MT803D - Tópicos em Matemática Aplicada

Pontos Inteiros em Corpos Convexos

1 Enumerador de Pontos Inteiros

Dado um conjunto $K \subset \mathbb{R}^n$, com $0 < \operatorname{vol} K$, nosso objetivo é estimar $\#(K \cap \mathbb{Z}^n)$. É intuitivo que se K seja "suficientemente grande", a quantidade de pontos inteiros em K aproxime-se de vol K, a menos, possivelmente, de alguns pontos na fronteira. Nesta seção demonstraremos que isto é verdade, e exibiremos cotas para $|\#(K \cap \mathbb{Z}^n) - \operatorname{vol} K|$, quando K é a expansão homogênea de um conjunto convexo.

Definamos $L_K(r) = \#(rK \cap \mathbb{Z}^n)$ como a quantidade de pontos inteiros em uma expansão homogênea de K. Provaremos o seguinte

Teorema 1 (Informal)**.** *Se $K \subset \mathbb{R}^n$ é "razoável", então*

$$\lim_{r\to\infty} \frac{L_K(r)}{\operatorname{vol} rK} = 1. \tag{1}$$

Exemplo 1. *Seja $K = [-1,1]^n$ um cubo de lado 2. Temos claramente*

$$\#(rK \cap \mathbb{Z}^n) = (2r+1)^n = 2^n r^n + \sum_{i=0}^{n-1} \binom{n}{i} (2r)^i = \operatorname{vol} rK + O(r^{n-1}).$$

Portanto:

$$\lim \frac{L_K(r)}{\operatorname{vol} rK} = 1.$$

Mais do que isso, o "erro" na estimativa de $L_K(r)$ é dado por

$$|L_K(r) - \operatorname{vol} rK| = \sum_{i=0}^{n-1} \binom{n}{i} (2r)^i = O(r^{n-1}).$$

O exemplo acima nos mostra que, para conjuntos gerais não podemos esperar que o erro seja quantitativamente melhor que $O(r^{n-1})$. De fato, é intuitivo que o exemplo do cubo represente, de uma certa forma, o "pior" erro de estimativa de $L_K(r)$ por vol rK. Veremos a seguir que, a menos de constantes, esse fato é verdade.

Teorema 1. (Conjuntos Convexos) *Se $K \subset \mathbb{R}^n$ é um corpo convexo fechado, o Teorema 1 é válido. Neste caso, temos*

$$|L_K(r) - \text{vol } rK| \leq \text{vol } K \sum_{i=0}^{n-1} \binom{n}{i} r^i l_0^{n-i} = O(r^{n-1}),$$

em que

$$l_0 = \max_{\boldsymbol{x} \in [-\frac{1}{2}, \frac{1}{2}]^n} F_K(\boldsymbol{x}).$$

é uma constante que depende de K.

Demonstração. Seja $F_K(\boldsymbol{x})$ a funcão de distância de K. Provaremos as inclusões de conjunto

$$(r - l_0)K \subset \bigcup_{\boldsymbol{x} \in \mathbb{Z}^n \cap K} \left(\boldsymbol{x} + \left[-\frac{1}{2}, \frac{1}{2} \right]^n \right) \subset (r + l_0)K \tag{2}$$

(i) Seja $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{u}$, com $\boldsymbol{x} \in \mathbb{Z}^n$ e $\boldsymbol{u} \in [-1/2, 1/2]^n$. Da desigualdade triangular e da definição de l_0 segue que

$$F_K(\boldsymbol{y}) \leq F_K(\boldsymbol{x}) + F_K(\boldsymbol{u}) \leq r + l_0,$$

o que implica $\boldsymbol{y} \in (r + l_0)K$.

(ii) Seja $\boldsymbol{y} \in (r - l_0)K$. Escrevemos $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{u}$, $\boldsymbol{x} \in \mathbb{Z}^n$ e $\boldsymbol{u} \in [-1/2, 1/2]^n$. Queremos mostrar que $\boldsymbol{x} \in K$. Temos

$$F_K(\boldsymbol{x}) \leq F_K(\boldsymbol{y}) + F_K(-\boldsymbol{u}) \leq (r - l_0) + l_0 = r,$$

o que completa a demonstração.

Da tripla inclusão de conjuntos (2), e da Proposição 1a. da primeira aula temos

$$\text{vol } (r - l_0)K \leq \text{vol} \left(\bigcup_{\boldsymbol{x} \in \mathbb{Z}^n \cap K} \left(\boldsymbol{x} + \left[-\frac{1}{2}, \frac{1}{2} \right]^n \right) \right) \leq \text{vol } (r + l_0)K$$

$$(r - l_0)^n \text{vol } K \leq L_K(r) \leq (r + l_0)^n \text{vol } K.$$

Aplicando o limite nos três termos, temos o resultado desejado. Uma simples manipulação da igualdade acima nos dá o limitante para o erro. $\square$

Observação 1. *Para o teorema acima não precisamos, de fato, que K seja fechado, entretanto neste caso a demonstração é "mais limpa".*

Exemplo 2 (Problema do Círculo de Gauss)**.** *Seja* $K = \{(x_1, x_2) : x_1^2 + x_2^2 \leq 1\} = B_2(1)$. *Na notação do teorema acima,* $l_0 = \sqrt{2}/2$ *e portanto*

$$|L_K(r) - \pi r^2| \leq \sqrt{2}\pi r + 1/2.$$

Este problema data de Gauss e expoentes muito melhores que r^{n-1} são conhecidos. O melhor limitante assintótico conhecido para o erro, $O(r^{131/208})$, é devido a Huxley [Hux03].

Teorema 1. (Conjuntos Mensuráveis) *Se* $K \subset \mathbb{R}^n$ *é limitado e* $0 < \operatorname{vol} K < \infty$, *então o Teorema 1 é válido com* $|L_K(r) - \operatorname{vol} rK| = O(r^{n-1})$.

Demonstração. Veja os argumentos *en passant* de [GL87, p. 141] ou as notas de aula do Prof. Fukshansky, p. 64 para uma demonstração sob algumas hipóteses adicionais na fronteira de K. □

2 Teoremas de Minkowski e Blitchfield

Os resultados da seção anterior nos mostram estimativas para a quantidade de pontos inteiros em K. Caracterizaremos, agora, condições suficientes para que $\#(K \cap \mathbb{Z}^n) \neq \{0\}$, ou seja, para que haja, de fato, um ponto inteiro não nulo em K. Iniciaremos pelo seguinte resultado, largamente utilizado, que pode ser visto como uma espécie de "princípio das casas dos pombos" da Geometria dos números.

Teorema 2 (Blitchfield)**.** *Se* $\operatorname{vol} K > 1$, *então existem* $\boldsymbol{x}, \boldsymbol{y} \in K$, $\boldsymbol{x} \neq \boldsymbol{y}$, *tais que* $\boldsymbol{x} - \boldsymbol{y} \in \mathbb{Z}^n$.

Demonstração. A demonstração é feita utilizando uma técnica similar ao *tangram.* Seja $\mathcal{P} = [0,1)^n$ um cubo fundamental de $\mathbb{Z}^n$. Como $\mathcal{P}$ ladrilha o espaço, existem $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_m$ tais que

$$K = (K \bigcap \mathcal{P} + \boldsymbol{x}_1) \bigcup (K \bigcap \mathcal{P} + \boldsymbol{x}_2) \cdots \bigcup (K \bigcap \mathcal{P} + \boldsymbol{x}_m).$$

Portanto

$$\operatorname{vol} K = \sum_{i=1}^{m} \operatorname{vol} \left(K \bigcap (\mathcal{P} + \boldsymbol{x}_i) \right) > 1.$$

Transladando cada intersecção $K \bigcap (\mathcal{P} + \boldsymbol{x}_i)$ por $-\boldsymbol{x}_i$, temos que

$$\bigcup_{i=1}^{M} (K - \boldsymbol{x}_i) \bigcap \mathcal{P} \subset \mathcal{P} \Rightarrow \operatorname{vol} \left(\bigcup_{i=1}^{m} (K - \boldsymbol{x}_i) \bigcap \mathcal{P} \right) \leq 1$$

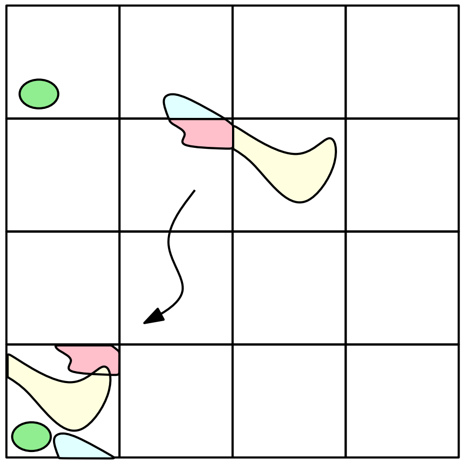

Figura 1: Ideia da prova do Teorema de Blitchfield. O conjunto K (neste caso desconexo) é constituído pelas partes coloridas, a serem trasladadas para o cubo fundamental $[0,1)^n$.

Portanto devem existir $i \neq j$ tais que $(K - \boldsymbol{x}_i)$ e $(K - \boldsymbol{x}_j)$ não são disjuntos (veja Figura 1), caso contrário teríamos

$$\text{vol}\left(\bigcup_{i=1}^{m}(K - \boldsymbol{x}_i)\bigcap \mathcal{P}\right) = \sum_{i=1}^{m}\text{vol}\,\left((K - \boldsymbol{x}_i)\bigcap \mathcal{P}\right) = \text{vol}\,K > 1.$$

Tomando $\boldsymbol{u} \in (K - \boldsymbol{x}_i)\bigcap(K - \boldsymbol{x}_j)$, vemos que $\boldsymbol{u} = \boldsymbol{k}_1 - \boldsymbol{x}_i = \boldsymbol{k}_2 - \boldsymbol{x}_j$, com $\boldsymbol{k}_1, \boldsymbol{k}_2 \in K$ e $\boldsymbol{x}_i, \boldsymbol{x}_j \in \mathbb{Z}^n$, ou seja, $\boldsymbol{k}_1 - \boldsymbol{k}_2 \in \mathbb{Z}^n$, como queríamos demonstrar. $\square$

O Teorema de Blitchfield é o melhor possível para conjuntos gerais. Para ver isso, tome $K = (0,1)^n$. Utilizando o Teorema de Blitchfield podemos demonstrar o

Teorema 3 (Primeiro Teorema de Minkowski)**.** *Se K é um corpo convexo, simétrico em relação à origem, e* vol $K > 2^n$*, então existe um ponto $\boldsymbol{x} \neq 0$ tal que $\boldsymbol{x} \in K \cap \mathbb{Z}^n$.*

Demonstração. Considere o conjunto $HK = (1/2)K$. Temos vol $HK = (1/2^n)$vol $K > 1$. Portanto, pelo Teorema 2, existem dois pontos $(1/2)k_1$ e $(1/2)k_2$ em HK tais que $(1/2)k_1 - (1/2)k_2 \in \Lambda$. Como K é convexo e simétrico pela origem, $(1/2)K - (1/2)K = K$, o que completa a demonstração. $\square$

Observação 2. *Do teorema acima, pelo fato de K ser simétrico em relação à origem, temos $\#(K \cap \mathbb{Z}^n) = L_K(1) \geq 3$.*

Observação 3. *Nos teoremas de Minkowski e Blitchfield, se K é fechado, então podemos substituir $>$ por $\geq$.*

É possível generalizar ambos os teoremas, conforme descrito a seguir

Teorema 4 (Blitchfield 2.0)**.** *Seja $m \in \mathbb{N}$. Se* vol $K > m$, *então existem $m+1$ pontos $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{m+1} \in K$ tais que*

$$\boldsymbol{x}_i - \boldsymbol{x}_j \in \mathbb{Z}^n, \forall 1 \leq i, j \leq m+1.$$

Demonstração. Analisaremos o conjunto $K \cap (1/r)\mathbb{Z}^n$, para r suficientemente grande. Vemos claramente que $\#(K \cap (1/r)\mathbb{Z}^n) = L_K(r)$ e, portanto $\lim \#(K \cap (1/r)\mathbb{Z}^n)/r^n \text{vol } K = 1$. Como vol $K > m$, existe r_0 tal que, para $r > r_0$, $\#(K \cap (1/r)\mathbb{Z}^n) > r^n m$. Para cada $\boldsymbol{x} \in K \cap (1/r)\mathbb{Z}^n$, seja $\boldsymbol{u} = r\boldsymbol{x} \in \mathbb{Z}^n$. Como há pelo menos $r^n m + 1$ possíveis vetores $\boldsymbol{u}$, e há r^n classes de equivalência de $\boldsymbol{u} \mod r$, temos, pelo princípio das casas dos pombos generalizado, que pelo menos $m+1$ desses vetores estão na mesma classe de equivalência módulo r. Denotando por $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{m+1}$ esses vetores e $\boldsymbol{x}_i = (1/r)\boldsymbol{u}_i$, temos:

$$\boldsymbol{x}_i - \boldsymbol{x}_j = (1/r)(\boldsymbol{u}_i - \boldsymbol{u}_j) \in \mathbb{Z}^n \cap K,$$

como queríamos demonstrar. □

Muito similarmente ao Teorema 3, podemos mostrar

Teorema 5 (Minkowski 2.0)**.** *Se K é um conjunto convexo, simétrico em relação à origem, e* vol $K > m2^n$, *então existem m pontos não-nulos $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m$ tais que $\boldsymbol{x}_i \in K \cap \mathbb{Z}^n$.*

Pelas mesmas razões do Primeiro Teorema de Minkowski (e com um pouco de cuidado...) temos $L_K(1) = \#(K \cap \mathbb{Z}^n) \geq 2m + 1$.

Da maneira que enunciamos os teoremas das duas primeiras seções, é difícil visualizar claramente qualquer aplicação. Entretanto, uma simples generalização torna-os ferramentas poderosas.

3 Enumeradores de Pontos Inteiros e Teoremas de Minkowski Revisitados

Seja $A \in \mathbb{R}^{n \times n}$ uma matriz invertível e $A\mathbb{Z}^n = \{A\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^n\}$. Temos que $\boldsymbol{x} \in K \cap (A\mathbb{Z}^n)$ se, e somente se, $A^{-1}\boldsymbol{x} \in A^{-1}K \cap \mathbb{Z}^n$. Assim, existe uma bijeção entre os pontos de $K \cap (A\mathbb{Z}^n)$ e $\in A^{-1}K \cap \mathbb{Z}^n$, e portanto a cardinalidade de ambos os conjuntos é a mesma. Desta simples observação, obtemos versões dos teoremas estudados quando o conjunto $\mathbb{Z}^n$ é substituido pela imagem de $\mathbb{Z}^n$ sob uma transformação linear. Essas versões são generalizações poderosas.

Teorema 1. (Sob Transformações Lineares) *Se $K \subset \mathbb{R}^n$ é um conjunto limitado tal que $0 < \text{vol } K < \infty$, então*

$$\lim_{r \to \infty} \frac{\#(K \cap A\mathbb{Z}^n)}{\text{vol } rK} = \frac{1}{\det A}.$$

Teorema 2. (Blitchfield sob Transformações Lineares) *Se* $\text{vol } K > \det A$, *então existem $\boldsymbol{x}, \boldsymbol{y} \in K$, $\boldsymbol{x} \neq \boldsymbol{y}$, tais que $\boldsymbol{x} - \boldsymbol{y} \in A\mathbb{Z}^n$.*

Teorema 3. (Blitchfield sob Transformações Lineares) *Se* $\text{vol } K > \det A$, *então existem $\boldsymbol{x}, \boldsymbol{y} \in K$, $\boldsymbol{x} \neq \boldsymbol{y}$, tais que $\boldsymbol{x} - \boldsymbol{y} \in A\mathbb{Z}^n$.*

Similarmente, podemos generalizar os teoremas 5 e 6. Veremos uma aplicação destas generalizações sobre formas quadráticas (e representações de inteiros) nas próximas aulas. Por enquanto, enunciaremos uma aplicação em aproximações diofantinas.

3.1 Um Teorema sobre Equações Diofantinas

Uma *forma linear* é uma transformação $\xi : \mathbb{R}^n \to \mathbb{R}$ do tipo

$$\xi(\boldsymbol{x}) = m_1\boldsymbol{x}_1 + \ldots m_n\boldsymbol{x}_n,$$

com $m_i \in \mathbb{R}$. Dado $\boldsymbol{y}$, uma equação do tipo $\xi(\boldsymbol{x}) = \boldsymbol{y}$ é dita uma *equação diofantina linear*. Dadas n formas lineares em n variáveis, associamos a estas uma matriz $A_{ij} = \xi_i(\boldsymbol{e}_j)$ e dizemos que o determinante dessas formas é igual a $\det A$.

Teorema 6. *Sejam $\xi_1, \ldots \xi_n$ formas lineares em n variáveis. Considere a matriz A_{ij} como descrito acima. Sejam números positivos $t_1, \ldots, t_n$ tais que $t_1 t_2 \ldots t_n = |\det A|$. Existem um vetor $\boldsymbol{x} \in \mathbb{Z}^n$ não-nulo tal que*

$$|\xi(\boldsymbol{x}_i)| < t_i.$$

Demonstração. Seja K o parallelotopo $K = \{\boldsymbol{x} \in \mathbb{R}^n : |\xi(\boldsymbol{x})| \leq t_i\}$. Temos $A^{-1}K = \{\boldsymbol{y} \in \mathbb{R}^n : |y_i| \leq t_i\}$. Claramente $A^{-1}K$ (e portanto $\mathcal{P}$) é um corpo convexo, fechado, simétrico com relação à origem e

$$\text{vol } (A^{-1}K) = |\det A^{-1}| \text{vol } \mathcal{P} = 2^n t_1 \ldots t_n.$$

Assim , vol $K = 2^n$ e o teorema segue do Primeiro Teorema de Minkowski 3, e da Observação 3. $\square$

Como um caso especial do teorema acima, tome

$$A = \begin{pmatrix} -1 & 0 & 0 & \dots & 0 & \alpha_1 \\ 0 & -1 & 0 & \dots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & \alpha_{n-1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}.$$

As formas lineares $\xi_i(\boldsymbol{x}) = x_i - \alpha_i x_n$ possuem soluções para quaisquer t_i satisfazendo as hipóteses do teorema. Em particular, pra $\tau > 0$, se $t_i = \tau^{1/(m-1)}, i = 1, \dots m-1$ e $t_n = 1/\tau$, então é possível encontrar soluções do tipo

$$|\alpha_i - x_i/x_n| \leq \tau^{1/(m-1)}/x_n,$$

ou seja, encontramos aproximações racionais com mesmo denominador para α_i. Este caso torna-se não-trivial se consideramos $\alpha_i \notin \mathbb{Q}$, $i = 1, \dots, n$.

Exercício 1. Demonstre o Teorema 5. Por que só podemos garantir a existência de m pontos, e não $m+1$? Explique também o"pouco de cuidado" que temos que tomar para garantir que $L_K(1) = \#(K \cap \mathbb{Z}^n) \geq 2m+1$.

Exercício 2. Escreva uma demonstração formal dos Teoremas 1, 2 e 3.

Exercício 3. Demonstre a Observação 3.

Exercício 4. Seja K um politopo cruz $\{\boldsymbol{x} \in \mathbb{R}^n : |x_1| + \ldots + |x_n| \leq 1\}$

(i) Quanto vale vol K?

(ii) Quanto vale $L_K(r)$?

(iii) Calcule o erro $|L_K(r) - \text{vol } K|$ e compare com o Teorema 1

Exercício 5. Repita o exercício acima para o simplex $K = \{\boldsymbol{x} \in \mathbb{R}^n : 0 \leq x_1 \leq x_n \leq 1\}$.

Referências

[GL87] P. M. Gruber and C. G. Lekkerkerker. *Geometry of Numbers*. North-Holland, 1987.

[Hux03] M. N. Huxley. Exponential sums and lattice points iii. *Proceedings of the London Mathematical Society*, 87:591–609, 11 2003.