NOTAS DE AULA DO

PICME

Programa de Iniciação Científica e Mestrado em Combinatória

http://www.ime.usp.br/~tcco/picme

Anotado por: Fabrício Caluza Machado e Henrique Stagni

2º semestre de 2015

Conteúdo

1 Aplicações de Topologia à Combinatória

◇ ◇ ◇ *Aula 1(18 de Agosto) — Yoshiharu Kohayakawa* ◇ ◇ ◇

A seguir, veremos dois problemas geométricos e de combinatória que podem ser resolvidos com o auxilio de um teorema de topologia.

posição geral

Em ambos os problemas, usaremos o conceito de *posição geral*. Um conjunto de pontos $A \subset \mathbb{R}^d$ está em posição geral se não contém $d+1$ pontos em um mesmo hiperplano (em particular, se $|A| > d$, então A não contém três pontos colineares, nem quatro coplanares, etc).

1.1 Dois problemas

(1) **Partições arco-íris**.

Seja $A \subset \mathbb{R}^d$ um conjunto de nd pontos em posição geral. Suponha que esses pontos estão coloridos com n cores distintas e que cada cor aparece n vezes. Em outras palavras, suponha que particionamos A em conjuntos $A_1, \ldots, A_d$, dois a dois disjuntos, com $|A_i| = n$ para todo i.

partição arco-íris

Teorema 1.1 (Akiyama & Alon '89)**.** *Nas condições acima, A admite uma partição* arco-íris, *isto é, uma partição $\{V_1, \ldots, V_n\}$ tal que*

i) $|V_j| = d$, *para todo j;*

ii) $\mathrm{conv}(V_i) \cap \mathrm{conv}(V_j) = \emptyset$;

iii) $|A_i \cap V_j| = 1$.

Figura 1: Um exemplo com $d = 2$ e $n = 4$.

(2) **Colares**.

Considere um colar aberto com d tipos de pedras, sendo que há um número par de pedras de cada tipo. Dois ladrões querem dividir o colar em duas partes justas (com mesmo número de pedras de cada tipo em cada parte) minimizando o número de cortes no colar.

Figura 2: Dois exemplos. À direita, vemos que se as pedras de mesmo tipo estiverem agrupadas, d cortes são necessários.

Teorema 1.2 (T. Goldberg & West '85)**.** *Se um colar aberto tem d tipos de pedra, então d cortes são suficientes para dividir o colar em duas partes justas.*

Deixamos como exercício para o leitor encontrar uma prova puramente combinatória para essa proposição no caso $d = 2$.

É possível generalizar a proposição para l ladrões, alterando o número de cortes e o requerimento de que existem um número par de pedras de cada tipo para um múltiplo de l.

Vejamos agora um teorema de topologia usado na resolução destes dois problemas.

1.2 *The Ham Sandwich Theorem*

A versão informal, que dá nome ao teorema, é a seguinte. Suponha que você tem um sanduíche de presunto, formado por duas fatias de pão e uma fatia de presunto. Independente de como esteja montado o sanduíche, é possível dividi-lo em duas partes iguais (a mesma quantidade de cada fatia de pão e de presunto em cada parte) com apenas um corte.

Mais formalmente, sejam $\mu_1, ..., \mu_d$ d medidas finitas sobre $\mathbb{R}^d$ (isto é, $\mu_i(\mathbb{R}^d) < \infty$ para todo i), com todo aberto de $\mathbb{R}^d$ μ_i-mensurável.

Como exemplo de medida finita, considere um compacto $A \subset \mathbb{R}^d$ e faça $\mu_A(X) = \lambda^{(d)}(X \cap A)$ para todo X boleriano, onde $\lambda^{(d)}$ é a medida de Lebesgue usual.

Teorema 1.3 (*Ham Sandwich Theorem*)**.** *Sejam $\mu_1, ..., \mu_d$ medidas finitas sobre $\mathbb{R}^d$, com todo aberto de $\mathbb{R}^d$ μ_i-mensurável, tais que para qualquer hiperplano $H \subset \mathbb{R}^d$ temos $\mu_i(H) = 0$, $\forall i$. Então existe um hiperplano h tal que $\mu_i(h^+) = \frac{1}{2}\mu_i(\mathbb{R}^d)$, $\forall i$, onde h^+ é um dos semi-espaço fechados definidos por h.*

Demonstração. Seja $\mathbf{u} = (u_0, ..., u_d) \in S^d = \{(x_0, ..., x_d) \in \mathbb{R}^{d+1} \mid x_0^2 + ... + x_d^2 = 1\}$. Também podemos escrever $\mathbf{u}$ como $\mathbf{u} = (u_0, w), w \in \mathbb{R}^d, w = (u_1, ..., u_d)$.

Se $|u_0| \neq 1$, defina $h^+(\mathbf{u}) = \{x \in \mathbb{R}^d \mid \langle x, w\rangle \leq u_0\}$. Ademais, pomos $h^+(1, 0, ..., 0) = \mathbb{R}^d$ e $h^+(-1, 0, ..., 0) = \emptyset$.

Para entender a função h^+, consideremos inicialmente $u_0 = 0$. Temos $w = v \in S^{d-1}$ e neste caso, $h^+(0, v)$ é um semi-espaço que passa pela origem (veja a figura 3).

Se $u_0 \neq 0$, $\mathbf{u} = (u_0, w)$, com $w = \alpha v$, $v \in S^{d-1}$ e $|\alpha| < 1$. Temos $u_0^2 + \|w\|^2 = 1 \Rightarrow u_0^2 + \alpha^2 = 1$ e $\langle x, w\rangle \leq u_0 \Leftrightarrow \langle x, v\rangle \leq \frac{u_0}{\sqrt{1-u_0^2}}$. Assim, vemos que $h^+(\mathbf{u})$ é um semi-espaço deslocado na direção de v, se $u_0 > 0$ e na direção oposta, caso contrário (veja a figura 4). Note que $h^+(\mathbf{u}) \to \mathbb{R}^d$, quando $u_0 \to 1$ e $h^+(\mathbf{u}) \to \emptyset$, quando $u_0 \to -1$, o que justifica a definição de h^+ nestes casos. Aproveitamos para observar que $h^+(\mathbf{u})$ e $h^+(-\mathbf{u})$ são semi-espaço opostos.

Seja $f : S^d \to \mathbb{R}^d$, com $f = (f_1, ..., f_d)$ e $f_i = \mu_i(h^+(\mathbf{u}))$, $\forall i$.

Afirmação 1.4. *f é contínua.*

Demonstração. Provaremos que para todo i, $\mu_i(h^+(\mathbf{u}))$ é contínua em $\mathbf{u}$. Suponha que $\mathbf{u}_n \to \mathbf{u}$, vamos provar que $\mu_i(h^+(\mathbf{u}_n)) \to \mu_i(h^+(\mathbf{u}))$. Para isso, escrevemos $\mu_i(h^+(\mathbf{u}_n)) = \int \mathbb{1}_{h^+(\mathbf{u}_n)} d\mu_i$ e $\mu_i(h^+(\mathbf{u})) = \int \mathbb{1}_{h^+(\mathbf{u})} d\mu_i$. Como $|\mathbb{1}_{h^+(\mathbf{u}_n)}| \leq 1$ $\forall n$ e $\forall x \in \mathbb{R}^d \backslash h^+(\mathbf{u})$, $\mathbb{1}_{h^+(\mathbf{u}_n)}(x) \to_n \mathbb{1}_{h^+(\mathbf{u})}(x)$, temos que $\mathbb{1}_{h^+(\mathbf{u}_n)} \to \mathbb{1}_{h^+(\mathbf{u})}$ quase certamente e pelo teorema da convergência dominada, $\int \mathbb{1}_{h^+(\mathbf{u}_n)} d\mu_i \to \int \mathbb{1}_{h^+(\mathbf{u})} d\mu_i$. Logo, $\mu_i(h^+(\mathbf{u}_n)) \to \mu_i(h^+(\mathbf{u}))$ $\forall i$ e f é contínua. □

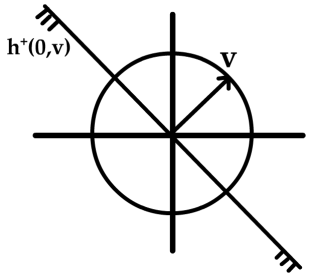


Figura 3:

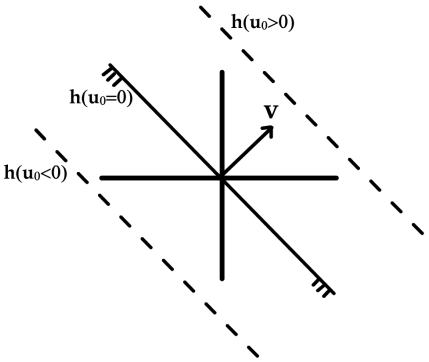


Figura 4:

Pelo teorema de Borsuk-Ulam[1] , existe $\mathbf{u} \in S^d$ tal que $f(\mathbf{u}) = f(-\mathbf{u})$. Assim, $f_i(\mathbf{u}) = f_i(-\mathbf{u})\ \forall i \Leftrightarrow \mu_i(h^+(\mathbf{u})) = \mu_i(h^+(-\mathbf{u}))\ \forall i$.

Como $h^+(-\mathbf{u})$ é o semi-espaço oposto de $h^+(\mathbf{u})$ e sua intersecção é um hiperplano, por hipótese com medida nula em μ_i, para todo i, segue que $\mu_i(h^+(\mathbf{u})) = \frac{1}{2}\mu_i(\mathbb{R}^d)$. □

Para a resolução dos problemas apresentados no início dessa seção, precisamos de uma versão discreta do Teorema 1.3. Para enunciá-la, denotaremos os semi-espaço abertos definidos por um hiperplano h por h^{++} e h^{--}. Mais especificamente, se $h = (a, b)$, com $a \in \mathbb{R}^d$ e $b \in \mathbb{R}$, definimos

h^{++}, h^{--}

$$h^{++} = \{x \in \mathbb{R}^d \,|\, \langle a, x\rangle > b\} \quad e \quad h^{--} = \{x \in \mathbb{R}^d \,|\, \langle a, x\rangle < b\}.$$

Teorema 1.5 (*Ham Sandwich* discreto)**.** *Sejam $A_1, ..., A_d \subset \mathbb{R}^d$ conjuntos finitos de pontos em $\mathbb{R}^d$ com:*

1. *$A_i \cap A_j = \emptyset$ para todo $i \neq j$;*
2. *$\bigcup_{i=1}^d A_i$ em posição geral.*

Então existe um hiperplano h em $\mathbb{R}^d$ tal que cada A_i é justamente bipartitionado *por h, isto é, cada um dos semi-espaço abertos $h^+ +$ e h^{--} contém exatamente $\lfloor \frac{|A_i|}{2} \rfloor$ pontos (observe que $|h \cap A_i| = 0$ se A_i for par e $|h \cap A_i| = 1$ se A_i for ímpar.)*

justamente bipartitionado

Demonstração. Suponha inicialmente $|A_i|$ ímpar para todo i. Para cada A_i, considere $A_i^\epsilon = \{x \in \mathbb{R}^d \mid d(x, A_i) \leq \epsilon\}$, com ϵ pequeno o suficiente para A_i^ϵ ser uma união de bolas disjuntas de raio ϵ.

Definida a medida μ_i, fazendo $\mu_i(X) = \lambda^{(d)}(X \cap A_i^\epsilon)$. Usando o teorema 1.3, obtemos um hiperplano h que divide igualmente esses conjuntos.

Fixado A_i, $\mu_i(h^+(A_i^\epsilon)) = \frac{1}{2}\mu_i(A_i^\epsilon)$. Segue que $h \cap A_i^\epsilon \neq \emptyset$ (caso contrário, teríamos $\left\lfloor \frac{|A_i|}{2} \right\rfloor + 1$ bolas de um dos lados de h) e h intersecta alguma bola de A_i^ϵ. Variando i, usando a hipótese de que os pontos estão em posição geral e fazendo $\epsilon \to 0$, obtemos que h deve intersectar exatamente d pontos, um de cada A_i e particioná-los justamente.

[1] O teorema de Borsuk-Ulam foi tema de uma apresentação do PICME no semestre passado, seção 6.3 das notas de aula disponíveis em: http://www.ime.usp.br/~tcco/picme/wp-content/uploads/2015/08/PICME_2015_1.pdf.

Se $|A_i|$ é par, fixe $a \in A_i$ e considere $A_i \setminus \{a\}$. Pode-se mostrar que uma pequena pertubação de h produz o resultado desejado. □

◇ ◇ ◇ *Aula 2(01 de Setembro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Observação 1.6. Apesar da prova do Teorema 1.5 não ser construtiva, não é difícil construir algoritimicamente um tal hiperplano h. Suponha que $|A_i|$ seja ímpar para todo i. Então existem apenas $\prod_i |A_i|$ hiperplanos candidatos a satisfazerem as condições do Teorema, a saber, aqueles que intersectam com cada A_i em exatamente um ponto. No caso em que alguns A_i têm cardinalidade par, basta adicionar pontos artificais de forma a cair no caso anterior e perturbar o hiperplano obtido de forma a biparticionar justamente as coleções originais (sem pontos extras).

Prova do Teorema 1.1. Por indução em n. Para $n = 0$ não há nada a ser provado. Para $n > 0$, aplique o Teorema 1.5 e observe que ambas as coleções de pontos contidas em h^{++} e h^{--} satisfazem as condições do teorema e, portanto, possuem partições arco-íris por hipótese de indução. Se n for par, a união dessas duas partições já é uma partição arco-íris de A. Se n for ímpar, basta também considerar a parte formada pelos pontos contidos em h. □

Prova (Alon) do Teorema 1.2. No caso em que $d = 2$, podemos associar as pedras a pontos em um círculo e aplicar o Teorema 1.5 para obter a bipartição desejada.

curva dos momentos

No caso geral, usaremos a *curva dos momentos* de dimensão d, dada pela equação paramétrica

$$\gamma(t) = (t, t^2, \ldots, t^d) \in \mathbb{R}^d, \quad t \geq 0.$$

As seguintes propriedades da curva γ serão suficientes para provarmos o teorema.

1. *Se $t_0, \ldots, t_d \geq 0$ são todos distintos, então $\gamma(t_0), \ldots, \gamma(t_d)$ não estão em um mesmo hiperplano.*

   Demonstração. Suponha o contrário e seja $a = (a_1, \ldots, a_d) \neq 0 \in \mathbb{R}^d$ e $b \in \mathbb{R}$ tais que

   $$\langle a, \gamma(t_i) \rangle = b, \qquad (i = 0, \ldots, d)$$

   ou seja,

   $$\begin{array}{ccccccc} a_1 t_0 & + & \ldots & + & a_d t_0^d & = & b \\ a_1 t_1 & + & \ldots & + & a_d t_1^d & = & b \\ \vdots & & & & \vdots & = & \vdots \\ a_1 t_d & + & \ldots & + & a_d t_d^d & = & b \end{array}$$

   Defina o polinômio $P(x) = -b + a_1 x + \cdots + a_d x^d$. Vemos que $P(x)$ tem $d + 1$ raízes distintas, da onde segue que $P(x) = 0$, o que contradiz a hipótese de que $a \neq 0$. □

2. *Todo hiperplano em $\mathbb{R}^d$ encontra a curva γ em no máximo d pontos.*

   Demonstração. Segue da propriedade anterior. □

Assim, se um colar tem n pedras, basta associá-las (na ordem em que aparecem no colar) a pontos $\gamma(1), \ldots, \gamma(n)$ e aplicar o Teorema 1.5. □

A seguir, vamos mostrar uma variante do Teorema 1.5 em que descartamos a hipótese dos pontos estarem em posição geral. Nesse caso, o exemplo da figura 5 mostra que infelizmente não podemos garantir a existência de um hiperplano que biparticione *justamente* cada A_i.

Figura 5: Não existe hiperplano que biparticiona justamente as duas coleções de pontos acima

biparticiona fracamente

Seja $A \subset \mathbb{R}^d$ um conjunto finito de pontos. Dizemos que um hiperplano h *biparticiona fracamente* A se $|h^{++} \cap A|, |h^{--} \cap A| \leq |A|/2$.

Teorema 1.7. *Sejam $A_1, \ldots, A_d \subset \mathbb{R}^d$, com cada A_i finito. Então existe um hiperplano h que biparticiona fracamente cada um dos A_i.*

Demonstração. Considere $A_i^{(\eta)}$ uma η-perturbação de A_i. Podemos supor que $\cup_i A_i^{(\eta)}$ está em posição geral. Aplique o Teorema 1.5 para obter um hiperplano $h^{(\eta)}$ dado por $(a^{(\eta)}, b^{(\eta)})$. Faça $\eta \to 0$. Como $\|a^{(\eta)}\| = 1$ e $|b^{(\eta)}|$ é limitado, podemos supor que $a^{(\eta)} \to a$ e $b^{(\eta)} \to b$. O hiperplano $h = (a, b)$ satisfaz as condições desejadas. □

1.3 Conjectura de Kneser

O seguinte resultado foi conjecturado por Kneser ('55) e demonstrado por Lovász ('78). A demonstração de Lovász faz uso do Teorema de Borsuk-Ulam e será apresentada na seção 3.

Teorema 1.8 (Conjectura de Kneser/Teorema de Lovász)**.** *Seja $n > 2k-1$ e suponha que existam conjuntos $\mathcal{C}_1, \ldots, \mathcal{C}_{n-2k+1} \in 2^{\binom{[n]}{k}}$ tais que*

$$\binom{[n]}{k} = \mathcal{C}_1 \dot\cup \ldots \dot\cup \mathcal{C}_{n-2k+1}.$$

Então existe i e conjuntos $A, B \in \mathcal{C}_i$ tais que $A \cap B = \emptyset$.

Observação 1.9. O resultado acima é falsa para o caso em que $\binom{[n]}{k}$ é particionado em $n-2k+2$ partes. Uma 3-coloração do grafo de Petersen é um contraexemplo para o caso em que $n = 5$ e $k = 2$.

2 Centro de Massa e Aplicações em Geometria

◇ ◇ ◇ *Aula 3(15 de Setembro) — Rodrigo Eidji Uemura Iwanaga* ◇ ◇ ◇

2.1 Sistemas de Massas

Consideraremos sistemas de pontos no plano nos quais valores de *massa* são associados a cada ponto.

Notação 2.1. Um ponto $(x, y) \in \mathbb{R}^2$ no plano associado a uma massa $m \in \mathbb{R}$ será denotado por $(x, y)[m]$.

O *centro de massa* de um sistema de pontos $\{(x_i, y_i)[m_i]\}_{i=1}^n$ é o ponto $(x_c, y_c)[m]$, onde

$$m = \sum_{i=1}^{n} m_i, \qquad x_c = \frac{\sum_{i=1}^n x_i}{m}, \qquad y_c = \frac{\sum_{i=1}^n y_i}{m}.$$

Proposição 2.2. *O centro de massa $G[m+n]$ de dois pontos $A[m]$ e $B[n]$ é tal que A, B e G são colineares e, além disso,*

$$\overline{AG} \cdot m = \overline{GB} \cdot n.$$

□

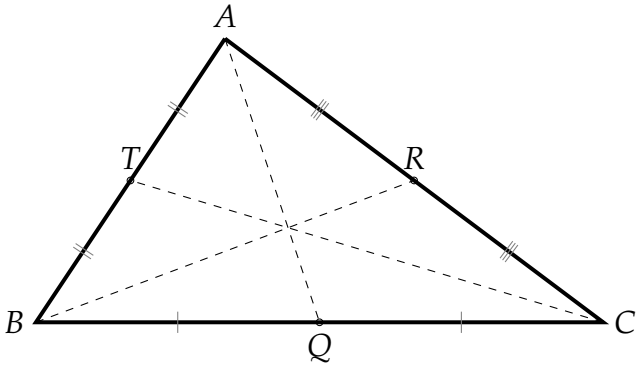
Proposição 2.3. *Sejam $(x_c, y_c)[m]$ o centro de massa de um sistema $S = \{(x_i, y_i)[m_i]\}_{i=1}^n$ e $(x'_c, y'_c)[m']$ o centro de massa de um sistema $S' = \{(x'_i, y'_i)[m'_i]\}$. Então o centro de massa de $S \cup S'$ é o centro de massa de $\{(x_c, y_c)[m], (x'_c, y'_c)[m']\}$.* □

A seguir consideraremos triângulos ABC quaisquer e denotaremos por a, b, c os comprimentos dos lados opostos aos vértices A, B, C respectivamente.

Uma *seviana* é qualquer segmento de reta que une um vértice a um ponto do lado oposto. Em particular, a *mediana* é uma seviana que une que um vértice ao ponto médio do lado oposto. O *baricentro* de um triânglo é o ponto de encontro de suas três medianas.

Lema 2.4. *O baricentro de um triângulo ABC é dado pelo centro de massa de $A[p]$, $B[p]$ e $C[p]$, onde p é um valor arbitrário de massa.*

Demonstração. Seja $G[3p]$ o centro de massa de $A[p], B[p]$ e $C[p]$ e seja Q, R e T os pontos que definem as três medianas, como abaixo.

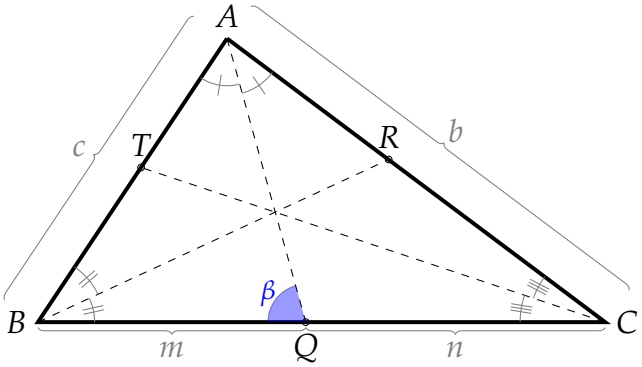


Pela Proposição 2.2, o ponto $Q[2p]$ é o centro de massa de $B[p]$ e $C[p]$. Pela Proposição 2.3, $G[3p]$ é, também, o centro de massa de $A[p]$ e $Q[2p]$, da onde segue que G está sobre a mediana AQ. De maneira simétrica, é possível concluir que M também está sobre as demais medianas e, portanto, que G é o baricentro de ABC. □

O *incentro* de um triângulo é o ponto de encontro das sevianas que bissectam cada ângulo.

Lema 2.5. *O incentro de um triângulo ABC é dado pelo centro de massa dos pontos $A[a]$, $B[b]$ e $C[c]$.*

Demonstração. Seja $I[a+b+c]$ o centro de massa de $A[a]$, $B[b]$ e $C[c]$ e sejam Q, R e S pontos que definem cada uma das bissetrizes de ABC (ver figura abaixo).

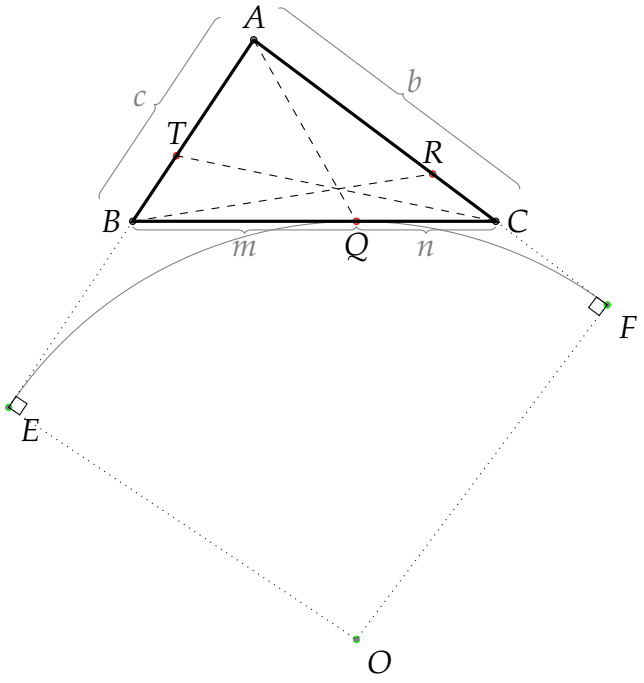


Se aplicarmos a *Lei dos Senos* aos triângulos ABQ e AQC, obtemos, respectivamente, que

$$\frac{m}{\sin\alpha} = \frac{c}{\sin\beta} \qquad \text{e} \qquad \frac{n}{\sin\alpha} = \frac{b}{\sin(\pi-\beta)} = \frac{b}{\sin\beta}.$$

Daí concluímos que $mb = nc$. Pela Proposição 2.2, o ponto $Q[b+c]$ é o centro de massa de $B[b]$ e $C[c]$. Logo I é também o centro de massa $A[a]$ e $Q[b+c]$ e, portanto, está contido na bissetriz AQ. Por simetria, concluímos que I também está sobre as demais bissetrizes e, é, portanto, o incentro de ABC. □

(Definição ponto Nagel)



Lema 2.6. *O ponto de Nagel do triângulo ABC acima é dado pelo centro de massa dos pontos $A[p-a]$, $B[p-b]$ e $C[p-c]$, onde p é o semiperímetro de ABC.*

Demonstração. Seja N o centro de massa definido como acima e $\overline{AQ}$, $\overline{BR}$ e $\overline{CT}$ as sevianas que definem o ponto de Nagel.

Como $\overline{BE} = \overline{BD} = m$ e $\overline{CD} = \overline{CF} = n$, devemos ter

$$c + m = \overline{AE} = \overline{AF} = b + n.$$

Substituindo $m = a - n$, obtemos

$$c - a - n = b + n,$$

isto é,

$$n = \frac{a - b + c}{2} = p - b.$$

De forma simular, temos $m = p - c$. Logo, $Q[a]$ é o centro de massa de $B[p-b]$ e $C[p-c]$. Então N também pode ser escrito como o centro de massa de $Q[a]$ e $A[p-a]$, da onde segue que N está contido em $\overline{AQ}$. De forma análoga, é possível mostrar que N também está contido em $\overline{CT}$ e $\overline{BR}$. □

Teorema 2.7. *Sejam G, I, N o baricentro, o incentro e o ponto de Nagel (respectivamente) de um triângulo ABC. Então G, I, N são colineares e*

$$\frac{\overline{NG}}{\overline{GI}} = \frac{2}{1}.$$

Demonstração. Pelo Lema 2.5, sabemos que $I[2p]$ é o centro de massa do sistema $\{A[a], B[b], C[c]\}$ e pelo Lema 2.6 que $N[p]$ é o centro de massa do sistema $\{A[p-a], B[p-b], C[p-c]\}$. Logo, o centro de massa de $I[2p]$ e $N[p]$ é o centro de massa do sistema

$$\{A[a+p-a], B[b+p-b], C[c+p-c]\} = \{A[p], B[p], C[p]\},$$

que é o ponto $G[3p]$, pelo Lema 2.4. Concluímos então que G, I, N são colineares e que

$$\overline{GN} \cdot p = \overline{IG} \cdot 2p,$$

o que implica a relação desejada. □

Teorema 2.8 (Ceva)**.**

3 Conjectura de Kneser

◇ ◇ ◇ *Aula 4(22 de Setembro) — Gabriel Lisboa* ◇ ◇ ◇

3.1 Demonstração de Lovász para Conjectura de Kneser

Veremos uma demonstração do Teorema 1.8 que faz uso do seguinte resultado de topologia que será demonstrado posteriormente.

Teorema 3.1. *Se a esfera $S^d \in \mathbb{R}^d$ é coberta por conjuntos $C_1, \dots, C_{d+1}$ abertos ou fechados, isto é, se*

$$S^d = C_1 \cup \cdots \cup C_{d+1},$$

então existe índice i e $x \in S^d$ tais que $x, -x \in C_i$.

Uma *k-coloração* própria de um grafo G é uma função $c : V(G) \to \{1, 2, \dots, k\}$ tal que $c(u) \neq c(v)$ sempre que $\{u, v\} \in E(G)$. O *número cromático* $\chi(G)$ de G é o menor inteiro k para o qual existe uma tal k-coloração.

Sejam k, n inteiros, $0 < k < n$. Denotamos por $\binom{[n]}{k}$ o conjunto de todos os subconjuntos de $[n] := \{1, \dots, n\}$ que possuem exatamente k elementos.

O *grafo de Kneser* $KG_{n,k}$ é o grafo $G = (V, E)$. Com

$$V = \binom{[n]}{k} \qquad E = \{\{F_1, F_2\} : F_1, F_2 \in V \text{ e } F_1 \cap F_2 = \emptyset\}$$

O Teorema 1.8 pode ser reescrito da seguinte forma.

Teorema 3.2 (Conjectura Kneser/Teorema de Lovász)**.** *Para todo $k > 0$ e $n \geq 2k - 1$, o número cromático $\chi(KG_{n,k})$ do grafo de Kneser é $n - 2k + 2$.*

Para mostrar que $\chi(KG_{n,k}) \leq n - 2k + 2$, isto é, que é possível colorir $KG_{n,k}$ com apenas $n - 2k + 2$ cores, basta usar a seguinte coloração[2] que contém i e que ainda não foram coloridos com cores

$$c(v) = \min\{\min v, n - 2k + 2\}.$$

De fato, se

$$\chi(v_1) = \chi(v_2) = i < n - 2k + 2,$$

então $\emptyset \neq V_1 \cap V_2 \ni i$, o que implica $\{v_1, v_2\} \notin E(KG_{n,k})$. Se

$$\chi(v_1) = \chi(v_2) = n - 2k + 2,$$

então $v_1, v_2 \in \{n - 2k + 2, \dots, n\}$, que possui $2k - 1$ elementos. Como $|v_1| + |v_2| = 2k$, pelo Princípio da Casa dos Pombos, v_1 e v_2 devem conter pelo menos um elemento em comum e, portanto, $\{v_1, v_2\} \notin E(KG_{n,k})$.

Demonstração do Teorema 1.8 (Lovász '78). Considere $KG_{n,k}$ e seja $d := n - 2k + 1$. Seja $X \subset S^d$ um conjunto com n pontos tais que nenhum hiperplano passando pela origem contenha mais do que d pontos de X.

Exercício 3.3. Mostre que, com probabilidade 1, um conjunto de n pontos escolhidos uniformemente ao acaso em S^d é uma escolha válida para X.

Vamos assumir que existe uma coloração c de $KG_{n,k}$ com apenas $d = n - 2k + 1$ cores. Defina conjuntos A_i, $1 \leq i \leq d$, da seguinte maneira.

$$A_i = \{x \in S^d : \text{existe } y \in V(KG_{n,k}) \text{ satisfazendo } y \subset H(x) \text{ e } c(y) = i\}.$$

[2] equivale associar à cor i todos os vértices que contêm i e que ainda não foram coloridos com cores menores que i.

Exercício 3.4. Mostre que A_i é aberto.

Defina, ainda, o conjunto fechado $A_{d+1} = S^d \setminus \bigcup_{i=1}^{d} A_i$. Pelo Teorema 3.1 aplicado a $A_1, \ldots, A_{d+1}$, existe $i \in [d+1]$ tal que $x, -x \in A_i$. Dividimos o restante da demonstração em dois casos:

Caso 1: $i \leq d$ Neste caso existem duas k-uplas y, y', associadas à *mesma cor* i e contidas, respectivamente, em $H(x)$ e $H(-x)$. Então $y \cap y' \neq \emptyset$ e, portanto, $\{y, y'\} \in E(KG_{n,k})$, o que contradiz a hipótese de c ser uma coloração válida.

Caso 2: $i = d+1$ Neste caso, $H(x)$ não pode conter um conjunto $y \in V(KG_{n,k})$ de k pontos de X, caso contrário teríamos $x \in A_{c(i)}$. Pelo mesmo motivo, $H(-x) \cap X < k$. Concluímos então que $|S(x)| \geq n - 2k + 2 = d + 1$, o que contradiz a hipótese inicial sobre X.

Logo, toda coloração de $KG_{n,k}$ deve usar pelo menos $n - 2k + 2$ cores. □

◇ ◇ ◇ *Aula 5(29 de Setembro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

3.2 Prova de Bárány ('78) para Conjectura de Kneser

A demonstração do Teorema 1.8 (Conjectura de Kneser) da aula passada depende do Teorema 3.1 sobre topologia. Veremos nesta aula uma outra demonstração para o Teorema 1.8 que depende apenas do seguinte resultado de topologia, que é equivalente ao Teorema de Bursuk-Ulam.

Teorema 3.5 (Lyusternik-Schnirelmann)**.** *Se a esfera $S^d \in \mathbb{R}^d$ é coberta por conjuntos $C_1, \ldots, C_{d+1}$* abertos*, isto é, se*

$$S^d = C_1 \cup \cdots \cup C_{d+1},$$

então existe i e $x \in S^d$ tais que $x, -x \in C_i$.

Consideraremos hiperplanos em $\mathbb{R}^d$ que passam pela origem. Mais especificamente, um hiperplano $h \in \mathbb{R}^d$ e os semiespaços abertos correspondetes h^+ e h^- são determinados por um um vetor $a \in \mathbb{R}^d$ da seguinte maneira:

$$\begin{aligned} h &= \{x \in \mathbb{R}^d : \langle a, x\rangle = 0\}, \\ h^+ &= \{x \in \mathbb{R}^d : \langle a, x\rangle > 0\}, \\ h^- &= \{x \in \mathbb{R}^d : \langle a, x\rangle < 0\}. \end{aligned}$$

Lema 3.6 (Lema de Jade ('56))**.** *Para quaisquer inteiros $d \geq 0$ e $k \geq 1$, existe $X \subset S^d \subset \mathbb{R}^{d+1}$, com $|X| = 2k + d$, tal que para todo hiperplano h (passando pela origem) os semiespaços abertos h^+ e h^- são tais que:*

$$|h^+ \cap X| \geq k \qquad e \qquad |h^- \cap X| \geq k.$$

Demonstração. Vamos construir $V = \{v_1, \ldots, v_{2k+d}\} \subset \mathbb{R}^{d+1}$ tal que para todo hiper-

plano h, $|h^+ \cap V|, |h^- \cap V| \geq k$. Assim, podemos tomar X como abaixo.

$$X = \left\{ \frac{v_1}{\|v_1\|}, \ldots, \frac{v_{2k+d}}{\|v_{k+d}\|} \right\}$$

Consideramos a curva dos momentos

$$\overline{\gamma}(t) = (1, t, t^2, \ldots, t^d) \in \mathbb{R}^{d+1} \quad (t \in \mathbb{R}).$$

Seja $W = \{w_1, \ldots, w_{2k+d}\}$ um conjunto de pontos sobre $\overline{\gamma}$ "em ordem". Por exemplo, podemos tomar $w_i = \overline{\gamma}(i)$ $(1 \leq i \leq 2k+d)$.

Pomos $v_i = (-1)^i w_i$. Mostraremos a seguir que $|h^+ \cap V|, |h^- \cap V| \geq k$, ou, equivalentemente, que:

1. $|\{w_i \in h^+ : i \text{ é par}\}| + |\{w_i \in h^- : i \text{ é ímpar}\}| \geq k$ e
2. $|\{w_i \in h^- : i \text{ é par}\}| + |\{w_i \in h^+ : i \text{ é ímpar}\}| \geq k$.

Seja $W_{on} = W \cap h$ o conjunto dos $w_i \in W$ que pertencem ao hiperplano h. Note que $W_{on} \leq d$. De fato, suponha que h seja dado pelos pontos ortogonais a $a = (a_1, \ldots, a_{d+1}) \in \mathbb{R}^d$. Então todo $t \in \mathbb{R}$ tal que $\overline{\gamma}(t) \in h$ satisfaz a equação

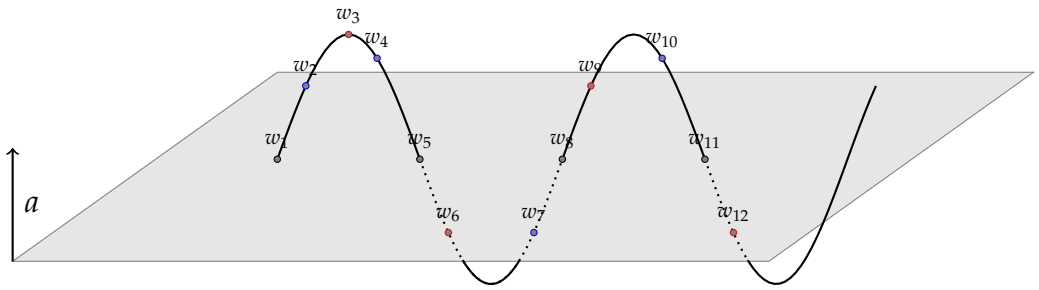
$$a_1 + a_2 t + a_3 t^2 + \cdots + a_{d+1} t^d = \langle a, \overline{\gamma}(t) \rangle = 0,$$

que admite no máximo d raízes reais.

Podemos supor, sem perda de generalidade, que $W_{on} = d$, movendo o hiperplano h até que exatamente d pontos de W pertençam a h, e de forma a não mudar nenhum ponto de lado.

Considere o conjunto $W_{off} = W \setminus W_{on}$. Colorimos cada ponto w_i em W_{off} de

- azul, se i for par e pertencer a h^+, ou se i for ímpar e pertencer a h^-.
- vermelho, se i for par e pertencer a h^-, ou se i for ímpar e pertencer a h^+.



Note que ao longo de $\overline{\gamma}$ os pontos em W_{off} estão coloridos alternadamente de azul e vermelho. Como $|W_{off}| = 2k$, concluímos que exatamente k pontos em W_{off} serão coloridos de azul e exatamente k, de vermelho. □

Observação 3.7. Não poderíamos trocar a hipótese de que $|X| = 2k + d$ por $|X| = 2k + d - 1$ no enunciado do Lema 3.6. Nesse caso, ao tomarmos um hiperplano h passando por quaisquer d pontos de X, restariam apenas $2k - 1$ pontos nos espaços abertos h^+ e h^- (e portanto algum deles teria $k - 1$ pontos).

Demonstração de Bárány para a Conjectura de 1.8. Seja $d = n - 2k$ e $X \subset S^d \subset \mathbb{R}^{d+1}$ um conjunto de n pontos em S^d como no Lema de Gale. Identificamos $[n]$ com X.

Suponha por contradição que

$$N = \binom{[n]}{k} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_{n-2k+1}$$

é tal que não existe $A, B \in \mathcal{C}_i$ com $A \cap B \neq \emptyset$, isto é, que todos os $\mathcal{C}_i$ sejam intersectantes.

Para todo $i \in \{0, \ldots, n-2k+1\}$, pomos

$$A_i = \left\{ x \in S^d : H(x) \text{ contém um } S \in \binom{X}{k} \text{ com } S \in \mathcal{C}_i \right\},$$

onde $H(x) = \{y \in \mathbb{R}^d : \langle x, y \rangle > 0\}$. Esses A_i são abertos (*exercício*). Ademais, segue da escolha de X e do Lema de Gale que tais A_i cobrem S^d.

Logo, pelo Teorema 3.5, existe i tal que $x, -x \in A_i$. Isso implica a existência de conjuntos $S, S' \in \binom{X}{k}$ coloridos, ambos, com a cor i mas contidos, respectivamente, em $H(x)$ e $H(-x)$ e, portanto, disjuntos. □

3.3 Teorema de Schrijver

Seja C_n o circuito de comprimento n, cujos vértices (na ordem em que aparecem no circuito) são os inteiros $1, \ldots, n$. Um conjunto de vértices $S \subset [n]$ de C_n é *estável em* C_n se não induz uma aresta.

Seja

$$\binom{[n]}{k}_{stab} = \left\{ S \in \binom{[n]}{k} : S \text{ é estável em } C_n \right\}.$$

O seguinte resultado afirma que o Conjectura de Kneser vale mesmo quando particionamos $\binom{[n]}{k}_{stab} \subset \binom{[n]}{k}$.

Teorema 3.8 (Schrijver). *Seja $n > 2k-1$ e suponha que existam conjuntos $\mathcal{C}_1, \ldots, \mathcal{C}_{n-2k+1} \in 2^{\binom{[n]}{k}}$ tais que*

$$\binom{[n]}{k}_{stab} = \mathcal{C}_1 \,\dot\cup\, \ldots \,\dot\cup\, \mathcal{C}_{n-2k+1}.$$

Então existe $i \in [n-2k+1]$ e conjuntos $A, B \in \mathcal{C}_i$ tais que $A \cap B = \emptyset$.

4 Ultrafiltros e o Teorema de Hindman

◇ ◇ ◇ *Aula 6(13 de Outubro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

4.1 Teoria de Ramsey

Seja $\mathbb{N} = \{1, 2, \ldots, \}$.

Teorema 4.1 (Teorema de Ramsey, versão infinita). *Sejam $k, r \geq 1$ e $C_1, \ldots, C_r \subseteq \binom{\mathbb{N}}{k}$*

conjuntos tais que

$$\binom{\mathbb{N}}{k} = C_1 \cup \cdots \cup C_r.$$

Então existe índice i e conjunto $A \subset \mathbb{N}$, com $|A| = \infty$ tais que

$$\binom{A}{k} \subseteq C_i.$$

Demonstração. Se $k = 1$, a afirmação é verdadeira, uma vez que se podemos identificar $\binom{\mathbb{N}}{1}$ por $\mathbb{N}$. Logo, se $C_1, \ldots, C_r$ são tais que $\mathbb{N} = C_1 \cup \cdots \cup C_r$, então algum C_i deve ter tamanho infinito.

Suponha $k, r \geq 2$ e que a afirmação é verdadeira para valores menores de k.

Seja

$$\binom{\mathbb{N}}{k} = C_1 \cup \cdots \cup C_r.$$

Construiremos uma sequência infinita $x_1 < x_2 < \ldots$ tal que para todo conjunto $K = \{x_{i_1}, \ldots, x_{i_{k-1}}\}$ $(i_1 < \cdots < i_{k-1})$, existe índice $1 \leq j_K \leq r$ tal que

$$\forall i_k > i_{k-1} \text{temos: } K \cup \{x_{i_k}\} \subset C_{j_K}.$$

Suponha que já definimos $x_1 < x_2 < \cdots < x_t$ e conjunto $Y_t \subset \mathbb{N}$ infinito, com $Y_t > x_t$, tais que: para todo $K \subset \{x_1, \ldots, x_t\}$, $|K| = k - 1$, existe j_K tal que todo $y \in Y_t$ satisfaz

$$K \cup \{y\} \in C_{j_k}.$$

Vamos definir agora x_{t+1} e Y_{t+1}. Pomos $x_{t+1} = \min Y_t$ e $Y' = Y_t \setminus \{x_{t+1}\}$. Seja $\Pi = [r]^{\binom{x_1,\ldots,x_t}{k-2}}$ o conjunto de funções que associam índices em $[r]$ a subconjuntos de $\{x_1, \ldots, x_t\}$ de tamanho $k - 2$. Considere a seguinte partição de Y':

$$Y' = \bigcup_{\pi \in \Pi} D_\pi,$$

onde

$$D_\pi = \{y \in Y' : \forall J \in \binom{x_1, \ldots, x_t}{k-2}, J \cup \{x_{t+1}, y\} \in C_{\pi(J)}\}.$$

Como Y' é infinito, deve existir $\pi \in \Pi$ tal que D_π é infinito. Tomamos $Y_{t+1} = D_\pi$.

Observe agora que $\{x_1, \ldots, x_{t+1}\}$ e Y_{t+1} satisfazem a mesma condição que antes tínhamos para $\{x_1, \ldots, x_t\}$ e Y_{t+1}, de forma que podemos aplicar esse processo indefinidamente. A sequência $x_1 < x_2 < \ldots$ construída assim é como queríamos.

Podemos agora particionar $\binom{\{x_1, x_2, \ldots\}}{k-1}$ de acordo com o índice j_K associado, isto é, temos que

$$\binom{\{x_1, x_2, \ldots\}}{k-1} = C_1' \cup \cdots \cup C_r',$$

onde, para todo $j \in [r]$,

$$C_j' = \{K \in \binom{\{x_1, x_2, \ldots\}}{k-1} : j_K = j\}.$$

Aplicando o caso $k-1$ do teorema de Ramsey para $\{x_1, x_2, \dots\}$, temos que existe um conjunto infinito $A \subseteq \{x_1, x_2, \dots\}$ e um índice j tal que todo $K \in \binom{A}{k-1}$ está contido em C'_j. Segue da definição de C'_j que todo $L \in \binom{A}{k} \in C_j$, como desejado. □

◇ ◇ ◇ *Aula 7(20 de Outubro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

4.2 Ultrafiltros

Nesta seção, X será um conjunto, geralmente infinito, como o conjunto do naturais $\mathbb{N} = \{1, 2, \dots\}$. Se A é um subconjunto de X, denotaremos $X \setminus A$ por A^c.

Uma coleção $\mathcal{F} \subseteq 2^X$ é um *filtro* sobre X se

1. $\emptyset \notin \mathcal{F}, X \in \mathcal{F}$;
2. $\mathcal{F}$ é fechado por superconjuntos, isto é, se $A \subseteq B$ e $A \in \mathcal{F}$, então $B \in \mathcal{F}$;
3. $\mathcal{F}$ é fechado por intersecções, isto é, se $A, B \in \mathcal{F}$, então $A \cap B \in \mathcal{F}$.

Dizemos que um filtro $\mathcal{F}$ é um *ultrafiltro* se a seguinte condição extra for satisfeita:

4 Para todo $A \subseteq X$, A ou A^c pertence a $\mathcal{F}$.

Observação 4.2. Ultrafiltros $\mathcal{U}$ podem ser pensados como uma classificação dos subconjuntos de X emm duas categorias: conjuntos *grandes* (membros de $\mathcal{U}$) e conjuntos *pequenos* (fora de $\mathcal{U}$).

Ultrafiltros podem também ser definidos como uma medida aditivia tomando apenas os valores 0 ou 1. Isto é, se $\mathcal{U}$ é um ultrafiltro, então podemos definir a medida

$$m_{\mathcal{U}} : 2^X \to \{0,1\}$$
$$A \mapsto \begin{cases} 0, \text{ se } A \in \mathcal{U}; \\ 1, \text{ se } A \notin \mathcal{U}. \end{cases}$$

A medida $m_{\mathcal{U}}$ é aditiva, isto é, se $A, B \subset X$ e $A \cap B = \emptyset$, então

$$m_{\mathcal{U}}(A \cup B) = m_{\mathcal{U}}(A) + m_{\mathcal{U}}(B).$$

Para verificar essa igualdade, notamos que a condição 4.2 da definição de ultrafiltros pode ser trocada pela seguinte:

4′ Se $C \in \mathcal{F}$ e $C = A \cup B$, então $A \in \mathcal{F}$ ou $B \in \mathcal{F}$.

De fato, se $A \notin \mathcal{F}$ e $B \notin \mathcal{F}$, então a condição 4.2 implica que $A^c \in \mathcal{F}$ e $B^c \in \mathcal{F}$, da onde segue que $C^c = A^c \cap B^c \in \mathcal{F}$, e, novamente pela condição 4.2, que $C \notin \mathcal{F}$.

As seguintes famílias são exemplos de filtros.

- $\mathcal{F} = \{X\}$ (filtro trivial).
- $\emptyset \neq Y \subset X$, $\mathcal{F}_Y = \{A \subseteq X : Y \subseteq A\}$.
- $\mathcal{F}_{cofin} = \{A \subseteq X : A^c \text{ é finito}\}$ (filtro de Frechet).

Dado $x \in X$, a família

$$\mathcal{F}_x = \mathcal{F}_{\{x\}} = \{A \subseteq X : x \in A\}$$

é um exemplo de ultrafiltro. Ultrafiltros dessa forma, são chamados de *ultrafiltros principais*.

Dizemos que um filtro $\mathcal{F}$ é *maximal* se

$$\mathcal{F} \subseteq \mathcal{F}' \text{ e } \mathcal{F}' \text{ é filtro } \Rightarrow \mathcal{F} = \mathcal{F}'.$$

Fato 4.3. Seja $\mathcal{F} \subseteq 2^X$ um filtro. Então $\mathcal{F}$ é um ultrafiltro se, e somente se, $\mathcal{F}$ é um filtro maximal.

Demonstração. Se $\mathcal{F}$ é ultrafiltro e $A \notin \mathcal{F}$, então $A^c \in \mathcal{F}$ e, portanto, $\mathcal{F} \cup A$ não pode ser ul ultrafiltro.

Para provar a recíproca, suponha que $\mathcal{F}$ tal que $A, A^c \notin \mathcal{F}$ para algum $A \subseteq \mathcal{F}$. Então condidere o filtro $\mathcal{F}'$ gerado por $\mathcal{F} \cup \{A\}$, isto é, formado por conjuntos em $\mathcal{F}$ e por A e fechado por interseção finita e por superconjuntos. □

Observação 4.4. Se $|X| < \infty$, então os ultrafiltros sobre X são todos da forma $\mathcal{F}_x$.

Observação 4.5. Suponha X infinito e $\mathcal{U}$ um ultrafiltro sobre X *não-principal*, isto é, $\mathcal{U} \neq \mathcal{F}_x$, para todo $x \in X$. Então $U \supseteq \mathcal{F}_{cofin}$.

Teorema 4.6. *Seja X um conjunto, com $|X| = \infty$. Então existem ultrafiltros não principais sobre X*

Demonstração. Seja $\mathbb{F} = \{\text{filtros } \mathcal{F} \subseteq 2^X : \mathcal{F} \supseteq \mathcal{F}_{cofin}\}$. Note que $\mathbb{F}$ é parcialmente ordenado por inclusão. Usamos o Lema de Zorn para provar que $\mathbb{F}$ contém um elemento maximal $\mathcal{F}^*$. Tal $\mathcal{F}^*$ é um ultrafiltro (Fato 4.3).

Fixe uma cadeia arbitrária $(\mathcal{F}_\lambda)_{\lambda \in \Lambda}$ em $\mathbb{F}$, isto é, um conjunto totalmente ordenado (por inclusão). Para que possamos aplicar o Lema de Zorn, precisamos mostrar que existe um $F_0 \in \mathbb{F}$ tal que para todo λ, $\mathcal{F}_\lambda \subseteq F_0$. Basta tomar $\mathcal{F}_0 = \bigcup_{\lambda \in \Lambda} \mathcal{F}_\lambda$ e notar que $\mathcal{F}_0$ é um filtro e contém $\mathcal{F}_{cofin}$.

Logo, pelo Lema de Zorn, $\mathbb{F}$ tem um elemento maximal $\mathcal{F}^*$. Tal F^* é um ultrafiltro (Fato 4.3) não-principal (pois contém $\mathcal{F}_{cofin}$). □

4.3 Ultrafiltros e topologia

Seja $a_1, a_2, \cdots \in [0,1]$. Dizemos que $\lim a_n = L$ se para todo $\varepsilon > 0$, existe inteiro n_0 tal que para todo $n > n_0$, $a_n \in (L - \varepsilon, L + \varepsilon)$.

Seja $A_\varepsilon = \{n : n \geq n_0\}$. Então $A_\varepsilon \in \mathcal{F}_{cofin}$, onde $\mathcal{F}_{cofin}$ é o filtro dos elementos cofinitos sobre $\mathbb{N}$. Filtros podem ser usados para generalizar o conceito de limites de sequências. No que se segue, sequências em um conjunto Y serão representadas como funções $f : \mathbb{N} \to Y$ (isto é $a_n = f(n)$).

Fato 4.7. Seja Y um conjunto e $f : \mathbb{N} \to Y$. Suponha que $\mathcal{F}$ seja um filtro/ultrafiltro sobre $\mathbb{N}$. Defina

$$f*(\mathcal{F}) = \{A \subseteq Y : f^{-1}(A) \in \mathcal{F}\}.$$

Então $f^*(\mathcal{F})$ é um filtro/ultrafiltro sobre Y.

Seja $\mathcal{F}$ um filtro sobre um espaço topológico Y. Dizemos que $\mathcal{F}$ *converge* a um ponto $y \in Y$ se todo aberto $\mathcal{U}$ em Y com $y \in \mathcal{U}$ é um membro de $\mathcal{F}$.

Seja Y um espaço topológico, $f : \mathbb{N} \to Y$ e $\mathcal{F}$ um filtro sobre $\mathbb{N}$. Então $y \in Y$ é um *$\mathcal{F}$-limite* de f se $f_*(\mathcal{F})$ converge para y.

Pendente: Resto da aula

◇ ◇ ◇ *Aula 8(03 de Novembro) — Yoshiharu Kohayakawa* ◇ ◇ ◇

4.4 Teorema de Hindman

Definição 4.8 (semigrupo)**.** Um semigrupo é um par $(E, \cdot)$ em que E é um conjunto e $\cdot : E \times E \to E$ é uma operação associativa, isto é, tal que para quaisquer $a, b \in E$, temos:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Lema 4.9 (Elemento idempotente em semigrupos)**.** *Seja E um semigrupo Hausdorff-compacto tal que para todo $g \in E$, a função*

$$\begin{aligned} \Psi_g : E &\to E \\ f &\mapsto fg \end{aligned}$$

é contínua. Então existe E contém um elemento g indepotente*, isto é, tal que $g^2 = g$.*

Demonstração. Defina

$$\mathcal{A} = \{\emptyset \neq A \subseteq E : A \text{ é compacto e fechado por } \cdot\}.$$

Como $E \in \mathcal{A}$, temos $\mathcal{A} \neq \emptyset$. Seja $\mathcal{C} \subset \mathcal{A}$ uma cadeia (pela operação de inclusão). Seja $L = \bigcap \mathcal{C}$. Note que L é não vazio, compacto (pois todos os membros de $\mathcal{C}$ também o são), e fechado pelo produto. Logo $L \in \mathcal{A}$, isto é, $\mathcal{C}$ tem um limitante inferior. Podemos portanto aplicar o Lema de Zorn para concluir que existe um membro minimal $A \in \mathcal{A}$.

Fixe $g \in A$. Então $\emptyset = Ag \subseteq A$. Ademais, Ag é subsemigrupo de A, uma vez que

$$(fg)(f'g) = \underbrace{fgf'}_{\in A} g \in Ag,$$

e Ag é compacto pois $Ag = \Psi_g(A)$ e Ψ_g é contínua. Assim, a minimalidade de A implica $Ag = A$. Seja

$$B = \{f \in A : fg = g\}.$$

Então $B \neq \emptyset$, uma vez que $g \in A = Ag$. Note que B também é semigrupo pois se $f, f' \in B$, então

$$(ff')g = f(f'g) = fg = g.$$

Ademais, $B = \Psi_g(\{g\})$, também temos que B é fechado e, portanto, compacto. Pela minimalidade de A, segue que $A = B$. Mas como $g \in A$, temos $g \in B$, isto é, g é idempotente. □

Para a prova do Teorema de Hindman, consideraremos o conjunto $\beta\mathbb{N}$ de ultrafil-

tros sobre $\mathbb{N}$ e denotaremos ultrafiltros como medidas $0-1$ aditivas.

Dados $\mu, \nu \in \beta\mathbb{N}$, a operação de adição $+ : \beta\mathbb{N} \times \beta\mathbb{N} \to \beta\mathbb{N}$ de adição (cuja existência foi provada em **??**) é dada por

$$(\mu + \nu)(A) = \mu(\{n : \nu(A - n) = 1\}).$$

Note também

Teorema 4.10 (Hindman). *Seja $k \geq 1$ e suponha que existem conjuntos disjuntos $C_1, \dots, C_k \subset \mathbb{N} = \{1, 2, \dots\}$ tais que*

$$\mathbb{N} = C_1 \cup \cdots \cup C_k.$$

Então existe i e $X \subseteq C_i$, $|X| = \infty$, tal que $FS(X) \subseteq C_i$, onde

$$FS(X) = \left\{ \sum_{x \in S} x : S \subseteq X, S \text{ finito} \right\}.$$

Demonstração. Primeiro, observamos que $(\beta\mathbb{N}, +)$ é um semigrupo e que a função

$$\begin{aligned} \Psi_\eta : \beta\mathbb{N} &\to \beta\mathbb{N} \\ \mu &\to \mu + \nu \end{aligned}$$

é contínua para todo ν.

Então pelo Lema 4.9, existe $\mu \in \beta\mathbb{N}$ tal que $\mu + \mu = \mu$. Ademais, μ é não-principal, caso contrário teríamos $\mu = \hat{n}$, $\mu + \mu = 2\hat{n} \neq \mu$.

Sejam $A \subset \mathbb{N}$ tal que $\mu(A) = 1$ e $A^* = \{n : \mu(A - n) = 1\}$. Então

$$\mu(A^*) = (\mu + \mu)(A) = \mu(A) = 1.$$

Fixe $a \in A \cap A^*$ e tome $B = (A - a) \cap (A \setminus \{a\})$. Temos $\mu(B) = 1$ e $B \subseteq A$.

Logo, a partir de um conjunto A, com $\mu(A) = 1$, obtivémos $a \in A$ e $B \subset A \setminus \{a\}$, com $\mu(B) = 1$, tais que

$$a + B \subset A.$$

Suponha agora que $\mathbb{N} = C_1 \cup \cdots \cup C_k$. Então existe um único i tal que $\mu(C_i) = 1$. Seja $A_1 = C_i$ e para todo $k \geq 1$, construímos $a_k \in A_k$ e $A_{k+1} \subset A_k \setminus \{a_k\}$ como acima, isto é, tais que

$$a_k + A_{k+1} \subseteq A_k \subseteq C_i.$$

Agora basta notar que se tomarmos $X = \{a_1, a_2, \dots\}$, temos $FS(X) \subseteq C_i$. □

5 O teorema de Fermat sobre a soma de dois quadrados

◇ ◇ ◇ *Aula 9(03 de Novembro) — Bruno Pasqualotto Cavalar* ◇ ◇ ◇

Dizemos que um inteiro $n \geq 0$ é *representável* se pode ser escrito como soma de dois quadrados, isto é, se existem inteiros x, y tais que $n = x^2 + y^2$.

Teorema 5.1 (Teorema de Fermat sobre a soma de quadrados). *Um primo $p > 2$ é representável se e somente se $p \equiv 1 (mod 4)$.*

Pendente: parte inicial (do dia 03/11)

◇ ◇ ◇ *Aula 10(10 de Novembro) — Bruno Pasqualotto Cavalar* ◇ ◇ ◇

Corolário 5.2. *Um inteiro $n \geq 0$ é representável se, e somente se, todo primo da forma $4m+3$ aparece com expoente par na decomposição de n.*

Demonstração. Usaremos os seguintes fatos:

i) 1 e 2 são representáveis.

ii) Se n é representável, então z^2n é representável para qualquer inteiro n. De fato, se $n = a^2 + b^2$, então $z^2n = (za)^2 + (zb)^2$.

iii) Se x e y são representáveis, então xy é representável. De fato, suponha que $x = a^2 + b^2$ e $y = c^2 + d^2$. Então

$$\begin{aligned} xy &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 \\ &= (ad - bc)^2 + (ac + bd)^2. \end{aligned}$$

Seja n um inteiro tal que todo primo da forma $4m+3$ aparece com expoente par na decomposição de n. Então, como os demais fatores primos são representáveis pelo Teorema 5.1, segue dos fatos acima que n é representável.

Por outro lado, seja p um primo da forma $p = 4m+3$, tal que $p|n$ e $n = x^2 + y^2$. Afirmamos que $p|x$ e $p|y$. De fato, temos $x^2 + y^2 \equiv 0(mod p)$. Mas se $x \not\equiv 0(mod p)$, podemos multiplicar ambos os lados da equação anterior por x^{-2} para obter que $(x^{-1}y)^2 \equiv -1(mod p)$, que não tem soluções quando $p = 4m+3$. Então, $p \mid x$ e, analogamente, $p \mid y$, o que implica $p^2|n$. Logo, $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ também é representável. Segue, por indução, que p aparece com expoente par em $\frac{n}{p^2}$ e, portanto, também em n. □

Seja A um conjunto. Uma função $f : A \to A$ é uma *involução* se $f = f^{-1}$.

Fato 5.3. Seja A finito e $f : A \to A$ uma involução. Então

$$|A| \equiv |\{x : f(x) = x\}|(mod 2),$$

isto é, $|A|$ tem a mesma paridade que o número de pontos fixos de f.

Demonstração. Para $x, y \in A$, dizemos que $x \sim y \Leftrightarrow x = f(y)$. Particione A de acordo com as classes definidas por $\sim$[3] Como f é uma involução, cada classe é composta por um ou por dois elementos. As classes de tamanho 1 são, exatamente, os pontos fixos de f. □

Prova do Teorema 5.1. Suponha que $p \equiv 1(mod 4)$ seja um primo. Definimos os seguin-

[3]TODO:não é bem uma classe de equivalência

tes três conjuntos de triplas de inteiros:

$$S = \{(x,y,z) \in \mathbb{Z}^3 : 4xy + z^2 = p, x > 0, y > 0\},$$
$$T = \{(x,y,z) \in S : z > 0\} \text{ e}$$
$$U = \{(x,y,z) \in S : x - y + z > 0\}.$$

Conside a função

$$f : S \to S$$
$$(x,y,z) \mapsto (y,x,-z).$$

Primeiro note que f é uma involução e está bem definida pois $4xy + z^2 = 4(yx) + (-z)^2$. Ademais, f não tem pontos fixos, caso contrário teríamos $z = 0$ o que implicaria $p \equiv 0(mod 4)$. Note também que

i) Se $(x,y,z) \in T$, então $f(x,y,z) \in S \setminus T$. Analogamente, se $(x,y,z) \in S \setminus T$, então $f(x,y,z) \in T$ (lembrando que $z \neq 0$).

ii) Se $(x,y,z) \in U$, então $f(x,y,z) \in S \setminus U$, pois se $x - y + z = z - (y - x) > 0$, então $(y - x) - z < 0$. Analogamente, se $(x,y,z) \in S \setminus U$, então $f(x,y,z) \in U$ (note que $x - y + z \neq 0$, caso contrário teríamos $p = (y - x)^2 + 4xy = (y + x)^2$).

Concluímos, então, que $f(U \setminus T) = f(T \setminus U)$. Segue que $|U \setminus T| = |T \setminus U|$, e portanto, que $|U| = |T|$.

Considere agora a função

$$g : U \to U$$
$$(x,y,z) \mapsto (x - y + z, y, 2y - z)$$

Observe que g está bem definida pois $4(x - y + z)y + (2y - z)^2 = 4xy + z^2$ e $(x - y + z) - y + (2y - z) = x > 0$.

Além disso, (x,y,z) é um ponto fixo de g se, e somente se, $y = z$. Mas neste caso, devemos ter $y(4x + y) = 4xy + y^2 = p$, o que implica que $y = 1$ e $4x + 1 = p$. Logo $(\frac{p-1}{4}, 1, 1)$ é o *único* ponto fixo de g. Concluímos que $|U|$ é ímpar (e, portanto, $|T|$ é ímpar).

Finalmente, considere a função

$$h : T \to T$$
$$(x,y,z) \mapsto (y,x,z)$$

Note que h está bem definido e é uma involução. Mas como $|T|$ é ímpar, h tem pelo menos um ponto fixo. Existem portanto $x, z \in \mathbb{Z}$ tais que $4x^2 + z^2 = p$, da onde segue que p é representável. □

6 Provas da infinidade de primos

pendente

7 Teorema de Hoffman e Singleton

A *cintura* $g(G)$ de um grafo G é o tamanho do menor ciclo do grafo. Também definimos o *grau mínimo* $\delta(G)$ de G como o menor grau de um vértice em G.

Dados inteiros r e g, estamos interessados em determinar o menor número de vértices que um grafo G de grau mínimo r e cintura g pode ter. Denotaremos esse número por $n(r,g)$. Mais formalmente, podemos definir

$$n(r,g) = \min\{|V(G)| : \delta(G) = r \text{ e } g(G) = g\}.$$

É fácil verificar, por exemplo, que

- $n(2,5) = 5$ (o ciclo de tamanho 5 atinge o mínimo),
- $n(3,3) = 4$ (o grafo completo K^4 atinge o mínimo) e
- $n(3,4) = 6$ (o grafo bipartido $K_{3,3}$ atinge o mínimo).

Proposição 7.1. *Se $g = 2k+1$, então*

$$n(r,g) \geq 1 + r + r(r-1) + \cdots + r(r-1)^{k-1}.$$

Demonstração. Seja G um grafo tal que $\delta(G) = r$ e $g(G) = g$. Considere uma árvore de busca em largura a partir de um vértice arbitrário v de G. Como $\delta(G) = r$, o primeiro nível tem pelo menos r vértices e, para $i \geq 1$, o i-ésimo nível tem pelo menos $r(r-1)^{i-1}$ vértices. Ademais, os vértices que aparecem até o nível k são todos distintos, caso contrário haveria dois caminhos distintos de tamanho no máximo k de um mesmo vértice u até v, ou seja, um ciclo de tamanho menor que $2k+1$. □

Proposição 7.2. *Se $g = 2k$, então*

$$n(r,g) \geq 1 + r + r(r-1) + \cdots + r(r-1)^{k-2} + (r-1)^{k-1}.$$

Demonstração. Seja G um grafo tal que $\delta(G) = r$ e $g(G) = g$. Procedemos como no caso anterior, considerando uma árvore em busca em largura a partir de um vértice arbitrário v. Temos que levar em consideração que um vértice u no nível k pode aparecer múltiplas vezes. Note, contudo, que u não pode ser adjacente a mais do que r vértices do nível $k-1$ (caso contrário haveria caminhos distintos de tamanho $k-1$ de u a um vizinho de v). Portanto há pelo menos $(r-1)^{k-1}$ vértices distintos no k-ésimo nível. □

Exercício 7.3. Provar a proposição anterior, considerando uma árvore de busca em largura a partir de um vértice artificial $v \notin V(G)$ adjacente a dois vértices $v_1, v_2 \in V(G)$ com $v_1v_2 \in E(G)$ (note que a cota inferior da proposição é igual a $2\sum_{i=0}^{k-1}(r-1)^i$).

Nesta seção, estamos interessados em demonstrar o seguinte resultado.

Teorema 7.4. *Seja $r \geq 3$ e suponha que exista um grafo G de tamanho $n = 1 + r + r(r-1) = r^2 + 1$, cintura $g(G) = 5$ e grau mínimo $\delta(G) = r$. Então $r = 3, 5$ ou 57.*

Dizemos que $\lambda \in \mathbb{R}$ é um *autovalor* de uma matriz $A \in \mathbb{R}^{n\times n}$ se existe $x \in \mathbb{R}^n$, $x \neq 0$, tal que $Ax = \lambda x$. Nesse caso, dizemos que x é um *autovetor* associado a λ. O *autoespaço* associado a λ é o conjunto de todos os autovetores associados a λ.

Exercício 7.5. Mostrar que o autoespaço associado a um autovalor λ é, de fato, um espaço linear.

Lema 7.6. *Toda matriz simétrica $A \in \mathbb{R}^{n\times n}$ possui n autovetores dois a dois ortogonais.*

Demonstração. Primeiro note que quaisquer $x, y \in \mathbb{R}^n$ satisfazem $\langle Ax, y\rangle = \langle x, Ay\rangle$. De fato,

$$\langle Ax, y\rangle = (Ax)^T y = x^T A^T y = x^T Ay = \langle x, Ay\rangle .$$

Sejam v_1, v_2 autovetores de A associados a autovalores distintos λ e μ, respectivamente. Então

$$\lambda \langle v_1, v_2\rangle = \langle \lambda v_1, v_2\rangle = \langle Av_1, v_2\rangle = \langle v_1, Av_2\rangle = \langle v_1, \mu v_2\rangle = \mu \langle v_1, v_2\rangle .$$

Logo, $(\lambda - \mu)\langle v_1, v_2\rangle = 0$, da onde segue que $\langle v_1, v_2\rangle = 0$.

Considere $\{u_1, \ldots, u_\ell\}$ uma base do autoespaço associado a um autovalor λ. Usando o processo de ortogonalização de Grahn-Schimidt, conseguimos uma base ortogonal $\{u_1', \ldots, u_\ell'\}$ exercicio do autoespaço associado a λ.

Talvez faltaria falar que a soma das dimensões desses autoespaços é n? □