \in \frac{\lambda}{|\alpha|} K \right\} = \\ &= |\alpha| \inf \{ \lambda > 0 : \mathbf{x} \in \lambda K \} = |\alpha| F_K(\mathbf{x}) \end{aligned}$$

(iii) (Desigualdade Triangular) Se  $K$  é convexo e  $\lambda_1, \lambda_2 > 0$ , então, de acordo com o Exercício 1 (v),  $\lambda_1 K + \lambda_2 K = (\lambda_1 + \lambda_2)K$ . Assim, sejam  $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$  tais que  $F_K(\mathbf{x}) = \lambda_1$  e  $F_K(\mathbf{y}) = \lambda_2$ . Para qualquer  $\varepsilon/2 > 0$ ,  $\mathbf{x} \in (\lambda_1 + \varepsilon/2)K$  e  $\mathbf{y} \in (\lambda_2 + \varepsilon/2)K$ . Deste modo,  $\mathbf{x} + \mathbf{y} \in (\lambda_1 + \lambda_2 + \varepsilon)K$  para qualquer  $\varepsilon > 0$ , e portanto:

$$F_K(\mathbf{x} + \mathbf{y}) = \inf \{ \lambda > 0 : \mathbf{x} + \mathbf{y} \in \lambda K \} \leq \lambda_1 + \lambda_2 = F_K(\mathbf{x}) + F_K(\mathbf{y}).$$

Por fim, suponhamos que  $K$  seja fechado. A bola fechada centrada na origem de raio  $r$  é dada por

$$B = \{ \mathbf{x} \in \mathbb{R}^n : F_K(\mathbf{x}) \leq r \}.$$

Se  $\mathbf{x} \in rK$  então  $F_K(\mathbf{x}) \leq r$ . Reciprocamente, se  $\mathbf{x} \in B$ ,  $F_K(\mathbf{x}) \leq r$ , ou seja  $\mathbf{x} \in (r + \varepsilon)K$  para qualquer  $\varepsilon > 0$ . Como  $K$  é fechado, isso implica que  $\mathbf{x} \in rK$ , o que conclui a prova.  $\square$

Quando  $K$  é fechado, uma propriedade interessante da função de gauge é a elegante igualdade de conjuntos

$$K = \{ \mathbf{x} \in \mathbb{R}^n : F_K(\mathbf{x}) \leq 1 \}.$$

De fato, a recíproca do teorema acima também é verdadeira. A partir de qualquer função  $F$  com as propriedades (i)-(iii) do teorema, podemos definir o conjunto convexo centralmente simétrico  $K = \{ \mathbf{x} \in \mathbb{R}^n : F(\mathbf{x}) \leq 1 \}$ , cuja função de gauge é  $F$ . Caso o conjunto que estejamos tratando não

seja centralmente simétrico, a condição (ii) pode ser substituída por: (ii')  $F_K(\alpha K) = \alpha F_K(\mathbf{x}), \alpha > 0$ , e o teorema continua válido. A função de distância de um corpo convexo é sempre contínua, como será demonstrado na Proposição 3.

Uma das vantagens das funções de distância é poder traduzir problemas geométricos em uma linguagem analítica. Por exemplo, a pergunta se existem pontos de  $K$  com todas as coordenadas inteiras pode ser resolvida calculando  $\lambda = \min_{\mathbf{x} \in \mathbb{Z}^n \setminus \{0\}} F_K(\mathbf{x})$  e verificando se  $\lambda > 1$  ou  $\leq 1$ . Uma outra vantagem é facilitar o estudo de corpos estrela, parentes próximos de corpos convexos.

## 4 Corpos Estrela

Uma boa parte dos teoremas de Geometria dos Números acerca de corpos convexos pode ser estendido com um pouco de esforço adicional para estruturas mais gerais, denominadas corpos estrela. A definição de um corpo estrela é um pouco menos direta que a de um corpo convexo, como vemos a seguir.

Seja  $S \subset \mathbb{R}^n$ . Dizemos que  $S$  é um *conjunto raio* se para todo  $\mathbf{x} \in S$ ,  $\lambda \mathbf{x} \in S, \forall \lambda \in [0, 1]$ . Se  $S$  é um conjunto raio limitado que contém a origem, então  $F_S(\alpha \mathbf{x}) = \alpha F_S(\mathbf{x})$  para  $\alpha > 0$  e para os pontos em que  $F_S(\mathbf{x})$  existe. Um *corpo estrela*  $S$  é um conjunto raio, fechado, tal que se  $0 < \lambda < 1$  e  $\mathbf{x} \in S$ , então  $\lambda \mathbf{x} \in \text{int} S$ .

Geometricamente, um conjunto raio é um conjunto tal que o segmento que liga a origem a qualquer um de seus pontos está inteiramente contido nele. Um corpo estrela é um conjunto tal que esses segmentos não apenas estão contidos, mas estão no seu interior. Abaixo estão ilustrações de conjuntos raio e corpos estrela.

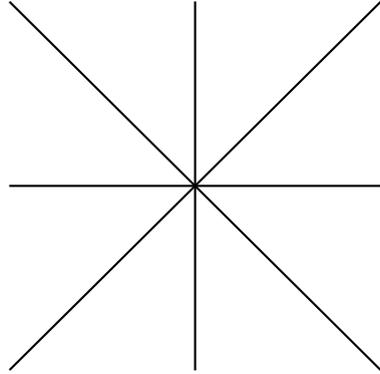
**Lema 1.** *Se  $S$  é um conjunto raio e  $0 < \alpha_1 < \alpha_2$ , então  $\alpha_1 S \subset \alpha_2 S$ . Se, adicionalmente,  $S$  é um corpo estrela então  $\alpha_1 S \subset \alpha_2 \text{int} S$ .*

*Demonstração.* Provemos apenas a afirmativa para corpos estrela; o caso em que  $S$  é um conjunto raio é análogo. Se  $\mathbf{x} \in \alpha_1 S$ , então

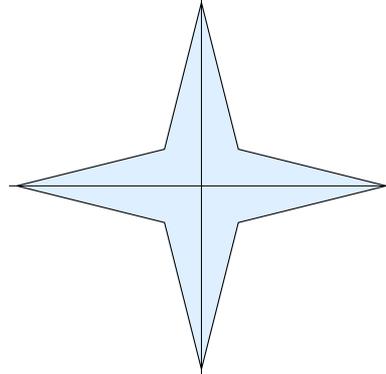
$$\frac{1}{\alpha_1} \mathbf{x} \in S \stackrel{(a)}{\Rightarrow} \frac{\alpha_1}{\alpha_2} \frac{1}{\alpha_1} \mathbf{x} \in \text{int} S \Rightarrow \mathbf{x} \in \alpha_2 \text{int} S,$$

onde (a) vem da definição de corpo estrela e do fato de que  $0 < \alpha_1/\alpha_2 < 1$ .  $\square$

O seguinte teorema nos provém uma caracterização analítica de corpos estrela.



(a) Conjunto raio (4 segmentos de reta)



(b) Corpo Estrela

Figura 2: Exemplos de um conjunto raio e um corpo estrela.

**Teorema 3.** *Seja  $S$  um conjunto raio limitado. A função de gauge (2)  $F_S$  é contínua se, e somente se,  $S$  é um corpo estrela limitado.*

*Demonstração.* ( $\Rightarrow$ ) A função de gauge de um corpo estrela limitado  $S$  é contínua. Com efeito, seja  $\mathbf{x} \in \mathbb{R}^n$ ,  $F_S(\mathbf{x}) = \lambda$ . Temos que  $\mathbf{x}$  é um ponto interior de  $(\lambda + \varepsilon)S$  para  $\varepsilon > 0$  suficientemente pequeno, caso contrário, pelo Lema 1,  $F_S(\mathbf{x}) > \lambda$ . Além disso,  $\mathbf{x} \notin (\lambda - \varepsilon)S$ , caso contrário teríamos  $F_S(\mathbf{x}) < \lambda$ . Seja agora uma sequência  $\mathbf{x}_n \rightarrow \mathbf{x}$ . Para  $n$  suficientemente grande, temos que  $\mathbf{x}_n$  é um ponto interior de  $(\lambda + \varepsilon)S \setminus (\lambda - \varepsilon)S$ . Assim,  $\lambda - \varepsilon < F_S(\mathbf{x}_n) < \lambda + \varepsilon$ , e portanto  $F_S(\mathbf{x}_n) \rightarrow F_S(\mathbf{x})$ .

( $\Leftarrow$ ) Reciprocamente, suponhamos que a função de gauge de  $S$  seja contínua. Seja  $\mathbf{x} \in S$ , isto é,  $F_S(\mathbf{x}) \leq 1$ . Se  $0 < \lambda < 1$ ,  $\lambda\mathbf{x} \in \lambda S \subset S$  e portanto  $F_S(\lambda\mathbf{x}) < 1$ . Mais que isso, como  $F$  é contínua, existe uma vizinhança de  $\lambda\mathbf{x}$  para o qual qualquer  $\mathbf{y}$  é tal que  $F_S(\mathbf{y}) < 1$ . Isso implica que  $\lambda\mathbf{x}$  é ponto interior de  $S$ , finalizando a demonstração.  $\square$

Com um pouco de esforço a mais, o Teorema 3 pode ser sutilmente generalizado para:

**Teorema 3'.** *Seja  $S$  um conjunto raio. A função de gauge (2)  $F_S$  é contínua se, e somente se,  $S$  é um corpo estrela.*

## 5 Exemplos Adicionais

Abaixo estão alguns exemplos interessantes de corpos estrela e corpos convexos que aparecem na literatura.

## 5.1 Superbolas

Como já observado na Seção 2, bolas com respeito a uma norma  $\|\cdot\|$  são corpos convexos. Seja  $\|\cdot\|$  uma norma  $p$ ,  $p > 1$ , isto é

$$\|\mathbf{x}\|_p = (|x_1|^p + \dots + |x_n|^p)^{1/p}.$$

O conjunto de todos os pontos tais que  $\|\mathbf{x}\|_p \leq R$ , denotado por  $B_p(R)$ , é denominado *superbola*. *As far as I am concerned*, essa terminologia foi introduzida em [RS87] por Rush e Sloane. É claro que neste caso, a função de gauge de uma superbola de raio 1 é  $F_K(\mathbf{x}) = \|\mathbf{x}\|_p$ .

Em outras referências, encontramos o termo superbola também relacionado a “bolas” na norma  $p$ ,  $0 < p < 1$ , isto é, ao conjunto

$$S = \left\{ \mathbf{x} \in \mathbb{R}^n : (|x_1|^p + \dots + |x_n|^p)^{1/p} \leq R \right\}.$$

A função de gauge de  $F_S(\mathbf{x}) = (|x_1|^p + \dots + |x_n|^p)^{1/p}$  não é sub-aditiva, portanto não representa uma norma. Entretanto, como  $F_S$  é contínua,  $S$  é um corpo estrela centralmente simétrico. Alguns exemplos de superbola estão ilustrados abaixo para  $n = 2$ . Uma boa parte da literatura no tema trata do *empacotamento* de superbolas. Para  $p = 1$ , as superbolas são conhecidas como polítopos-cruz.

### 5.1.1 O volume de uma superbola

Seja  $V_{n,p}$  o volume de uma bola  $B_p(1) \subset \mathbb{R}^n$  na norma  $l_p$  (ou superbola), com  $p > 1$ . Seguindo a exposição de Siegel [Sie89], Vamos mostrar como calcular  $V_{n,p}$  de maneira indutiva em  $n$ . Para tal, necessitamos das funções auxiliares beta e gamma. A função gamma  $\Gamma(n)$ ,  $n > 0$ , é definida como

$$\Gamma(n) = \int_0^\infty t^{n-1} e^{-t} dt.$$

Note que  $\Gamma(n+1) = n\Gamma(n)$  e, para  $n$  natural,  $\Gamma(n+1) = n!$ . A função beta,  $\beta(m, n)$ ,  $m, n > 0$ , é dada por

$$\beta(m, n) = \int_0^1 t^{m-1} (1-t)^{n-1} dt = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)}.$$

**Teorema 4.**

$$V_{n,p} = \frac{\left(2\Gamma\left(\frac{1}{p} + 1\right)\right)^n}{\Gamma\left(\frac{n}{p} + 1\right)}.$$

*Demonstração.* Notemos primeiramente que

$$V_{n,p} = \text{vol } B_p(1) = 2^n \text{vol } (B_p(1) \cap \{x_1 \geq 0, \dots, x_n \geq 0\}).$$

Seja  $W_{n,p} = \text{vol } (B_p(1) \cap \{x_1 \geq 0, \dots, x_n \geq 0\})$ . Temos

$$\begin{aligned} W_{n,p} &= \int \dots \int_{\substack{x_1^p + \dots + x_n^p \leq 1 \\ x_1 \geq 0, \dots, x_n \geq 0}} dx_1 \dots dx_n = \int_0^1 \left( \int \dots \int_{\substack{x_1^p + \dots + x_{n-1}^p \leq 1 - x_n^p \\ x_1 \geq 0, \dots, x_{n-1} \geq 0}} dx_1 \dots dx_{n-1} \right) dx_n \\ &\stackrel{(a)}{=} \int_0^1 W_{n-1,p} (1 - x_n^p)^{(n-1)/p} dx_n, \end{aligned}$$

em que (a) é resultado da mudança de variáveis  $x'_j = x_j / (1 - x_n^p)^{1/p}$ . Transformamos agora, a integral de  $(1 - x_n^p)^{(n-1)/p}$  em uma função beta através da mudança  $t = x_n^p$ , resultando em

$$\int_0^1 (1 - x_n^p)^{(n-1)/p} dx_n = \frac{1}{p} \int_0^1 (1 - t)^{(n-1)/p} t^{1/p-1} dt = \frac{1}{p} \beta \left( \frac{n-1}{p} + 1, \frac{1}{p} \right).$$

Obtemos assim a recursão  $W_{n,p} = W_{n-1,p} (1/p) \beta \left( \frac{n-1}{p} + 1, \frac{1}{p} \right)$ . Continuando este processo indutivamente, sabendo que  $W_{1,p} = 1$ , temos a fórmula desejada.  $\square$

Em particular, como  $\Gamma(3/2) = (1/2)\Gamma(1/2) = \sqrt{\pi}/2$ , chegamos à fórmula para o volume da esfera Euclidiana de raio unitário.

$$V_{n,2} = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2} + 1)}.$$

Da Proposição 2.1, temos  $\text{vol } B_p(r) = r^n V_{n,p}$ . Dividindo nos casos par e ímpar, com um pouco de álgebra, pode-se mostrar que:

$$V_{2k,2} = \frac{\pi^k}{k!} \text{ e } V_{2k+1,2} = \frac{2^{k+1} \pi^k}{(2k+1)!!}$$

onde o fatorial duplo !! denota o produto de todos os ímpares menores ou iguais a  $2k+1$ .

## 5.2 Elipsoides

Elipsoides são particularmente importantes na teoria de corpos convexos e surgem, por exemplo, em métodos para minimizar uma função linear sujeita

a restrições lineares. Um dos motivos para a importância dos elipsoides reside no fato de que qualquer conjunto convexo é *parecido* com o elipsoide, como formalizado no Teorema 5 a seguir.

Seja  $A$  uma matriz simétrica definida positiva de dimensões  $n \times n$  e  $\mathbf{y} \in \mathbb{R}^n$ . O conjunto

$$K = \{\mathbf{x} \in \mathbb{R}^n : (\mathbf{x} - \mathbf{y})^t A (\mathbf{x} - \mathbf{y}) \leq 1\}$$

é denominado um elipsoide (centrado em  $\mathbf{y}$ ). É fácil ver que um elipsoide é sempre um corpo convexo, e que esferas na norma  $p = 2$  são elipsoides. De fato, de uma maneira geral, um elipsoide é a imagem de uma esfera por uma transformação linear cujos auto-valores são a raiz dos auto-valores de  $A$ . Pela Proposição 2.1, o volume de um elipsóide é  $\text{vol } E = \text{vol } B_2(1) \sqrt{\det A}$ .

**Teorema 5** (de John para corpos centralmente simétricos). *Seja  $K \subset \mathbb{R}^n$  um corpo convexo fechado centralmente simétrico. Existe um elipsóide  $E$  tal que  $E \subset K \subset \sqrt{n}E$ .*

*Demonstração.* ([GL87], Teorema 8, Pagina 13).

□

**Exercício 1.** (Conjuntos Soma/Diferença) Seja  $K \subset \mathbb{R}^n$  e considere os conjuntos  $HK = K - K$  e  $SK = K + K$ .

- (i) Se  $K$  é um conjunto qualquer,  $2K \subset K + K$ .
- (ii) Se  $K$  é convexo  $K + K = 2K$ .
- (iii) Se  $K$  é convexo centralmente simétrico,  $K - K = K + K = 2K$ .
- (iv) Exiba um exemplo de conjunto  $K$  para o qual  $K + K \neq 2K$ .
- (v) Depois de pegar o gosto pelos itens (ii),(iii), prove que se  $K$  é convexo e  $a, b \geq 0$ , então  $aK + bK = (a+b)K$ . Se, além disso,  $K$  é centralmente simétrico, então para quaisquer  $a, b$ ,  $aK + bK = (|a| + |b|)K$ .

**Exercício 2.** Sejam  $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbb{R}^n$  e  $K = \text{ConvHull}(\mathbf{x}_1, \dots, \mathbf{x}_m)$ . Mostre que  $K$  é um corpo convexo com a seguinte propriedade: se  $\mathbf{x}_1, \dots, \mathbf{x}_m \in K'$  e  $K'$  é convexo, então  $K \subset K'$ .

**Exercício 3.** O conjunto  $S = \{\mathbf{x} \in \mathbb{R}^n : |x_1 x_2 \dots x_n| \leq 1\}$  é convexo? É um corpo estrela? Quanto vale vol  $S$ ? Esboce o caso  $n = 2$  (e  $n = 3$ , no computador).

**Exercício 4.** Um simplex regular em  $\mathbb{R}^n$  é definido por

$$S = \{(x_1, \dots, x_n) : 0 \leq x_1 \leq x_2 \leq \dots \leq x_n \leq 1\}.$$

Mostre que  $S$  é um politopo de duas formas: (i) Encontrando matrizes tais que  $S = \{\mathbf{x} \in \mathbb{R}^n : A\mathbf{x} \leq \mathbf{b}\}$ . (ii) Encontrando  $\mathbf{x}_1, \dots, \mathbf{x}_m \in \mathbb{R}^n$  tais que  $S = \text{ConvHull}(\mathbf{x}_1, \dots, \mathbf{x}_m)$  (qual o menor valor de  $m$  possível?). Em sua opinião muito pessoal, qual das duas maneiras é mais simples? Quanto vale vol  $S$  e  $\#(S \cap \mathbb{Z}^n)$ ?

**Exercício 5.** Verifique que as seguintes propriedades de politopos são válidas:

- (i) A projeção de um politopo é um politopo
- (ii) A soma de Minkowski de dois politopos é um politopo
- (iii) A intersecção de um politopo com um subespaço de  $\mathbb{R}^n$  é um politopo

**Exercício 6.** Seja  $K$  um corpo convexo (resp. centralmente simétrico) e  $A$  uma matriz invertível de ordem  $n \times n$ . Mostre que  $AK = \{A\mathbf{x} : \mathbf{x} \in K\}$  é um corpo convexo (resp. centralmente simétrico). Utilizando isto, mostre que um elipsoide centrado na origem é um corpo convexo centralmente simétrico

**Exercício 7.** Um conjunto  $K \subset \mathbb{R}^n$  é *conexo por caminhos* se para quaisquer dois pontos  $\mathbf{x}, \mathbf{y} \in K$ , existe uma função contínua  $\gamma : [0, 1] \rightarrow K$  tal que  $\gamma(0) = \mathbf{x}$  e  $\gamma(1) = \mathbf{y}$ . Um conjunto conexo por caminhos é *simplesmente conexo* se qualquer curva fechada pode ser contraída suavemente a um ponto de  $K$ <sup>2</sup>. Prove:

- (i) Todo conjunto convexo é conexo por caminhos
- (ii) Todo conjunto convexo é simplesmente conexo
- (iii) (Bônus!) O mesmo vale para corpos estrela?

## Referências

- [GL87] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland, 1987.
- [Min10] H. Minkowski. *Geometrie der Zahlen*. Teubner, 1910.
- [RS87] J. A. Rush and N. J. A. Sloane. An improvement to the Minkowski-Hlawka bound for packing superballs. *Mathematika*, 34:8–18, 1987.
- [Sie89] C. L. Siegel. *Lectures on Geometry of Numbers*. Springer-Verlag, 1989.
- [Zie95] G. M. Ziegler. *Lectures on Polytopes*. Springer, 1995.

---

<sup>2</sup>Formalmente: se para quaisquer dois caminhos  $\gamma_1$  e  $\gamma_2$  ligando dois pontos de  $K$ , existe uma homotopia  $h : [0, 1] \times [0, 1] \rightarrow K$ ,  $h(t, p)$ , contínua tal que  $h(t, 0) = \gamma_1(t)$  e  $h(t, 1) = \gamma_2(t)$ .