NOTAS DE AULA DO

PICME

Programa de Iniciação Científica e Mestrado em Combinatória

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

Anotado por: Marcelo Sales

1º semestre de 2017

Conteúdo

1 Ramsey Euclideano

◇ ◇ ◇ *Aula 1 (28 de Março) — Yoshiharu Kohayakawa* ◇ ◇ ◇

O teorema de Ramsey para grafos nos diz que dado um grafo G e um inteiro r existe um inteiro n tal que toda r coloração de K_n contém uma cópia monocromática de G. Em geral podemos estender esse conceito para outras estruturas. Nas aulas que seguem faremos isso para alguns conjuntos geométricos. Dado o $\mathbb{R}^n$ e um inteiro r podemos colorir todos os pontos de $\mathbb{R}^n$ com uma dessas r cores. Para que conjuntos $K \in \mathbb{R}^n$ podemos garantir que essa coloração contém uma "cópia"de K monocromática? Vamos estudar essa questão para conjuntos K finitos. Primeiro, algumas definições.

Definição 1.1. Uma isometria entre dois conjuntos é uma função bijetora $\phi : A \to B$ tal que $d(\phi(a_1), \phi(a_2)) = d(a_1, a_2)$, para todo $a_1, a_2 \in A$ (onde $d(x, y)$ é a distância entre os pontos x e y). Quando existe uma isometria entre dois conjuntos A e B, dizemos que eles são congruentes e denotamos por $A \cong B$.

Assim definimos com mais precisão o conceito de "cópia". Em geral, como estamos trabalhando no espaço euclideano, as relaçoes de distância serão dadas pela métrica induzida por $\|.\|_2$. No caso de Ramsey para grafos precisamos que o grafo em que ocorra a coloração seja muito grande para garantir a existência de um grafo G fixo. Poderíamos pensar que colorir o espaço em que o conjunto K está contido fosse suficiente, porém um exemplo simples como o conjunto $K = \{0, 1\} \subset \mathbb{R}$ mostra que não é bem assim.

Para o caso em que $r = 2$ nós podemos colorir $\mathbb{R}$ com duas cores sem uma cópia monocromática de K. Isso é dado pela seguinte coloração $\phi : \mathbb{R} \to \{0, 1\}$:

$$\phi(x) = \begin{cases} 0, & \text{se } x \pmod{2\mathbb{Z}} \in [0, 1) \\ 1, & \text{se } x \pmod{2\mathbb{Z}} \in [1, 2) \end{cases}$$

Porém se considerarmos uma 2-coloração de $\mathbb{R}^2$ nós obtemos uma cópia de K monocromática. Basta considerar um triângulo equilátero de lado 1, qualquer coloração dos vértices desse triângulo terá dois vértices da mesma cor e portanto uma cópia monocromática de K. Podemos da mesma forma

obtermos uma cópia monocromática de K para uma r-coloraçao com $r > 2$ considerando um simplexo r-dimensional em que todos os vértices distam 1. Esse complexo terá $r+1$ pontos e qualquer r-coloraçao terá dois pontos monocromáticos. Esse resultado nos faz pensar que a questão principal é: Dado um conjunto finito K e r um inteiro, existe uma dimensão em que qualquer r-coloração possui uma cópia de K? Quando a resposta é afirmativa dizemos que o conjunto é Ramsey. Em outras palavras

Definição 1.2. Dizemos que vale a propriedade $R(K,n,r)$ se para toda r-coloração de $\mathbb{R}^n$ existe um conjunto K' monocromático com $K' \cong K$.

Definição 1.3. Um conjunto $K \subset \mathbb{R}^d$ finito é **Ramsey** se para todo $r > 0$ inteiro, existe um n tal que a proprieadade $R(K,n,r)$ vale.

Nesta aula vamos provar que os vértices de triângulos acutângulos e retângulos são Ramsey. Observe que para provarmos que $\{0,1\}$ é Ramsey, nós exibimos um conjunto finito e mostramos que a coloração desse conjunto implica uma cópia monocromática de $\{0,1\}$. Em geral, para conjuntos finitos isso sempre será verdade. A demonstração desse fato é um pouco técnica e precisa de alguns resultados em topologia que não serão demonstrados.

Definição 1.4. Dado $\{X_\lambda\}_{\lambda\in\Lambda}$ uma coleção de espaços topológicos e $X = \prod_{\lambda\in\Lambda} X_\lambda$, definimos a topologia produto como a topologia gerada pela base de abertos

$$\mathcal{B} = \{\prod_{\lambda\in\Lambda} U_\lambda : U_\lambda \text{ aberto e } U_\lambda \neq X_\lambda \text{ apenas um número finito de vezes}\}$$

Convencionaremos que a topologia utilizada do espaço produto é a topologia produto. Com isso vale o seguinte teorema

Teorema 1.5 (Tychonoff)**.** *Seja $\{X_\lambda\}_{\lambda\in\Lambda}$ uma coleção de espaços compactos. Então $\prod_{\lambda\in\Lambda} X_\lambda$ é compacto.*

Também precisaremos de uma outra caracterização de espaços compactos.

Definição 1.6. Uma coleção $\mathcal{F}$ de subconjuntos de um conjunto X tem a **propriedade da intersecção finita** (PIF) se para toda subcoleção finita $\{F_1,\dots,F_n\} \subset \mathcal{F}$ vale que $\bigcap_{i=1}^n F_i \neq \varnothing$.

Teorema 1.7. *Um espaço topológico X é compacto se, e somente se, para toda coleção $\mathcal{F}$ de fechados de X com a PIF, nós temos que $\bigcap \mathcal{F} \neq \varnothing$.*

Estamos preparados para demonstrar que só precisamos considerar conjuntos finitos.

Lema 1.8. *Seja $K \subset \mathbb{R}^d$ Ramsey e n,r inteiros tais que $R(K,n,r)$ vale. Então existe um conjunto finito $T \subset \mathbb{R}^n$ tal que toda r-coloração de T contém um conjunto monocromático congruente a K.*

Demonstração. Denote o conjunto das cores por $[r]$. Vamos interpetar $[r]$ também como o espaço topologico discreto, isto é, cada ponto é um aberto e fechado. É fácil ver da finitude de $[r]$ que ele é compacto. Pelo teorema de Tychonoff segue que $X = \prod_{x\in\mathbb{R}^n}[r]$ é compacto.

Suponha que o enunciado não seja verdadeiro, ou seja, que para todo T finito existe uma r-coloração de $\mathbb{R}^n$ que não contém nenhuma cópia monocromática de K em T. Defina o subconjunto $F_T \subset X$ por

$$F_T = \{\prod_{x\in\mathbb{R}^n} \phi(x) : \text{ onde } \phi : \mathbb{R}^n \to [r] \text{ é uma coloração de } \mathbb{R}^n \text{ sem cópias monocromáticas de } K \text{ em } T\}$$

Pela observação acima temos que $F_T \neq \varnothing$. Como para garantir que ϕ não tenha cópias monocromáticas de K em T só precisamos nos preocupar com as cores que aplicamos a T e não a todo $\mathbb{R}^n$ temos que $F_T = A \times [r]^{\mathbb{R}^n \setminus T}$ onde $A \subset [r]^T$. Pela finitude de T, do fato de $[r]$ ser discreto e da topologia produto, temos que cada conjunto de $\{a\} \times [r]^{\mathbb{R}^n \setminus T}$, com $a \in [r]^T$ é um aberto e um fechado. Portanto F_T é aberto e fechado.

Agora note que a coleçao de fechados $\{F_T\}_{|T|<\infty}$ satisfaz PIF. De fato, para $T_1,\dots,T_k$, temos que $T = \bigcup_{i=1}^k T_i$ é finito e logo $\bigcap_{i=1}^k F_{T_i} = F_T \neq \varnothing$. Assim usando que X é compacto, pelo Teorema 1.7. temos que $\bigcap_{|T|<\infty} F_T \neq \varnothing$. Porém como $\bigcap_{|T|<\infty} F_T$ é exatamente o conjunto de r-colorações de $\mathbb{R}^n$ que não possui nenhuma cópia monocromática de K, obtemos uma contradição. □

Com esse lema podemos mostrar uma técnica para obter conjuntos Ramsey a partir de outros conjuntos Ramsey. Dado dois pontos $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ e $y = (y_1, \ldots, y_m) \in \mathbb{R}^m$ consideramos $x * y = (x_1, \ldots, x_n, y_1, \ldots, y_m) \in \mathbb{R}^{n+m}$ a concatenação desses dois pontos. O produto cartesiano de dois conjuntos $A \subset \mathbb{R}^n$ e $B \subset \mathbb{R}^m$ é um subconjunto $A \times B \subset \mathbb{R}^{n+m}$ dado por $A \times B = \{x * y : x \in A, y \in B\}$.

Teorema 1.9. *Se $K_1 \subset \mathbb{R}^n$ e $K_2 \subset \mathbb{R}^m$ são Ramsey, então o produto cartesiano $K_1 \times K_2 \subset \mathbb{R}^{m+n}$ é Ramsey.*

Demonstração. Fixe um inteiro r. Do fato de K_1 ser Ramsey, existe inteiro n tal que $R(K_1, n, r)$ vale. Além disso, pelo Lema 1.8. existe um conjunto $T = \{a_1, \ldots, a_t\} \subset \mathbb{R}^n$ com T finito tal que toda r-coloração de T contém uma cópia monocromática de K_1. Como K_2 também é Ramsey, existe inteiro m tal que $R(K_2, m, r^t)$ vale. Afirmamos que $R(K_1 \times K_2, n + m, r)$ vale.

Para vermos isso considere uma r-coloração $\phi : \mathbb{R}^{n+m} \to [r]$ arbitrária. Dessa coloração considere a coloração induzida $\phi_2 : \mathbb{R}^m \to [r]^t$ dada por

$$\phi_2(y) = (\phi(a_1, y), \ldots, \phi(a_t, y))$$

onde $a_1, \ldots, a_t$ são os pontos de T. Como $R(K_2, m, r^t)$ vale, existe um conjunto $K_2' \cong K_2$ monocromático em $\mathbb{R}^m$ com relação a coloração ϕ_2. Agora induza a coloração $\phi_1 : T \to [r]$ (pelo Lema 1.8. nós precisamos nos preocupar apenas com colorações em T) dada por

$$\phi_1(x) = \phi(x, y), \quad y \in K_2'.$$

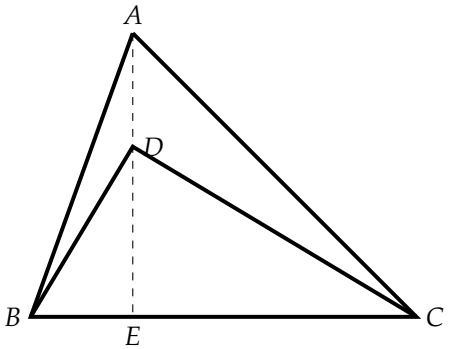
Essa coloração está bem definida, pois pela escolha de K_2', $\phi(x, y_1) = \phi(x, y_2)$ para $y_1, y_2 \in K_2'$ e $x \in T$. Assim T contém um $K_1' \cong K_1$ monocromático. Isso signfica que para quaisquer $x_1, x_2 \in K_1'$ vale que $\phi_1(x_1) = \phi_1(x_2)$, que da forma que ϕ_1 foi induzido significa que para todos $x_1, x_2 \in K_1'$ e $y_1, y_2 \in K_2'$ temos $\phi(x_1, y_1) = \phi(x_2, y_2)$. Obtemos assim uma cópia monocromática de $K_1 \times K_2$. □

Uma implicação imediata do Teorema 1.9. é que os vértices de paralelepípedos são Ramsey. Isso vem do fato já viso anteriormente que vértices de segmentos são Ramsey, independente do seu tamanho. Na verdade, é fácil ver que se um conjunto K é Ramsey, qualquer conjunto semelhante a K também é Ramsey. De fato, pelo Lema 1.8 existe um cojunto T finito tal que qualquer coloração possui uma cópia de K monocromática, então qualquer coloração de um cojunto semelhante a T (dada a proporçao desejada) terá uma cópia monocromática de um semelhante a K de mesma proporção. O Teorema 1.9 diz que o produto cartesiano de segmentos é Ramsey. Essa implicação é suficiente para provar

Corolário 1.10. *Todo triângulo acutângulo ou retângulo é Ramsey.*

Demonstração. Vamos mostrar primeiro que todo triângulo retângulo é Ramsey. Pela observação acima todo retângulo é Ramsey, dado um triângulo retâgulo XYZ com catetos XY e YZ. O retângulo de lados de comprimento XY e YZ é Ramsey e logo como todo subconjunto de um conjunto Ramsey é Ramsey, segue que XYZ é Ramsey.

Agora seja ABC um triângulo acutângulo qualquer. Considere a altura relativa a A e seja E o pé dessa altura. Também consider o ponto D tal que o ângulo $\angle BDC$ seja reto, como na figura abaixo.



Façamos agora a seguinte construção geométrica. Rotacione o triângulo ABC, no espaço euclideano $\mathbb{R}^3$, sobre o eixo BC. Ao fazermos essa rotação o ponto A projeta no plano em algum ponto da reta AE. Em algum momento A projeta no ponto D, esse ponto A chamaremos de A'. É fácil ver que $A'DCB$ é uma pirâmide obtida pelo produto cartesiano de BDC com AD. Como BDC é retângulo, ele é Ramsey

e logo do Teorema 1.9 segue que $A'DCB$ é Ramsey. Daí $A'BC$ é Ramsey e é uma cópia de ABC o que conclui que este também é. □

◇ ◇ ◇ *Aula 2 (04 de Abril) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Vamos dar um exemplo de um conjunto que não é Ramsey.

Teorema 1.11. *O conjunto* $\{-1,0,1\} \subset \mathbb{R}$ *não é Ramsey.*

Para mostrarmos isso, vamos precisar do seguinte lema puramente combinatório.

Lema 1.12. *Existe uma* 4*-coloração de* $\mathbb{R}$ *tal que para todos* $x,y,z \in \mathbb{R}$ *satisfazendo*

$$x - 2y + z = 2$$

o conjunto $\{x,y,z\}$ *não é monocromático.*

Demonstração. Tome a seguinte coloração $\phi : \mathbb{R} \to \{0,1,2,3\}$:

$$\phi(x) = \begin{cases} 0, & \text{se } x \pmod{4\mathbb{Z}} \in [0,1) \\ 1, & \text{se } x \pmod{4\mathbb{Z}} \in [1,2) \\ 2, & \text{se } x \pmod{4\mathbb{Z}} \in [2,3) \\ 3, & \text{se } x \pmod{4\mathbb{Z}} \in [3,4) \end{cases}$$

Suponha que existam x,y,z com $\phi(x) = \phi(y) = \phi(z)$, satisfazendo $x + z - 2y = 2$. Como todos possuem a mesma cor, então existem inteiros n_1, n_2, n_3 inteiros tais que $x = 4n_1 + t + \alpha$, $y = 4n_2 + t + \beta$ e $z = 4n_3 + t + \gamma$, onde $t \in \{0,1,2,3\}$ e $0 \le \alpha, \beta, \gamma < 1$. Assim

$$x - 2y + z = 4(n_1 - 2n_2 + n_3) + \alpha - 2\beta + \gamma.$$

Como $-2 < \alpha - 2\beta + \gamma < 2$ para qualquer escolha de α, β, γ e como $n_1 - 2n_2 + n_3$ é inteiro, temos que $x - 2y + z \neq 2$, o que é uma contradição. □

Com essa coloração podemos mostrar que com 4 cores, é impossível achar uma cópia monocromática de $\{-1,0,1\}$.

Demonstração do Teorema 1.11. Para qualquer n natural, considere a coloração $\psi : \mathbb{R}^n \to \{0,1,2,3\}$ do $\mathbb{R}^n$ dada por $\psi(x) = \phi(||x||^2)$, onde ϕ é a coloração do Lema 1.12. Vamos mostrar que o $\mathbb{R}^n$ colorido dessa forma não possui cópia monocromática de $\{-1,0,1\}$.

Uma cópia de $\{-1,0,1\}$ em $\mathbb{R}^n$ pode ser descrita por um ponto $x \in \mathbb{R}^n$ e um vetor unitário $u \in \mathbb{R}^n$. A cópia então será o conjunto $\{x-u, x, x+u\}$. Suponha que esta cópia é monocromática, isto é, $\psi(x-u) = \psi(x) = \psi(x+u)$ ou $\phi(||x-u||^2) = \phi(||x||^2) = \phi(||x+u||^2)$. Porém uma simples conta nos mostra que

$$||x-u||^2 - 2||x||^2 + ||x+u||^2 = ||x||^2 - 2\langle x,u\rangle + ||u||^2 - 2||x||^2 + ||x||^2 + 2\langle x,u\rangle + ||u||^2 = 2||u||^2 = 2.$$

O que contradiz o fato de ϕ ser uma coloração satisfazendo a hipótese do Lema 1.12. □

Definição 1.13. Dizemos que um conjunto $K \subset \mathbb{R}^d$ é **esférico** se é um subconjunto de uma esfera (de dimensão qualquer).

Queremos agora provar que um conjunto Ramsey é esférico. Note que $\{-1,0,1\}$ é um conjunto em que os pontos não estão em uma esfera.

Teorema 1.14. *Se* K *é Ramsey, então* K *é esférico.*

Vamos mostrar isso de uma maneira muito semelhante ao Teorema 1.11. Para isso precisamos caracterizar melhor os conjuntos não esféricos. O lema a seguir nos dá uma caracterização algébrica desses conjuntos.

Lema 1.15. *Um conjunto* $K = \{x_0, x_1, \ldots, x_k\}$ *não é esférico se, e somente se, existem* $c_1, \ldots, c_k$ *não todos nulos e* $b \neq 0$ *tais que*

1. $\sum_{i=1}^{k} c_i(x_i - x_0) = 0$
2. $\sum_{i=1}^{k} c_i(||x_i||^2 - ||x_0||^2) = b \neq 0$

Demonstração. Note inicialmente que um conjunto K satisfazendo 1. satisfaz

$$\sum_{i=1}^{k} c_i||x_i - x_0||^2 = \sum_{i=1}^{k} c_i(||x_i||^2 - 2\langle x_i, x_0\rangle + ||x_0||^2) = \sum_{i=1}^{k} c_i(||x_i||^2 - ||x_0||^2 - 2\langle x_i - x_0, x_0\rangle) =$$
$$\sum_{i=1}^{k} c_i(||x_i||^2 - ||x_0||^2) - 2\langle\sum_{i=1}^{k} c_i(x_i - x_0), x_0\rangle = \sum_{i=1}^{k} c_i(||x_i||^2 - ||x_0||^2).$$

Isso significa que podemos substituir a condição 2. por $\sum_{i=1}^{k} c_i||x_i - x_0||^2 = b \neq 0$.

Se K é esférico vamos mostrar que não existem $c_1, \ldots, c_k, b$ satisfazendo as condições do enunciado. Seja z o centro da esfera que contém K e r seur raio. Se $\{x_1 - x_0, \ldots, x_k - x_0\}$ forem todos linearmente independentes, não temos o que fazer, pois é impossível satisfazer a condição 1. Suponha então que existam $c_1, \ldots, c_k$ não todos nulos tais que $\sum_{i=1}^{k} c_i(x_i - x_0) = 0$. Temos que

$$r^2 = ||x_i - z||^2 = ||(x_i - x_0) - (z - x_0)||^2 = ||x_i - x_0||^2 - 2\langle x_i - x_0, z - x_0\rangle + ||z - x_0||^2 =$$
$$||x_i - x_0||^2 - 2\langle x_i - x_0, z - x_0\rangle + r^2 \Leftrightarrow ||x_i - x_0||^2 = 2\langle x_i - x_0, z - x_0\rangle.$$

Somando para todo i obtemos

$$\sum_{i=1}^{k} c_i||x_i - x_0||^2 = \sum_{i=1}^{k} 2c_i\langle x_i - x_0, z - x_0\rangle = 2\langle\sum_{i=1}^{k} c_i(x_i - x_0), z - x_0\rangle = 0.$$

O que pelo parágrafo inicial contradiz com a condição 2.

Agora suponha K não esférico, vamos determinar $c_1, \ldots, c_k, b$ satisfazendo a hipótese. Note que podemos supor que K é não esférico minimal, ou seja, que qualquer subconjunto de K é esférico. Isso ocorre porque se K é não esférico qualquer, ele possui um subconjunto K' não esférico minimal. Então encontrada as constantes para K' basta escolher $c_i = 0$ para $x_i \in K \setminus K'$ e as condições do enunciado continuas sendo satisfeitas.

Observe que o conjunto de vetores $\{x_1 - x_0, \ldots, x_k - x_0\}$ não pode ser linearmente independente, pois caso contrário K seria um simplexo e logo esférico (um simplexo n dimensional está contido em uma esfera $(n-1)$ dimensional). Assim existem $c_1, \ldots, c_k$ não todos nulos tais que $\sum_{i=1}^{k} c_i(x_i - x_0) = 0$. Suponha sem perda de generalidade que $c_k \neq 0$. Considere agora $K' = \{x_0, \ldots, x_{k-1}\}$. Pela minimalidade de K temos que K' é esférico, seja z o centro dessa esfera e r o seu raio.

Pelo mesmo argumento feito em um parágrafo anterior, temos que

$$\sum_{i=1}^{k-1} c_i||x_i - x_0||^2 = 2\langle\sum_{i=1}^{k-1} c_i(x_i - x_0), z - x_0\rangle = 2\langle -c_k(x_k - x_0), z - x_0\rangle = -2c_k\langle x_k - x_0, z - x_0\rangle.$$

Agora somando com o x_k obtemos

$$\sum_{i=1}^{k} c_i||x_i - x_0||^2 = c_k||x_k - x_0||^2 - 2c_k\langle x_k - x_0, z - x_0\rangle = c_k(||x_k - x_0||^2 - 2\langle x_k - x_0, z - x_0\rangle) =$$
$$c_k(||x_k - z||^2 - ||z - x_0||^2) = c_k(||x_k - z||^2 - r^2) \neq 0$$

de $c_k \neq 0$ e $||x_k - z|| \neq r$ (x_k não pertence a esfera, pois K não é esférico). Tomando então $b = c_k(||x_k - z||^2 - r^2)$ concluímos a demonstração.

□

◇ ◇ ◇ *Aula 3 (18 de Abril) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Continuamos com os preparativos para demonstrar que todo conjunto Ramsey é esférico. Começando por um resultado de álgebra linear.

Proposição 1.16. *Sejam $K \subset \mathbb{R}^d$, $K' \subset \mathbb{R}^N$ e d, N inteiros com $N \geq d$. Suponha que $\mathbb{R}^d$ esteja imerso em $\mathbb{R}^N$ da forma canônica. Se $K \cong K'$, seja $\iota : K \to K'$ uma isometria entre K e K'. Então existe isometria $I : \mathbb{R}^N \to \mathbb{R}^N$ que*

estende ι, isto é, $I(x) = \iota(x)$, para todo $x \in K$. Além disso, podemos escrever $I(x) = Ax + t$, onde A é uma matriz $N \times N$ ortogonal e $t \in \mathbb{R}^N$.

Demonstração. Suponha que o maior simplexo em K seja de dimensão r. Isto é, existem $r+1$ pontos em K que formam um r-simplexo, mas não existem $r+2$ pontos que formam um $(r+1)$-simplexo. Podemos supor sem perda de generalidade que um desses pontos seja 0 (Basta transladar todo o $\mathbb{R}^N$ de maneira que esse ponto caia no 0). Chame os demais pontos de $\{x_1, \ldots, x_r\}$. Note que os pontos desse simplexo são linearmente independentes e geram um subespaço E de dimensão r de $\mathbb{R}^N$. É fácil ver da maximalidade de r que $K \subset E$. Seja $\{u_1, \ldots, u_r\}$ uma base ortonormal desse espaço, ela existe pois estamos em um espaço vetorial real munido de produto interno de dimensão finita. Por $\{x_1, \ldots, x_r\}$ ser também uma base de E podemos escrever $u_i = \sum_{j=1}^{r} c_{ij} x_j$ para todo $1 \le i \le r$.

Agora sejam $x_0' = \iota(0), x_1' = \iota(x_1), \ldots, x_r' = \iota(x_r)$ os pontos correspondentes a esse simplexo em K'. Defina uma transformação linear $T : E \to \mathbb{R}^N$ tal que para todo $1 \le i \le r$ vale

$$Tx_i = x_i' - x_0'.$$

Por estar definida em uma base, T está definida em todo E. Vamos mostrar que T é ortogonal. Primeiro note que

$$||Tx_i|| = ||x_i' - x_0'|| = ||\iota(x_i) - \iota(0)|| = ||x_i - 0|| = ||x_i||.$$

para todo $1 \le i \le r$ e

$$\langle Tx_i, Tx_j \rangle = \frac{||Tx_i||^2 + ||Tx_j||^2 - ||T(x_i - x_j)||^2}{2} = \frac{||x_i||^2 + ||x_j||^2 - ||x_i - x_j||^2}{2} = \langle x_i, x_j \rangle$$

para todo $1 \le i < j \le r$, pois $||T(x_i - x_j)|| = ||Tx_i - Tx_j|| = ||(x_i' - x_0') - (x_j' - x_0')|| = ||x_i' - x_j'|| = ||\iota(x_i) - \iota(x_j)|| = ||x_i - x_j||$. Com isso podemos mostrar que $Tu_1, \ldots, Tu_r$ é uma base ortonormal. De fato, para todo $1 \le i \le r$

$$||Tu_i||^2 = ||T(\sum_{j=1}^{r} c_{ij} x_j)||^2 = \sum_{j=1}^{r} c_{ij}^2 ||Tx_j||^2 + 2 \sum_{1 \le j < k \le r} c_{ij} c_{ik} \langle Tx_j, Tx_k \rangle =$$

$$\sum_{j=1}^{r} c_{ij}^2 ||x_j||^2 + 2 \sum_{1 \le j < k \le r} c_{ij} c_{ik} \langle x_j, x_k \rangle = ||\sum_{j=1}^{r} c_{ij} x_j||^2 = ||u_i||^2 = 1$$

e para $1 \le i < j \le r$ temos

$$\langle Tu_i, Tu_j \rangle = \langle T(\sum_{t=1}^{r} c_{it} x_t), T(\sum_{k=1}^{r} c_{jk} x_k) \rangle = \sum_{t=1}^{r} \sum_{k=1}^{r} c_{it} c_{jk} \langle Tx_t, Tx_k \rangle$$

$$\sum_{t=1}^{r} \sum_{k=1}^{r} c_{it} c_{jk} \langle x_t, x_k \rangle = \langle \sum_{t=1}^{r} c_{it} x_t, \sum_{k=1}^{r} c_{jp} x_k \rangle = \langle u_i, u_j \rangle = 0.$$

Seja F o subespaço vetorial de $\mathbb{R}^N$ gerado por $Tu_1, \ldots, Tu_r$. A ortogonalidade de T nos garante que $\dim(F) = \dim E$ e podemos escrever $F = \text{span}(Tx_1, \ldots, Tx_r)$. Considere a função $J : E \to F$ dada por $J(x) = Tx + x_0'$. Afirmamos que J é uma isometria entre esses espaços que estende ι e consequentemente $K' \subset F$.

Vamos precisar do seguinte resultado. Sejam $m \le n$ inteiros e V um subespaço vetorial de $\mathbb{R}^n$ de dimensão m. Dado uma base $\{f_1, \ldots, f_m\}$ de V defina $\psi : \mathbb{R}^n \to \mathbb{R}^{m+1}$ por

$$\psi(x) = (||x||, ||x - f_1||, \ldots, ||x - f_m||).$$

Mostraremos que se $\psi(x) = \psi(y)$ para $x, y \in \mathbb{R}^n$, então a projeção de x e y em V é a mesma. Seja $\{e_1, \ldots, e_n\}$ uma base ortonormal de $\mathbb{R}^n$ tal que $\text{span}(e_1, \ldots, e_m) = V$ e seja D a matriz de mudança de base que leva a base $\{e_1, \ldots, e_m\}$ na base $\{f_1, \ldots, f_m\}$. Isto é, $f_i = \sum_{j=1}^{m} d_{ij} e_j$ para todo $1 \le i \le m$. Sejam $x = \sum_{j=1}^{n} a_j e_j$ e $y = \sum_{j=1}^{n} b_j e_j$ tais que $\psi(x) = \psi(y)$. Temos que

$$||x|| = ||y|| \Leftrightarrow a_1^2 + \ldots + a_n^2 = b_1^2 + \ldots + b_n^2.$$

Daí para todo $1 \leq i \leq n$ vale

$$||x - f_i|| = ||y - f_i|| \Leftrightarrow \sum_{j=1}^{m}(a_j - d_{ij})^2 + \sum_{j=m+1}^{n} a_j^2 = \sum_{j=1}^{n}(b_j - d_{ij})^2 + \sum_{j=m+1}^{n} b_j^2 \Leftrightarrow \sum_{j=1}^{m} 2d_{ij}(a_j - b_j) = 0.$$

Seja $x_V = \sum_{j=1}^{m} a_j e_j$ e $y_V = \sum_{j=1}^{m} b_j e_j$ as projeções de x e y em V. A última equação significa que $2D(x_V - y_V) = 0$. Como D é matriz de mudança de base, ela é invertível. Portanto $x_V - y_V = 0$, ou seja, as projeções são iguais.

Da ortogonalidade de T, é fácil ver que J é uma isometria. Seja agora $x \in K$ tal que $x \notin \{0, x_1, \ldots, x_r\}$. Do fato de J ser uma isometria que estende ι em $\{0, x_1, \ldots, x_r\}$ temos que $||J(x) - x_i'|| = ||\iota(x) - x_i'||$ para todo $0 \leq i \leq r$. Podemos então usar o fato do parágrafo anterior para $V = F$, $\mathbb{R}^N$ e $f_i = Tx_i = x_i' - x_0'$. Definindo a $\psi : \mathbb{R}^N \to \mathbb{R}^{r+1}$ do mesmo jeito, temos que $\psi(J(x) - x_0') = \psi(\iota(x) - x_0')$ e logo $(J(x) - x_0')_F = (\iota(x) - x_0')_F$. Porém $J(x) - x_0' = Tx \in F$ e portanto é a projeção em F de $\iota(x) - x_0$. Por pitágoras

$$||J(x) - x_0'||^2 = ||\iota(x) - x_0'||^2 = ||(\iota(x) - x_0)_F||^2 + ||(\iota(x) - x_0') - (\iota(x) - x_0')_F||^2 =$$
$$||J(x) - x_0'||^2 + ||(\iota(x) - x_0') - (\iota(x) - x_0')_F||^2 \Leftrightarrow ||(\iota(x) - x_0') - (\iota(x) - x_0')_F|| = 0$$

e daí segue que $\iota(x) - x_0 \in F$. Mas isso implica $J(x) - x_0' = \iota(x) - x_0'$ e conseguentemente $J(x) = \iota(x)$. Ou seja, J estende ι em K.

Para finalizarmos, chame $v_1 = Tu_1, \ldots, v_r = Tu_r$ a base ortonormal que gera F. Pelo processo de ortogonalização de Gram-Schmidt, podemos estender as bases ortonormais $\{u_1, \ldots, u_r\}$, $\{v_1, \ldots, v_r\}$ de E e F para bases ortonormais $\{u_1, \ldots, u_N\}$ e $\{v_1, \ldots, v_N\}$. Seja $S : \mathbb{R}^N \to \mathbb{R}^N$ a transformação linear dada por $Su_i = v_i$ para todo $1 \leq i \leq N$. É fácil ver que $S|_E = T$ e que S é ortogonal. Então $I : \mathbb{R}^N \to \mathbb{R}^N$ dada por $I(x) = Sx + x_0'$ é a isometria desejada. □

Como já dito, a estratégia utilizada será a mesma que usamos para mostrar que $\{-1, 0, 1\}$ não é Ramsey. Já possuimos uma caracterização algébrica dos conjuntos não esféricos. O próximo lema nos fornece a coloração necessária.

Lema 1.17. *Suponha $c_1, \ldots, c_k, b \in \mathbb{R}$ com $b \neq 0$. Então existe r inteiro e r-coloração de $\mathbb{R}$ tal que todo conjunto $\{y_0, \ldots, y_k\} \subset \mathbb{R}$ satisfazendo*

$$\sum_{i=1}^{k} c_i(y_i - y_0) = b$$

não é monocromático.

Iremos mostrar na verdade o seguinte teorema um pouco mais forte.

Teorema 1.18. *Sejam dados $c_1, \ldots, c_k, b \in \mathbb{R}$ com $b \neq 0$. Então existe uma $(2k)^k$-coloração ψ de $\mathbb{R}$ tal que a equação*

$$\sum_{i=1}^{k} c_i(y_i - y_i') = b$$

não tem solução com $\psi(y_i) = \psi(y_i')$, para todo $1 \leq i \leq k$.

Note que o Lema 1.17 segue de imediato do Teorema 1.18 se tomarmos $y_i' = y_0$ para todo $1 \leq i \leq k$. Para provarmos esse teorema vamos primeiro fazer um caso particular.

Lema 1.19. *Dado $\alpha \in \mathbb{R}$, existe $2k$-coloração η de $\mathbb{R}$ tal que*

$$\sum_{i=1}^{k}(x_i - x_i') = \alpha$$

não tem solução com $\eta(x_i) = \eta(x_i')$, para todo $1 \leq i \leq k$.

Demonstração. Tome a coloração $\eta : \mathbb{R} \to [2k]$ dada por $\eta(x) = i$ se $\alpha(i-1)/k \leq x (\mathrm{mod}\ 2\alpha\mathbb{Z}) < \alpha i/k$.

Assumimos aqui que $x \equiv a (\mathrm{mod}\ 2\alpha\mathbb{Z})$ se $x - a = 2t\alpha$ para $t \in \mathbb{Z}$. Essa coloração satisfaz a hipótese do enunciado.

Suponha que existam $x_1, \ldots, x_k, x_1', \ldots, x_k'$ tais que $\sum_{i=1}^k (x_i - x_i') = \alpha$ e que $\eta(x_i) = \eta(x_i')$ para todo $1 \leq i \leq k$. De $\eta(x_i) = \eta(x_i')$ vale que $\alpha(2t_i - \frac{1}{k}) < x_i - x_i' < \alpha(2t_i + \frac{1}{k})$ para algum $t_i \in \mathbb{Z}$. Assim temos que

$$\alpha(2(t_1 + \ldots + t_k) - 1) < \sum_{i=1}^k (x_i - x_i') < \alpha(2(t_1 + \ldots + t_k) + 1) \Leftrightarrow$$
$$\alpha(2(t_1 + \ldots + t_k) - 1) < \alpha < \alpha(2(t_1 + \ldots + t_k) + 1) \Leftrightarrow 2(t_1 + \ldots + t_k) - 1 < 1 < 2(t_1 + \ldots + t_k) + 1 \Leftrightarrow$$
$$0 < 2(1 - t_1 - \ldots - t_k) < 2$$

o que é impossível, pois não existem números pares entre 0 e 2. □

Demonstração do Teorema 1.18. Vamos usar da coloração do lema anterior para obter uma coloração. Para cada $1 \leq i \leq k$ defina $\psi_i : \mathbb{R} \to [2k]$ a coloração do Lema 1.17 para $\alpha = \frac{b}{c_i}$. Então $\psi : \mathbb{R} \to [2k]^k$ dada por

$$\psi(x) = (\psi_1(x), \ldots, \psi_k(x))$$

satisfaz os nossos propósitos.

Suponha que não, e seja $y_1, \ldots, y_k, y_1', \ldots, y_k'$ reais tais que $\sum_{i=1}^k c_i(y_i - y_i') = b$ e que $\psi(y_i) = \psi(y_i')$ para todo $1 \leq i \leq k$. De $\psi(y_i) = \psi(y_i')$ temos que $\psi_i(y_i) = \psi_i(y_i')$ e portanto $\frac{b}{c_i}(2t_i - \frac{1}{k}) < y_i - y_i' < \frac{b}{c_i}(2t_i + \frac{1}{k}) \Leftrightarrow b(2t_i - \frac{1}{k}) < c_i(y_i - y_i') < b(2t_i + \frac{1}{k})$ para algum $t_i \in \mathbb{Z}$. Logo

$$b(2(t_1 + \ldots + t_k) - 1) < \sum_{i=1}^k c_i(y_i - y_i') < b(2(t_1 + \ldots + t_k) + 1) \Leftrightarrow$$
$$b(2(t_1 + \ldots + t_k) - 1) < b < b(2(t_1 + \ldots + t_k) + 1) \Leftrightarrow 0 < 2(1 - t_1 - \ldots - t_k) < 2$$

que, como já argumentamos, é uma contradição. □

Podemos agora demonstrar que todo conjunto Ramsey é esférico.

Demonstração do Teorema 1.14. Vamos mostrar que se $K \subset \mathbb{R}^d$ é um conjunto não esférico, então ele não pode ser Ramsey. Suponha que $K = \{x_0, \ldots, x_k\}$. Pelo Lema 1.15 existem $c_1, \ldots, c_k$ não todos nulos e $b \neq 0$ satisfazendos as equações

1. $\sum_{i=1}^k c_i(x_i - x_0) = 0$
2. $\sum_{i=1}^k c_i(||x_i||^2 - ||x_0||^2) = b \neq 0$.

O Lema 1.17 nos diz que existe uma r-coloração $\psi : \mathbb{R} \to [r]$ tal que todo $\{y_0, \ldots, y_k\} \subset \mathbb{R}$ satisfazendo $\sum_{i=1}^k c_i(y_i - y_0) = b$ não é monocromático. Fixe essa ψ. Para $N \in \mathbb{N}$ defina a coloração $\phi : \mathbb{R}^N \to [r]$ dada por $\phi(x) = \psi(||x||)$. Afirmamos que $\mathbb{R}^N$ com essa coloração não possui nenhuma cópia monocromática de K.

Seja $K' \subset \mathbb{R}^N$ uma cópia de K. Se imergimos $\mathbb{R}^d$ em $\mathbb{R}^N$ de forma canônica, podemos usar a Proposição 1.16 para acharmos uma isometria $I : \mathbb{R}^N \to \mathbb{R}^N$ tal que $I(K) = K'$ e $I(x) = Ax + t$ onde $t \in \mathbb{R}^N$ e A é uma matriz ortogonal. Sejam $I(x_0), \ldots, I(x_k)$ os vértices de K'. Então

$$\sum_{i=1}^k c_i(||I(x_i)||^2 - ||I(x_0)||^2) = \sum_{i=1}^k c_i(||Ax_i + t||^2 - ||Ax_0 + t||^2) =$$
$$\sum_{i=1}^k c_i((||Ax_i||^2 + 2\langle Ax_i, t\rangle + ||t||^2) - (||Ax_0||^2 + 2\langle Ax_0, t\rangle + ||t||^2)) =$$
$$\sum_{i=1}^k c_i(||Ax_i||^2 - ||Ax_0||^2 + 2\langle A(x_i - x_0), t\rangle) = \sum_{i=1}^k c_i(||x_i||^2 - ||x_0||^2) + 2\langle A(\sum_{i=1}^k c_i(x_i - x_0)), t\rangle =$$
$$\sum_{i=1}^k c_i(||x_i||^2 - ||x_0||^2) + \langle 0, t\rangle = \sum_{i=1}^k c_i(||x_i||^2 - ||x_0||^2 = b$$

□

Conjectura 1.20 (Graham). *K é Ramsey se, e somente se, K é esférico.*

2 Uma demonstração topológica de Van der Waerden

◇ ◇ ◇ *Aula 4 (02 de Maio) — Marcelo Soares Campos* ◇ ◇ ◇

Em teoria de Ramsey, estamos interessados em saber quando colorir algum conjunto implica um subconjunto monocromático com determinada propriedade. No tópico de hoje queremos colorir números e obter progressões aritméticas monocromáticas. O Teorema de Van der Waerden nos garante que isso vale quando o conjunto colorido são os inteiros

Teorema 2.1 (Van der Waerden). *Sejam q,k naturais. Para toda q-coloração $c : \mathbb{Z} \to [q]$ dos inteiros, existem $a \in \mathbb{Z}$ e $d \in \mathbb{N}^*$ tais que*

$$c(a) = c(a+d) = \ldots = c(a+(k-1)d).$$

A demonstração original desse teorema é baseada em uma indução dupla, mas aqui daremos uma demonstração usando dinâmica topológica. O bônus dessa demonstração é que ela permite facilmente estender o resultado para o seguinte teorema

Teorema 2.2. *Sejam q natural e $v_1, \ldots, v_k \in \mathbb{Z}^n$ vetores. Para toda q-coloração $c : \mathbb{Z}^n \to [q]$, existem $a \in \mathbb{Z}^n$ e $d \in \mathbb{N}^*$ tais que*

$$c(a+dv_1) = \ldots = c(a+dv_2).$$

Note que o Teorema 2.2 é realmente uma generalização do Teorema 2.1. De fato, para ver que o segundo implica o primeiro basta considerar $n = 1$ e $v_i = i-1$, para todo $1 \le i \le k$.

Antes de começarmos a prova do Teorema 2.1 precisamos introduzir o nosso setup topológico. Vamos trabalhar com um espaço métrico nas q-colorações de $\mathbb{Z}$. Seja $M = \{x : \mathbb{Z} \to [q]\}$ o nosso espaço e defina a métrica $d : M \times M \to \mathbb{R}^+$ dada por

$$d(x,y) = \begin{cases} \frac{1}{m+1}, & \text{onde } m = \min\{|i| : x(i) \neq y(i)\} \\ 0, & \text{caso } x = y \end{cases}$$

Afirmação 2.3. *(M,d) é um espaço métrico.*

Demonstração. A única propriedade que precisa de uma verificação é a desigualdade triangular. Sejam $x,y,z \in M$ com $d(x,y) = a$ e $d(y,z) = b$. Então temos que $x(i) = y(i)$ para todo $-a < i < a$ e $y(i) = z(i)$ para todo $-b < i < b$. Assim $x(i) = z(i)$ para todo $-\min(a,b) < i < \min(a,b)$ e portanto $\min\{|i| : x(i) = z(i)\} \ge \min(a,b)$. Daí

$$d(x,z) \le \frac{1}{\min(a,b)+1} \le \frac{1}{a+1} \le \frac{1}{a+1} + \frac{1}{b+1} \le d(x,y) + d(y,z)$$

□

Além disso, usando o Teorema de Tychonoff (Teorema 1.5) da seção anterior podemos provar que

Afirmação 2.4. *(M,d) é compacto.*

Demonstração. Uma outra maneira de ver M é como se fosse o produto enumerável de espaços $[q]$, ou seja, $M = [q]^{\mathbb{N}}$. Se considerarmos $[q]$ com a topologia discreta, temos que M com a topologia produto é compacto (pelo teorema de Tychonoff). Basta mostrar que a topologia induzida pela métrica d é a mesma que a topologia produto.

Observe que $\mathcal{B}_{\mathcal{M}} = \{B(x, \frac{1}{n}) : x \in M \text{ e } n \in \mathbb{N}^*\}$ é uma base de abertos de M com a topologia induzida pela métrica d. Vamos traduzir isso para a linguagem de produtos. O conjunto $B(x, \frac{1}{n}) = \{y \in M : x(i) = y(i), \forall -(n-1) < i < (n-1)\}$ pode ser escrito como $\{a\} \times \prod_{|i| \ge n-1}[q]$, onde $a \in \prod_{|i|<n-1}[q]$ é

um ponto. Isso significa que

$$\mathcal{B}_M = \{A \times \prod_{|i|\geq n} [q] : \text{ onde } A \text{ é um ponto em } \prod_{|i|<n} [q]\}.$$

Agora seja $\mathcal{B}_\prod$ a base de abertos vinda da topologia produto. Como a topologia em $[q]$ é discreta, entao todo ponto em $[q]$ é aberto. Daí da definição segue que $\mathcal{B}_M \subset \mathcal{B}_\prod$. Seja $U \in \mathcal{B}_\prod$ um aberto qualquer. U é um aberto da forma $V \times \prod_{|i|\geq n}[q]$ para algum n, onde $V \subset \prod_{|i|\leq n}[q]$. Logo U é união de abertos de $\mathcal{B}_M$ e portanto $\mathcal{B}_M$ gera $\mathcal{B}_\prod$. □

Defina o operador bijetor $T : M \to M$ dado por $T(x) = y$, onde $y(i) = x(i+1)$, para todo $i \in \mathbb{Z}$. Isto é, se considerarmos um elemento de M como um vetor de coordenadas inteiras com entradas em $[q]$, então T é o operador shift que empurra todo o vetor uma coordenada para esquerda (vendo as coordenadas na ordem crescente). O operador T é contínuo pois dado $U \in \mathcal{B}_M$ aberto da base da forma $U = \{a\} \times \prod_{|i|\geq n}[q]$, com $a \in \prod_{|i|<n}[q]$, a pré-imagem $T^{-1}(U)$ é algo da forma $\{b\} \times \prod_{|i+1|\geq n}[q]$ com $b \in \prod_{|i+1|<n}[q]$ que também é um aberto.

Queremos entender o que acontece ao iterarmos o operador T algumas vezes, para isso vamos precisar usar do seguinte resultado em sistemas dinâmicos, que enunciaremos sem demonstração.

Teorema 2.5 (Teorema de Recorrência de Birkhoff)**.** *Seja (M,d) um espaço métrico compacto e $T_1,\dots,T_r : M \to M$ operadores contínuos tais que $T_i(T_j(x)) = T_j(T_i(x))$, para todo $1 \leq i,j \leq r$ e $x \in M$. Então existe um ponto $y \in M$ tal que para todo $\epsilon > 0$, existe $n \in \mathbb{N}^*$ com $d(T_i^n(y), y) < \epsilon$ para todo $1 \leq i \leq r$.*

Agora já temos o arsenal técnico suficiente para demonstramos Van der Waerden.

Demonstração do Teorema 2.1. Dada uma coloração $c \in M$ e um inteiro k, considere

$$M_c = \overline{\{T^n(c) : n \in \mathbb{Z}\}}$$

o fecho de todos os shifts sobre a coloração c. Como M_c é um fechado de M, então (M_c, d) é compacto. Além disso, T é invariante em M_c. De fato, se $x \in M_c$, existe uma sequência $\{i_t\}$ de $\mathbb{Z}$ tal que $x = \lim_{t\to\infty} T^{i_t}(c)$. Como T é contínua, temos que $T(x) = T(\lim_{t\to\infty} T^{i_t}(c)) = \lim_{t\to\infty} T^{i_t+1}(c) \in M_c$. Assim podemos considerar T como um operador contínuo de M_c em M_c.

Defina $T_1,\dots,T_{k-1} : M_c \to M_c$ por $T_j = T^j$, para todo $1 \leq j \leq k-1$. De T ser contínuo, segue que todos os T_i's são contínuos e obviamente $T_i \circ T_j = T^{i+j} = T_j \circ T_i$ para todo i,j. Podemos agora aplicar o Teorema 2.5 para $\epsilon = \frac{1}{3}$. O teorema nos garante que existe um $d \in \mathbb{N}^*$ e um $y \in M_c$ tal que $d(T_j^d(y), y) = d(T^{jd}(y), y) < \frac{1}{3}$ para todo $1 \leq j \leq k-1$. Fixe esse $y \in M_c$.

Do fato de y ser um limite de $T^j(c)$'s, para todo $\delta > 0$, existe um $a \in \mathbb{Z}$ tal que $d(T^a(c), y) < \delta$. Tome $\delta = \frac{1}{(k-1)d+3}$. Se $d(T^a(c), y) < \frac{1}{(k-1)d+3}$, então $T^a(c)(i) = y(i)$ para todo $-((k-1)d+2) < i < (k-1)d+2$. Isso significa que se aplicarmos o operador T^{jd} nos dois termos, as coordenadas vão coincidir para todo i com $-((k-j-1)d+2) < i < (k-j-1)d+2$ e portanto

$$d(T^{a+jd}(c), T^{jd}(y)) \leq \frac{1}{(k-j-1)d+3} \leq \frac{1}{3}.$$

Usando a desigualdade triangular e as desigualdades já obtidas temos

$$d(T^a(c), T^{a+jd}(c)) \leq d(T^a(c), y) + d(y, T^{jd}(y)) + d(T^{jd}(y), T^{a+jd}(y)) < \frac{1}{(k-1)d+3} + \frac{1}{3} + \frac{1}{3} \leq 1$$

para todo $1 \leq j \leq k-1$. Porém, o fato de todas as distâncias a $T^a(c)$ serem menores que 1 signfica que $T^{a+d}(c),\dots,T^{a+(k-1)d}(c)$ coincidem na coordenada 0 com $T^a(c)$. Como $T^i(c)(0) = c(0+i) = c(i)$ para todo $i \in \mathbb{Z}$, temos que $c(a) = c(a+d) = \dots = c(a+(k-1)d)$.

□

◇ ◇ ◇ *Aula 5 (09 de Maio) — Marcelo Soares Campos* ◇ ◇ ◇

Na aula passada provamos o teorema de Van der Waerden usando um resultado em sistemas dinâmicos, que é o Teorema de Recorrência de Birkhoff (Teorema 2.5). Vamos dar uma demonstração de uma versão um pouco mais fraca desse teorema, que continua servindo para os nosso propósitos.

Teorema 2.6. *Seja (M,d) um espaço métrico compacto e $T_1,\dots,T_r : M \to M$ homeomorfismos tais que $T_i \circ T_j = T_j \circ T_i$ para todos $1 \le i,j \le r$. Então para todo $\epsilon > 0$, existe um $x \in M$ e um $n \in \mathbb{N}^*$ tal que $d(x, T_i^n(x)) < \epsilon$ para todo $1 \le i \le r$.*

As duas principais diferenças são que agora pedimos que os operadores T_i's sejam homeomorfismos, que na nossa aplicação é verdade, pois a inversa do operador shift também é continua. E agora garantimos a existência de um dado y a partir do valor ϵ escolhido, porém na nossa demonstração nós escolhemos um valor único de ϵ durante toda a demonstração. Assim o teorema acima é suficiente para provar Van der Waerden.

Antes de começarmos com a demonstração vamos fazer alguns preparativos. Seja $\mathcal{G}$ o grupo dos homeomorfismos gerados por $T_1,\dots,T_r$. A hipótese de comutatividade do enunciado nos diz que $\mathcal{G}$ é abeliano e assim podemos escrever $\mathcal{G} = \{T_1^{i_1} \circ \dots \circ T_r^{i_r} : i_1,\dots,i_r \in \mathbb{Z}\}$. Podemos análisar a ação desse grupo sobre os elementos de M. Dado $x \in M$, definimos a órbita de x como $O(x) = \{g(x) : g \in \mathcal{G}\}$, ou seja, os elementos obtidos aplicando algum homeomorfismo do grupo sobre x. Vamos estudar as órbitas de elementos contidos em subconjuntos especiais de M, que definiremos a seguir.

Defina $\mathcal{A} = \{Y \subset M : Y \neq \varnothing, Y \text{ fechado e } g(Y) \subseteq Y, \forall g \in \mathcal{G}\}$ o conjunto de todos os fechados de M que são invariantes por $\mathcal{G}$. Queremos considerar um conjunto $X \in \mathcal{A}$ que seja minimal, com relação a ordem parcial $(\mathcal{A}, \subseteq)$. Para isso vamos precisar usar um resultado clássico de teoria dos conjuntos, o lema de Zorn.

Dado um cojunto parcialmente ordenado $(P, \le)$, dizemos que um subconjunto C é uma **cadeia**, se para todo $x,y \in C$ vale que $x \le y$ ou $y \le x$. Um minorante de um conjunto $A \subset P$ é um elemento $p \in P$ tal que $p \le x$ para todo $x \in A$. Assim o lema de Zorn nos diz que

Lema 2.7 (Zorn)**.** *Suponha que um conjunto parcialmente ordenado $(P, \le)$, não vazio, possua a propriedade de que toda cadeia possua um minorante. Então P possui um elemento minimal.*

Com isso podemos provar

Afirmação 2.8. *O conjunto $\mathcal{A}$ possui um elemento minimal. Mais do que isso, se $Z \in \mathcal{A}$, existe um conjunto minimal $X \in \mathcal{A}$ tal que $X \subseteq Z$.*

Demonstração. Dado $Z \in \mathcal{A}$ seja $\mathcal{A}_Z = \{Y \in \mathcal{A} : Y \subseteq Z\}$. O conjunto parcialmente ordenado que estamos considerando é o natural $(\mathcal{A}_Z, \subseteq)$. Note que $\mathcal{A}_Z \neq \varnothing$, pois $Z \in \mathcal{A}_Z$. Do lema 2.7 precisamos apenas mostrar que toda cadeia de $\mathcal{A}_Z$ possui um minorante. Seja $\mathcal{C}$ uma cadeia de $\mathcal{A}_Z$. Note que o conjunto $\mathcal{C}$ é uma família de fechados de M com a propriedade da intersecção finita. Pois se escolhermos um conjunto finito $X_1, X_2, \dots, X_k \in \mathcal{C}$, por todos serem comparáveis, é possível ordená-los. Suponha sem perda de generalidade que $X_1 \subseteq \dots \subseteq X_k$, daí $\bigcap_{i=1}^k X_i = X_1 \neq \varnothing$. Do fato de M ser compacto, podemos usar o teorema 1.7, que nos diz que $X = \bigcap \mathcal{C} \neq \varnothing$.

Se $X \in \mathcal{A}_Z$ acabamos, pois por definição $X \subseteq Y$, para todo $Y \in \mathcal{C}$. X é fechado, pois a intersecção infinita de fechados é fechado. Além disso $X \subseteq Z$, pois $X \subseteq Y \subseteq Z$ para algum $Y \in \mathcal{C}$. Basta ver que X é invariante por $\mathcal{G}$. Dado $g \in \mathcal{G}$ se $x \in X$, então $x \in Y$ para todo $Y \in \mathcal{C}$ e logo $g(x) \in Y$, para todo $Y \in \mathcal{C}$ (Y são invariantes). Isso significa que $g(x) \in \bigcap \mathcal{C} = X$, para todo $x \in X$ e logo $g(X) \subseteq X$. □

Fixe um conjunto minimal X de $\mathcal{A}$. Vamos estudar a órbita de um elemento $x \in X$.

Afirmação 2.9. *Dado $x \in X$, o conjunto $O(x)$ é denso em X. Em outras palavras, $X = \overline{O(x)}$.*

Demonstração. Seja $g \in \mathcal{G}$ um homeomorfismo qualquer do grupo. Dado $y \in O(x)$, podemos escrever $y = h(x)$ para algum $h \in \mathcal{G}$. Como $g(y) = (g \circ h)(x)$ e $g \circ h \in \mathcal{G}$, pois $\mathcal{G}$ é um grupo, segue que $g(y) \in O(x)$. Isso prova que $O(x)$ é invariante por $\mathcal{G}$.

Agora considere $y \in \overline{O(x)}$. Podemos escrever $y = \lim_{k\to\infty} y_k$ onde $y_k \in O(x)$, logo $y_k = h_k(x)$ para $h_k \in \mathcal{G}$. Pela continuidade de g temos que

$$g(y) = g(\lim_{k\to\infty} y_k) = \lim_{k\to\infty} g(y_k) = \lim_{k\to\infty} (g \circ h_k)(x) \in \overline{O(x)}$$

pois $g \circ h_k \in \mathcal{G}$ para todo k. Logo $\overline{O(x)}$ também é invariante por $\mathcal{G}$. Além disso $\overline{O(x)} \neq \varnothing$ e é fechado. Então $\overline{O(x)} \in \mathcal{A}$. Também temos que de $x \in X$, vale que $g(x) \in X$ para todo $g \in \mathcal{G}$ (X é invariante por

$\mathcal{G}$). Assim $\overline{O(x)} \subseteq X$. Porém pela minimalidade de X, X não possui subconjuntos próprios em $\mathcal{A}$ e daí $X = \overline{O(x)}$. □

Vamos mostrar agora que a ação do grupo $\mathcal{G}$ sobre um aberto contendo um ponto de X forma uma cobertura de X.

Lema 2.10. *Seja $x \in X$ e U aberto de M com $x \in U$. Então existe $\mathcal{H} \subset \mathcal{G}$ finito tal que*

$$X \subseteq \bigcup_{h \in \mathcal{H}} h(U).$$

Demonstração. Primeiro vamos mostrar que $X \subseteq \bigcup_{g \in \mathcal{G}} g(U)$, ou seja, que a ação do grupo $\mathcal{G}$ sobre U forma uma cobertura aberta de X. Seja $y \in X$, a afirmação 2.9 nos diz que $X = \overline{O(y)}$. Isso significa que podemos escrever $x = \lim_{k\to\infty} y_k$ com $y_k \in O(y)$. Em particular, existe m tal que $y_m \in U$. De $y_m \in O(y)$ podemos escrever $y_m = g_m(y)$ com $g_m \in \mathcal{G}$. Logo $y \in g_m^{-1}(U)$, e de g_m ser homeomorfismo, temos $g_m^{-1} \in \mathcal{G}$. Assim $X \subseteq \bigcup_{g \in \mathcal{G}} g(U)$.

Como X é um fechado de M, que é compacto, temos que X também é compacto. Logo qualquer cobertura de X em abertos possui uma subcobertura finita. Isso nos garante um $\mathcal{H} \subseteq \mathcal{G}$ finito tal que $X \subseteq \bigcup_{h \in \mathcal{H}} h(U)$ ($g(U)$ são abertos, pois g é homeomorfismo). □

Por último, um resultado em análise importante para nossa demonstração.

Lema 2.11 (Número de Lebesgue)**.** *Seja X um compacto em um espaço métrico (M,d) e $U_1, \ldots, U_k$ uma cobertura aberta finita de X. Então existe um $\delta > 0$ tal que para todo $x \in X$ a bola $B_\delta(x)$ está totalmente contida em algum U_i da cobertura.*

Demonstração. Dado um $x \in X$, seja U_i um aberto da cobertura que contém x. Por U_i ser aberto, existe um $\delta_x > 0$ tal que $B_{2\delta_x}(x) \subset U_i$. Faça isso para todo $x \in X$. É fácil ver que

$$X \subseteq \bigcup_{x \in X} B_{\delta_x}(x).$$

Do fato de X ser compacto, existe uma subcobertura finita dessa cobertura, que chamaremos de $V_1, \ldots, V_t$ onde $V_j = B_{\delta_{x_j}}(x_j)$. Seja $\delta = \min\{\delta_{x_j} : 1 \le j \le t\}$. Afirmamos que esse δ funciona.

Dado $x \in X$, existe x_j tal que $x \in B_{\delta_{x_j}}(x_j)$. Agora como $\delta \le \delta_{x_j}$ temos que $B_\delta(x) \subset B_{2\delta x_j}(x_j)$. Porém, pela escolha de δ_{x_j}, existe um U_i da cobertura inicial tal que $B_{2\delta x_j}(x_j) \subset U_i$ e logo $B_\delta(x) \subset U_i$, como queriamos. □

Podemos agora começar a prova do Teorema 2.6.

Demonstração do Teorema 2.6. Façamos a demonstração por indução em r. Na nossa hipótese de indução vamos ser um pouco mais fortes do que no enunciado do teorema. Vamos supor que dado X conjunto minimal de $\mathcal{A}$ e $\epsilon > 0$, existe $x \in X$ e $n \in \mathbb{N}^*$ tal que $d(T_i^n(x), x) < \epsilon$, para todo i. Ou seja, cada conjunto minimal fechado, que é $\mathcal{G}$ invariante, possui solução. Primeiro vamos provar o caso base $r = 1$, ou seja, quando temos apenas um homeomorfismo, que chamaremos de T. Para isso modificaremos levemente os resultados mostrados antes da demonstração. Dado X conjunto minimal de $\mathcal{A}$ defina $\mathcal{B} = \{Y \subseteq M : Y \neq \varnothing, Y \subseteq X, Y \text{ fechado e } T(Y) \subseteq Y\}$, o conjunto dos fechados de M invariantes por T (Note que não queremos que seja invariante pelo grupo de homomorfismos gerado por T). Defina também para $x \in M$, $O^+(x) = \{T^n(x) : n > 0\}$ uma espécie de órbita de x. Note que $X \in \mathcal{B}$ pois X é invariante pelo grupo gerado por T e logo por T.

Podemos de maneira análoga a afirmação 2.8 e 2.9 mostrar que $\mathcal{B}$ possui um elemento minimal X' e que $X' = \overline{O^+(x)}$ para $x \in X'$. A necessidade de fazer essas modificações ficam claras agora. Suponha que $x \in O^+(x)$. Então isso significa que existe um $n \in \mathbb{N}^*$ tal que $T^n(x) = x$ e logo $d(T^n(x), x) = 0 < \epsilon$ e terminamos. Agora se $x \notin O^+(x)$, como $x \in X' = \overline{O^+(x)}$, segue que $x = \lim_{k\to\infty} T^{n_k}(x)$ com $n_k \to \infty$ (e aqui aparece a necessidade de considerarmos $O^+(x)$, queremos que n_k seja positivo). Agora a última passagem basicamente nos diz que dado $\epsilon > 0$ existe $n \in N^*$ tal que $d(T^n(x), x) < \epsilon$. Note que no caso $r = 1$ conseguimos na verdade demonstrar a afirmação para todo $x \in X' \subseteq X$, o que na verdade pode não significar muito se X' for um ponto. Também note que do modo que definimos $O^+(x)$ não necessitamos que T seja um homeomorfismo, apenas que seja contínua.

Agora vamos para o passo indutivo. Suponha que provamos o teorema para menos do que r homeomorfismos, queremos provar para r homeomorfismos. Dado X conjunto minimal de $\mathcal{A}$ defina $\Delta^r = \{x \in X^r : x_i = x_j, \forall i,j\}$ a diagonal de X^r. Por convenção chamaremos de $\overline{x} \in \Delta^r$ o vetor tal que $\overline{x}_i = x$, para todo $1 \leq i \leq r$ ($\overline{x} = (x,\ldots,x)$). Defina também uma métrica ρ em X^r tal que $\rho(x,y) = \max\{d(x_i,y_i) : 1 \leq i \leq r\}$. Seja $F : X^r \to X^r$ dada por

$$F(x_1,x_2,\ldots,x_r) = (T_1(x_1), T_2(x_2), \ldots, T_r(x_r)).$$

O que queremos mostrar é que dado um $\epsilon > 0$, existe um ponto $\overline{x} \in \Delta^r$ e $n \in \mathbb{N}^*$ tal que $\rho(F^n(\overline{x}),\overline{x}) < \epsilon$.

Dividiremos a prova em algumas partes. Primeiro vamos provar que dado $\epsilon > 0$, existem $\overline{x},\overline{y} \in \Delta^r$ e $n \in \mathbb{N}^*$ tal que $\rho(F^n(\overline{x}),\overline{y}) < \epsilon$. Considere os $r-1$ homeomorfismos $T_1 \circ T_r^{-1}, \ldots, T_{r-1} \circ T_r^{-1}$. Seja $\mathcal{G}'$ o grupo dos homeomorfismos gerados por esses $r-1$ homeomorfismo. É fácil ver que $\mathcal{G}' \subseteq \mathcal{G}$ e logo X é $\mathcal{G}'$ invariante. Seja X'' um fechado minimal de M tal que $X'' \subseteq X$ e X'' é invariante sobre $\mathcal{G}'$ (ele existe pela afirmação 2.8). Por hipótese de indução existe $y \in X''$ e $n \in \mathbb{N}^*$ tal que $d(y,(T_i \circ T_r^{-1})^n(y)) = d(y, T_i^n \circ T_r^{-n}(y)) < \epsilon$ para todo $1 \leq i \leq r-1$ (usamos aqui que T_i's comutam). Se fizermos $x = T_r^{-n}(y)$ temos que $d(T_i^n(x),y) < \epsilon$, para $1 \leq i \leq r-1$ e $d(T_r^n(x),y) = d(y,y) = 0$. Assim $\rho(F^n(\overline{x}),\overline{y}) < \epsilon$.

Segundo vamos provar que dado $\epsilon > 0$ e $\overline{y} \in \Delta^r$ existe $\overline{x} \in \Delta^r$ e $n \in \mathbb{N}^*$ tal que $\rho(F^n(\overline{x}),\overline{y}) < \epsilon$. Seja $U = B_\epsilon(y)$, pelo lema 2.10 existe um subconjunto finito $\mathcal{H} \subset \mathcal{G}$ tal que

$$X \subseteq \bigcup_{h \in \mathcal{H}} h(U).$$

Isto é, $\{h(U)\}_{h\in\mathcal{H}}$ é uma cobertura aberta finita de X. Pelo lema do número de Lebesgue (lema 2.11) existe um $\delta > 0$ tal que toda bola de raio δ está contida em algum $h(U)$. Fixe esse δ. O parágrafo anterior nos diz que conseguimos $\overline{w},\overline{z} \in \Delta^r$ e $n \in \mathbb{N}^*$ tal que $\rho(F^n(\overline{w}),\overline{z}) < \delta$. Então existe $h \in \mathcal{H}$ tal que $T_i(w) \in B_\delta(z) \subset h(U)$, ou seja, $(h^{-1} \circ T_i^n)(w) \in U$, para todo $1 \leq i \leq r$. Usando da comutatividade de $\mathcal{G}$ obtemos $d(T_i^n(h^{-1}(w)),y) < \epsilon$, para todo $1 \leq i \leq r$. Logo o ponto $\overline{x} \in \Delta^r$, onde $\overline{x}_i = h^{-1}(w)$ é tal que $\rho(F^n(\overline{x}),\overline{y}) < \epsilon$.

Agora por meio de uma série de iterações dos resultados anteriores terminaremos a demonstração. Seja z_0 um ponto qualquer em X. Dado $\epsilon_0 > 0$, pelo resultado do parágrafo anterior existe $z_1 \in X$ e $n_1 \in \mathbb{N}^*$ tal que $\rho(F^{n_1}(\overline{z_1}),\overline{z_0}) < \epsilon_0$. Mais do que isso, da continuidade de F, e consequentemente de F^{n_1}, existe um $\epsilon_1 < \epsilon_0$ tal que para todo $w \in X^r$ com $\rho(w,\overline{z_1}) < \epsilon_1$ vale que $\rho(F^{n_1}(w), F^{n_1}(\overline{z_1})) < \delta_1$ e daí

$$\rho(F^{n_1}(w),\overline{z_0}) \leq \rho(F^{n_1}(w), F^{n_1}(\overline{z_1})) + \rho(F^{n_1}(\overline{z_1}),\overline{z_0}) < \epsilon_0$$

desde que δ_1 seja muito pequeno ($0 < \delta_1 < \epsilon_0 - \rho(F^{n_1}(\overline{z_1}),\overline{z_0})$).

Podemos recursivamente definir z_k, ϵ_k e n_k dessa forma. Suponha que todos os z_i's, ϵ_i's e n_i's de índices menores já foram definidos. Seja $z_k \in X$ e $n_k \in \mathbb{N}^*$ tais que $\rho(F^{n_k}(\overline{z_k}),\overline{z_{k-1}}) < \epsilon_{k-1}$ (esses valores existem pelo resultado de um parágrafo anterior). Pela continuidade de F^{n_k}, podemos escolher um $\epsilon_k < \epsilon_{k-1}$ tal que para $w \in X^r$, $d(w,z_k) < \epsilon_k$ implica $\rho(F^{n_k}(w), F^{n_k}(z_k)) < \delta_k$. E escolhendo δ_k muito pequeno temos também que

$$\rho(F^{n_k}(w),\overline{z_{k-1}}) \leq \rho(F^{n_k}(w), F^{n_k}(\overline{z_k})) + \rho(F^{n_k}(\overline{z_k}),\overline{z_{k-1}}) < \epsilon_{k-1}$$

para estes valores de w.

Uma observação crucial da construção dessa sequência é que para $a,b \in \mathbb{N}$ com $a < b$ vale que $\rho(F^{n_{a+1}+\ldots+n_b}(\overline{z_b}),\overline{z_a}) < \epsilon_a$. Para mostrarmos isso, vamos demonstrar o fato mais forte de que se $w \in X^r$ é tal que $\rho(w,\overline{z_b}) < \epsilon_b$ então $\rho(F^{n_{a+1}+\ldots+n_b}(w),\overline{z_a}) < \epsilon_a$. Esse resultado sai por indução no tamanho de $b-a$. Se $b-a = 1$ o resultado é exatamente a forma como ϵ_b é definido, logo não há o que fazer. Para os demais casos note que se $\rho(w,\overline{z_b}) < \epsilon_b$, então $\rho(F^{n_b}(w),\overline{z_{b-1}}) < \epsilon_{b-1}$ e que pela hipótese de indução $w' \in X^r$ satisfazendo $\rho(w',\overline{z_{b-1}}) < \epsilon_{b-1}$ implica $\rho(F^{n_{a+1}+\ldots+n_{b-1}}(w'),\overline{z_a}) < \epsilon_a$. Aplicando isso para $w' = F^{n_b}(w)$ obtemos o resultado desejado.

Considere a cobertura $\{B_{\epsilon_0/2}(x)\}_{x\in X}$ aberta de X. Como X é compacto essa cobertura possui uma subcobertura finita. Do princípio da casa dos pombos existem dois elementos z_a, z_b da sequência que estão no mesmo aberto da subcobertura e logo $d(z_a,z_b) < \epsilon_0$. Porém, supondo $a < b$ a nossa observação do parágrafo anterior nos diz que $\rho(F^{n_{a+1}+\ldots+n_b}(\overline{z_b}),\overline{z_a}) < \epsilon_a < \epsilon_0$. Daí $\rho(F^{n_{a+1}+\ldots+n_b}(\overline{z_b}),\overline{z_b}) < 2\epsilon_0$. Fazendo $\epsilon_0 < \epsilon/2$, $n = n_{a+1} + \ldots + n_b$ e $x = z_b$ obtemos que $\rho(F^n(\overline{x}),\overline{x}) < \epsilon$, para todo i, como queríamos.

□

◇ ◇ ◇ *Aula 6 (23 de Maio) — Marcelo Soares Campos* ◇ ◇ ◇

A aula dessa semana foi o resto da demonstração do teorema 2.6.

3 Ramsey Online

◇ ◇ ◇ *Aula 7 (30 de Maio) — Marcelo Sales* ◇ ◇ ◇

Vamos interpretar o teorema de Ramsey como um jogo. Os dois jogadores desse jogo são o *construtor* e o *pintor*. As suas funções são meio que auto explicativas o construtor constrói um grafo e o pintor pinta este grafo com um conjunto de cores pré-determinado. Ao longo dessa seção vamos considerar que o pintor dispõe de apenas duas cores: vermelho e azul.

Na versão original de Ramsey o jogo é bem simples. Dado um grafo H determinado préviamente pelos dois jogadores, construtor vence o jogo se fornecer um grafo G que independente da pintura possui uma cópia de H monocromático. Pintor vence se ele conseguir uma pintura sem cópias monocromáticas de H. Nesse contexto o teorema de Ramsey pode ser enunciado como

Teorema 3.1 (Ramsey)**.** *Para qualquer grafo H, construtor possui uma estratégia vencedora.*

Agora ao invés de fornecer o grafo completo, construtor poderia fornecer aresta por aresta e perguntar a pintor como ele gostaria de colorir as arestas. Essa versão do jogo, um pouco mais dinâmica, é chamada de a versão online de Ramsey. Mais formalmente, no jogo de Ramsey Online a cada rodada construtor constrói uma aresta e pintor colore essa exata aresta com uma das duas cores a sua disposição. Porém quando terminar? O natural seria terminar quando construtor consegue forçar uma cópia monocromática de H e se ele não conseguir, pintor seria o vencedor. Infelizmente, dessa forma pintor só vence se a partida nunca terminar, o que não é algo factível no mundo real. Uma forma de consertar isso é adicionando a seguinte regra ao jogo: Na primeira rodada, antes de construir uma aresta, construtor deve fornecer um número finito de vértices onde o jogo será jogado (esse número pode depender do grafo H previamente dado). Dessa maneira, construtor vence se ele consegue nesse conjunto de vértices forçar pintor a colorir uma cópia moncromática de H e pintor vence caso ao esgotar as arestas não exista essa cópia monocromática.

Note que essa versão online é mais fraca do que a versão original do jogo de Ramsey, no sentido que se construir um grafo G na versão original garantia a vitória, então na versão online também garantirá. Tendo em vista isso, para podermos tornar o jogo mais interessante restringiremos o universo dos grafos que construtor pode construir. No caso dessa aula estamos interessados em restringir os grafos de acordo com o número cromático.

Então podemos fazer a seguinte pergunta: Dado um grafo H, qual o menor inteiro $f(H)$ tal que construtor pode vencer o jogo construindo apenas grafos com número cromático no máximo $f(H)$? É simples ver que $f(H) \geq \chi(H)$, pois para o construtor forçar uma cópia de H monocromática ele precisa pelo menos construir uma cópia de H e portanto o grafo final que o construtor construiu tem número cromático pelo menos $\chi(H)$.

O teorema principal da aula de hoje mostra que de fato $f(H) = \chi(H)$, ou em outras palavras

Teorema 3.2 (Grytczuk, Hałuszczak e Kierstead)**.** *Construtor consegue forçar qualquer grafo de número cromático q, construido apenas grafos com número cromático no máximo q.*

Para provarmos esse teorema vamos usar dois resultados conhecidos da teoria de Ramsey, o primeiro é o teorema de Ramsey para hipergrafos, que omitiremos a prova.

Teorema 3.3 (Ramsey para hipergrafos)**.** *Sejam $k, m > 0$ inteiros. Existe $R^{(k)}(m)$ tal que para todo $n \geq R^{(k)}(m)$ toda 2-coloração de $\binom{[n]}{k}$ contém um conjunto $M \in \binom{[n]}{m}$ monocromático, isto é, todo $S \in \binom{[n]}{k}$ em M é da mesma cor.*

O segundo resultado é o que chamamos de teorema de Ramsey Bipartido.

Teorema 3.4 (Ramsey Bipartido)**.** *Seja $t > 0$ inteiro. Existe $B(t)$ inteiro tal que para todo $n \geq B(t)$ toda 2-coloração de $K_{n,n}$ contém um $K_{t,t}$ monocromático.*

Demonstração. Tome $B(t) = t \cdot 2^{2t}$ e suponha $n \geq B(t)$. Sejam A, B as partições de $K_{n,n}$ e considere uma coloração nesse grafo. Escolha $2t$ pontos de A e chame eles de $x_1, \ldots, x_{2t}$. Defina uma função

$\phi : B \to \{0,1\}^{2t}$ que associa a cada ponto $b \in B$ um vetor $\phi(b)$ de tamanho $2t$ tal que

$$\phi(b)_i = \begin{cases} 0 & \text{se a aresta } \{x_i, b\} \text{ for da cor azul} \\ 1 & \text{se a aresta } \{x_i, b\} \text{ for da cor vermelha} \end{cases}$$

Como existem apenas 2^{2t} imagens possíveis para essa função e $|B| \geq t \cdot 2^{2t}$, pelo princípio da casa dos pombos existem pelo menos t pontos $y_1, \ldots, y_t \in B$ tais que $\phi(y_1) = \ldots = f(y_t)$. Sejam $I_0 \subset [2t]$ os índices i tais que $\phi(b)_i = 0$ e I_1 os índices i tais que $\phi(b)_i = 1$. É fácil ver que $(\{x_i\}_{i\in I_0}, \{y_j\}_{j\in[t]})$ e $(\{x_i\}_{i\in I_1}, \{y_j\}_{j\in[t]})$ são grafos bipartidos moncromáticos. Do fato que $I_0 \cup I_1$ é uma bipartição de $[2t]$ segue que algum dos dois contém pelo menos t elementos. Suponha sem perda de generalidade que $|I_0| \geq t$, assim $(\{x_i\}_{i\in I_0}, \{y_j\}_{j\in[t]})$ contém um $K_{t,t}$ monocromático. □

Uma observação é que os dois últimos teoremas possuem versões para qualquer número de cores, mas para o nosso objetivo isso não será necessário.

Primeiro usaremos o Teorema 3.4 para reduzir o problema original ao caso em que H é um grafo completo. Dado um grafo G, denotaremos por G^t o grafo obtido substituindo todos os vértices por conjuntos independentes de tamanho t, e todas as arestas por grafos bipartidos completos entre os dois conjuntos independentes correspondentes aos vértices das arestas. O grafo G^t é o blow-up de tamanho t de G. É fácil ver da forma que esse grafo é construido que $\chi(G^t) = \chi(G)$. Basta colorir todos os vértices do mesmo conjunto em G^t com a cor correspondente ao vértice desse conjunto em G.

Lema 3.5. *Se $t > 0$, então $f(H^t) \leq f(H)$.*

Demonstração. Seja $n := n(H)$ o número de vértices que construtor necessita para vencer o jogo de Ramsey online em H e seja m o menor número de arestas necessárias para garantir uma cópia monocromática de H nesse jogo (com certeza $m \leq \binom{n}{2}$). Então afirmamos que construtor consegue vencer o jogo usando no máximo $nB^{(m)}(t)$ vértices ($B^{(m)}(t)$ significa B aplicada m vezes sobre t).

Para isso considere o grafo vazio G_0 em que construtor irá jogar, divida os vértices desse grafo em n conjuntos $V_{i,0}$ todos de tamanho $B^{(m)}(t)$. Também considere um grafo auxiliar vazio Q_0 de n vértices $\{x_1, \ldots, x_n\}$.

Vamos mostrar como construtor deve proceder recursivamente. Por hipótese, construtor possui uma estratégia vencedora para H utilizando no máximo n vértices. Jogaremos essa estratégia no grafo Q_0. Suponha que o primeiro movimento seja construir a aresta $\{x_i, x_j\}$, então construiremos em G_0 o grafo bipartido completo entre $V_{i,0}$ e $V_{j,0}$. Pintor fará alguma coloração sobre essas arestas, o Teorema 3.4 nos garante que independente da coloração existirá um $K_{B^{(m-1)}(t),B^{(m-1)}(t)}$ monocromático nesse grafo bipartdo. Então construtor pintará a aresta $\{x_i, x_j\}$ de Q_0 da mesma cor desse $K_{B^{(m-1)}(t),B^{(m-1)}(t)}$ e chamará esse novo grafo de Q_1. Em G_0 construtor fará $V_{i,1}$ e $V_{j,1}$ os conjuntos em $V_{i,0}$ e $V_{j,0}$ correspondentes a esse $K_{B^{(m-1)}(t),B^{(m-1)}(t)}$ monocromático. Para os demais conjuntos $V_{k,0}$ selecionará $B^{(m-1)}(t)$ vértices quaisquer e chamará de $V_{k,1}$. O grafo obtido após essa redução de vértices será G_1. Note que G_1 consiste de n conjuntos independentes de tamanho $B^{(m-1)}(t)$ tal que pares de conjuntos independentes correspondentes a vértices de uma aresta colorida de Q_1 formam um grafo bipartido completo monocromático da mesma cor dessa aresta.

Agora suponha que estamos na r-ésima rodada do jogo. Recebemos grafos Q_{r-1} e G_{r-1} onde Q_{r-1} possui $r-1$ arestas coloridas e G_{r-1} é o grafo com n conjuntos independentes de tamanho $B^{(m-r+1)}(t)$ e onde cada par de conjuntos independentes correspondentes a vértices de uma aresta colorida em Q_{r-1} formam um grafo bipartido completo monocromático de mesma cor que essa aresta. Procedemos de forma análoga a da primeira rodada. Em Q_{r-1}, construtor possui uma estratégia vencedora e ela é construir a aresta $\{x_a, x_b\}$. Em G_{r-1} construiremos o grafo bipartido completo saindo de $V_{a,r-1}$ e $V_{b,r-1}$. Pintor fará alguma coloração sobre essas arestas e pelo Teorema 3.4 garantimos a existência de um $K_{B^{(m-r)}(t),B^{m-r}(t)}$ monocromático. Construtor pinta $\{x_a, x_b\}$ com a cor desse grafo bipartido e chama Q_r esse novo grafo. As partições desse grafo bipartido monocromático serão os $V_{a,r}$ e $V_{b,r}$. Para os outros $V_{k,r-1}$ apenas escolha um subconjunto de tamanho $B^{(m-r)}(t)$ para ser $V_{k,r}$. O grafo obtido após essa redução será G_r. Dessa forma, G_r consiste de n conjuntos independentes de tamanho $B^{(m-r)}(t)$ onde cada par de conjuntos independentes correspondentes a vértices de uma aresta de Q_r formam um grafo bipartido completo monocromático de mesma cor que essa aresta.

Após $p \leq m$ rodadas o jogo termina para H e em Q_p possuimos uma cópia monocromática de

H. Logo em G_p possuímos uma cópia monocromática de $H^{B(m-p)(t)}$. Como $B^{(0)}(t) = t$ segue que $H^t \subset H^{B(m-p)(t)}$. Por fim, é fácil ver que $\chi(G_p) = \chi(Q_p)$ e portanto $f(H^t) \leq f(H)$. □

O próximo lema garante o caso em que H é completo.

Lema 3.6. *Existe um inteiro $n(a,b,k)$ tal que para todos inteiros $2 \leq a, b \leq k$, Construtor consegue com $n(a,b,k)$ vértices forçar Pintor a colorir ou um K_a azul ou um K_b vermelho apenas construindo grafos com número cromático menor ou igual a k.*

Demonstração. Procederemos por uma indução dupla. Primeiro em k e para cada k fixo, na soma $a+b$. Note que $n(2,i,k) = n(i,2,k) = i$, pois para estes casos basta construir um K_i.

Para o caso geral afirmamos que $n(a,b,k) = s(a,b,k) + t(a,b,k)$ onde

1. $s(a,b,k) = 2^{k-1}\binom{t(a,b,k)}{k-1} n(a-1,b-1,k-1)$
2. $t(a,b,k) = R^{(k-1)}(u(a,b,k))$
3. $u(a,b,k) = \max\{n(a-1,b,k), n(a,b-1,k)\}$

lembrando que $R^{(k-1)}(u)$ é o número de Ramsey para $(k-1)$-grafos obtido no Teorema 3.3.

Seja $T = [t]$ e $S = \binom{[t]}{k-1} \times [2^{k-1} n(a-1,b-1,k-1)]$ dois conjuntos independentes de vértices de tamanho t e s, respectivamente. Construtor inicialmente construirá arestas entre S e T. Para cada $(X,i) \in S$, ele construirá arestas $\{(X,i), j\}$ onde $j \in X$. Dessa forma temos um grafo bipartido que todos os vértices de S possuem grau $(k-1)$. Iremos construir agora um grafo ou em S, ou em T (não em ambos).

Note que se construirmos um grafo F em T com $\chi(F) = k$, então o nosso grafo terá número cromático k. De fato, podemos colorir os vértices de T com k cores, pois $\chi(F) = k$. Para cada vértice $s \in S$ ele possui apenas $k-1$ vizinhos em T. Isso significa que existe uma cor que não está nos vizinhos de s. Colorimos s com essa cor. Fazendo isso o nosso grafo é k-colorível. Também note que se construirmos um grafo F em S com $\chi(F) = k-1$, então o nosso grafo será k-colorível. Basta colorir os vértices de S com $k-1$ cores e todos os vértices de T com a cor que falta.

Agora para determinar onde vamos construir o que, vamos observar o conjunto de vértices $S_X = \{(X,i) \in S : i \in [2^{k-1} n(a-1,b-1,k-1)]\}$. Suponha que após Pintor colorir todas as arestas S_X não possua um vértice em que todas as arestas incidentes sejam monocromáticas. Para cada vértice $s \in S_X$ note que $N(s) = X$ e logo podemos associar uma função $\phi : S_X \to \{0,1\}^X$ dada por

$$\phi(s)_j = \begin{cases} 0 & \text{se a aresta } \{s,j\} \text{ é da cor azul} \\ 1 & \text{se a aresta } \{s,j\} \text{ é da cor vermelha} \end{cases}, \quad \forall s \in S_X,\ j \in X.$$

Como $|X| = k-1$ existem no máximo 2^{k-1} possíveis imagens de ϕ. Assim, pelo principio da casa dos pombos e por $|S_X| = 2^{k-1} n(a-1,b-1,k-1)$ existem pelo menos $n(a-1,b-1,k-1)$ vértices em S_X com a mesma imagem. Seja $Y \subset S_X$ o conjunto desses vértices e $v \in \{0,1\}^X$ a imagem desses valores. Agora observe que $v \notin \{(0,0,\ldots,0),(1,1,\ldots,1)\}$, pois esse dois valores correspondem a um vértice em S_X cuja as arestas incidentes são monocromáticas, o que por suposição não existe. Então existem vértices $p,q \in X$ tais que $v_p = 0$ e $v_q = 1$. Isso significa que todas as arestas da forma $\{s,p\}$, com $s \in Y$, são azuis e todas as arestas da forma $\{s,q\}$, com $s \in Y$, são vermelhas.

Pela hipótese de indução, do fato de $|Y| \geq n(a-1,b-1,k-1)$, podemos construir um grafo F em Y que force o Pintor ou a colorir um K_{a-1} azul, ou um K_{b-1} vermelho com $\chi(F) \leq k-1$. Se temos um K_{a-1} azul, unindo com o vértice p obtemos um K_a azul. Se temos um K_{b-1} vermelho, unindo com o vértice q obtemos um K_b vermelho. Assim, inevitavelmente conseguimos ou um K_a azul, ou um K_b vermelho e como já vimos, o grafo final é k-colorível.

Então para todo $X \in \binom{[t]}{k-1}$, o conjunto $S_X \subset S$ possui um vértice cuja arestas incidentes são monocromáticas. Pinte X dessa cor. Assim obtemos uma 2-coloração de $\binom{[t]}{k-1}$. Do fato de $t = R^{(k-1)}(u)$, pelo Teorema 3.3 existe um conjunto U de tamanho u monocromático. Suponha que U seja monocromático de cor azul, então como $u \geq n(a-1,b,k)$ podemos por hipótese de indução construir um grafo F em U, com $\chi(F) \leq k$, que força Pintor a colorir um K_{a-1} azul, ou um K_b vermelho. Se temos um K_b vermelho terminamos. Se temos um K_{a-1} azul, então seja $Z \in \binom{U}{k-1}$ uma $(k-1)$-upla que contém esse K_{a-1} azul ($a-1 \leq k-1$). Da escolha de U, existe um ponto em S que liga para todos os vértices de Z com arestas

azuis, logo unindo esse vértice ao K_{a-1} obtemos um K_a azul. O caso em que U é monocromático de cor vermelha é análogo (pois $u \geq n(a, b-1, k)$). Como já vimos, o grafo total após adicionar F é k-colorível e terminamos. □

A demonstração do teorema agora é simples

Demonstração do Teorema 3.2. Dado um grafo H com $\chi(H) = q$, é fácil ver que $H \subset K_q^{v(H)}$ e então $f(H) \leq f(K_q^{v(H)})$. Mas pelo Lema 3.5 temos que $f(K_q^{v(H)}) \leq f(K_q)$ e o Lema 3.6 nos garante que existe um $n(q, q, q)$, ou melhor, que $f(K_q) = q$. Juntando tudo obtemos que $f(H) \leq q$, isto é, que construtor vence construindo apenas grafos q-coloríveis. □

4 O método polinomial

◇ ◇ ◇ *Aula 8 (06 de Junho) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Nesta seção falaremos sobre o método polinomial. Em geral, esse método consiste de representar algum conjunto, normalmente de origem geométrica, como raízes de polinômios. Ao estudarmos os zeros desses polinômios conseguimos cotas para os conjuntos. Vamos estudar isso atráves de alguns exemplos, começando hoje pelos conjuntos de Kakeya e Nikodym.

O problema de Kakeya pode ser enunciado da seguinte forma. Dizemos que um conjunto $S \in \mathbb{R}^2$ é um conjunto de *Kakeya* se S contém um segmento unitário em todas as direções possíveis. Por exemplo, o disco fechado de raio 1/2 é um conjunto de Kakeya. Uma pergunta interessante é qual a menor área possível para S? Besicovitch mostrou que existem conjuntos de Kakeya de medida zero, o que é um resultado impressionante.

O problema de Nikodym é muito próximo a esse. Dizemos que um conjunto $N \in [0,1]^2$ é *Nikodym* se para todo $x \in [0,1]^2$, existe uma reta L passando por x tal que $L \cap N \subset \{x\}$. Não é muito difícil ver que uma reta, por exemplo a reta $y = x$ é um conjunto de Nikodym. A pergunta aqui seria qual a maior área possível para esse conjunto N? Nikodym mostrou que existem conjuntos N de medida um, o que também é um resultado supreendente.

Para assemelhar mais ainda ao problema de Kakeya podemos reescrever o problema de Nikodym de outra forma. Chamamos um conjunto $C \in [0,1]^2$ de *CoNikodym* se para todo $x \in [0,1]^2$, existe uma reta L passando por x tal que $L \setminus \{x\} \subset C$. É fácil ver dessa definição que C é o complementar de um conjunto de Nikodym. Poderíamos ai perguntar qual a menor area possível para um conjunto C. O que Nikodym mostrou é que existem conjuntos Conikodym de medida zero.

Os dois problemas já sao muito interessantes por si só, mas nessa seção estamos interessados em uma versão mais discreta desses problemas. Seja $\mathbb{F}_q$ um corpo finito de ordem q. Dados $a, b \in \mathbb{F}_q^n$ chame de $L_{a,b}$ a seguinte reta

$$L_{a,b} = \{at + b : t \in \mathbb{F}_q\}.$$

Podemos definir um conjunto $S \in \mathbb{F}_q^n$ de *Kakeya* se S contém uma reta em todas as direções, isto é, para todo $a \in \mathbb{F}_q^n$, existe um $b \in \mathbb{F}_q^n$ tal que $L_{a,b} \subset S$. Da mesma forma podemos definir um conjunto $C \in \mathbb{F}_q^n$ de *CoNikodym* se para todo ponto $b \in \mathbb{F}_q^n$, existe uma reta que, tirando possivelmente esse b, está totalmente contida em C. Em outras palavras, existe um $a \in \mathbb{F}_q^n$ tal que $L_{a,b} \setminus \{b\} \subset C$. Queremos saber quão pequenos esses conjuntso podem ser. Como são conjuntos finitos em corpos finitos, podemos naturalmente introduzir uma densidade $d(X) = \frac{|X|}{q^n}$ para conjuntos $X \in \mathbb{F}_q^n$. Com essa densidade, podemos perguntar se dado n, existe $X \in \mathbb{F}_q^n$ com X Kakeya ou CoNikodym, tal que $d(X) \to 0$, quando $q \to \infty$?

O intuito da aula de hoje é mostrar que não existe esse X. Ou seja, diferente do caso contínuo, na versão discreta se um conjunto é CoNikodym ou Kakeya ele não pode ser arbitrariamente pequeno. Isso se traduz nos dois teoremas a seguir

Teorema 4.1 (Dvir, 2008)**.** *Se $C \in \mathbb{F}_q^n$ é CoNikodym, então*

$$|C| \geq (\frac{1}{3n})^n q^n.$$

Teorema 4.2 (Dvir, 2008). *Se $S \in \mathbb{F}_q^n$ é Kakeya, então*

$$|S| \geq \frac{1}{2n^n} q^n.$$

A demonstração dos dois teoremas se baseiam no método polinomial. Vamos agora introduzir as duas técnicas utilizadas para atacar esses problemas. Para a primeira usaremos de um aquecimento.

Exercício 4.3. Dado o conjunto $A = \{(i, 2^i) : 1 \leq i \leq 10^6\}$ e um polinômio $p \in \mathbb{R}[X, Y]$ tal que $p(x, y) = 0$ para todo $(x, y) \in A$, quão pequeno pode ser ∂p (grau de p)?

Uma possível tentativa é o polinômio $q(x, y) = \prod_{i=1}^{1} 0^6(x - i)$, porém esse polinômio tem grau 10^6 que ainda é um pouco grande. O próximo resultado nos ajudará um pouco com isso. Dado um corpo $\mathbb{F}$ (não necessariamente finito), defina $Poly_D(\mathbb{F}^n)$ como o conjunto dos polinômios de n variáveis em $\mathbb{F}$ com grau menor ou igual a D. Observe que um polinômio de n variáveis é a soma de varios monômios da forma $cx_1^{e_1} \dots x_n^{e_n}$ e dizemos que o grau desse monômio é $e_1 + \dots + e_n$, assim o grau de um polinômio é o maior grau dentre os seus monômios.

Lema 4.4 (Contagem de Parâmetros). *Seja $S \in \mathbb{F}^n$ um conjunto de pontos tal que $|S| \leq \binom{n+D}{n}$, então existe polinômio $f \in Poly_D(\mathbb{F}^n)$, $f \neq 0$ tal que $f(x) = 0$ para todo $x \in S$.*

Demonstração. Seja $|S| = s$ e $S = \{x_1, \dots, x_s\}$. Considere a aplicação $\Phi : Poly_D(\mathbb{F}^n) \to \mathbb{F}^s$ dada por $\Phi(f) = (f(x_1), \dots, f(x_s))$. Note que a aplicação Φ é uma aplicação linear. De fato, $\Phi(f + g) = ((f + g)(x_1), \dots, (f + g)(x_s)) = (f(x_1), \dots, f(x_s)) + (g(x_1), \dots, g(x_s)) = \Phi(f) + \Phi(g)$ e que dado λ escalar vale $\Phi(\lambda f) = (\lambda f(x_1), \dots, \lambda f(x_s)) = \lambda(f(x_1), \dots, f(x_s)) = \lambda\Phi(f)$.

Note agora que $Poly_D(\mathbb{F}^n)$ é um espaço vetorial de dimensão $\binom{n+D}{n}$. Uma maneira de ver isso é notando que uma base desse espaço consiste dos monômios da forma $x_1^{e_1} \dots x_n^{e_n}$ onde $e_1 + \dots + e_n \leq D$. Agora considere D bolas enfileiradas e separe essas D bolas com n gravetos. Esses n gravetos criam $n + 1$ divisórias das bolas. Podemos biunivocamente associar as n primeiras divisórias com cada e_i e a última associamos com o quanto sobrou para completar D (Por exemplo, se quisermos contar o número de soluções de $e_1 + \dots + e_n = D - 3$, nessa última divisória teríamos 3 bolas). Assim o número de soluções da inequação é exatamente a quantidade de maneiras de distribuir em filas D bolas e n gravetos, o que nos dá que $\dim(Poly_D(\mathbb{F}^n)) = \binom{n+D}{n}$.

Se $s < \binom{n+D}{n}$ temos que a dimensão de $Poly_D(\mathbb{F}^n)$ é maior que a de $\mathbb{F}^s$ e como Φ é linear, segue pelo teorema do nucleo e da imagem que $\ker(\Phi) \neq \{0\}$. Em outras palavras, isso significa que existe $f \neq 0$ tal que $f(x) = 0$, para todo $x \in S$. □

Observe que $\binom{n+D}{n} > \frac{(D+1)^n}{n!} > (\frac{D+1}{n})^n$ e se tomarmos $s \leq (\frac{D+1}{n})^n$ podemos aplicar o lema anterior, assim vale o seguinte corolário.

Corolário 4.5. *Seja $S \in \mathbb{F}^n$ um conjunto de pontos e $D = \lfloor n|S|^{\frac{1}{n}} \rfloor$. Então existe um polinômio $f \in Poly_D(\mathbb{F}^n)$, $f \neq 0$, tal que $f(x) = 0$ para todo $x \in S$.*

Em particular o Corolário 4.5 nos dá uma cota bem melhor para o Exercício 4.3. Por ele podemos obter um polinômio de grau $D = 2 \cdot (10^6)^{\frac{1}{2}} = 2000$, apesar de não sabermos como é esse polinômio.

A outra técnica do método polinomial consiste nos lemas de anulamentos. Estes lemas determinam que se um polinômio se anula em muitos pontos, então ele deve ser o polinômio nulo. Para os dois problemas enunciados nessa aula o seguinte lema de anulamento é suficiente.

Lema 4.6. *Seja $\mathbb{F}_q$ um corpo finito e $f \in Poly_{q-1}(\mathbb{F}_q^n)$. Se $f(x) = 0$ para todo $x \in \mathbb{F}_q^n$, então f é o polinômio nulo.*

Demonstração. Façamos por indução em n. Para $n = 1$ o problema consiste no resultado clássico de que um polinômio não nulo de grau D zera em no máximo D valores. Suponha agora que o enunciado seja verdade para todo $k < n$ e vamos provar para n.

Podemos escrever $f(x_1, \dots, x_n)$ como um polinômio em x_n, onde os coeficientes são polinômios nas demais variáveis, isto é

$$f(x_1, \dots, x_n) = a_t(x_1, \dots, x_{n-1})x_n^t + \dots + a_1(x_1, \dots, x_{n-1})x_n + a_0(x_1, \dots, x_{n-1}).$$

onde $a_0, \ldots, a_t$ são polinômios em $x_1, \ldots, x_{n-1}$ e $t \leq q-1$. Fixe essas variáveis e deixe x_n variar. Com as demais variáveis fixas, isso é um polinômio em uma variável de grau menor ou igual a $q-1$ que zera para todo valor de $x_n \in \mathbb{F}_q$. Logo esse polinômio é nulo. Isso significa que para todo $0 \leq j \leq t$ e para todo $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_q^{n-1}$ temos $a_j(x_1, \ldots, x_{n-1}) = 0$.

Aplicando a hipótese de indução para $n-1$, temos que os polinômios $a_0, a_1, \ldots, a_t \in Poly_{q-1}(\mathbb{F}_q^{n-1})$ são todos nulos. Consequentemente f é o polinômio nulo. □

Note que o último lema é forte no sentido que existem polinômios de grau q que zeram em todo $\mathbb{F}_q^n$. Como exemplo, tome $f(x_1, \ldots, x_n) = x_1^q - x_1 \neq 0$. Podemos também obter o seguinte lema de anulamento mais geométrico.

Lema 4.7. *Dado $\mathbb{F}$ um corpo qualquer, seja $L_{a,b} = \{at + b : a, b \in \mathbb{F}^n \text{ e } t \in \mathbb{F}\}$ uma reta no $\mathbb{F}^n$ e $f \in Poly_D(\mathbb{F}^n)$ um polinômio tal que f zera em mais de D pontos da reta. Então $f(x) = 0$ para todo $x \in L_{a,b}$.*

Demonstração. Esse resultado vem do lema anterior no caso unidimensional. Fixado $a, b \in \mathbb{F}^n$ seja $g \in \mathbb{F}[t]$ um polinômio tal que $g(t) = f(at + b)$. É facil ver que $\partial g = \partial f \leq D$. De fato, seja $cx_1^{e_1} \ldots x_n^{e_n}$ um monômio de f. Aplicado a $at + b = (a_1 t + b_1, \ldots, a_n t + b_n)$ esse monômio pode ser escrito como $c(a_1 t + b_1)^{e_1} \ldots (a_n t + b_n)^{e_n}$ que tem grau $e_1 + \ldots + e_n$ em t.

Sejam $p_1, p_2, \ldots, p_{D+1} \in L_{a,b}$ pontos da reta tais que $f(p_i) = 0$ para todo $1 \leq i \leq D+1$. Podemos escrever eles como $p_i = at_i + b$ com $t_i \in \mathbb{F}$ e logo $g(t_i) = f(p_i) = 0$. Como g é um polinômio em uma variável de grau menor que D e possui pelo menos $D+1$ raízes, então g é o polinômio nulo e $f(x) = 0$ para todo $x \in L_{a,b}$. □

O objetivo agora é o seguinte: Dado um conjunto de pontos, construiremos um polinômio que zere nesse conjunto com grau determinado pela cardinalidade do conjunto (técnica de contagem de parâmetros). Usando das propriedades geométricas desse conjunto, mostraremos que o polinômio se anula em muito mais pontos do que devia. Os lemas de anulamento então garantirão que o grau do polinômio deve ser relativamente grande, obtendo assim uma cota inferior pro tamanho do conjunto. Vejamos em prática.

Demonstração do Teorema 4.1. Façamos por absurdo. Seja $C \in \mathbb{F}_q^n$ um conjunto CoNikodym com $|C| < (\frac{1}{3n})^n q^n$. Pelo Corolário 4.5, para $D = \lfloor n|C|^{\frac{1}{n}} \rfloor < n((\frac{1}{3n})^n q^n)^{\frac{1}{n}} = \frac{q}{3} < q-1$ existe um polinômio $f \in Poly_D(\mathbb{F}_q^n)$, não nulo, tal que $f(x) = 0$ para todo $x \in C$. Como D é inteiro isso significa que vale $D \leq q-2$.

A propriedade de CoNikodym nos diz que para todo $b \in \mathbb{F}_q^n$ existe um $a \in \mathbb{F}_q^n$ tal que $L_{a,b} \setminus \{b\} \subset C$. Isso significa que para todo $b \in \mathbb{F}_q^n$ existe uma reta $L_{a,b}$ tal que $f(x) = 0$ para todo $x \in L_{a,b} \setminus \{b\}$. Como $|\mathbb{F}_q| = q$, isso significa que a reta $L_{a,b}$ zera em $q-1 > D$ pontos, portanto pelo lema 4.7 temos que $f(x) = 0$ para todo $x \in L_{a,b}$. Em particular, $f(b) = 0$. Do fato de isso valer para todo $b \in \mathbb{F}_q^n$ segue que $f(x) = 0$ para todo $x \in \mathbb{F}_q^n$. Usando o lema 4.6 ($D \leq q-1$) concluimos que f tem de ser o polinômio nulo, o que é uma contradição. □

◇ ◇ ◇ *Aula 9 (20 de Junho) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Continuarmos agora com o problema de Kakeya.

Demonstração Teorema 4.2. Suponha por absurdo que exista um conjunto de Kakeya $S \in \mathbb{F}_q^n$ com $|S| < \frac{1}{2n^n} q^n$. Pelo Corolário 4.5, para $D = \lfloor n|S|^{\frac{1}{n}} \rfloor < n(\frac{1}{2n^n} q^n)^{\frac{1}{n}} = \frac{1}{2^{\frac{1}{n}}} q < q$ existe um polinômio $f \in Poly_D(\mathbb{F}_q^n)$, $f \neq 0$, tal que $f(x) = 0$ para todo $x \in S$. Como D é inteiro, segue que $D \leq q-1$.

A propriedade de Kakeya nos diz que para todo $a \in \mathbb{F}_q^n$ existe $b \in \mathbb{F}_q^n$ tal que $L_{a,b} \subset S$. Fixe $a \in \mathbb{F}_q^n$. Existe reta $L_{a,b} \subset S$, ou seja, reta $L_{a,b}$ tal que $f(x) = 0$ para todo $x \in L_{a,b}$. Como visto na demonstração do Lema 4.7, se considerarmos $g(t) = f(at + b)$ o polinômio unidimensional correspondente a essa reta, temos que g é o polinômio nulo.

Para obtermos mais precisamos analisar cuidadosamente o polinômio f. Seja $0 < d = \partial f \leq D \leq q-1$ o grau de f e divida o polinômio em $f = f_d + h$ onde f_d são os monômios de grau exatamente d. Note que do fato de f não ser o polinômio nulo, então o polinômio f_d também não é nulo. Como já argumentado $\partial g = \partial f = d$. Queremos calcular o coeficiente de t^d em g.

Seja $cx_1^{e_1} \ldots x_n^{e_n}$ um monômio de f_d, isto é, um monômio tal que $e_1 + \ldots + e_n = d$. Em g esse monômio corresponde ao polinômio $c(a_1 t + b_1)^{e_1} \ldots (a_n t + b_t)^{e_n}$ cujo coeficiente de t^d é $ca_1^{e_1} \ldots a_n^{e_n}$ que é o mesmo

que aplicar esse monômio no ponto a. É fácil ver que apenas monômios em f_d contribuem para o coeficiente de t^d em g então segue que o coeficiente de t^d em g é $f_d(a)$.

Mas como já vimos, g é o polinômio nulo. Logo o coeficiente de t^d é 0, ou seja, $f_d(a) = 0$. Isso vale para todo $a \in \mathbb{F}_q^n$. Como $\partial f = d \leq D \leq q-1$, pelo Lema 4.6 segue que f_d é o polinômio nulo, o que é um absurdo. □

Observe que apesar das duas demonstrações serem semelhantes, as cotas são um pouco distintas. No problema de CoNikodym por termos de usar $L_{a,b} \setminus \{b\}$ que possui apenas $q-1$ pontos, temos que forçar um polinômio de grau no máximo $q-2$ e por isso uma estimativa um pouco pior.

Uma outra aplicação geométrica do método polinomial ocorre no problema dos joints. Seja $\mathcal{L}$ um conjunto de retas no $\mathbb{R}^3$. Dizemos que um ponto $p \in \mathbb{R}^3$ é um *joint* se existem três retas em cL, não coplanares, concorrentes em p. O problema é estimar o número máximo de joints em função do número de retas de $\mathcal{L}$. Seja $n = |\mathcal{L}|$.

Uma maneira de obter uma cota inferior é a seguinte: Considere o grid $[S] \times [S] \times [S]$. Esse grid consiste de $3S^2$ retas e todos os S^3 vértices são joints. Então segue que $n = 3S^2$ ou $S = \frac{n^{\frac{1}{2}}}{\sqrt{3}}$, daí

$$\#\{joints\} = S^3 = \frac{1}{3\sqrt{3}} n^{\frac{3}{2}}$$

Outra maneira é considerando M planos em posição geral no $\mathbb{R}^3$. Qualquer intersecção entre dois planos nos fornece uma reta e logo $n = \binom{M}{2} \sim \frac{M^2}{2}$, o que nos dá $M \sim (2n)^{\frac{1}{2}}$. Qualquer interseção entre três planos nos fornece um joint e portanto existem $\binom{M}{3}$ joints. Assim

$$\#\{joints\} = \binom{M}{3} \sim \frac{M^3}{6} \sim \frac{\sqrt{3}}{3} n^{\frac{3}{2}}$$

Ambos os exemplos nos dizem que existe conjunto de n retas, que formam pelo menos $\Omega(n^{\frac{3}{2}})$ joints. O que iremos mostrar aqui é que esses exemplos são justos, a menos de constante.

Teorema 4.8 (Guth, Katz, 2008)**.** *Todo conjunto de n retas no $\mathbb{R}^3$ possui no máximo $6n^{\frac{3}{2}}$ joints.*

Como o nosso corpo agora é o $\mathbb{R}$, que não é finito, vamos precisar usar um novo lema de anulamento. Para isso relembremos alguma notação de cálculo. Dada uma função $f : \mathbb{R}^3 \to \mathbb{R}$ diferenciável, denotamos por

$$\nabla f = \left(\frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \frac{\partial f}{\partial x_3}\right)$$

o gradiente de f. É um resultado conhecido em cálculo que se $\nabla f(x) = 0$ para todo $x \in \mathbb{R}^3$, então f é constante.

Lema 4.9. *Seja P um polinômio real de três variáveis de grau d. Se $\nabla P(x) = 0$ para pelo menos d pontos em $\mathbb{R}^3$ então P é constante.*

Demonstração. O lema segue do fato que $\frac{\partial P}{\partial x_i}$ é um polinômio de grau menor que d para todo $i = 1, 2, 3$. Isso significa que os polinômios $\frac{\partial P}{\partial x_i}$ zeram em um número maior de pontos do que os seus graus, logo eles tem de serem nulos. A conclusão é que $\nabla P = 0$ e portanto P é constante. □

O método polinomial é usado no seguinte lema.

Lema 4.10. *Se um conjunto de retas $\mathcal{L}$ no $\mathbb{R}^3$ possui J joints, então existe uma reta com no máximo $3J^{\frac{1}{3}}$ joints.*

Demonstração. Suponha que não, que todas as retas possuem mais de $3J^{\frac{1}{3}}$ joints. Pelo Corolário 4.5, para $D = \lfloor 3J^{\frac{1}{3}} \rfloor$ existe um polinômio $P \in Poly_D(\mathbb{R}^3)$, não nulo, tal que $P(x) = 0$ para todo x joint.

Seja L uma das retas e chame de $p_1, \ldots, p_t$ os joints em L. Pela construção de P temos que $P(p_i) = 0$ para todo $i = 1, \ldots, t$. Como $t > 3J^{\frac{1}{3}} \geq D$, pelo Lema 4.7 temos que $P(x) = 0$ para todo $x \in L$. Como a escolha da reta L foi arbitrária, podemos dizer que o polinômio P zera em todas as retas de $\mathcal{L}$.

Seja x um joint e L_1, L_2, L_3 as três retas que determinam x ser um joint. Denote por u_1, u_2, u_3 os três vetores cada um na direção das retas L_1, L_2, L_3, respectivamente (i.e., $L_i = \{x + tu_i : t \in \mathbb{R}\}$). Por P zerar nessas três retas, temos que as derivadas direcionais em x, $\frac{\partial P}{\partial u_i}(x) = \lim_{t\to 0} \frac{P(x+tu_i)-P(x)}{t} = 0$ para todo $i = 1, 2, 3$. Não é difícil ver que de P ser diferenciável

$$0 = \frac{\partial P}{\partial u_i}(x) = \frac{\partial P}{\partial(u_{i1}e_1 + u_{i2}e_2 + u_{i3}e_3)}(x) = u_{i1}\frac{\partial P}{\partial x_1}(x) + u_{i2}\frac{\partial P}{\partial x_2}(x) + u_{i3}\frac{\partial P}{\partial x_3}(x) = \langle \nabla P(x), u_i \rangle.$$

Como u_1, u_2, u_3 geram $\mathbb{R}^3$, pois L_1, L_2, L_3 não são coplanares, segue que $\langle \nabla P(x), y \rangle = 0$ para todo $y \in \mathbb{R}^3$ e portanto $\nabla P(x) = 0$. Como x é um joint arbitrário, concluimos que $\nabla P(x) = 0$ para todo x joint, ou seja, ∇P zera para pelo menos J pontos.

De P possuir grau no máximo $D \le 3J^{\frac{1}{3}} < J$ (pois o número de joints é maior que o número de joints em uma reta) podemos aplicar o Lema 4.9 e obtremos que P é constante. Porém P zera em todo joint, logo P é o polinômio nulo, o que é uma contradição. □

Demonstração Teorema 4.8. Vamos usar o resultado anterior recursivamente. Seja $f(n)$ o maior número de joints possível com um conjunto de n retas no $\mathbb{R}^3$. Suponha agora que a gente possua n retas na configuração máxima, ou seja, n retas formando $f(n)$ joints. Pelo Lema 4.10 existe uma reta desse conjunto que possui no máximo $3f(n)^{\frac{1}{3}}$ joints. Ao retirarmos essa reta do conjunto ficamos com um conjunto de $n-1$ retas. Note que perdemos no máximo $3f(n)^{\frac{1}{3}}$ (nem todo joint na reta será perdido, mas com certeza não perdemos mais joints do que os existentes na reta). Como em $n-1$ retas possuimos no máximo $f(n-1)$ joints, temos a desigualdade $f(n) \le f(n-1) + 3f(n)^{\frac{1}{3}}$.

Podemos iterar essa desigualdade de modo a obter $f(n) \le 3\sum_{i=1}^{n} f(i)^{\frac{1}{3}} \le 3nf(n)^{\frac{1}{3}}$. Resolvendo a inequação conseguimos

$$f(n) \le (3n)^{\frac{3}{2}} \le 6n^{\frac{3}{2}}.$$

□

◇ ◇ ◇ *Aula 10 (27 de Junho) — Yoshiharu Kohayakawa* ◇ ◇ ◇

Vamos mostrar uma nova forma de aplicar o método polinomial. Nos exemplos anteriores o método consistia em construir um polinômio de grau determinado pelo conjunto em que estávamos trabalhando e após isso mostrar que esse polinômio zerava em demasiados pontos, implicando que o grau devia ser suficientemente grande para o polinômio não ser nulo. Dessa forma, se obtem uma cota inferior para o conjunto.

A forma que veremos agora, difere um pouco desse tratamento. Basicamente trabalharemos com dimensões de um polinômio. A idéia é que dado um conjunto que estamos trabalhando, podemos codificar ele em um polinômio e contar sua dimensão de duas formas. Em uma das formas mostramos que a dimensão não pode ser muito grande porcausa da estrutura do problema e em outra calculamos a dimensão explicitamente por via do polinômio. Isso nos fornece uma cota superior para o conjunto.

Usaremos esse método para provarmos o problema dos capsets e o dos girassóis. Dizemos que um conjunto $A \subset \mathbb{F}_3^n$ é um *capset* se para todo $x, y, z \in A$ tais que $x + y + z = 0$, temos que $x = y = z$. Poderíamos nos perguntar quão grande esses conjuntos são, e o teorema que vamos provar nos diz que

Teorema 4.11 (Capsets)**.** *Se $A \subset \mathbb{F}_3^n$ é um capset, então $|A| < (3-\epsilon)^n$ para algum $\epsilon > 0$.*

Ou seja, um subconjunto da ordem de 3^n não pode ser um capset e logo contém x, y, z não todos iguais com $x + y + z = 0$. Note que por estarmos em $\mathbb{F}_3^n$, se $x + y + z = 0$, então para cada coordenada $x_i = y_i = z_i$ ou $\{x_i, y_i, z_i\} = \mathbb{F}_3$. Em ambos os casos existe um $\beta_i \in \mathbb{F}_3$ tal que $z_i = x_i + 2\beta_i$ e $y_i = x_i + \beta_i$. Sendo $\beta = (\beta_1, \ldots, \beta_n)$ temos que $z = x + 2\beta$ e $y = x + \beta$, ou seja, x, y, z estão em uma mesma reta em $\mathbb{F}_3^n$. É fácil ver também que três pontos em uma mesma reta em $\mathbb{F}_3^n$ somam zero. Logo, interpretando dessa forma, o Teorema 1.1 nos diz que um conjunto muito grande de $\mathbb{F}_3^n$ possui 3 pontos em uma mesma reta.

Dados conjuntos de $2^{[n]}$, dizemos que $A, B, C \in 2^{[n]}$ formam um *girassol* se $A \cap B = B \cap C = C \cap A$, ou seja, se os únicos elementos em comum pertencem aos três conjuntos. Note que nessa definição

podemos perguntar qual o tamanho da maior família $\mathcal{F} \subset 2^{[n]}$ tal que $\mathcal{F}$ não contenha um girassol. O próximo teorema mostra que isso não é da ordem de 2^n.

Teorema 4.12 (Girassóis). *Se $\mathcal{F} \subset 2^{[n]}$ é uma família de conjuntos que não contém um girassol, então $|\mathcal{F}| < (2-\epsilon)^n$ para algum $\epsilon > 0$.*

A noção de dimensão que vamos utilizar é um pouco diferente da usual, para começar vamos lidar com um caso simples. Seja A um conjunto qualquer finito e $\mathbb{F}$ um corpo. Podemos definir uma matriz indexada nos elementos de A pela função $F : A \times A \to \mathbb{F}$. Em um curso de álgebra linear, o posto dessa matriz é definido como o número de colunas linearmente independentes dessa matriz. Em particular uma matriz de posto 1 seria uma matriz em que todas as colunas são múltiplas de um vetor. Seja $f : A \to \mathbb{F}$ esse vetor, o que dizemos então é que se F tem posto 1, existe uma $g : A \to \mathbb{F}$ tal que

$$F(x,y) = f(x)g(y), \quad \forall\, x,y \in A.$$

É fácil ver que toda F definida dessa forma tem posto 1, pois essa matriz seria o produto externo dos vetores f e g.

Uma matriz de posto t seria uma matriz em que existem t vetores colunas linearmente independentes. Observe que podemos escrever essa matriz como combinação linear de t matrizes de posto 1. Basta tomar matrizes em que as colunas são geradas pelos t vetores colunas linearmente independentes. É óbvio também que não podemos escrever essa matriz como soma de $t-1$ matrizes de posto 1, pois isso implicaria que existem apenas $t-1$ vetores linearmente independentes. Isso tudo nos permite dar a definição alternativa de posto de F como $\min\{r : F = \sum_{i=1}^{r} c_i F_i$ onde F_i são todos de posto $1\}$.

Podemos generalizar esse conceito para funções de A_k, o que seriam hipermatrizes. Seja $F : A^k \to \mathbb{F}$ uma função. A generalização usual seria dizer que F é de posto 1 se existem $f : A \to \mathbb{F}$ e $g : A^{k-1} \to \mathbb{F}$ tal que

$$F(x_1,\dots,x_k) = f(x_1)g(x_2,\dots,x_k).$$

Dessa forma teríamos que F é de posto 1 se todas os vetores colunas são múltiplos de um vetor coluna de dimensão $|A|$ em uma direção. Mas para os nossos propósitos será muito mais efetivo considerar que isso tem de ocorrer em todas as direções. Então definimos F como de posto 1 se existem $f : A \to \mathbb{F}$ e $g : A^{k-1} \to \mathbb{F}$ e $i \in [k]$ tal que

$$F(x_1,\dots,x_k) = f(x_i)g(x_1,\dots,\hat{x_i},\dots,x_k)$$

onde $\hat{x_i}$ significa que x_i não é variável dessa função. Definimos o posto de F como

$$rank(F) = \min\{r : F = \sum_{i=1}^{r} c_i F_i \text{ onde } F_i \text{ são todos de posto } 1\}.$$

Assim nessa definição permitimos que combinemos matrizes múltiplas de um vetor coluna em x_1 com matrizes múltiplas de um vetor coluna em x_k, por exemplo. Isso já torna um pouco mais difícil de calcular o posto.

Estamos interessados em um tipo de função em particular, a função com entradas só na diagonal. O lema técnico a seguir determina o posto dessaas funções. Dado $a \in A$, represente por $\delta_a : A \to \mathbb{F}$ a função característica de a, isto é, $\delta_a(x) = 0$ se $x \neq a$ e $\delta_a(x) = 1$ se $x = a$.

Lema 4.13. *Seja $F : A^k \to \mathbb{F}$ a função diagonal dada por*

$$F(x_1,\dots,x_k) = \sum_{a \in A} c_a \delta_a(x_1)\dots\delta_a(x_k)$$

onde $c_a \in \mathbb{F}$ para todo $a \in A$. Denotando $A^* = \{a \in A : c_a \neq 0\}$ temos que $rank(F) = |A^*|$, ou seja, o posto de F é o número de entradas na diagonal diferentes de 0.

Demonstração. Faremos por indução em k. Para $k = 2$ a definição de posto coincide com a usual de matrizes e logo o posto é exatemente o número de entradas na diagonal diferentes de 0. Suponha agora que mostramos o enunciado para $k-1$, vamos mostrar para k.

Primeiro note que se algum $x_i \in A \setminus A^*$ então $F(x_1, \ldots, x_k) = 0$ e porcausa disso podemos supor que $A^* = A$. De fato, se $F = \sum_{i=1}^{r} c_i F_i$, então definindo $G_i(x) = F_i(x)$ para $x \in (A^*)^k$ e $G_i(x) = 0$ para os demais pontos temos que $F = \sum_{i=1}^{r} c_i G_i$ para todo A^k. Logo para cada combinação linear com funções definidas em A^k conseguimos uma combinação linear de funções com valores não nulos apenas em $(A^*)^k$ e portanto os elementos em $A \setminus A^*$ são irrelevantes para o cálculo do posto.

Como $c_a \delta(x_1) \ldots \delta(x_k)$ é uma função de posto 1 para todo $a \in A$ temos que F é uma combinação linear de $|A|$ funções de posto 1 e da definição de posto temos $rank(F) \leq |A|$.

Para o outro lado considere que $F = \sum_{i=1}^{r} F_i$ onde $r = rank(F)$ e F_i são funções de posto 1 (note que podemos absorver os escalares da combinação linear nos F_i's e escrevermos dessa forma). Podemos dividir os índices em k conjuntos $I_1, \ldots, I_k$ tais que

1. $[r] = I_1 \dot\cup \ldots \dot\cup I_k$
2. Para $i \in I_t$ vale que $F_i(x_1, \ldots, x_k) = f_i(x_t) g_i(x_1, \ldots, \hat{x_t}, \ldots, x_k)$ para algum $f_i : A \to \mathbb{F}$ e $g_i : A^{k-1} \to \mathbb{F}$.

Dessa forma podemos reescrever F como a soma

$$F(x_1, \ldots, x_k) = \sum_{i=1}^{k} \sum_{\alpha \in I_i} f_{i,\alpha}(x_i) g_{i,\alpha}(x_1, \ldots, \hat{x_i}, \ldots, x_k).$$

Suponha por absurdo que $r < |A|$, então $|I_1| + \ldots + |I_k| < |A|$. Vamos considerar os elementos de I_k. Para cada $\alpha \in I_k$ temos determinado uma $f_{k,\alpha} : A \to \mathbb{F}$. Essa função pode ser vista como um vetor de tamanho $|A|$. Como para cada α temos uma função assim, então elas geram um subespaço vetorial W de dimensão no máximo $|I_k|$. Do fato de que a dimensão do espaço vetorial $\mathbb{F}^A$ é finita, segue que $d = dim(W^\perp) \geq |A| - |I_k| > 0$.

Seja $h_1, \ldots, h_d$ uma base de $W^\perp$. Podemos considerar a matriz H de dimensões $|A| \times d$ cuja as colunas são os vetores $h_1, \ldots, h_d$. Como o posto das colunas de uma matriz é igual ao posto das linhas e o posto de H é d, então existem d linhas na matriz H que são linearmente independentes. Suponha sem perda de generalidade que são as primeiras d linhas. Assim o primeiro bloco $d \times d$ de H consiste de uma matriz invertível e suas colunas geram o $\mathbb{F}^d$. Em particular, existe $h \in W^\perp$ tal que h é não nulo em pelo menos d valores de A.

Por $h \in W^\perp$ temos que

$$\langle f_{k,\alpha}, h \rangle = \sum_{x \in A} f_{k,\alpha}(x) h(x) = 0.$$

Multiplicando F por h e somando com x_k variando em A obtemos uma função $G : A^{k-1} \to \mathbb{F}$. Podemos calcular G da seguinte forma

$$G(x_1, \ldots, x_{k-1}) = \sum_{x_k \in A} F(x_1, \ldots, x_k) h(x_k) = \sum_{x_k \in A} \Big(\sum_{a \in A} c_a \delta_a(x_1) \ldots \delta_a(x_k) \Big) h(x_k) =$$
$$\sum_{a \in A} c_a \delta_a(x_1) \ldots \delta_a(x_{k-1}) \Big(\sum_{x_k \in A} \delta_a(x_k) h(x_k) \Big) = \sum_{a \in A} c_a h(a) \delta_a(x_1) \ldots \delta_a(x_{k-1}).$$

Que é uma função diagonal definida em A^{k-1}. Note que o número de $a \in A$ tal que $c_a h(a) \neq 0$ é pelo menos d, pois $c_a \neq 0$ para todo A e $h(a) \neq 0$ para pelo menos d valores. Aplicando a hipótese de indução temos que $rank(G) = |\{a \in A : c_a h(a) \neq 0\}| \geq d$.

Agora podemos calcular G também como

$$G(x_1,\dots,x_{k-1}) = \sum_{x_k\in A} F(x_1,\dots,x_k)h(x_k) =$$

$$\sum_{x_k\in A}(\sum_{i=1}^{k}\sum_{\alpha\in I_i} f_{i,\alpha}(x_i)g_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_k))h(x_k) =$$

$$\sum_{i=1}^{k}\sum_{\alpha\in I_i}\sum_{x_k\in A} f_{i,\alpha}(x_i)g_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_k))h(x_k) =$$

$$\sum_{i=1}^{k-1}\sum_{\alpha\in I_i}\sum_{x_k\in A} f_{i,\alpha}(x_i)g_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_k))h(x_k) + \sum_{\alpha\in I_k}\sum_{x_k\in A} f_{k,\alpha}(x_k)h(x_k)g_{k,\alpha}(x_1,\dots,x_{k-1}) =$$

$$\sum_{i=1}^{k-1}\sum_{\alpha\in I_i}\sum_{x_k\in A} f_{i,\alpha}(x_i)g_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_k))h(x_k) =$$

$$\sum_{i=1}^{k-1}\sum_{\alpha\in I_i} f_{i,\alpha}(x_i)\sum_{x_k\in A} g_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_k))h(x_k) =$$

$$\sum_{i=1}^{k-1}\sum_{\alpha\in I_i} f_{i,\alpha}(x_i)\tilde{g}_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_{k-1})$$

onde $\tilde{g}_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_{k-1}) = \sum_{x_k\in A} g_{i,\alpha}(x_1,\dots,\hat{x_i},\dots,x_k))h(x_k)$ é uma função de A^{k-2} em $\mathbb{F}$. Assim temos que G é uma combinação linear de $|I_1|+\dots+|I_{k-1}|$ funções de posto 1 e logo $rank(G) \le |I_1|+\dots+|I_{k-1}|$.

Juntando as duas desigualdades temos

$$d \le rank(G) \le |I_1|+\dots+|I_{k-1}| < |A|-|I_k| \le d$$

o que é uma contradição. □

Com essa função diagonal e a nova definição de posto somos capazes de provar os dois teoremas citados.

Demonstração do Teorema 4.11. Seja $A \in \mathbb{F}_3^n$ um capset. O corpo que utilizaremos é $\mathbb{F} = \mathbb{F}_3$. A nossa função $F : A^3 \to \mathbb{F}_3$ será

$$F(x,y,z) = \delta_0(x+y+z)$$

onde δ_0 é a função característica de $0 \in \mathbb{F}_3^n$. Ou seja, F devolve 1 se os três pontos estiverem na mesma reta, caso contrário devolve 0. Como o conjunto A é um capset, a única forma de três pontos estiverem na mesma reta é se os três pontos forem iguais (note que se dois forem iguais, imediatamente o terceiro também tem de ser). Então podemos reescrever F como

$$F(x,y,z) = \sum_{a\in A}\delta_a(x)\delta_a(y)\delta_a(z)$$

que é uma função diagonal. Pelo Lema 4.13 a função F tem posto $|A|$, pois todas as entradas da diagonal são iguais a 1. A estratégia agora é determinar um polinômio que represente F e calcular o posto via esse polinômio.

Uma forma de emular a função característica δ_0 em $\mathbb{F}_3[X]$ é com o polinômio $p(x) = 1-x^2$. Esse polinômio satisfaz $p(0) = 1$ e $p(x) = 0$ para $x \in \mathbb{F}_3$ diferente de 0. Com isso em mente podemos construir o polinômio $f \in Poly_{2n}(\mathbb{F}_3^{3n})$ dado por

$$f(x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n) = \prod_{i=1}^{n}(1-(x_i+y_i+z_i)^2).$$

Esse polinômio devolve 1 se para todo i vale que $x_i + y_i + z_i = 0$ e 0, caso contrário. Ou seja,

$$F(x,y,z) = f(x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n)$$

se enxergarmos x_i, y_i, z_i como as i-ésimas cordenadas de de $x, y, z \in A$. Uma outra forma de escrever isso é que $F = f\mid_{A^3}$ onde vemos f como uma função de $(\mathbb{F}_3^n)^3$.

Observe que $rank(F) \le rank(f)$. Isso ocorre porque se $f = \sum_{i=1}^r c_i f_i$ para $f_i : (\mathbb{F}_3^n)^3 \to \mathbb{F}_3$ de posto 1, então definindo $F_i : A^3 \to \mathbb{F}_3$ por $F_i = f\mid_{A^3}$ temos que $F = f\mid_{A^3} = \sum_{i=1}^r c_i f_i\mid_{A^3} = \sum_{i=1}^r c_i F_i$. Tomando $r = rank f$ obtemos o desejado.

Agora o problema se resume a achar estimativas para o posto de f visto como uma função de 3 variáveis em $\mathbb{F}_3^n$. Um monômio em f é da forma $cx_1^{i_1}\dots x_n^{i_n} y_1^{j_1}\dots y_n^{j_n} z_1^{k_1}\dots z_n^{k_n}$ onde $i_1+\dots+i_n+j_1+\dots+j_n+k_1+\dots+k_n \le 2n$ e $i_t, j_t, k_t \in \{0,1,2\}$. Podemos separar esses monômios em 3 tipos:

1. $i_1+\dots+i_n \le \frac{2n}{3}$.
2. $j_1+\dots+j_n \le \frac{2n}{3}$.
3. $k_1+\dots+k_n \le \frac{2n}{3}$.

Um monômio pode ser de mais de um tipo, nesse caso apenas escolha arbitrariamente. Com esses tipos temos que

$$\begin{aligned} f(x_1,\dots,x_n,y_1,\dots,y_n,z_1,\dots,z_n) = &\sum_{i_1+\dots+i_n\le 2n/3} a_{i_1,\dots,i_n} x_1^{i_1}\dots x_n^{i_n} f_{i_1,\dots,i_n}(y_1,\dots,y_n,z_1,\dots,z_n) \\ &+ \sum_{j_1+\dots+j_n\le 2n/3} b_{j_1,\dots,j_n} y_1^{j_1}\dots y_n^{j_n} g_{j_1,\dots,j_n}(x_1,\dots,x_n,z_1,\dots,z_n) \\ &+ \sum_{k_1+\dots+k_n\le 2n/3} c_{k_1,\dots,k_n} z_1^{k_1}\dots z_n^{k_n} h_{k_1,\dots,k_n}(x_1,\dots,x_n,y_1,\dots,y_n). \end{aligned}$$

Ou seja, f é a combinação linear de $3|\{(t_1,\dots,t_n)\in\{0,1,2\}^n : t_1+\dots+t_n \le 2n/3\}|$ funções de posto 1. Chamando $N = |\{(t_1,\dots,t_n)\in\{0,1,2\}^n : t_1+\dots+t_n \le 2n/3\}|$, temos que $rank(f) \le 3N$.

Para estimarmos N vamos usar o método probabilístico. Sorteie uniformemente e independentemente cada t_i de $\{0,1,2\}$, isto é, $\mathbb{P}(t_i=0) = \mathbb{P}(t_i=1) = \mathbb{P}(t_i=2) = 1/3$. Seja X a variável aleatória que conta o valor de $t_1+\dots+t_n$ e X_i a variável que conta o valor de t_i. Um cálculo simples mostra que

$$\mathbb{E}(X) = \sum_{i=1}^n \mathbb{E}(X_i) = \sum_{i=1}^n (0\cdot\mathbb{P}(t_i=0) + 1\cdot\mathbb{P}(t_i=1) + 2\cdot\mathbb{P}(t_i=2)) = n.$$

Como os X_i's são independentes e identicamente distribuidos, segue de resultados sobre grandes desvios que existe $\mu > 0$ tal que

$$\mathbb{P}(X \le \frac{2n}{3}) = \mathbb{P}(X \le \frac{2}{3}\mathbb{E}(X)) < e^{-\mu\mathbb{E}(X)} = e^{-\mu n}.$$

Mas note também que $\mathbb{P}(X \le 2n/3) = N/3^n$ pois das 3^n escolhas possíveis de $t_1,\dots,t_n$ o número delas tal que $t_1+\dots+t_n \le 2n/3$ é exatamente N. Daí

$$\frac{N}{3^n} < e^{-\mu n} \Leftrightarrow N < (3e^{-\mu})^n$$

e agora estamos resolvidos pois $|A| = rank(F) \le rank(f) < 3N < 3(3e^{-\mu})^n < (3-\epsilon)^n$ para $\epsilon > 0$ apropriado. □

Note dessa demonstração que a definição alternativa de posto foi essencial. Pela definição de posto usual o posto da matriz dependeria apenas de uma variável e teríamos que considerar todos os monômios da forma $x_1^{i_1}\dots x_n^{i_n}$ com $i_1+\dots+i_n \le 2n$. Infelizmente existem 3^n maneiras de escolher esses índices e conseguimos apenas a cota trivial $|A| \le 3^n$.

Demonstração do Teorema 4.12. Precisamos de alguma forma algebrizar a relação de ser um girassol. Uma forma de fazer isso é ver cada conjunto $X \in 2^{[n]}$ como um vetor $x \in \{0,1\}^n$, onde $x_i = 1$ se $i \in X$ e

$x_i = 0$ caso contrário. Assim três vetores $x, y, z \in \{0,1\}^n$ formam um girassol se para toda coordenada temos que $x_i + y_i + z_i \in \{0,1,3\}$. Ou seja, a única possibilidade que devemos excluir é a de um elemento estar na intersecção de apenas dois conjuntos.

Na demonstração do capset tinhamos que se um conjunto A é capset, então para $(x,y,z) \in A^3$ com $x+y+z = 0$ temos que $x = y = z$. Nessa observação utilizavamos o fato que se $x+y+z = 0$, então ou os três valores são iguais, ou os três valores são distintos. Infelizmente nos girassóis não funciona do mesmo jeito, podemos ter um girassol da forma (X, X, Y) desde que $X \subset Y$. A maneira de corrigir isso é comparando apenas conjuntos da mesma cardinalidade, dessa forma se X, Y, Z formam um girassol, então ou $X = Y = Z$, ou os três são distintos.

Dada família $\mathcal{F}$ de conjuntos livre de girassóis, seja $A \subset \{0,1\}^n$ o conjunto dos vetores representantes dos conjuntos de $\mathcal{F}$. Particione $A = \bigcup_{t=1}^{n} A_t$, onde A_t é o conjuto dos vetores que representam conjuntos de cardinalidade t, isto é, que o suporte tem cardinalidade t. De A ser livre de girassóis, temos que cada A_t é livre de girassóis.

Utilizaremos como corpo $\mathbb{F} = \mathbb{R}$. Fixado $t \in [n]$, queremos uma $F : A_t^3 \to \mathbb{R}$ tal que $F(x,y,z) \neq 0$ se (x,y,z) for um girassol e $F(x,y,z) = 0$ caso contrário. Pela observação feita em um parágrafo anterior, como A_t é livre de girassóis, a única forma de obtermos um girassol é com $x = y = z$. Portanto

$$F(x,y,z) = \sum_{a \in A_i} c_a \delta_a(x) \delta_a(y) \delta(z)$$

com $c_a = F(a,a,a) \neq 0$ e pelo Lema 4.13 temos $rank(F) = |A_t|$.

Queremos que essa F seja a restrição de um polinômio $f \in Poly_n(\mathbb{R}^{3n})$. O polinômio natural é

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = \prod_{i=1}^{n} (2 - (x_i + y_i + z_i)).$$

É fácil ver que $x, y, z \in \{0,1\}^n$ formam um girassol se, e somente se, $f(x,y,z) \neq 0$. Daí basta definir $F(x,y,z) = \sum_{a \in A_i} f(a,a,a) \delta_a(x) \delta_a(y) \delta_a(z)$. A demonstração agora ocorre análogamente a anterior.

Como $F = f|_{A_t^3}$ então $rank(F) \leq rank(f)$. Mas para o cálculo do posto note que um monômio de f é da forma $c x_1^{i_1} \ldots x_n^{i_n} y_1^{j_1} \ldots y_n^{j_n} z_1^{k_1} \ldots z_n^{k_n}$ com $i_1 + \ldots + i_n + j_1 + \ldots + j_n + k_1 + \ldots + k_n \leq n$ e $i_s, j_s, k_s \in \{0,1\}$. Podemos dividir os monômios em três tipos como na outra demonstração.

1. $i_1 + \ldots + i_n \leq n/3$.
2. $j_1 + \ldots + j_n \leq n/3$.
3. $k_1 + \ldots + k_n \leq n/3$.

Podemos escrever então

$$\begin{aligned} f(x_1, \ldots, x_n, y_1, \ldots, y_n, z_1, \ldots, z_n) = & \sum_{i_1 + \ldots + i_n \leq n/3} a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n} f_{i_1, \ldots, i_n}(y_1, \ldots, y_n, z_1, \ldots, z_n) \\ & + \sum_{j_1 + \ldots + j_n \leq n/3} b_{j_1, \ldots, j_n} y_1^{j_1} \ldots y_n^{j_n} g_{j_1, \ldots, j_n}(x_1, \ldots, x_n, z_1, \ldots, z_n) \\ & + \sum_{k_1 + \ldots + k_n \leq n/3} c_{k_1, \ldots, k_n} z_1^{k_1} \ldots z_n^{k_n} h_{k_1, \ldots, k_n}(x_1, \ldots, x_n, y_1, \ldots, y_n). \end{aligned}$$

Disso temos que f é combinação linear de $3|\{(i_1, \ldots, i_n) \in \{0,1\}^n : i_1 + \ldots + i_n \leq n/3\}|$. Chamando $N = |\{(i_1, \ldots, i_n) \in \{0,1\}^n : i_1 + \ldots + i_n \leq n/3\}|$, segue que $rank(f) \leq 3N$.

Assim $|A_t| = rank(F) \leq rank(f) \leq 3N$ para um t arbitrário. Portanto

$$|A| = \sum_{i=1}^{n} |A_i| \leq 3nN.$$

Para estimar N podemos usar de novo o método probabilístico. Uma outra forma é observando que

$$N = \sum_{k \leq n/3} \binom{n}{k} \leq n \binom{n}{n/3} \approx n \left(\frac{1}{(1/3)^{1/3}(2/3)^{2/3}}\right)^n \leq n(1,9)^n$$

onde usamos que $\binom{n}{\alpha n} = (\frac{1}{\alpha^\alpha (1-\alpha)^{1-\alpha}})^{(1+o(1))n}$ pela fórmula de stirling. Daí

$$|A| \leq 3n^2(1,9)^n \leq (1,99)^n$$

como queríamos. □