PICME/IME/USP COMBINATÓRIA

NOTAS - 2011 (SEMESTRE 1)

YOSHIHARU KOHAYAKAWA, MIGUEL ABADI E GUILHERME MOTA (IME/USP)

1. Conjuntos equiláteros

12/04/2011

Dados dois vetores $\underline{x}$, $\underline{y} \in \mathbb{R}^d$, definimos a distância ℓ_p entre tais vetores (para $p \in \{1, 2, \infty\}$) como $\|\underline{x} - \underline{y}\|_p$, onde

$$\|\underline{x} - \underline{y}\|_1 = \sum_{i=1}^d |x_i - y_i|;$$
$$\|\underline{x} - \underline{y}\|_2 = \left(\sum_{i=1}^d (x_i - y_i)^2\right)^{1/2};$$
$$\|\underline{x} - \underline{y}\|_\infty = \max_{1 \le i \le d} |x_i - y_i|.$$

Dados $\underline{p_i} \in \mathbb{R}^d$, para $i \in \{1, 2, \ldots, n\}$, dizemos que o conjunto $\{\underline{p_1}, \underline{p_2}, \ldots, \underline{p_n}\}$ é *p-equilátero* se as distâncias $\|\underline{p_i} - \underline{p_j}\|_p$ são iguais para todo par $\{\underline{p_i}, \underline{p_j}\}$ onde $i \neq j$.

Seja $n_p(d) = \max\{n\colon$ existe um conjunto p-equilátero $\underline{x_i} \in \mathbb{R}^d$, para $i \in \{1, \ldots, n\}\}$. Claramente, $n_2(2) = 3$. O seguinte lema dá o valor de $n_2(d)$ para um $d \ge 1$.

Lema 1. *Dado $d \ge 1$, temos $n_2(d) = d + 1$.*

Demonstração. Para mostrar que $n_2(d) \ge d+1$ basta exibirmos um conjunto com $d+1$ vetores em $\mathbb{R}^d$ que é 2-equilátero. Sabendo que $e_i \in \mathbb{R}^d$ é o vetor com 0 em todas as coordenadas, com exceção da coordenada i, que possui valor 1, observamos que o conjunto dos vetores $\{e_i\colon 1 \le i \le d+1\}$ é 2-equilátero e não é difícil ver que tal conjunto de vetores está contido em $\mathbb{R}^d$.

Deixe-nos mostrar agora que $n_2(d) \le d + 1$. Seja $(\underline{p_i})_{i=1}^{n+1}$ um conjunto 2-equilátero de vetores, com $\underline{p_i} \in \mathbb{R}^d$, para $i \in \{1, \ldots, n+1\}$. Suponha s.p.g. que $\underline{p_{n+1}} = 0$ e $\|p_i\|_2 = 1$. Considere a matriz de Gram $G = (g_{i,j})_{i,j=1}^n$, com $g_{i,j} = \langle \underline{p_i}, \underline{p_j} \rangle$ para todo i, $j \in \{1, \ldots, n\}$. Assim, temos que $G = (I_n + J_n)/2$, onde I_n é a matriz identidade $n \times n$ e J_n é a matriz $n \times n$ com todas as coordenadas iguais a 1. Portanto, a matriz G tem posto cheio, isto é, posto$(G) = n$. Mas, por outro lado, $G = P^T P$, onde $P = [\underline{p_1} | \ldots | \underline{p_n}]_{d \times n}$. Assim, posto$(G) \le d$, donde concluímos que $n \le d$ e o resultado está provado, pois isto mostra que o conjunto $(\underline{p_i})_{i=1}^{n+1}$ possui no máximo $d+1$ vetores. □

Notas por Guilherme Mota

Observe que o cubo $\{0,1\}^d$ é um conjunto ∞-equilátero com 2^d elementos, pois quaisquer dois elementos $\underline{x}$ e $\underline{y}$ deste conjunto possuem distância ℓ_∞ igual a 1. Portanto, $n_\infty(d) \geq 2^d$. Mas será que existe algum conjunto ∞-equilátero com mais de 2^d elementos? (veja exercício 1.1.1).

No restante desta seção iremos focar nossa atenção na distância ℓ_1. Por simplicidade, a partir de agora, dizemos que um conjunto é *equilátero* se tal conjunto é 1-equilátero. Observe que o conjunto $\{e_1, -e_1, e_2, -e_2, \ldots, e_d, -e_d\}$ de tamanho $2d$ é equilátero, logo, $n_1(d) \geq 2d$. É conjecturado há muito tempo que não existem conjuntos equiláteros com mais de $2d$ elementos, porém, durante muito tempo não se soube um limite superior melhor que $2^d - 1$. Em 2003, Alon e Pudlák [1] mostraram que $n_1(d) = O(d \log d)$. Mostaremos aqui uma prova simples de que $n_1(d) = O(d^4)$, mas antes deixe-nos enunciar alguns lemas que serão utilizados na prova deste resultado.

Lema 2 (Lema da imersão aproximada)**.** *Para todos d, $q \in \mathbb{N}$, existe uma função $f_{d,q}\colon [0,1]^d \to \mathbb{R}^{dq}$ tal que, para quaisquer $\underline{x}$, $\underline{y} \in [0,1]^d$, temos*

$$\left| \frac{1}{q} \|f_{d,q}(\underline{x}) - f_{d,q}(\underline{y})\|_2^2 - \|\underline{x} - \underline{y}\|_1 \right| \leq \frac{2d}{q}.$$

Demonstração. Provamos inicialmente o resultado para $d = 1$. Para $x \in [0,1]$, considere a função $f_{1,q}$ tal que as primeiras $\lfloor qx \rfloor$ coordenadas de $f_{1,q}(x)$ são iguais a 1 e as $q - \lfloor qx \rfloor$ restantes são iguais a 0. Temos que $\|f_{1,q}(\underline{x}) - f_{1,q}(\underline{y})\|_2^2 = |\lfloor xq \rfloor - \lfloor yq \rfloor| = q\|x - y\|_1 \pm 2$.

Seja $d > 1$. Para $\underline{x} = (x_i)_{i=1}^d$, fazemos $f_{d,q}(\underline{x}) = (f_{1,q}(x_1), \ldots, f_{1,q}(x_d)) \in \mathbb{R}^{dq}$. Desta forma, para todo $\underline{x}$, $\underline{y} \in \mathbb{R}^d$, temos $\|f_{d,q}(\underline{x}) - f_{d,q}(\underline{y})\|_2^2 = \sum_{i=1}^d (|x_i - y_i|q \pm 2) = \|\underline{x} - \underline{y}\|_1 q \pm 2d$. □

Lema 3 (Lema do posto)**.** *Seja $A = [a_{i,j}]_{n \times n}$ uma matriz não nula real e simétrica. Então*

$$\text{posto}(A) \geq \frac{(\sum_{i=1}^n a_{ii})^2}{\sum_{i,j=1}^n a_{ij}^2}.$$

Demonstração. Se A uma matriz não nula $n \times n$ real e simétrica, então possui n autovalores reais $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. Ademais, se $\text{posto}(A) = r$, então existem exatamente r autovalores não nulos. Sem perda de generalidade, suponha que $\lambda_1, \ldots, \lambda_r \neq 0$ e $\lambda_{r+1}, \ldots, \lambda_n = 0$. Pela desigualdade de Cauchy–Schwarz ($(\sum_{i=1}^r x_i y_i)^2 \leq (\sum_{i=1}^r x_i^2)(\sum_{i=1}^r y_i^2)$), temos que $\sum_{i=1}^r \lambda_i^2 \geq 1/r(\sum_{i=1}^r \lambda_i)^2$, isto é,

$$r \geq \frac{(\sum_{i=1}^r \lambda_i)^2}{\sum_{i=1}^r \lambda_i^2} = \frac{(\sum_{i=1}^n \lambda_i)^2}{\sum_{i=1}^n \lambda_i^2}.$$

Dada uma matriz A, é sabido que a soma dos autovalores de A é igual ao traço de A ($\sum_{i=1}^{n} a_{ii}$) e a soma dos quadrados dos autovalores de A é igual ao traço da matriz A^2. Assim, temos que

$$r \geq \frac{(\sum_{i=1}^{n} a_{ii})^2}{\sum_{i,j=1}^{n} a_{ij}^2}.$$

□

O seguinte corolário é facilmente deduzido do Lema 3.

Corolário 4. *Seja $A = [a_{i,j}]_{n\times n}$ uma matriz não nula real e simétrica com $a_{ii} = 1$ para todo $i \in [n]$ e $|a_{ij}| \leq 1/\sqrt{n}$ para todo $i \neq j$. Então* $\text{posto}(A) \geq n/2$.

Lema 5 (Lema sobre conjuntos quase equiláteros)**.** *Sejam $\underline{p_1}, \ldots, \underline{p_n} \in \mathbb{R}^d$ tais que, para todo $i \neq j$, temos*

$$\left| \|\underline{p_i} - \underline{p_j}\|_2^2 - 1 \right| \leq \frac{1}{\sqrt{n}}.$$

Então $n \leq 2(d+2)$.

Demonstração. Seja $A = [a_{i,j}]_{n\times n}$ com $a_{ij} = 1 - \|\underline{p_i} - \underline{p_j}\|^2$. A hipótese do lema juntamente com o corolário nos dizem que $\text{posto}(A) \geq n/2$. Vamos agora limitar superiormente o posto de A. Para tanto, considere, para todo $i \in [n]$, a função $f_i \colon \mathbb{R}^d \to \mathbb{R}$ tal que $f_i(\underline{x}) = 1 - \|\underline{x} - \underline{p_i}\|^2$ para $\underline{x} \in \mathbb{R}^d$. Assim, temos que $a_{ij} = f_i(\underline{p_j})$. Portanto, a i-ésima linha da matriz A é dada por $(f_i(\underline{p_1}), \ldots, f_i(\underline{p_n})) \in \mathbb{R}^n$. Mas

$$\begin{aligned} f_i(\underline{x}) &= 1 - \|\underline{x} - \underline{p_i}\|^2 \\ &= 1 - \langle \underline{x} - \underline{p_i}, \underline{x} - \underline{p_i} \rangle \\ &= 1 - \langle \underline{x} - \underline{x} \rangle - \langle \underline{p_i} - \underline{p_i} \rangle + 2(x_1 p_{i1} + \ldots + x_d p_{id}) \\ &= 1 - \|\underline{x}\|_2^2 - \|\underline{p_i}\|_2^2 + 2(x_1 p_{i1} + \ldots + x_d p_{id}). \end{aligned}$$

Portanto, é fácil ver que cada função f_i é uma combinação linear de $d+2$ funções (a função constante 1, as funções $\underline{x} \mapsto \|x\|_2^2$ e as d funções $\underline{x} \mapsto x_k$). Assim, o espaço gerado pelas funções f_i possui dimensão no máximo $d+2$. Logo, $\text{posto}(A) \leq d+2$. Mas sabemos que $\text{posto}(A) \geq n/2$. Estes dois fatos nos dizem que $n \leq 2(d+2)$. □

Teorema 6. *Para todo $d \geq 1$, temos $n_1(d) < 100d^4$.*

Demonstração. Por contradição, suponha que exista um conjunto equilátero em $\mathbb{R}^d$ com $n = 100d^4$ elementos. Sem perda de generalidade, suponha que um dos n elementos é o ponto $(1/2, \ldots, 1/2)$ e

que a distância entre quaisquer dois pontos é $1/2$. Assim, o conjunto destes n pontos está totalmente contido em $[0,1]^d$.

Aplicando o Lema 2 com $q = 40d^3$, sabemos que existe uma função $f_{d,q}$ tal que

$$\left| \frac{1}{q} \|f_{d,q}(\underline{x}) - f_{d,q}(\underline{y})\|_2^2 - \frac{1}{2} \right| \leq \frac{2d}{q}.$$

Isto é, $2d - q/2 \leq \|f_{d,q}(\underline{x}) - f_{d,q}(\underline{y})\|_2^2 \leq 2d + q/2$. Aplicando uma escala de fator $\sqrt{q/2}$, obtemos um conjunto tal que o quadrado da distância Euclidiana entre quaisquer dois pontos está entre $1 - 4d/q$ e $1 + 4d/q$ (note que $4d/q = 1/10d^2 = 1/\sqrt{n}$). Aplicando o Lema 5, temos $n \leq 2(dq + 2)$, mas $2(dq + 2) = 2(40d^4 + 2) < 100d^4$, uma contradição com a escolha de n. □

Para mais detalhes sobre este resultado e sobre outras interessantes aplicações de álgebra linear, veja [4].

1.1. **Problemas e exercícios.** Todos estão convidados a trabalhar no seguinte exercício.

1. Encontre um bom limite superior para $n_\infty(d)$.

2. Duas distâncias / Cobrindo hipercubos

19/04/2011

Primeiramente, consideramos o problema de encontrar a máxima quantidade de pontos que podem existem em $\mathbb{R}^d$, $d \geq 2$, tal que as distâncias entre quaisquer dois pontos têm no máximo dois valores diferentes.

Dado $d \geq 2$, dizemos que o conjunto $\underline{p_1}, \underline{p_2}, \ldots, \underline{p_n} \in \mathbb{R}^d$ é um *conjunto com duas distâncias* se existem a, $b \in \mathbb{R}$ tais que $\|\underline{p_i} - \underline{p_j}\|_2 = a$ ou $\|\underline{p_i} - \underline{p_j}\|_2 = b$ para todo $i \neq j$. Ademais, definimos $m(2,d) = \max\{n\colon \text{existe um conjunto de tamanho } n \text{ com duas distâncias}\}$.

Claramente, os vértices de um pentágono regular formam um conjunto de cinco pontos com duas distâncias. Isto mostra que $m(2,2) \geq 5$. Mas será que existe um conjunto com duas distâncias que tenha mais que 5 elementos? (veja exercício 2.1.1).

Considere os $\binom{d}{2}$ pontos $\underline{p_{ij}}$ $(1 \leq i < j \leq d)$ em $\{0,1\}^d$ que contém exatamente dois 1's (nas posições i e j). Claramente, o conjunto de tais pontos é um conjunto com duas distâncias, pois só é possível que existam as distâncias 2 e $\sqrt{2}$. Porém, este conjunto está contido no hiperplano $\sum_{i=1}^{d} x_i = 2$. Desta forma, o conjunto está contido em $\mathbb{R}^{d-1}$. Portanto, acabamos de mostrar que $m(2,d) \geq \binom{d+1}{2} = d(d+1)/2$. O seguinte teorema mostra que o fator quadrático em tal limite inferior é o melhor possível.

Teorema 7. *Seja $d \geq 1$. Então $m(2,d) \leq (d^2+5d+4)/2$.*

Demonstração. Tome n pontos $\underline{p_1}, \ldots, \underline{p_n} \in \mathbb{R}^d$ e suponha que tais pontos formem um conjunto com duas distâncias, digamos, a, $b \in \mathbb{R}$. Para cada $i \in \{1, \ldots, n\}$, definimos a função $f_i\colon \mathbb{R}^d \to \mathbb{R}$ tal que $f_i(\underline{x}) = (\|\underline{x} - \underline{p_i}\|^2 - a^2)(\|\underline{x} - \underline{p_i}\|^2 - b^2)$ para todo $\underline{x} \in \mathbb{R}^d$.

Considere o espaço vetorial de todas as funções de $\mathbb{R}^d$ em $\mathbb{R}$. Observe que $f_1, \ldots, f_n$ são linearmente independentes. De fato, suponha que $\sum_{i=1}^{n} \alpha_i f_i = 0$. Assim, para qualquer j, temos

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \alpha_i f_i(\underline{p_j}) \\ &= \alpha_j f_j(\underline{p_j}) \\ &= \alpha_j a^2 b^2, \end{aligned}$$

donde concluímos que $\alpha_j = 0$.

Seja $\underline{x} = (x_k)_{k=1}^d$ e $\underline{p_i} = (p_{ik})_{k=1}^d$. Veja que

$$\begin{aligned} f_i(\underline{x}) &= \left(\sum_{i=1}^d (x_k - p_{ik})^2 - a^2\right)\left(\sum_{i=1}^d (x_k - p_{ik})^2 - b^2\right) \\ &= \sum_S \alpha_S X_S, \end{aligned}$$

onde a última soma é sobre todos os multiconjuntos $S \subset [d]$ tais que $|S| \leq 4$ e $X_S = \prod_{k \in S} x_k$. Desta forma, temos que f_i está contido em um espaço de dimensão $1 + d + d^2 + d^3 + d^4$. Portanto, temos $n \leq 1 + d + d^2 + d^3 + d^4$, mas não é este o valor que queremos encontrar.

Para encontrar o limite que desejamos, vamos fazer uma análise mais cuidadosa. No que segue, considere $X = \sum_{i=1}^d x_j^2$, $P_i = \sum_{i=1}^d p_{ij}^2$, $A_i = P_i - a^2$ e $B_i = P_i - b^2$. Temos que

$$\begin{aligned} f_i(\underline{x}) &= \left(\sum_{i=1}^d (x_k - p_{ik})^2 - a^2\right)\left(\sum_{i=1}^d (x_k - p_{ik})^2 - b^2\right) \\ &= \left(X - \sum_{j=1}^d 2p_{ij}x_j + A_i\right)\left(X - \sum_{j=1}^d 2p_{ij}x_j + B_i\right) \\ &= X^2 - 4X\sum_{j=1}^d p_{ij}x_j + 4\left(\sum_{j=1}^d p_{ij}x_j\right)^2 + (A_i + B_i)\left(X - 2\sum_{j=1}^d p_{ij}x_j\right) + A_iB_i. \end{aligned}$$

Portanto, os pontos f_i $(1 \leq i \leq n)$ pertencem ao espaço gerado por

$$\begin{aligned} &X^2, \\ &x_kX, \quad k = 1, \ldots, d, \\ &x_k^2, \quad k = 1, \ldots, d, \\ &x_kx_\ell, \quad 1 \leq k < \ell \leq d, \\ &x_k, \quad k = 1, \ldots, d, \\ &1. \end{aligned}$$

Assim, os pontos estão contidos em um espaço de dimensão $1 + 3d + \binom{d}{2} + 1 = (d^2 + 5d + 4)/2$. Desta forma, $n \leq (d^2 + 5d + 4)/2$, uma vez que os $f_i's$ são linearmente independentes.

□

Vamos considerar agora o problema de cobrir hipercubos utilizando hiperplanos. Considere os pontos $\{0,1\}^d \setminus \{\underline{0}\}$ do hipercubo d-dimensional unitário. Observe que todos os pontos estão contidos nos hiperplanos $W_k = \{\underline{x} = (x_i)_1^d \colon \sum_{i=1}^d x_i = k\}$, para $k \in \{1, \ldots, d\}$. Portanto, acabamos

de ver que é possível cobrir os vértices (sem o ponto $\underline{0}$) de um hiperplano d-dimensional utilizando d hiperplanos.

Dizemos que os hiperplanos $H_1, \ldots, H_N$ *AF-cobrem* $\{0,1\}^d$ se $0 \notin \bigcup_{k=1}^N H_k$ e, além disso, temos que $\{0,1\}^d \setminus \{\underline{0}\} \subset \bigcup_{k=1}^N H_k$. Desta forma, definimos

$$\mathrm{af}(d) = \min\{N\colon \text{existem hiperplanos } H_1, \ldots, H_N \text{ que AF-cobrem } \{0,1\}^d\}.$$

Pelo que foi discutido anteriormente, sabemos que $\mathrm{af}(d) \leq d$. O seguinte teorema mostra que, de fato, $\mathrm{af}(d) = d$.

Teorema 8. *Seja $d \geq 1$. Então* $\mathrm{af}(d) = d$.

Demonstração. Suponha que $H_1, \ldots, H_N$ AF-cobrem $\{0,1\}^d$. Sem perda de generalidade, vamos considerar $H_i = \{\underline{x} = (x_k)_1^d\colon \langle \underline{a_i}, \underline{x}\rangle = 1\}$ para $\underline{a_i} \in \mathbb{R}^d$.

Seja V o espaço vetorial das funções de $\{0,1\}^d$ nos reais. Considere a função

$$f(\underline{x}) = \prod_{i=1}^{N}(1 - \langle \underline{a_i}, \underline{x}\rangle) - \prod_{j=1}^{d}(1 - x_j). \tag{1}$$

Claramente, f define um elemento de V, a saber, o elemento $0 \in V$. Por outro lado, f é um polinômio nas variáveis $x_1, \ldots, x_d$. Suponha agora, por contradição, que $N < d$. Então, por (1), para $\underline{x} \in \{0,1\}^d$, temos que

$$x_1 \ldots x_d = \sum_S \alpha_S X_S, \tag{2}$$

onde a soma é sobre todos os multiconjuntos $S \subset [d]$ tais que $|S| < d$ e $X_S = \prod_{k \in S} x_k$.

Note que, em $\{0,1\}^d$, temos $x_S = x_{\hat{S}}$, onde $\hat{S}$ é o conjunto dos elementos em S (exemplo: ${x_1}^2 {x_2}^4 x_4 = x_1 x_2 x_4$ em $\{0,1\}^4$). Portanto, por (2), temos que o polinômio $x_1 \ldots x_d$ é uma combinação linear de monômios multilineares (i.e., da forma X_S para um conjunto S). Vamos provar que X_S ($S \subset [d]$) são linearmente independentes em V, uma contradição. Para tal, suponha que $\sum_{S \in [d]} \alpha_S X_S = 0$ e suponha que S_0 é tal que $\alpha_{S_0} \neq 0$ mas, para todo $T \subset S_0$ com $T \neq S_0$, temos $\alpha_T = 0$. Assim, se substituirmos (em (2)), $x_i = 1$ sempre que $i \in S_0$ e $x_i = 0$ sempre que $i \notin S_0$, então $0 = \alpha_{S_0}$. □

Estes resultados sobre cobertura de hipercubos podem ser vistos em [2].

2.1. **Problemas e exercícios.** Todos estão convidados a trabalhar nos seguintes exercícios.

1. Decida se $m(2,2) \geq 6$.
2. Prove que a cota $(d^2+5d+4)/2$ vale para conjuntos que definem duas distâncias *aproximadamente*. Note que é necessário definir precisamente o que vem a ser conjuntos com duas distâncias aproximadamente.
3. Estude $m(s,d) = \max\{n\colon \text{existem } n \text{ pontos em } \mathbb{R}^d \text{ definindo } s \text{ distâncias}\}$. Como sugestão, inicialmente mostre que $m(s,d) \geq \binom{d+1}{s}$.
4. Prove que $m(2,d) \leq \binom{d+2}{2}$.

3. Problema da agulha de Kakeya

26/04/2011

O problema de Kakeya consiste em determinar a menor área de uma região no plano em que podemos girar uma agulha em 360 graus. Considerando uma agulha de comprimento unitário, dizemos que um conjunto X é um *conjunto de Kakeya* se X contém um segmento de comprimento 1 em todas as direções (i.e., para qualquer direção que considerarmos, a agulha cabe em tal conjunto).

Um pesquisador chamado Besicovitch deu uma construção engenhosa de um conjunto de Kakeya com medida nula [3]. Daremos aqui uma ideia de como é possível construir um conjunto de Kakeya com medida arbitrariamente pequena. Considere um triângulo T de altura 1 e considere uma altura $h \in [0, 1)$ e um inteiro $k \geq 2$. Definimos um (k, h)-*corte de* T *com translação* o seguinte procedimento: dividimos T em k triângulos menores, todos com mesma base, transladamos os triângulos $T_2, \ldots, T_k$ de modo que os k triângulos se sobrepõem na altura h. Um exemplo de um $(3, h)$-corte com translação pode ser visto na Figura 1.

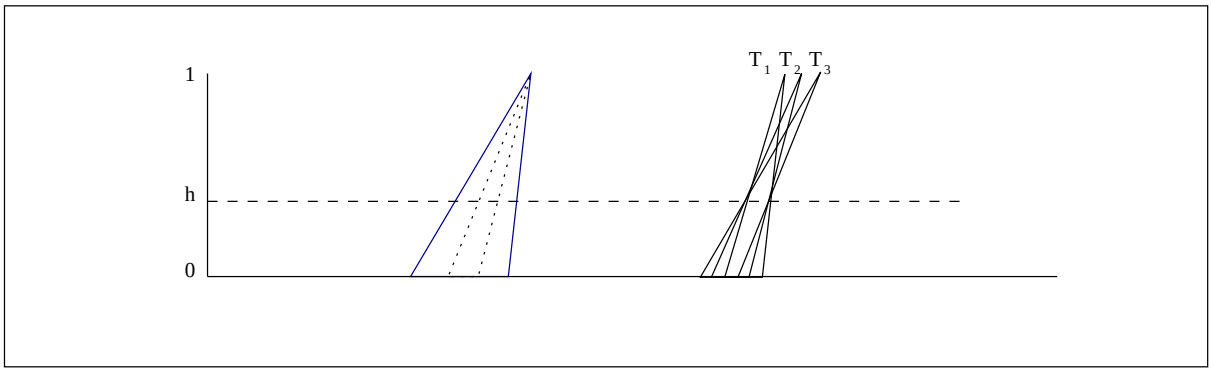

Figura 1. $(3, h)$-corte com translação.

Aplicando estes cortes repetidas vezes, em alturas diferentes, podemos obter conjuntos de Kakeya com medida arbitrariamente pequena. Seja m um inteiro "grande" e T um triângulo com 90 graus no ângulo do topo. Aplicamos um $(m, 1/m)$-corte em T, então aplicamos um $(m, 2/m)$-corte em todos os triângulos resultantes e assim por diante até aplicarmos um $(m, (m-1)/m)$-corte. Tal procedimento gera m^m triângulos, de modo que denotamos a união destes triângulos por B_m. É possível mostrar que, em qualquer altura, o tamanho da interseção entre os triângulos é no máximo $1/m$.

Precisamos agora dar uma ideia de como é possível girar a agulha utilizando o conjunto B_m. Para esta tarefa, aumentamos o conjunto através da criação de certos "corredores" que são extensões dos triângulos.

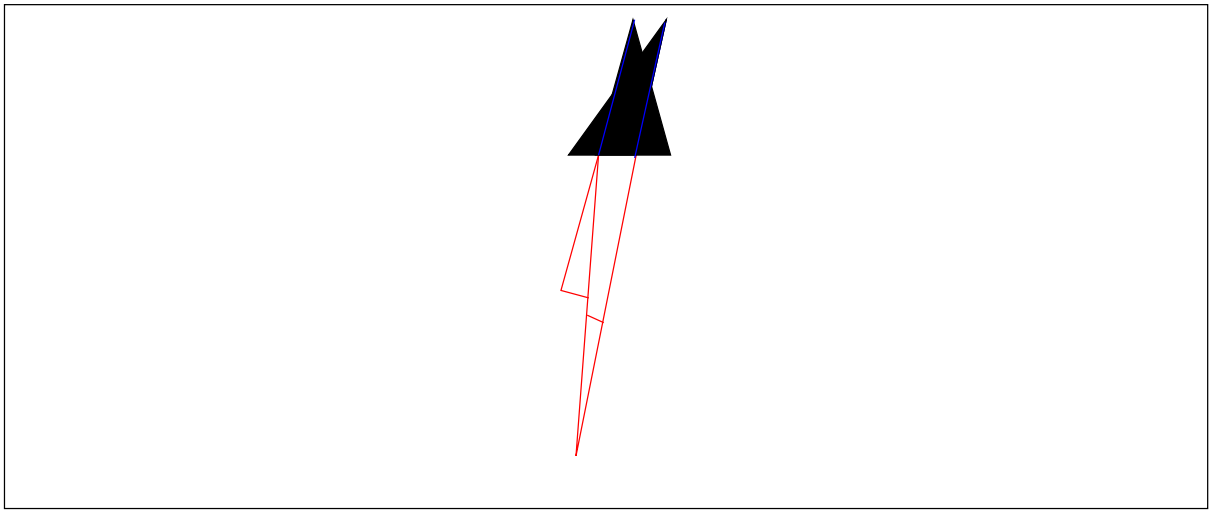

FIGURA 2. Corredores para movimentação da agulha em B_m.

Podemos mover a agulha (de uma marca azul para outra na Figura 2) para baixo pelo corredor vermelho, rotacioná-la e subir até a base do outro triângulo, rotacioná-la novamente, e, enfim, levá-la a este triângulo. Desde que façamos a agulha seguir por uma distância suficientemente grande pelo corredor, as rotações irão gerar uma área arbitrariamente pequena.

Consideremos agora o problema de Kakeya no contexto finito (ao invés de $\mathbb{R}^n$, vamos considerar $\mathbb{F}^n$, onde $\mathbb{F}$ é um corpo finito). Dizemos que $S \subset \mathbb{R}^n$ *contém direção* $\underline{u}$, com $\underline{u} \in \mathbb{R}^n$ e $\|\underline{u}\| = 1$ se existe $\underline{a} \in S$ tal que $\underline{a} + t\underline{u} \in S$ para todo $0 \leq t \leq 1$. Portanto, em $\mathbb{F}^n$, um subconjunto $S \subset \mathbb{F}^n$ *contém direção* $\underline{u}$, com $\underline{u} \in \mathbb{F}^n$ e $\underline{u} \neq 0$ se existe $\underline{a} \in S$ tal que $\underline{a} + t\underline{u} \in S$ para todo $t \in \mathbb{F}$. Com isso, dizemos que $S \subset \mathbb{F}^n$ é um *conjunto de Kakeya* em $\mathbb{F}^n$ se S contém toda direção $\underline{u} \in \{\mathbb{F}^n \setminus \{\underline{0}\}\}$.

Teorema 9. *Seja $\mathbb{F}$ um corpo com q elementos. Todo conjunto de Kakeya em $\mathbb{F}^n$ possui pelo menos $\binom{q+n-1}{n}$ elementos.*

Note que, para n fixo e q grande, conjuntos de Kakeya em $\mathbb{F}^n$ são uma proporção pelo menos $1/n!$ de $\mathbb{F}^n$, desde que $\binom{q+n-1}{n} = (q+n-1)_n/n! \geq q^n/n! = |\mathbb{F}^n|/n!$.

Os lemas 10 e 11 serão úteis na prova do Teorema 9.

Lema 10. *Sejam $\underline{a_1}, \underline{a_2}, \ldots, \underline{a_n} \in \mathbb{F}^n$ com $N < \binom{d+n}{n}$. Então existe polinômio $p = p(x_1, \ldots, x_n) \neq 0$ com coeficientes em $\mathbb{F}$ de grau no máximo d tal que $p(\underline{a_i}) = 0$ para $i \in \{1, \ldots, n\}$.*

Demonstração. Um polinômio de grau no máximo d em $x_1, \ldots, x_n$ pode ser escrito na forma $p(x_1, \ldots, x_n) = \sum_{\alpha_1 + \ldots + \alpha_n \leq d} (c_{\alpha_1, \ldots, \alpha_n} x^{\alpha_1} \ldots x^{\alpha_n})$, onde $\alpha_i \geq 0$ e $c_{\alpha_1, \ldots, \alpha_n} \in \mathbb{F}$. O número de

monômios na expressão acima é $\binom{d+n}{n}$. Para cada i, temos uma equação linear envolvendo os termos $c_{\alpha_1,\ldots,\alpha_n}$ dada por $p(\underline{a_i}) = 0$. Desde que temos $N < \binom{d+n}{n}$ equações e $\binom{d+n}{n}$ indeterminadas $c_{\alpha_1,\ldots,\alpha_n}$, existe uma solução não nula. □

Lema 11. *[Teorema de Schwartz–Zippel] Seja K um corpo e $S \subset K$ finito. Para todo polinômio não nulo $p = p(x_1, \ldots, x_n)$ com coeficientes em K, temos que, se escolhermos $(s_1, \ldots, s_m) \in S^m$ uniformemente ao acaso, então*

$$\Pr(p(s_1, \ldots, s_m) = 0) \leq \frac{d}{|S|},$$

onde d é o grau do polinômio p.

Demonstração. Utilizamos indução em m. Se $m = 1$, basta lembrar que $p(x) \in K[x]$ de grau d tem no máximo d raízes.

Suponha $m > 1$ e considere o resultado válido para valores menores de m. Ajustando a notação, podemos escrever o polinômio p da seguinte forma.

$$p(x_1, \ldots, x_m) = \sum_{i=0}^{k} p_i(x_1, \ldots, x_{m-1}) x_m^i,$$

com $p_i(x_1, \ldots, x_{m-1})$ não nulo.

Seja $R \subset S^m$ com $R = \{\underline{r} = (r_1, \ldots, r_m) \in S^m \colon p(\underline{r}) = 0\}$. Considere agora o conjunto $R_1 = \{\underline{r} \in R \colon p_k(r_1, \ldots, r_{m-1}) = 0\}$ e $R_2 = R \setminus R_1$. Então $|R_1| \leq ((d-k)|S|^{m-2})|S|$, desde que temos a hipótese indutiva e sabemos que o grau de p_k é no máximo $d - k$. Ademais, fixado $(r_1, \ldots, r_{m-1})$, temos no máximo k escolhas para r_m se queremos $\underline{r} \in R_2$. Assim, $|R_2| \leq k|S|^{m-1}$. Portanto, $|R| = |R_1| + |R_2| \leq d|S|^{m-1}$. □

Demonstração do Teorema 9. Fixe S conjunto de Kakeya em $\mathbb{F}^n$. Suponha $S = \{\underline{a_1}, \ldots, \underline{a_n}\}$ e $|S| = N < \binom{q+n-1}{n}$. Usando Lema 10, fixamos polinômio $p \neq 0$ com $p(\underline{a_i}) = 0$ para todo i e grau $d \leq q - 1$.

Fixe $u \in \mathbb{F}^n \setminus \{0\}$. Temos que existe $\underline{a} \in \mathbb{F}^n$ tal que $p(\underline{a} + t\underline{u}) = 0$ para todo $t \in \mathbb{F}$. Seja $f(t)$ o polinômio em t dado por $f(t) = p(\underline{a} + t\underline{u})$. Sabemos que o grau de $f(t)$ é no máximo $q - 1$. Como $f(b) = 0$ para todo $b \in \mathbb{F}$, f possui $q > q - 1$ zeros. Portanto, $f(t) \equiv 0$. Em particular, o coeficiente de t^d em $f(t)$ é zero. Tal coeficiente é $\overline{p}(\underline{u})$, onde $\overline{p}(\underline{u}) = \sum_{\alpha_1+\ldots+\alpha_n=d} C_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ é a assim chamada *parte homogênea* de p. Claramente, $\overline{p}(\underline{x}) \not\equiv 0$. Temos assim, $\overline{p}(\underline{u}) = 0$ para todo $\underline{u} \in \mathbb{F}^n$. Mas, pelo Lema 11 aplicado com $S = \mathbb{F}$, temos que se $R = \{\underline{r} \in \mathbb{F}^n \colon \overline{p}(\underline{r}) = 0\}$, então $|R| \leq d|\mathbb{F}|^{n-1} \leq (q-1)q^{n-1} < q^n$, uma contradição. □

Referências

[1] N. Alon and P. Pudlák, *Equilateral sets in l_p^n*, Geom. Funct. Anal. **13** (2003), no. 3, 467–482.

[2] N. Alon and Z. Füredi, *Covering the cube by affine hyperplanes*, European J. Combin. **14** (1993), no. 2, 79–83.

[3] A. S. Besicovitch, *On Kakeya's problem and a similar one*, Math. Z. **27** (1928), no. 1, 312–320.

[4] J. Matoušek, *Thirty-three miniatures*, Student Mathematical Library, vol. 53, American Mathematical Society, Providence, RI, 2010, Mathematical and algorithmic applications of linear algebra.