Tópicos em Combinatória Contemporânea

Carlos Gustavo T. de A. Moreira

Yoshiharu Kohayakawa

Dedicamos este texto à memória de Paul Erdős (1913–1996)
A combinatória contemporânea existe devido a este
Mago de Budapeste

Prefácio

Objetivamos neste texto a apresentação de alguns tópicos modernos da combinatória a alunos da graduação. Devido à natureza elementar da área, podemos discutir tópicos não tão distantes da fronteira do conhecimento em um texto como este, voltado a jovens iniciantes. Esperamos que os leitores possam ter uma idéia do que se faz em combinatória hoje através destas notas.

A combinatória é uma área vasta, que continua a crescer vigorosamente. Tópicos de pesquisa que têm se mostrado frutíferos incluem a teoria extremal dos conjuntos, os métodos probabilísticos e os métodos algébricos. Escolhemos alguns dos resultados mais conhecidos nestas linhas de pesquisa para formar uma fotografia da área. Com o intuito de apresentar a combinatória como uma disciplina integrada no grande universo da matemática, procuramos apresentar aplicações dos resultados e das técnicas da combinatória em outras áreas; em particular, damos especial atenção a aplicações em geometria elementar.

No Capítulo 1, discutimos alguns resultados fundamentais da teoria extremal dos conjuntos: discutimos, dentre outros, o teorema de Sperner (1928) e o teorema de Erdős, Ko e Rado (1961). Discutimos também alguns resultados básicos da teoria de Ramsey. Damos duas aplicações do teorema de Sperner (uma à análise/geometria e outra a um problema da teoria dos números). Apresentamos também neste capítulo algumas aplicações da álgebra linear à teoria extremal dos conjuntos. É no Capítulo 2 que apresentamos talvez a aplicação mais espetacular da teoria extremal dos conjuntos nos anos recentes: expomos o contra-exemplo de Kahn e Kalai (1993) para a conjectura de Borsuk (1933). Discutimos neste capítulo também o *número cromático* $c(n)$ do $\mathbb{R}^n$, o número mínimo de cores que precisamos usar para colorir os pontos do $\mathbb{R}^n$ se não queremos ter dois pontos à distância 1 da mesma cor. O crescimento exponencial de $c(n)$, conjecturado por Larman e Rogers (1972), foi provado por Frankl e Wilson em 1981. Surpreendentemente, a ferramenta básica deste capítulo é um resultado elementar da teoria extremal dos conjuntos, que pode ser provado através de considerações de independência linear de certos polinômios.

No Capítulo 3, elaboramos um pouco mais a noção de configurações monocromáticas inevitáveis em colorações do $\mathbb{R}^n$: estudamos uma área da teoria de Ramsey conhecida como a *teoria de Ramsey euclideana*; as investigações originais neste tópico foram realizadas por Erdős, Graham, Montgomery, Rothschild, Spencer e Straus no início da década de 70. Apresentamos neste capítulo alguns resultados mais novos de Frankl, Rödl e Kříž (os resultados realmente recentes estão além do escopo deste texto).

No Capítulo 4, discutimos um método probabilístico poderoso que teve suas origens em um trabalho de Ajtai, Komlós, e Szemerédi (1981), e atingiu seu pleno potencial na demonstração de Rödl (1985) da conjectura de Erdős e Hanani (1963), sobre coberturas e empacotamentos quase-ótimos (sistemas de Steiner aproximados). Terminamos o Capítulo 4 com alguns resultados recentes sobre coberturas em hipergrafos regulares.

Supomos que os leitores estão acostumados com argumentos combinatórios elementares e têm familiaridade com noções da álgebra linear, aritmética modular, e teoria elementar das probabilidades.

O leitor perceberá que temos, freqüentemente, preocupações assintóticas: muitas vezes definimos uma função $f(n)$ de forma combinatória (tipicamente como o tamanho máximo de algum objeto combinatório, parametrizado pelo inteiro n) e então nos perguntamos se sabemos quanto é $f(n)$ explicitamente, em função de n; caso não consigamos determinar o valor exato de $f(n)$, tentamos estimar $f(n)$ para n grandes. Para apreciar os resultados que apresentaremos, é importante que o leitor tenha familiaridade com a 'hierarquia' das funções mais comuns, como, por exemplo, o fato que

$$1 \ll \log\log n \ll \log n \ll n^{\varepsilon} \ll n^{c} \ll n^{\log n} \ll c^{n} \ll n! \ll n^{n} \ll c^{c^{n}},$$

onde supomos que ε e c são constantes arbitrárias com $0 < \varepsilon < 1 < c$ (escrevemos $f(n) \ll g(n)$ se $\lim_{n\to\infty} f(n)/g(n) = 0$). Ademais, o leitor terá maior facilidade em acompanhar a 'substância' do que estamos discutindo em várias ocasiões se ele tiver familiaridade com estimativas para fatoriais e coeficientes binomiais. Com isto em mente, compilamos um pequeno apêndice com algumas estimativas padrão para $n!$ e para expressões envolvendo coeficientes binomiais.

É com imenso prazer que agradecemos à organização do *23º Colóquio Brasileiro de Matemática* pelo apoio e oportunidade de ampla divulgação deste material.

Finalmente, agradecemos o apoio do CNPq através do PRONEX (projetos 416/96 e 107/97) e dos auxílios 300334/93–1, 300647/95–6, 910064/99–7 e 468516/2000–0. Agradecemos também o apoio da FAPERJ e da FAPESP.

Carlos Gustavo T. de A. Moreira `<gugu@impa.br>`
IMPA, Instituto de Matemática Pura e Aplicada
`http://www.impa.br/~gugu`

Yoshiharu Kohayakawa `<yoshi@ime.usp.br>`
Instituto de Matemática e Estatística, USP
`http://www.ime.usp.br/~yoshi`

Rio de Janeiro
São Paulo
Junho de 2001

Sumário

Notações e alguns termos de uso freqüente

$[n] = \{1, \ldots, n\}$

$\mathcal{P}(X) = \{Y : Y \subset X\}$, o conjunto das partes de X

k-conjunto: um conjunto com k elementos

Sistemas de conjuntos, *hipergrafos*: um sistema de conjuntos nada mais é que um conjunto de subconjuntos de um conjunto fixo. Um hipergrafo é um sistema de conjuntos cujos membros têm todos a mesma cardinalidade.

$\lfloor x \rfloor$, $\lceil x \rceil$, $\{x\}$: $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x e $\lceil x \rceil = -\lfloor -x \rfloor$. Escrevemos $\{x\}$ para a parte fracionária de x, isto é, $\{x\} = x - \lfloor x \rfloor$.

$|x|$, $\|x\|$, $|X|$: se x é um vetor em um espaço euclideano, então $\|x\|$ denota a norma euclideana de x. Por simplicidade, usamos também a notação $|x|$ para a norma de x. Para um conjunto X, escrevemos $|X|$ para a cardinalidade de X.

$\binom{x}{k}$, $\binom{X}{k}$: escrevemos $\binom{x}{k}$ para o coeficiente binomial, que é definido como $(x)_k/k! = x(x-1)\ldots(x-k+1)/k!$ se k é um inteiro não-negativo e é 0 se k é um inteiro negativo. Se X é um conjunto, $\binom{X}{k}$ é o conjunto $\{Y \subset X : |Y| = k\}$ dos k-subconjuntos de X. Claramente, $\left|\binom{X}{k}\right| = \binom{|X|}{k}$.

$O(f(n))$, $o(f(n))$: escrevemos $O(f(n))$ para qualquer função $g(n)$ satisfazendo $|g(n)| \leq Cf(n)$ para todo $n \geq n_0$, onde C e n_0 são constantes. Escrevemos $o(f(n))$ para qualquer função $g(n)$ satisfazendo $\lim_{n\to\infty} g(n)/f(n) = 0$; em particular, $o(1)$ denota uma quantidade que tende a 0.

$\sim$, $\ll$, $\gg$: escrevemos $f(n) \ll g(n)$ se $f(n) = o(g(n))$. Ademais, às vezes escrevemos $f(n) \sim g(n)$ se $\lim_{n\to\infty} f(n)/g(n) = 1$.

CAPÍTULO 1

Uma introdução à teoria extremal dos conjuntos

1. Introdução

Neste capítulo, discutimos alguns resultado fundamentais da teoria extremal dos conjuntos. Nós nos restringiremos a alguns resultados apenas, abrindo assim espaço para algumas aplicações um pouco mais elaboradas. Esperamos que este capítulo sirva como uma introdução a esta rica área da combinatória, mas também esperamos que o leitor que tenha seu interessado despertado consulte os excelentes textos de Anderson [**5**], Babai e Frankl [**7**], e Bollobás [**11**].

2. Dois teoremas extremais clássicos

Começamos discutindo dois teoremas clássicos, que são possivelmente os dois resultados mais conhecidos da teoria extremal dos conjuntos: o teorema de Sperner de 1928 e o teorema de Erdős, Ko, e Rado, provado em 1938, mas publicado apenas em 1961.

2.1. O teorema de Sperner. Começamos com uma observação da teoria elementar dos números.

2.1.1. *Um problema extremal da teoria dos números.* Dados $n+1$ inteiros distintos de $[2n] = \{1, \ldots, 2n\}$, não é difícil ver que há dois elementos desta seqüência que são relativamente primos (exercício!). Por outro lado, um pouco mais de meditação também revela que há dois elementos nesta seqüência com um dividindo o outro. Esta segunda afirmação é um exercício um pouco mais difícil (sugestão: escreva cada um dos $n+1$ números na forma $2^k m$, onde m é um inteiro ímpar).

Podemos enunciar a segunda afirmação acima da seguinte forma: *o maior número de elementos que podemos ter de* $[2n]$ *sem ter dois elementos, digamos* x *e* y*, com* x *dividindo* y *é* n*.* Note também que este limitante de n não pode ser melhorado, pois podemos considerar os n números $n+1, \ldots, 2n$.

2.1.2. *Um problema extremal para conjuntos.* Passemos agora a considerar *problemas extremais* análogos para conjuntos. Seja $\mathcal{A} \subset \mathcal{P}([n])$ uma família de conjuntos. O que podemos dizer sobre o tamanho de $\mathcal{A}$ se sabemos que $\mathcal{A}$ *não* contém dois membros, digamos A e B, com $A \subset B$? Seja $f(n)$ a maior cardinalidade possível para tal família $\mathcal{A}$.

Uma primeira observação que podemos fazer é que

$$f(n) \geq \binom{n}{k}, \tag{1}$$

para todo k. De fato, se tomamos para $\mathcal{A}$ a família de todos os subconjuntos de $[n]$ com k elementos, então a propriedade que exigimos está satisfeita, e temos $|\mathcal{A}| = \binom{n}{k}$. Para maximizar o limite inferior em (1), tomamos $k = \lfloor n/2 \rfloor$.

O nosso resultado desta seção, provado em 1928 por Sperner [**68**], mostra que vale a igualdade em (1) com $k = \lfloor n/2 \rfloor$, isto é,

$$f(n) = \binom{n}{\lfloor n/2 \rfloor}.$$

Na verdade, provaremos um resultado de aparência talvez um pouco técnica à primeira vista, mas que implica o resultado desejado. O Teorema 1 abaixo é devido, independentemente, a Bollobás [**9**] (em uma forma mais geral), Lubell [**57**], Yamamoto [**71**], e Meshalkin [**60**]. Dizemos que dois conjuntos A e B são *comparáveis* se $A \subset B$ ou $B \subset A$, e dizemos que A e B são *incomparáveis* caso contrário.

Teorema 1. *Seja $\mathcal{A} \subset \mathcal{P}([n])$ uma família de conjuntos cujos membros são incomparáveis entre si. Então*

$$\sum_{A \in \mathcal{A}} \binom{n}{|A|}^{-1} \leq 1. \tag{2}$$

DEMONSTRAÇÃO. Consideraremos permutações $\pi\colon [n] \to [n]$. Podemos representar π escrevendo a seqüência

$$\pi(1), \pi(2), \ldots, \pi(n), \tag{3}$$

que nada mais é que uma ordenação dos inteiros em $[n]$. Vamos dizer que uma permutação π e um conjunto A são *compatíveis* se os primeiros $|A|$ elementos na seqüência (3) formam uma permutação dos elementos de A, isto é, se

$$A = \{\pi(1), \ldots, \pi(|A|)\}. \tag{4}$$

Seja P o número de pares (π, A) com π uma permutação de $[n]$ e A um membro de $\mathcal{A}$ com π e A compatíveis. O que podemos dizer sobre P?

Por um lado, se temos um conjunto $A \in \mathcal{A}$ fixo então o número de permutações π compatíveis com A é exatamente

$$|A|!(n - |A|)!. \tag{5}$$

Qual é o número de conjuntos $A \in \mathcal{A}$ compatíveis com uma permutação fixa π? É fácil ver que a nossa hipótese sobre $\mathcal{A}$ garante que este número é *no máximo* 1! Concluímos que

$$\sum_{A \in \mathcal{A}} |A|!(n - |A|)! = P \leq \sum_{\pi} 1 = n!, \tag{6}$$

de onde segue que

$$\sum_{A \in \mathcal{A}} \frac{|A|!(n - |A|)!}{n!} \leq 1. \tag{7}$$

Naturalmente, (7) é equivalente à desigualdade (2), e o teorema está provado. $\square$

A demonstração brilhante do Teorema 1 que apresentamos acima é devida a Lubell [**57**]. Temos como corolário do Teorema 1 o seguinte resultado, que foi o resultado originalmente provado por Sperner [**68**].

Corolário 2. *Se $\mathcal{A} \subset \mathcal{P}([n])$ não contém dois elementos comparáveis, então*

$$|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}. \tag{8}$$

Demonstração. A desigualdade (8) segue de (2): basta observar que o coeficiente binomial $\binom{n}{k}$ é máximo quando $k = \lfloor n/2 \rfloor$. □

2.1.3. *Uma aplicação à análise.* Apresentamos aqui uma aplicação do teorema de Sperner à análise. Consideraremos um problema geométrico que tem origem nobre: trata-se de um problema que Littlewood e Offord **[55]** estudaram em um trabalho de 1943, com o objetivo de provar limitantes superiores para o número típico de raízes reais de certos polinômios aleatórios. Vamos descrever brevemente o resultado final de Littlewood e Offord, antes de passar ao problema geométrico.

Sejam $a_0, \ldots, a_n$ números complexos fixos e suponha que temos uma seqüência $\varepsilon_1, \ldots, \varepsilon_n$ com $\varepsilon_j \in \{-1, 1\}$ para todo j. Considere agora o polinômio

$$P(x) = a_0 + \varepsilon_1 a_1 x + \cdots + \varepsilon_n a_n x^n. \tag{9}$$

Quantas raízes reais tem a equação $P(x) = 0$ tipicamente? Aqui, entendemos por 'tipicamente' o seguinte: suponha que escolhemos os sinais ε_j aleatoriamente, de forma independente; em outras palavras, consideramos todos os 2^n polinômios da forma (9) com os a_j fixos, e escolhemos um ao acaso, com todos eles equiprováveis. Estamos interessados em saber, então, qual é tipicamente o número de raízes reais de tal polinômio aleatório. Foi esse o problema que Littlewood e Offord atacaram em **[55]**.

O resultado principal de **[55]** é o seguinte. Ponha

$$M = |a_0| + |a_1| + \cdots + |a_n|.$$

Então todos os 2^n polinômios $P(x)$ como em (9), exceto por no máximo

$$O\left(\frac{\log\log n}{\log n}2^n\right) = o(2^n)$$

deles, são tais a equação $P(x) = 0$ tem no máximo

$$10(\log n)\left(\log\frac{M}{\sqrt{|a_0a_n|}} + 2(\log n)^5\right)$$

raízes reais. Por exemplo, grosseiramente falando, se todos os a_j tem a mesma ordem de grandeza, então esse número de raízes é $O\left((\log n)^6\right)$.

Para provar o resultado acima, Littlewood e Offord consideraram um problema geométrico que basicamente pergunta o quão concentrada pode ser a distribuição das 2^n somas do tipo

$$\sum_{1\le j\le n}\varepsilon_j a_j,$$

onde os ε_j são novamente ± 1. É este o problema geométrico que passaremos a considerar agora. Por conveniência, mudamos a notação, e passamos a escrever z_j em vez de a_j $(1\le j\le n)$. Ainda, mencionamos que o que segue é independente da discussão acima.

Suponha que $z_1,\dots,z_n$ sejam números complexos fixos, não necessariamente distintos, com $|z_j|\ge 1$ $(1\le j\le n)$. Para cada $\boldsymbol{\varepsilon} = (\varepsilon_j)_{1\le j\le n}\in\{-1,1\}^n$, considere a soma

$$S(\boldsymbol{\varepsilon}) = \sum_{1\le j\le n}\varepsilon_j z_j. \tag{10}$$

Quantas das somas em (10) podem cair em um disco fechado de raio r? Littlewood e Offord provaram que este número é

$$\le C\frac{(r+1)2^n}{\sqrt{n}}\log n, \tag{11}$$

onde C é uma constante universal. Alguns exemplos simples mostram que o limitante (11) é ótimo, a menos possivelmente pelo fator logarítmico. (Esses exemplos são simples; nós os veremos em breve.)

Em 1945, Erdős publicou um melhoramento do limitante (11): ele provou que o fator logarítmico *não* é necessário [**18**]. A ferramenta que ele usou foi justamente o teorema de Sperner!

TEOREMA 3. *Sejam $z_1, \ldots, z_n$ números complexos fixos com $|z_j| \geq 1$ para todo $1 \leq j \leq n$, e $r > 0$ um número real. Então o número de somas da forma* (10) *que pertencem a um mesmo disco fechado de raio r é*

$$\leq B\frac{(r+1)2^n}{\sqrt{n}}, \tag{12}$$

onde B é uma constante universal.

É levemente mais conveniente fazer uma renormalização do problema, para enxergarmos melhor a sua natureza combinatória. Somemos $z_1 + \cdots + z_n$ à soma em (10) e dividamos por 2. Temos assim uma soma da forma

$$S(\boldsymbol{\delta}) = \sum_{1 \leq j \leq n} \delta_j z_j, \tag{13}$$

onde $\boldsymbol{\delta} = (\delta_j)_{1 \leq j \leq n}$ e os δ_j pertencem a $\{0, 1\}$. Note que uma certa coleção de somas da forma (10) está contida em um disco fechado de raio r se e só se as somas correspondentes da forma (13) pertencem a um disco fechado de *diâmetro* r. Temos assim uma formulação equivalente, com as somas em (13) ($\delta_j \in \{0, 1\}$, $1 \leq j \leq n$) e *diâmetro* r. Para evitar confusão, quando falamos nesta formulação escrevemos Δ para o diâmetro.

O exemplo que mostra que o resultado de Erdős não pode ser melhorado, a menos do valor da constante, é o seguinte exemplo simples: suponha que $\Delta \geq 0$ é um inteiro fixo e tome

$$z_1 = \cdots = z_n = 1. \tag{14}$$

Considere inteiros consecutivos $u_0 < \cdots < u_\Delta$ tais que

$$\binom{n}{u_0} + \cdots + \binom{n}{u_\Delta}$$

seja máximo. Grosseiramente falando, os u_k distribuem-se em torno de $n/2$, simetricamente. Considere agora a família de conjuntos

$$\mathcal{A} = \binom{[n]}{u_0} \cup \cdots \cup \binom{[n]}{u_\Delta}.$$

Note que se A, $A' \in \mathcal{A}$, então claramente $\big||A| - |A'|\big| \leq u_\Delta - u_0 \leq \Delta$, pois os inteiros u_j são consecutivos. Considere agora as somas

$$S(A) = \sum_{j \in A} z_j \tag{15}$$

para todo $A \subset [n]$ (naturalmente, estas são as somas da forma (13)). No nosso exemplo (14), se consideramos as somas em (15) com $A \in \mathcal{A}$, temos que (i) a diferença de quaisquer dois deles é $\leq \Delta$ e (ii) temos

$$|\mathcal{A}| = \sum_{0 \leq j \leq \Delta} \binom{n}{u_j} \geq c\frac{(\Delta+1)2^n}{\sqrt{n}} \tag{16}$$

dessas somas, onde c é uma constante absoluta positiva e supomos que $n \geq n_0(\Delta)$. Concluímos que o Teorema 3 não pode ser substancialmente melhorado. (A estimativa em (16) pode ser deduzida da fórmula de Stirling; veja o Apêndice A.)

Provemos agora o seguinte lema, que diz que o Teorema 3 vale no caso em que os z_j são todos reais positivos.

Lema 4. *Sejam $x_1, \ldots, x_n$ números reais fixos, com $x_j \geq 1$ para todo $1 \leq j \leq n$, e $\Delta \geq 0$ um número real. Então o número de somas da forma*

$$S(A) = \sum_{j \in A} x_j \qquad (A \subset [n]) \tag{17}$$

que pertencem a um mesmo intervalo fechado de comprimento Δ é

$$\leq (\lfloor\Delta\rfloor + 1)\binom{n}{\lfloor n/2 \rfloor} \leq C\frac{(\lfloor\Delta\rfloor+1)2^n}{\sqrt{n}}, \tag{18}$$

onde C é uma constante universal.

Demonstração. Suponha que as somas em (17) pertençam a um dado intervalo fechado I de comprimento Δ para certos $A \subset [n]$. Seja $\mathcal{A} = \mathcal{A}(I) \subset \mathcal{P}([n])$ o sistema de conjuntos formado exatamente por estes A, isto é,

$$\mathcal{A} = \{A \subset [n] \colon S(A) \in I\}. \tag{19}$$

O que podemos dizer sobre $\mathcal{A}$? Se temos em $\mathcal{A}$ uma cadeia de conjuntos

$$A_0 \subset \cdots \subset A_\ell \text{ com } A_{i-1} \neq A_i \text{ para todo } 1 \leq i \leq \ell, \tag{20}$$

então claramente

$$S(A_\ell) - S(A_0) \geq \ell, \tag{21}$$

de onde segue que $\ell \leq \Delta$, pela definição de $\mathcal{A}$. Um pequeno raciocínio agora mostra que se toda cadeia como em (20) contida em $\mathcal{A}$ é tal que $\ell \leq \Delta$, então

$$\mathcal{A} = \mathcal{A}_0 \cup \cdots \cup \mathcal{A}_{\lfloor \Delta \rfloor}, \tag{22}$$

onde cada $\mathcal{A}_j$ $(0 \leq j \leq \Delta)$ é um sistema de Sperner, isto é, não contém dois membros $A \neq A'$ com $A \subset A'$. Pelo Corolário 2 e a fórmula de Stirling (veja o Apêndice A), concluímos que

$$|\mathcal{A}| \leq (\lfloor \Delta \rfloor + 1)\binom{n}{\lfloor n/2 \rfloor} \leq C\frac{(\Delta+1)2^n}{\sqrt{n}}, \tag{23}$$

para uma constante absoluta C. O limite (18) segue de (19) e (23). □

Observação 5. Erdős **[18]** e Sperner **[68]** de fato provaram que se toda cadeia como em (20) contida em $\mathcal{A}$ é tal que $\ell \leq \Delta$, então $\mathcal{A}$ tem no máximo

$$\max \sum_{0 \leq j \leq \Delta} \binom{n}{u_j} \tag{24}$$

membros, onde o máximo é tomado sobre todas as seqüências de inteiros consecutivos $u_0 < \cdots < u_{\lfloor \Delta \rfloor}$. Claramente, (24) é a soma dos $\lfloor \Delta \rfloor + 1$ maiores coeficientes binomiais na n-ésima linha do triângulo de Pascal. Note que o limitante superior (24) pode ser atingido.

Agora podemos provar o Teorema 3.

Demonstração do Teorema 3. Fixe z_j $(1 \leq j \leq n)$ e r como no enunciado do teorema. Cada z_j é tal que a sua parte real $\operatorname{Re} z_j$ ou a sua parte imaginária $\operatorname{Im} z_j$ é em valor absoluto $\geq 1/\sqrt{2} > 1/2$. Considerando uma rotação por $\pi/2$, ou equivalentemente a troca dos z_j por iz_j $(1 \leq j \leq n,\ i = \sqrt{-1})$, podemos portando supor que $|\operatorname{Re} z_j| \geq 1/2$ para todo $1 \leq j \leq t$, onde $t \geq n/2$. Ademais, claramente podemos trocar z_j por $-z_j$ para qualquer j, de forma que podemos supor que temos

$$\operatorname{Re} z_j \geq \frac{1}{2}$$

para todo $1 \leq j \leq t$. Fixe agora os valores de $\varepsilon_j \in \{\pm 1\}$ para $j > t$, de forma arbitrária. Note que há 2^{n-t} formas de se fazer isto.

Considere as 2^t somas da forma

$$\sum_{1 \leq j \leq t} \varepsilon_j z_j, \text{ com } \varepsilon_j \in \{\pm 1\}\ (1 \leq j \leq t). \tag{25}$$

Ponha

$$x_j = 2 \operatorname{Re} z_j \geq 1 \qquad (1 \leq j \leq t). \tag{26}$$

Se N das somas da forma (25) pertencem a um disco fechado de raio r, então, considerando apenas a parte real dos z_j, temos N somas da forma

$$\sum_{1 \leq j \leq t} \varepsilon_j x_j, \text{ com } \varepsilon_j \in \{\pm 1\}\ (1 \leq j \leq t), \tag{27}$$

contidas em um intervalo fechado de comprimento $4r$ (veja (26)). Pelo Lema 4,

$$N \leq (4r+1)\binom{t}{\lfloor t/2 \rfloor} \leq C\frac{(4r+1)2^t}{\sqrt{t}}. \tag{28}$$

Provamos que para cada uma das formas de se fixar os $\varepsilon_j \in \{\pm 1\}$ $(t < j \leq n)$, o número máximo de somas da forma (25) que pertencem a um mesmo disco fechado de raio r é limitado superiormente por (28). Como temos 2^{n-t} formas para fixar os ε_j $(j > t)$ e $t \geq n/2$, temos, para uma constante absoluta B, no máximo

$$C\frac{(4r+1)2^t}{\sqrt{t}}2^{n-t} \leq B\frac{(r+1)2^n}{\sqrt{n}}$$

somas da forma (10) em um mesmo disco fechado de raio r, como queríamos demonstrar. A prova do Teorema 3 está completa. $\square$

Finalmente, mencionamos que a história desse problema geométrico não acaba com o resultado de Erdős acima. Passemos a considerar a versão com somas do tipo (13) ($\delta_j \in \{0,1\}$, $1 \leq j \leq n$) e diâmetro Δ. Passemos também a considerar os z_j no $\mathbb{R}^d$ (até agora, tínhamos $d = 2$). Agora a nossa hipótese sobre os z_j é que eles satisfazem $\|z_j\| \geq 1$ para todo $1 \leq j \leq n$. Colocamos $V = (z_j)_{1 \leq j \leq n}$. Ponha

$$\Sigma = \{S(\boldsymbol{\delta}) \colon \boldsymbol{\delta} \in \{0,1\}^n\}; \tag{29}$$

isto é, Σ é a família das 2^n somas possíveis da forma (13). Aqui, queremos considerar Σ como um 'multiconjunto', isto é, levamos em conta a multiplicidade com que cada elemento ocorre em Σ. Agora pomos

$$m(V,\Delta) = \max_B |B \cap \Sigma|,$$

onde o máximo é tomado sobre as bolas fechadas $B \subset \mathbb{R}^d$ de diâmetro Δ. Finalmente, pomos

$$m(n,\Delta) = m_d(n,\Delta) = \max_V m(V,\Delta),$$

onde o máximo é tomado sobre todas as seqüências V de vetores

$$z_1, \ldots, z_n \in \mathbb{R}^d$$

com $\|z_j\| \geq 1$ para todo j.

O Teorema 4 (veja também a Observação 5) diz que $m_1(n,\Delta)$ é a soma dos $\lfloor\Delta\rfloor+1$ maiores coeficientes binomiais na n-ésima linha do triângulo de Pascal.

Katona [**48**] e Kleitman [**49**] provaram que $m_2(n,\Delta)=\binom{n}{\lfloor n/2\rfloor}$ se $\Delta<1$, e isto foi generalizado por Kleitman [**50**] para $d\geq 2$ (inclusive para normas arbitrárias em $\mathbb{R}^d$). Vários resultados seguiram-se para $\Delta\geq 1$, até que, finalmente, em um trabalho publicado no *Annals of Mathematics* em 1988, Frankl e Füredi [**30**] provaram o seguinte teorema, que confirmou uma conjectura de Erdős (veja [**51**]).

TEOREMA 6. *Seja $d\geq 1$ um inteiro e $\Delta\geq 0$ um número real fixo. Então*
$$m_d(n,\Delta)=(\lfloor\Delta\rfloor+1+o(1))\binom{n}{\lfloor n/2\rfloor},$$
onde $o(1)\to 0$ conforme $n\to\infty$.

Concluímos observando que, com o que temos à disposição, podemos provar uma cota superior da forma

$$c(d)(\lfloor\Delta\rfloor+1)\binom{n}{\lfloor n/2\rfloor} \tag{30}$$

para $m_d(n,\Delta)$, onde $c(d)$ é uma constante que depende apenas da dimensão d.

2.1.4. *Uma aplicação à teoria dos números.* Nesta seção, apresentamos uma aplicação do teorema de Sperner à teoria dos números. Esta aplicação está relacionada com o que discutimos em §2.1.1. Dizemos que uma seqüência de inteiros positivos $a_1<a_2<\ldots$ é *primitiva* se nenhum a_i divide outro a_j $(i<j)$. Vimos em §2.1.1 que qualquer seqüência primitiva em $[2n]$ tem no máximo n elementos. No que segue, ao tratarmos de seqüências primitivas $A=(a_i)$, sempre supomos $a_1<a_2<\cdots$.

Uma medida interessante para o 'tamanho' de seqüências $A=(a_i)$ é a função

$$A(x)=\sum_{a_i\leq x}\frac{1}{a_i}, \tag{31}$$

isto é, a soma dos inversos dos membros de A que são $\leq x$ ($x \in \mathbb{R}$). Note que no caso em que a seqüência $A = (a_i)$ é $1 < 2 < \dots$, temos

$$\lim_{x\to\infty} \frac{1}{\log x} A(x) = 1, \tag{32}$$

pois

$$\log(n+1) < H_n = \sum_{1\leq k\leq n} \frac{1}{k} < \log n + 1 \tag{33}$$

para todo $n > 1$. As desigualdades em (33) podem ser provadas comparando-se a soma com a integral $\int_1^n dx/x = \log n$. (O número H_n acima é conhecido como o *n-ésimo número harmônico*. Aproximações mais precisas de H_n surgirão mais à frente nestas notas.) Em geral, o limite no lado esquerdo de (32) (quando ele existe) é conhecido como a *densidade logarítmica* de $A = (a_i)$.

O que podemos dizer sobre $A(x)$ se $A = (a_i)$ é uma seqüência primitiva? Nesta seção, vamos provar o seguinte teorema de Behrand [**8**], de 1935.

Teorema 7. *Existe uma constante absoluta $c > 0$ tal que, para toda seqüência primitiva de inteiros $A = (a_i)$, temos*

$$A(n) = \sum_{a_i\leq n} \frac{1}{a_i} \leq c\,\frac{\log n}{\sqrt{\log\log n}} \tag{34}$$

para todo $n \geq 3$.

Começamos com um aquecimento. Escreva $d(m)$ para o número de divisores (positivos) de um inteiro positivo m. Por exemplo, $d(6) = 4$.

Lema 8. *Temos*

$$\sum_{m\leq x} d(m) \leq 3x\log x, \tag{35}$$

para todo $x \geq 2$.

Demonstração. Note que $d(m)$ é o número de jeitos de se fatorar m como o produto ordenado de dois inteiros (os $d(6) = 4$ divisores de 6 correspondem às fatorações 1×6, 2×3, 3×2, e 6×1). Assim, a soma do lado esquerdo de (35) é

$$\sum\nolimits_{a,b}^{x} 1,$$

onde escrevemos $\sum_{a,b}^{x}$ para a soma sobre todos os pares (a, b) de inteiros positivos com $ab \leq x$. Entretanto,

$$\sum\nolimits_{a,b}^{x} 1 = \sum_{a \leq x} \sum_{b \leq x/a} 1 = \sum_{a \leq x} \left\lfloor \frac{x}{a} \right\rfloor \leq x \sum_{a \leq x} \frac{1}{a} \leq 3x \log x.$$

Na última desigualdade acima, usamos que o número harmônico $H_a = 1 + 1/2 + \cdots + 1/a$ é limitado superiormente por $\log a + 1 \leq 3 \log a$ para todo $a \geq 2$ (veja (33)). □

Fixemos agora uma seqüência primitiva $A = (a_i)$. Queremos provar a desigualdade (34). Para cada inteiro $u > 0$, seja $r(u)$ o número de elementos a_i em A tais que a_i divide u. Vamos considerar a soma

$$\varrho(n) = \sum_{u \leq n} r(u). \tag{36}$$

Escrevendo $\sum_{m,a_i}^{n}$ para a soma sobre todos os pares (m, a_i) com $ma_i \leq n$, m inteiro, e a_i um elemento de A, temos

$$\varrho(n) = \sum\nolimits_{m,a_i}^{n} 1,$$

que é igual a

$$\sum_{a_i \leq n} \sum_{ma_i \leq n} 1 = \sum_{a_i \leq n} \left\lfloor \frac{n}{a_i} \right\rfloor = n \sum_{a_i \leq n} \frac{1}{a_i} + O(n). \tag{37}$$

Como de costume, escrevemos $O(f(n))$ para qualquer função $g(n)$ com

$$|g(n)| \leq Cf(n)$$

para todo $n \geq n_0$, onde n_0 e C são constantes independentes de n. De (37), deduzimos

$$\sum_{a_i \leq n} \frac{1}{a_i} = \frac{1}{n}\varrho(n) + O(1). \tag{38}$$

Para provarmos (34), é suficiente estimar $\varrho(n)$ por cima de forma apropriada. Para tanto, estimaremos $r(u)$ (veja (36)).

O que podemos dizer sobre $r(u)$? Suponha inicialmente que

(*) todos os elementos de $A = (a_i)$ são livres de quadrados (isto é, nenhum divisor de a_i é um quadrado > 1 $(i \geq 1)$).

No que segue, escrevemos $\omega(v)$ para o número de divisores primos distintos de v (por exemplo, $\omega(12) = 2$). Claramente, segue da hipótese (*), da primitividade de $A = (a_i)$, e do teorema de Sperner, Corolário 2, que

$$r(u) \leq \binom{k}{\lfloor k/2 \rfloor} = O\left(\frac{2^k}{\sqrt{k}}\right). \tag{39}$$

(A última estimativa segue da fórmula de Stirling para fatoriais; veja o Apêndice A.) Estimemos $\varrho(n)$ distingüindo os u que têm muitos divisores primos daqueles que têm poucos divisores primos:

$$\begin{aligned}\varrho(n) &\leq \sum_{u \leq n,\, \omega(u) \leq \ell} O\left(\frac{2^{\omega(u)}}{\sqrt{\omega(u)}}\right) + \sum_{u \leq n,\, \omega(u) > \ell} O\left(\frac{2^{\omega(u)}}{\sqrt{\omega(u)}}\right) \\ &= O(1)\frac{2^\ell}{\sqrt{\ell}}n + O\left(\frac{1}{\sqrt{\ell}}\right)\sum_{u \leq n} 2^{\omega(u)}.\end{aligned} \tag{40}$$

Podemos agora usar que $\sum_{u \leq n} 2^{\omega(u)} \leq \sum_{u \leq n} d(u)$, que, pelo Lema 8, é $O(n \log n)$. Em (40), tomamos $\ell = \log\log n$. Disto resulta que

$$\varrho(n) = O\left(n \frac{\log n}{\sqrt{\log\log n}}\right), \tag{41}$$

e a estimativa (34) segue para o caso em que (*) vale, devido a (38). Precisamos agora eliminar a hipótese (*).

Seja $(a_i^{(k)})$ a subseqüência de $A = (a_i)$ formada pelos elementos $a_i^{(k)}$ de A com $a_i^{(k)} = k^2 q_i^{(k)}$, onde $q_i^{(k)}$ é um inteiro livre de quadrados; em outras palavras, a subseqüência $(a_i^{(k)})$ é formada pelos elementos de A cujos fatores quadráticos máximos são exatamente k^2. Temos

$$\begin{aligned}(42)\qquad \sum_{a_i \le n} \frac{1}{a_i} &= \sum_{k \ge 1} \sum_{a_i^{(k)} \le n} \frac{1}{a_i^{(k)}} \\ &= \sum_{k \ge 1} \frac{1}{k^2} \sum_{q_i^{(k)} \le n/k^2} \frac{1}{q_i^{(k)}} \le \sum_{k \ge 1} \frac{1}{k^2} \sum_{q_i^{(k)} \le n} \frac{1}{q_i^{(k)}}.\end{aligned}$$

Como a seqüência $(q_i^{(k)})$ é claramente primitiva e também é formada por inteiros livres de quadrados, podemos aplicar a desigualdade (34), isto é, temos

$$(43)\qquad \sum_{q_i^{(k)} \le n} \frac{1}{q_i^{(k)}} = O\left(\frac{\log n}{\sqrt{\log\log n}}\right).$$

Como $\sum_{k \ge 1} k^{-2}$ converge (de fato, esta soma é $\zeta(2) = \pi^2/6$), a desigualdade (34) segue de (42) e (43). O Teorema 7 está provado.

Observação finais. O leitor pode ficar curioso em saber o quão bom é o limitante (34). Uma seqüência primitiva canônica é a seqüência dos primos (p_k), e nesse caso temos

$$(44)\qquad \sum_{p_k \le n} \frac{1}{p_k} = \log\log n + O(1),$$

que é muito menor que o lado direito de (34) (para (44), veja, por exemplo, a Seção 7 do Capítulo 22 de Hardy e Wright [**44**]). Entretanto, podemos incrementar esta construção de forma simples. Consideremos primeiro como lidar, separadamente, com os segmentos iniciais dos inteiros $[n] = \{1, \ldots, n\}$. Fixe um inteiro $n \ge 3$. Seja $\mathcal{A}_n \subset [n]$ o conjunto dos inteiros $1 \le k \le n$ com exatamente $\ell = \lfloor \log\log n \rfloor$ divisores primos, levando em conta multiplicidades. Formalmente, se $\Omega(k)$ é número de divisores primos de k contando multiplicidades (por exemplo,

$\Omega(12) = 3$), então

$$\mathcal{A}_n = \{k\colon 1 \le k \le n \text{ e } \Omega(k) = \lfloor \log\log n \rfloor\}. \tag{45}$$

Antes de continuarmos, observamos que a escolha do valor de ℓ pode ser entendida levando-se em conta um resultado de Hardy e Ramanujan, que diz que $\Omega(k)$ é tipicamente $\log\log n$ para $1 \le k \le n$ (veja [**44**, Capítulo 22, Seção 10]).

Voltemos aos nossos conjuntos $\mathcal{A}_n$ em (45). É fácil ver que $\mathcal{A}_n \subset [n]$ é primitivo (ou melhor, a seqüência crescente correspondente é uma seqüência primitiva), isto é, para quaisquer dois elementos distintos a e a' em A, temos que a não divide a'. Vale o seguinte resultado, devido a Pillai [**61**].

Teorema 9. *Existe uma constante absoluta $c > 0$ tal que, para todo $n \ge 3$, temos*

$$\sum_{a \in \mathcal{A}_n} \frac{1}{a} \ge \frac{c \log n}{\sqrt{\log\log n}}. \tag{46}$$

Seja (c_n) uma seqüência decrescentes de reais positivos com $c_n \to 0$ conforme $n \to \infty$. Pode se construir uma seqüência infinita (a_i) a partir dos $\mathcal{A}_n$ ($n \ge 3$) para a qual vale o seguinte: *para infinitos valores de n, temos*

$$\sum_{a_i \le n} \frac{1}{a_i} \ge \frac{c_n \log n}{\sqrt{\log\log n}}. \tag{47}$$

Fechamos esta seção enunciando sem prova um resultado de Erdős, Sárközy, e Szemerédi [**27**], que melhora o teorema de Behrend.

Teorema 10. *Para toda seqüência primitiva de inteiros $A = (a_i)$, temos*

$$\sum_{a_i \le n} \frac{1}{a_i} = o\left(\frac{\log n}{\sqrt{\log\log n}}\right). \tag{48}$$

Em vista das observações acima, o Teorema 10 não pode ser substancialmente melhorado. Finalmente, o leitor deve comparar os Teoremas 9 e 10 para observar a diferença substancial que existe entre seqüências primitivas finitas e infinitas.

Uma excelente referência para os resultados desta seção é a monografia *Sequences*, de Halberstam e Roth [**43**].

2.2. O teorema de Erdős, Ko, e Rado. Na Seção 2.1, investigamos quantos membros um sistema de conjuntos $\mathcal{A} \subset \mathcal{P}([n])$ pode ter, se supomos que $\mathcal{A}$ não contém dois elementos comparáveis. Uma outra gama de problemas extremais para sistemas de conjuntos vêm da imposição de condições sobre as interseções dos membros do sistema. Por exemplo, o que podemos dizer sobre $|\mathcal{A}|$ se um sistema $\mathcal{A} \subset \mathcal{P}([n])$ é tal que todo membro de $\mathcal{A}$ intersecta qualquer outro? Dizemos que $\mathcal{A}$ é um *sistema intersectante* quando vale esta condição.

O problema acima é fácil: claramente podemos ter sistemas intersectantes com 2^{n-1} elementos; basta por exemplo considerar o sistema

$$\mathcal{A}_1 = \{A \subset [n] \colon 1 \in A\}.$$

Por outro lado, se temos $> 2^{n-1}$ membros em $\mathcal{A}$, então necessariamente $\mathcal{A}$ contém um conjunto A e seu complemento $A^c = [n] \setminus A$, que claramente implica que $\mathcal{A}$ não é intersectante.

O problema extremal de determinar o maior tamanho de um sistema intersectante contido em

$$\binom{[n]}{k} = \{A \subset [n] \colon |A| = k\}$$

é muito mais interessante. De fato, este problema foi estudado por Erdős, Ko, e Rado em 1938, embora o resultado tenha sido publicado [**25**] apenas em 1961.

É fácil construir um sistema intersectante $\mathcal{A}$ 'grande' de k-conjuntos (isto é, conjuntos com k elementos) contidos em $[n]$. Observemos inicialmente que se $2k > n$, então podemos tomar $\mathcal{A} = \binom{[n]}{k}$, pois quaisquer dois k-subconjuntos de $[n]$ se intersectam neste caso. Suporemos daqui para frente que $2k \leq n$. Neste caso, podemos tomar

$$\mathcal{A}_0 = \{A \subset [n] \colon |A| = k \text{ e } 1 \in A\}. \tag{49}$$

Claramente, temos que $\mathcal{A}_0$ é intersectante e

$$|\mathcal{A}_0| = \binom{n-1}{k-1}. \tag{50}$$

O teorema de Erdős, Ko, e Rado afirma que todo sistema intersectante formado por k-subconjuntos de $[n]$ tem tamanho no máximo $|\mathcal{A}_0| = \binom{n-1}{k-1}$, desde que $n \geq 2k$. Ademais, se um tal sistema tem tantos membros quanto $\mathcal{A}_0$, então ele é *isomorfo* a $\mathcal{A}_0$, desde que $n > 2k$; em outras palavras, existe essencialmente uma única forma de se construir um tal sistema de cardinalidade máxima!

Como o leitor já deve imaginar, dizemos que dois sistemas de conjuntos $\mathcal{A} \subset \mathcal{P}(X)$ e $\mathcal{B} \subset \mathcal{P}(Y)$ são isomorfos se existe uma bijeção $b \colon X \to Y$ tal que $A \in \mathcal{A}$ se e só se

$$b(A) = \{b(a) \colon a \in A\} \in \mathcal{B}.$$

O teorema de Erdős, Ko, e Rado é como segue.

Teorema 11. *Seja $\mathcal{A} \subset \binom{[n]}{k}$, com $n \geq 2k > 0$. Se $\mathcal{A}$ é um sistema intersectante, então*

$$|\mathcal{A}| \leq \binom{n-1}{k-1}. \tag{51}$$

Ademais, se $n > 2k$ e vale a igualdade em (51), então $\mathcal{A}$ é isomorfo ao sistema $\mathcal{A}_0$ definido em (49).

Demonstração. Usaremos um método muito engenhoso inventado por Katona. Consideremos 'permutações cíclicas' dos elementos de $[n]$:

$$\phi \colon a_0, a_1, \ldots, a_{n-1}, \tag{52}$$

onde os índices são considerados módulo n. Mais formalmente, consideramos bijeções

$$\phi\colon \mathbb{Z}/n\mathbb{Z} \to [n],$$

e colocamos $a_i = \phi(i)$ para todo i. Dado uma tal ϕ e um conjunto $A \subset [n]$ com $|A| = k$, dizemos que ϕ e A são *compatíveis* se A ocorre como um 'segmento' em (52). Formalmente, a condição que exigimos é que A seja igual a $\{a_{i+1}, \ldots, a_{i+k}\}$ para algum $i \in \mathbb{Z}/n\mathbb{Z}$. (Note que, como os índices são módulo n, o conjunto A pode 'dar a volta'.)

Observemos inicialmente que, dada uma permutação cíclica ϕ como em (52),

(*) *existem no máximo k membros de $\mathcal{A}$ que são compatíveis com esta permutação.*

De fato, seja $A \in \mathcal{A}$ um membro de $\mathcal{A}$ compatível com ϕ. Suponha que $A = \{a_{i+1}, \ldots, a_{i+k}\}$ para um dado $i \in \mathbb{Z}/n\mathbb{Z}$. Para cada $2 \le j \le k$, podemos considerar os conjuntos disjuntos

$$J_j^- \text{ e } J_j^+ \subset \mathbb{Z}/n\mathbb{Z}$$

dados por

$$J_j^- = \{a_{i+j-\lfloor n/2 \rfloor}, \ldots, a_{i+j-1}\}$$

e

$$J_j^+ = \{a_{i+j}, \ldots, a_{i+j+\lfloor n/2 \rfloor}\}.$$

Claramente, apenas um dentre J_j^- e J_j^+ pode conter um membro de $\mathcal{A}$, pois $J_j^- \cap J_j^+ = \emptyset$. Por outro lado, todo membro A' de $\mathcal{A}$ que é diferente de A mas é compatível com ϕ precisa estar contido em J_j^- ou J_j^+ para algum j, pois $A' \cap A \neq \emptyset$. A asserção (*) está provada.

Agora contamos de duas maneiras os pares da forma (ϕ, A) com ϕ uma permutação cíclica e A um membro de $\mathcal{A}$ com ϕ e A compatíveis. Seja P o número de tais pares. Devido à (*), fixada uma ϕ, existem no máximo k tais pares. Por outro lado, fixado $A \in \mathcal{A}$, temos

$$n \times k!(n-k)!$$

permutações cíclicas compatíveis com A. Concluímos que

$$|\mathcal{A}|nk!(n-k)! = P \leq \sum_{\pi} k = n!k,$$

de onde (51) segue.

A prova da unicidade das configurações extremas para o caso em que $n > 2k$ é um pouco delicada, e fica como um bom exercício para o leitor. $\square$

Antes de passarmos para o nosso próximo tópico, fica como exercício para o leitor esclarecer a situação no caso em que $n = 2k$. O que são os sistemas intersectantes $\mathcal{A} \subset \binom{[2k]}{k}$?

Consideremos agora sistemas *ℓ-intersectantes* de k-subconjuntos de $[n]$, isto é, sistemas de conjuntos $\mathcal{A} \subset \binom{[n]}{k}$ com $|A \cap B| \geq \ell$ para todo A e $B \in \mathcal{A}$. Naturalmente, até agora temos considerado sistemas 1-intersectantes. Erdős, Ko, e Rado também provaram limitantes superiores para o tamanho de sistemas ℓ-intersectantes para $\ell > 1$.

Considere a seguinte construção simples de sistemas ℓ-intersectantes ($\ell \geq 1$). Seja $L \subset [n]$ um conjunto com ℓ elementos. O sistema ℓ-intersectante *fixado* por L é o sistema

$$\mathcal{A}_L = \{A \subset [n] \colon |A| = k,\ L \subset A\}. \tag{53}$$

Note que $|\mathcal{A}_L| = \binom{n-\ell}{k-\ell}$. Para o caso em que n é grande em relação a k, os sistemas $\mathcal{A}_L$ fixados por ℓ-conjuntos L são os sistemas ℓ-intersectantes de tamanho máximo.

Teorema 12. *Para todo ℓ e k com $1 \leq \ell \leq k$ existe um $n_0 = n_0(\ell, k)$ para o qual vale o seguinte. Se $\mathcal{A} \subset \binom{[n]}{k}$ é um sistema ℓ-intersectante e $n \geq n_0$, então*

$$|\mathcal{A}| \leq \binom{n-\ell}{k-\ell}. \tag{54}$$

Ademais, se vale a igualdade em (54), então $\mathcal{A}$ é um sistema fixado por algum ℓ-conjunto $L \subset [n]$.

Demonstração. Seja $\mathcal{A}$ um sistema ℓ-intersectante como no enunciado. Naturalmente, não há nada a fazer se $k = \ell$, e portanto supomos $k > \ell$. Podemos também supor que $\mathcal{A}$ é *maximal*, isto é, ao adicionarmos qualquer k-conjunto B contido em $[n]$ a $\mathcal{A}$, se $B \notin \mathcal{A}$, o sistema $\mathcal{A}$ deixa de ser ℓ-intersectante.

Da maximalidade de $\mathcal{A}$ segue que há dois membros A e $A' \in \mathcal{A}$ com $|A \cap A'| = \ell$. Seja $L = A \cap A'$. Se todos os membros de $\mathcal{A}$ contém L, então $\mathcal{A} \subset \mathcal{A}_L$ e não há nada a provar. Supomos portanto que

$$\text{existe } B \in \mathcal{A} \text{ com } |B \cap L| < \ell. \tag{55}$$

Ponha $U = A \cup A' \cup B$ e suponha agora que $C \in \mathcal{A} \setminus \{A, A', B\}$. Afirmamos que

$$|C \cap U| \geq \ell + 1. \tag{56}$$

De fato, note que C contém um elemento de $B \setminus L$, pois $|B \cap L| < \ell$ e $|C \cap B| \geq \ell$. Portanto, se $L \subset C$, a nossa afirmação já está verificada. Suponha que $L \not\subset C$. Então, para que $|C \cap A|$, $|C \cap A'| \geq \ell$, precisamos que $|C \cap (A \cup A')| \geq \ell + 1$ (pois $L = A \cap A'$ tem exatamente ℓ elementos e $L \not\subset C$). Novamente, a nossa afirmação (56) está verificada.

Note que (56) vale também para $C \in \{A, A', B\}$. Portanto temos, muito generosamente,

$$|\mathcal{A}| \leq 2^{|U|} \sum_{j \leq k-\ell-1} \binom{n-|U|}{j}. \tag{57}$$

De fato, todo membro C de $\mathcal{A}$ pode ser escrito como $C_1 \cup C_2$ onde $C_1 = C \cap U$ e $C_2 = C \setminus U$. Como há $2^{|U|}$ possibilidades para C_1 e, dado C_1, há no máximo

$$\sum_{j \leq k-\ell-1} \binom{n-|U|}{j}$$

possibilidades para C_2 (pois $|C_2| \leq k-\ell-1$), a desigualdade (57) segue. Note que o lado direito de (57) é $O(n^{k-\ell-1})$ e o lado direito de (54) não é $O(n^{k-\ell-1})$. Finalmente, lembre que deduzimos (57) supondo (55).

O Teorema 12 está provado: se (55) vale, então (57) vale e portanto (54) vale estritamente para n suficientemente grande; por outro lado, se (55) não vale, então todo membro de $\mathcal{A}$ contém L. □

3. Técnicas da álgebra linear

Consideraremos nesta seção teoremas extremais para sistemas de conjuntos $\mathcal{A}$ com restrições de paridade nas cardinalidades das interseções entre pares de membros de $\mathcal{A}$. O nosso primeiro resultado é o seguinte.

Teorema 13. *Suponha que $\mathcal{A} \subset \mathcal{P}([n])$ é um sistema de conjuntos tal que*

(i) $|A|$ é ímpar para todo $A \in \mathcal{A}$,
(ii) $|A \cap A'|$ é par para todo A e $A' \in \mathcal{A}$ com $A \neq A'$.

Então $|\mathcal{A}| \leq n$.

Demonstração. A prova deste teorema usa uma técnica um tanto inesperada: álgebra linear sobre o corpo $\mathbb{F}_2 = \mathrm{GF}(2)$ dos inteiros módulo 2. De fato, consideremos os *vetores característicos* $\mathbf{x}_A = (x_i^{(A)})_{i\in[n]}$ dos membros $A \in \mathcal{A}$. Aqui, temos

$$x_i^{(A)} = \begin{cases} 0 & \text{if } i \notin A \\ 1 & \text{if } i \in A \end{cases}$$

para todo $i \in [n]$. Afirmamos que os vetores $\mathbf{x}_A$ ($A \in \mathcal{A}$) são linearmente independentes sobre $\mathbb{F}_2$. Note que isto termina a prova, pois estes vetores estão contidos em $\mathbb{F}_2^n$, que tem dimensão n.

Para provar a independência linear dos vetores $\mathbf{x}_A$ ($A \in \mathcal{A}$), suponha que tenhamos

$$\sum_{A\in\mathcal{A}} \lambda_A \mathbf{x}_A = 0, \tag{58}$$

com $\lambda_A \in \mathbb{F}_2$ para todo $A \in \mathcal{A}$. Usamos agora o fato que podemos definir um produto escalar $\mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ colocando

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T \mathbf{y} \bmod 2 = \sum_{1 \leq i \leq n} x_i y_i \bmod 2, \tag{59}$$

onde $\mathbf{x} = (x_i)$ e $\mathbf{y} = (y_i)$. (A única propriedade que queremos sobre $\langle \mathbf{x}, \mathbf{y} \rangle$ é que ele seja linear na segunda entrada: $\langle \mathbf{x}, \lambda_1 \mathbf{y}_1 + \lambda_2 \mathbf{y}_2 \rangle = \lambda_1 \langle \mathbf{x}, \mathbf{y}_1 \rangle + \lambda_2 \langle \mathbf{x}, \mathbf{y}_2 \rangle$). Fixe agora $A_0 \in \mathcal{A}$, e considere o vetor característico $\mathbf{x}_{A_0}$ de A_0. Segue de (58) que

$$\sum_{A \in \mathcal{A}} \lambda_A \langle \mathbf{x}_{A_0}, \mathbf{x}_A \rangle = \left\langle \mathbf{x}_{A_0}, \sum_{A \in \mathcal{A}} \lambda_A \mathbf{x}_A \right\rangle = 0. \tag{60}$$

Entretanto, as hipóteses (i) e (ii) do nosso teorema implicam que o lado esquerdo de (60) é λ_{A_0}! Daí segue que os vetores $\mathbf{x}_A$ $(A \in \mathcal{A})$ são linearmente independentes, como queríamos demonstrar. $\square$

A demonstração muito elegante do Teorema 13 acima merece ser estudada com cuidado. Este texto usará argumentos desse gênero várias vezes. O leitor apreciará o poder do argumento algébrico acima ao tentar encontrar uma prova puramente combinatória do resultado acima. Tente!

O que ocorre se mudamos as paridades no enunciado do Teorema 13? Suponha que exigimos agora que os membros de $\mathcal{A}$ tenham todos cardinalidade par, e mantenhamos a condição (ii) (todas as interseções pares). Temos aqui uma situação surpreendentemente diferente, como mostra a seguinte construção. Considere inicialmente uma partição de $[n]$ em pares, como por exemplo

$$[n] = \{1, 2\} \cup \{2, 3\} \cup \dots \tag{61}$$

(o último bloco desta partição é na verdade um conjunto unitário se n é ímpar). Sejam $p_1, \dots, p_{\lfloor n/2 \rfloor}$ os pares que compõe esta partição. Ponha

$$\mathcal{A} = \{A \subset [n] \colon \text{se } p_i \cap A \neq \emptyset, \text{ então } p_i \subset A\}. \tag{62}$$

Isto é, os membros de $\mathcal{A}$ são os conjuntos que podem ser escritos como uma união dos p_i $(1 \leq i \leq \lfloor n/2 \rfloor)$. Claramente, $|A|$ é par para todo $A \in \mathcal{A}$ e (ii) do Teorema 13 vale para $\mathcal{A}$. Entretanto,

$$|\mathcal{A}| = 2^{\lfloor n/2 \rfloor}.$$

Isto é, trocando a hipótese na paridade exigida em (i) no Teorema 13 passamos a permitir sistemas com um número exponencial de membros. (Antes os sistemas tinham no máximo n membros!)

Precisamos agora encontrar limitantes superiores para os nossos novos sistemas. Na verdade, o nosso resultado diz que a construção que estudamos acima fornece sistemas extremais.

TEOREMA 14. *Suponha que* $\mathcal{A} \subset \mathcal{P}([n])$ *é um sistema de conjuntos tal que*

(i) $|A|$ *é par para todo* $A \in \mathcal{A}$,
(ii) $|A \cap A'|$ *é par para todo* A *e* $A' \in \mathcal{A}$ *com* $A \neq A'$.

Então $|\mathcal{A}| \leq 2^{\lfloor n/2 \rfloor}$.

A prova do teorema acima exige que estudemos álgebra linear sobre corpos finitos (na verdade, $\mathbb{F}_2$) com um pouco mais de cuidado.

3.1. Alguns fatos da álgebra linear. Seja $\mathbb{F}$ um corpo, possivelmente finito, e seja V um espaço vetorial sobre $\mathbb{F}$. Uma função $\beta\colon V \times V \to \mathbb{F}$ é bilinear se ela for linear em cada coordenada:

$$\beta(\lambda u + \mu v, w) = \lambda\beta(u, w) + \mu\beta(v, w)$$

e

$$\beta(w, \lambda u + \mu v) = \lambda\beta(w, u) + \mu\beta(w, v)$$

para todo λ e $\mu \in \mathbb{F}$ e todo u, v, e $w \in V$. Se $V = \mathbb{F}^n$, as formas bilineares β sobre V são exatamente as aplicações $(u, v) \mapsto \beta(u, v) = u^T Bv$, onde B é uma matriz $n \times n$ com entradas em $\mathbb{F}$. Dizemos que β é *simétrica* se a matriz associada a β é uma matriz simétrica, isto é, $B^T = B$.

Um *produto interno* em V é simplesmente uma forma bilinear simétrica. Fixe um produto interno β sobre V, e suponha que V tenha dimensão n. Podemos identificar V com $\mathbb{F}^n$.

Dizemos que dois vetores u e v são *ortogonais* se $\beta(u, v) = 0$, e escrevemos $u \perp v$ nesse caso. O *espaço ortogonal* $W^\perp$ de um subespaço $W \leq V$ é dado por

$$W^\perp = \{v \in V \colon v \perp w \text{ para todo } w \in W\}. \tag{63}$$

Note que $W^\perp$ é um subespaço vetorial de V.

Dizemos que um vetor não-nulo $v \in V$ é *isotrópico* se $v \perp v$. Se U, $W \leq V$ são dois subespaços de V, dizemos que U e W são *ortogonais* se todo $u \in U$ é ortogonal a todo $w \in W$. Nesse caso, escrevemos $U \perp W$. Dizemos que um subespaço $W \leq V$ é *totalmente isotrópico* se $W \perp W$. Note que, em particular, se W é totalmente isotrópico, então todo elemento de W é isotrópico. Ademais, se W é totalmente isotrópico, temos $W \leq W^\perp$.

Finalmente, dizemos que o espaço V é *singular* se $V \cap V^\perp \neq (0)$.

PROPOSIÇÃO 15. *Seja V um espaço vetorial de dimensão n e seja β um produto interno sobre V.*

(*i*) *Para todo subespaço $W \leq V$, temos*

$$\dim W + \dim W^\perp \geq n.$$

(*ii*) *O espaço V não é singular se e só se a matriz B associada à β é não-singular, isto é, tem determinante não-nulo.*

(*iii*) *Se V não é singular, então para todo subespaço $W \leq V$, temos*

$$\dim W + \dim W^\perp = n.$$

DEMONSTRAÇÃO. Seja B a matriz associada à forma β. Usamos nesta prova alguns fatos elementares sobre sistemas de equações lineares.

(i) Seja $w_1, \dots, w_d$ uma base de W. Um vetor $v \in V$ pertence a $W^\perp$ se e só se

$$w_i^T B v = 0, \text{ para todo } 1 \leq i \leq d. \tag{64}$$

O sistema linear acima têm d equações, de forma que a dimensão do espaço das soluções $W^\perp$ é $\geq n-d$. Daí segue que $\dim W + \dim W^\perp \geq n$.

(ii) Suponha que B é singular. Então existe um vetor não-nulo $v \in V$ com $Bv = 0$. Claramente, $\beta(u, v) = u^T B v = 0$ para todo $u \in V$, de forma que $v \in V \cap V^\perp \neq (0)$ e V é, por definição, singular. Suponha agora que B seja não-singular. Então o sistema (64) (com $d = n$ e $w_1, \dots, w_n$ uma base de V) admite apenas a solução trivial $v = 0$ pois os vetores $w_i^T B$ ($1 \leq i \leq n$) são linearmente independentes. Dessa forma $V^\perp = (0)$, e V é não-singular.

(iii) Suponha que w_i ($1 \leq i \leq d$) formam uma base de W, como na prova de (i). De (ii), sabemos que B é não-singular. Portanto, os vetores $w_i^T B$ ($1 \leq i \leq d$) são linearmente independentes. Daí segue que o espaço de soluções do sistema (64) tem dimensão exatamente $n - d$, de onde temos $\dim W + \dim W^\perp = n$. □

Corolário 16. *Seja V um espaço vetorial de dimensão n, munido de um produto interno. Ademais, suponha que V seja não-singular. Então todo subespaço totalmente isotrópico W de V tem dimensão $\leq n/2$.*

Demonstração. Seja W um subespaço totalmente isotrópico de V; temos $W \leq W^\perp$. Como V não é singular, temos de (iii) da Proposição 15 que

$$2 \dim W \leq \dim W + \dim W^\perp = n,$$

o que completa a prova deste corolário. □

3.2. Prova do Teorema 14. Temos agora as ferramentas da álgebra linear necessárias para provar o nosso teorema.

Prova do Teorema 14. Seja $\mathcal{A} \subset \mathcal{P}([n])$ como no enunciado de nosso teorema. Como na demonstração do Teorema 13, consideremos os vetores característicos $\mathbf{x}_A$ ($A \in \mathcal{A}$) dos membros de $\mathcal{A}$. Seja W o subespaço de $V = \mathbb{F}_2^n$ gerado por estes $\mathbf{x}_A$ ($A \in \mathcal{A}$). Consideramos o produto interno canônico

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T \mathbf{y} \bmod 2 = \mathbf{x}^T I_n \mathbf{y} \bmod 2$$

sobre V; a identidade I_n é a matriz associada a este produto interno. Note que temos, portanto, um espaço não-singular. Pelas hipóteses (i) e (ii) de nosso teorema, temos que W é um subespaço totalmente isotrópico. Segue do Corolário 16 que $\dim W \leq n/2$. Naturalmente, temos $\dim W \leq \lfloor n/2 \rfloor$. Ademais, como estamos sobre $\mathbb{F}_2$, claramente $|\mathcal{A}| \leq |W| \leq 2^{\dim W} \leq 2^{\lfloor n/2 \rfloor}$. □

3.2.1. *Observações.* Note que os Teoremas 13 e 14 tratam dos casos "ímpar/par" e "par/par" da paridade das cardinalidades dos membros de $\mathcal{A}$ e interseções dos pares de membros de $\mathcal{A}$. Deixamos como um exercício para o leitor esclarecer a situação para as variantes "ímpar/ímpar" e "par/ímpar".

Terão papel fundamental no Capítulo 2 resultados extremais para sistemas de conjuntos envolvendo restrições módulo p (com p um primo ímpar) para as cardinalidades das interseções dois a dois de seus membros (veja o Teorema 33).

3.3. O teorema de Fisher. O que podemos dizer sobre um sistema de conjuntos se sabemos que a cardinalidade da interseção de quaisquer dois de seus membros é exatamente um valor dado? É intuitivo que tal restrição é muito mais forte que restrições de paridade, como temos visto até o momento. Provaremos o seguinte resultado, às vezes chamado de o teorema de Fisher não-uniforme, usando álgebra linear.

TEOREMA 17. *Fixe inteiros $1 \leq \ell < n$. Suponha que o sistema de conjuntos $\mathcal{A} \subset \mathcal{P}([n])$ é tal que $|A \cap A'| = \ell$ para quaisquer A, $A' \in \mathcal{A}$ distintos. Então $|\mathcal{A}| \leq n$.*

O resultado original provado por Fisher em 1940 aplica-se a sistemas com mais restrições. Bose **[12]** provou o resultado acima no caso em que todos os membros de $\mathcal{A}$ têm a mesma cardinalidade, usando álgebra linear; de fato, foi esta nota de Bose de duas páginas que introduziu esta técnica no estudo de problemas extremais para sistemas de conjuntos.

Na mesma época, independentemente, de Bruijn e Erdős **[16]** provaram o caso $\ell = 1$ do Teorema 17, por métodos combinatórios. Note que mesmo o caso em que $\ell = 1$ é de fato interessante: além da construção óbvia em que todos os membros de $\mathcal{A}$ contêm um elemento fixo e são disjuntos a menos deste elemento, há ainda os exemplos dos planos projetivos finitos, em que todo par de linhas se intersectam em exatamente um ponto.

Majumdar **[58]** e Isbell **[45]** independentemente provaram o Teorema 17; a prova que damos abaixo é devida a estes autores.

Prova do Teorema 17. Consideremos primeiro o caso em que existe um $A \in \mathcal{A}$ com $|A| = \ell$. Então todos os outros membros de $\mathcal{A}$ contém A e não se intersectam fora de A. Portanto $|\mathcal{A}| \leq 1+n-\ell \leq n$, e portanto o nosso resultado vale. Supomos daqui para frente que $|A| > \ell$ para todo $A \in \mathcal{A}$.

Para simplificar a notação, suponha que $\mathcal{A} = \{A_1, \ldots, A_m\}$. Considere os vetores característicos dos A_i: para cada i, seja $\mathbf{x}_i = (x_{ij})_{1\leq j<n}$ onde

$$x_{ij} = \begin{cases} 0 & \text{se } j \notin A_i \\ 1 & \text{se } j \in A_i. \end{cases} \tag{65}$$

Provaremos que os vetores $\mathbf{x}_i$ $(1 \leq i \leq m)$ são linearmente independentes, de onde poderemos concluir que $m \leq n$.

Considere a matriz $M = (x_{ij}) \in \{0,1\}^{m\times n}$ formada pelos x_{ij} definidos em (65); equivalentemente, as linhas da matriz M são justamente os vetores $\mathbf{x}_i$ $(1 \leq i \leq m)$. É fácil ver que vale a identidade

$$A = MM^T = \ell J + D, \tag{66}$$

onde J denota a matriz $m \times m$ com todas as entradas iguais a 1 e $D = \operatorname{diag}(d_1, \ldots, d_m)$ é a matriz diagonal com as entradas $d_i = |A_i| - \ell > 0$

($1 \le i \le m$). Fazemos agora duas observações: se as linhas $\mathbf{x}_i$ de M *não* são linearmente independentes, então existe um vetor não nulo $\mathbf{y} = (y_i) \in \mathbb{R}^m$ com $\mathbf{y}^T M = 0$, de forma que

$$\mathbf{y}^T A \mathbf{y} = 0. \tag{67}$$

A nossa segunda observação é que, devido a (66), o lado esquerdo de (67) pode ser escrito da seguinte forma:

$$\begin{aligned}
\mathbf{y}^T A\mathbf{y} = \mathbf{y}^T(\ell J - D)\mathbf{y} = \ell \mathbf{y}^T J\mathbf{y} + \mathbf{y}^T D\mathbf{y}& \\
= \ell \sum_{1\le i\le m} \sum_{1\le j\le m} y_i y_j + \sum_{1\le i\le m} d_i y_i^2& \\
= \ell\Big(\sum_{1\le i\le m} y_i\Big)^2 + \sum_{1\le i\le m} d_i y_i^2 > 0,&
\end{aligned}$$

o que contradiz (67). Assim, podemos concluir que as linhas $\mathbf{x}_i$ ($1 \le i \le m$) de M são de fato linearmente independentes, de forma que temos necessariamente $m \le n$. O Teorema 17 está provado. $\square$

3.3.1. *Uma interseção proibida.* Embora a relação com o Teorema 17 seja apenas na forma, não resistimos e mencionamos aqui sem prova um resultado profundo de Frankl e Rödl sobre sistemas de conjuntos com restrições na cardinalidade das interseções de pares de seus membros. Paul Erdős **[20]** propôs em 1976 a seguinte conjectura: *se um sistema de conjuntos $\mathcal{A} \subset \mathcal{P}([n])$ é tal que não há em $\mathcal{A}$ dois membros A e A' com $|A \cap A'| = \lfloor n/4 \rfloor$, então $|\mathcal{A}| \le (2-\varepsilon)^n$ para alguma constante absoluta $\varepsilon > 0$.* Em outras palavras, *a proibição de exatamente uma cardinalidade para as interseções dois a dois* provoca uma queda exponencial no tamanho do sistema. (No Teorema 17, exigimos que as interseções sejam todas de uma cardinalidade dada; aqui exigimos que elas sejam quaisquer, a menos de um único valor.) Erdős ofereceu 250 dólares pela resolução desta conjectura.

Onze anos mais tarde, esta conjectura foi provada por Frankl e Rödl **[36]**, na seguinte forma mais forte. Seja $m(n, \ell)$ o tamanho máximo de um sistema de conjuntos $\mathcal{A} \subset \mathcal{P}([n])$ que não contém dois membros A e A' com $|A \cap A'| = \ell$.

Teorema 18. *Para todo* $0 < \eta < 1/4$ *existe uma constante* $\varepsilon = \varepsilon(\eta) > 0$ *para o qual temos*

$$m(n, \ell) \leq (2 - \varepsilon)^n$$

para qualquer inteiro ℓ *com* $\eta n < \ell < (1/2 - \eta)n$.

Para o caso em que $\ell = \lfloor n/4 \rfloor$, o resultado explícito é que

$$m(n, \lfloor n/4 \rfloor) < 1{,}99^n, \tag{68}$$

e, mais geralmente, se $\ell = \lfloor \varrho n \rfloor$, temos

$$m(n, \lfloor \varrho n \rfloor) \leq (2 - \varrho^2/2 + o(\varrho^3))^n. \tag{69}$$

Tomando $\mathcal{A}_\varrho \subset \mathcal{P}([n])$ como sendo o sistema de todos os subconjuntos de $[n]$ com estritamente mais de $(1 + \varrho)n/2$ elementos, vemos que

$$m(n, \lfloor \varrho n \rfloor) \geq (2 - \varrho^2 + o(\varrho^3))^n$$

e, no caso específico em que $\varrho = 1/4$, vemos que

$$m(n, \lfloor n/4 \rfloor) \geq 1{,}9378^n.$$

Estes limites inferiores para $m(n, \ell)$ mostram que (68) e (69) não estão muito longe de serem limitantes ótimos.

A demonstração do Teorema 18 é bastante complexa.

4. O teorema de Ahlswede e Khachatrian

Vimos no Teorema 12 que se n é suficientemente grande em relação a k, então um sistema ℓ-intersectante de k-subconjuntos de $[n]$ tem no máximo $\binom{n-\ell}{k-\ell}$ membros. Ademais, os exemplos extremos são os sistemas $\mathcal{A}_L$ fixados por ℓ-conjuntos L. É natural perguntar se tal restrição sobre n é necessária.

Consideremos as seguintes construções alternativas para sistemas ℓ-intersectantes $\mathcal{A}_i$ $(0 \leq i \leq (n-\ell)/2)$ sobre $[n]$. Para cada inteiro i com $0 \leq 2i \leq n-\ell$, pomos

$$\mathcal{A}_i = \{A \subset [n] \colon |A| = k,\ |A \cap [\ell + 2i]| \geq \ell + i\}. \tag{70}$$

Note que, de fato, os $\mathcal{A}_i$ são ℓ-intersectantes: se A e A' são dois membros de $\mathcal{A}$ distintos, então temos que $A \cap A' \cap [\ell + 2i] \subset A \cap A'$ tem pelo menos ℓ elementos. Ademais, note que $\mathcal{A}_0$ nada mais é que o sistema ℓ-intersectante fixado pelo ℓ-conjunto $L = [\ell]$.

Consideremos um caso extremo: tome $\ell = 2$, $k = 2r$, e $n = 4r$. Então o sistema 2-intersectante $\mathcal{A}_i$ com $i = r-1$ é

$$\mathcal{A}_{r-1} = \{A \subset [n] \colon |A| = k,\ |A \cap [2r]| \geq r+1\},$$

e tem cardinalidade

$$|\mathcal{A}_{r-1}| = \frac{1}{2}\left(\binom{4r}{2r} - \binom{2r}{r}\right) = \left(\frac{1}{2} + o(1)\right)\binom{4r}{2r}. \tag{71}$$

Por outro lado, um sistema $\mathcal{A}_L$ fixado por um 2-conjunto L (veja (53)) tem

$$|\mathcal{A}_L| = \binom{4r-2}{2r-2} = \left(\frac{1}{4} + o(1)\right)\binom{4r}{2r}. \tag{72}$$

Comparando (71) e (72) vemos que, em geral, a construção (70) com $i > 0$ pode fornecer sistemas ℓ-intersectantes maiores que aqueles fixados por ℓ-conjuntos L.

Não é difícil provar que se $n \geq n_0(k)$, então $|\mathcal{A}_i|$ é máximo para $i = 0$. O exemplo acima mostra que para certos casos extremos, o máximo dos $|\mathcal{A}_i|$ é atingido para valores $i > 0$.

Seja $M(n,k,\ell)$ a cardinalidade máxima de um sistema ℓ-intersectante de k-subconjuntos de $[n]$. Então $M(n,k,\ell) \geq \max_i |\mathcal{A}_i|$. Ademais, se n é suficientemente grande em relação a k, então vale a igualdade (este é o Teorema 12).

Conjectura 19. *Para todo* $1 \leq \ell \leq k \leq n$, *vale que*

$$M(n,k,\ell) = \max_i |\mathcal{A}_i|, \tag{73}$$

onde o máximo é tomado sobre $0 \leq i \leq (n-\ell)/2$.

A conjectura acima é devida, nesta generalidade, a Frankl [**29**]. O caso $\ell = 2$, $k = 2r$, e $n = 4r$ já ocorre no artigo original de Erdős, Ko, e Rado [**25**], de 1961.

4.1. A resolução da Conjectura 19. Um dos grandes resultados da teoria extremal dos conjuntos em anos recentes foi a resolução completa da conjectura de Frankl, Conjectura 19, por Ahlswede e Khachatrian [**1**] em 1997.

Teorema 20. *A Conjectura 19 é verdadeira.*

A conjectura de 1938 de que $M(4r,2r,2)$ é dado por $|\mathcal{A}_{r-1}|$ (veja (71)) foi um dos problemas favoritos de Erdős. A demonstração do Teorema 20 é um tanto rebuscada, e está fora do escopo destas notas.

5. O teorema de Ramsey

Embora óbvio, o *princípio da casa do pombo*, também conhecido como o *princípio de Dirichlet*, pode ser empregado de formas sutis, muitas vezes permitindo provar resultados de forma inesperada. Este princípio pode ser enunciado da seguinte forma: se colocamos $n+1$ pombos em n casas, então alguma casa vai receber mais de um pombo.

Nesta seção, discutiremos brevemente uma versão mais sofisticada deste fenômeno básico da natureza, conhecida como o teorema de Ramsey. Para uma discussão introdutória à teoria de Ramsey, o leitor pode consultar [**15**]. Uma excelente referência (mais avançada) é a monografia [**42**].

5.1. O princípio de Dirichlet. Se o leitor não está familiarizado com aplicações do princípio da casa do pombo, então é bem natural que ele esteja um tanto desconfiado: como pode um princípio tão óbvio ter qualquer conseqüência mais interessante? Apenas para ilustrar o uso deste princípio, expomos aqui um resultado bem conhecido de 1842 de Dirichlet, sobre aproximações diofantinas. Este resultado não será usado no resto do texto; resolvemos incluí-lo porque ele é um dos melhores exemplos que ilustram o poder do princípio da casa do pombo.

TEOREMA 21. *Seja α um número irracional, então existem infinitas soluções racionais p/q para a desigualdade*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{74}$$

DEMONSTRAÇÃO. Fixe um inteiro $Q \geq 1$. Considere os $Q+1$ números $0, \{\alpha\}, \{2\alpha\}, \ldots, \{Q\alpha\} \in [0,1)$, onde escrevemos $\{x\}$ para a parte fracionária de x, isto é, $\{x\} = x - \lfloor x \rfloor$. Considere os Q intervalos

$$I_k = \left[\frac{k-1}{Q}, \frac{k}{Q}\right) \subset [0,1)$$

para $1 \leq k \leq Q$. Note que estes Q intervalos particionam o intervalo $[0,1)$. Pelo princípio de Dirichlet, dois dos $Q+1$ números $\{i\alpha\}$ $(0 \leq i \leq Q)$ pertencem a um mesmo intervalo I_k; suponha que eles sejam $\{i\alpha\}$ e $\{j\alpha\}$, com $i > j$. Então

$$\big|\{i\alpha\} - \{j\alpha\}\big| < \frac{1}{Q}. \tag{75}$$

Portanto, tomando $q = i - j > 0$ e $p = \lfloor i\alpha \rfloor - \lfloor j\alpha \rfloor$, deduzimos de (75) que

$$|q\alpha - p| < \frac{1}{Q}.$$

Dividindo por q e lembrando que $q = i - j \leq Q$, temos que

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{qQ} \leq \frac{1}{q^2}, \tag{76}$$

e assim encontramos uma solução para (74).

Como α é irracional, o lado esquerdo de (76) é estritamente positivo, digamos $> 1/Q'$, para algum inteiro positivo Q'. Repetindo o argumento acima para este Q', podemos encontrar uma aproximação p'/q' para α

tal que

$$\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{q'Q'} \leq \frac{1}{(q')^2}. \tag{77}$$

Como $1/q'Q' < 1/Q' < |\alpha - p/q|$, a aproximação p'/q' é uma nova aproximação de α. Podemos assim deduzir que (74) de fato tem infinitas soluções. □

Já encontramos neste texto uma outra aplicação do princípio da casa do pombo: uma seqüência primitiva de inteiros contida em $[2n]$ têm no máximo n elementos. (Você fez o segundo exercício sugerido no começo da Seção 2.1.1?)

5.2. O teorema de Ramsey para grafos. Passaremos agora a discutir um resultado clássico de Ramsey [**63**], de 1930. A grosso modo, o teorema de Ramsey é uma versão iterada do princípio da casa do pombo.

Uma área rica da combinatória, conhecida como a teoria de Ramsey, lida com resultados relacionados ao teorema de Ramsey e a outros resultados que são manifestações de um fenômeno básico, assim descrito por Theodore S. Motzkin: "*desordem completa é impossível*". Estudamos no Capítulo 3 uma subárea da teoria de Ramsey, a saber, a teoria de Ramsey euclideana, introduzida em um trabalho de 1973, dedicado a Motzkin pelos ilustres autores P. Erdős, R. L. Graham, P. Montgomery, B. L. Rothschild, J. Spencer, e E. G. Straus [**21**].

5.2.1. *O teorema de Ramsey.* Aqui, restringimo-nos à versão mais simples do teorema de Ramsey, que é a versão para grafos. Um grafo nada mais é que um par (V, E), onde V é o conjunto de *vértices* de G e E é um conjunto de pares de vértices de G: $E \subset \binom{V}{2}$. Os elementos de E são as *arestas* de G. Usualmente, dizemos que uma aresta $e = \{x, y\} \in E$ de um grafo $G = (V, E)$ *liga* os seus *extremos* x e y. Quando dois vértices x, $y \in V$ de G formam uma aresta $\{x, y\} \in E$ de G, dizemos que x e y são *adjacentes*.

Um *clique* em um grafo $G = (V, E)$ é um conjunto $U \subset V$ de vértices com $\binom{U}{2} \subset E$, isto é, tal que todos os pares de vértices em U formam arestas de G. Um conjunto independente em G é um conjunto $W \subset V$ de vértices com $\binom{U}{2} \cap E = \emptyset$, isto é, nenhum par de vértices em W forma uma aresta de G. Pomos

$$\omega(G) = \max\{|U| \colon U \text{ é um clique em } G\}$$

e

$$\alpha(G) = \max\{|W| \colon W \text{ é um conjunto independente em } G\}.$$

O teorema de Ramsey simplesmente diz que grafos grandes precisam conter cliques ou conjuntos independentes grandes.

TEOREMA 22. *Sejam k e ℓ inteiros positivos. Então existe um inteiro $n_0 = n_0(k, \ell)$ tal que todo grafo G com pelo menos n_0 vértices é tal que $\omega(G) \geq k$ ou $\alpha(G) \geq \ell$.*

Muitas vezes, se a conclusão do Teorema 22 vale para um inteiro n, escrevemos

$$n \to (k, \ell). \tag{78}$$

Ademais, definimos como o *número de Ramsey* $R(k, \ell)$ o menor valor possível para o inteiro $n_0(k, \ell)$ no enunciado do Teorema 22, ou, equivalentemente, o menor valor de n para o qual (78) vale. Naturalmente, o Teorema 22 afirma que $R(k, \ell) < \infty$ para todo k e $\ell \geq 1$.

A prova do Teorema 22 é baseada na aplicação do princípio da casa do pombo de forma iterada.

DEMONSTRAÇÃO DO TEOREMA 22. Claramente, temos

$$R(1, \ell) = R(k, 1) = 1 \tag{79}$$

para todo k e $\ell \geq 1$. Suponha agora que k e $\ell \geq 2$, e que $R(k', \ell') < \infty$ para todo par (k', ℓ') com $k' + \ell' < k + \ell$. Vamos provar que

$$R(k, \ell) \leq R(k-1, \ell) + R(k, \ell-1). \tag{80}$$

Seja $G = (V, E)$ um grafo com $n = R(k, \ell - 1) + R(k - 1, \ell)$ vértices. Devemos provar que G contém um clique de cardinalidade k ou um conjunto independente de cardinalidade ℓ. Fixe um vértice x de G. Pelo princípio da casa do pombo, ou (i) x é adjacente a $R(k-1, \ell)$ vértices, ou (ii) x não é adjacente a $R(k, \ell - 1)$ vértices de G.

Suponha que vale o caso (i) acima. Considere o grafo G' cujo conjunto de vértices Y é o conjunto de vértices y de G com x e y adjacentes (os 'vizinhos de x'); definimos o conjunto de arestas em G' como o conjunto $E \cap \binom{Y}{2}$, isto é, dois vértices y e $y' \in Y$ são adjacentes em G' se e só se o forem em G. Pela definição de $R(k-1, \ell)$, o grafo G' contém um clique de tamanho $k - 1$ ou contém um conjunto independente de tamanho ℓ. Note que se tal conjunto independente existir em G', então ele é também um conjunto independente em G e não há nada mais a fazer. Caso G' contenha um clique U' de tamanho k, então observamos que $U = U' \cup \{x\}$ é um clique em G de tamanho k, e assim terminamos a prova.

Suponha agora que vale o caso (ii) acima. Considere o grafo G'' cujo conjunto de vértices Z é o conjunto de vértices $z \in V \setminus \{x\}$ de G com x e z não-adjacentes e $z \neq x$; definimos o conjunto de arestas em G'' como o conjunto $E \cap \binom{Z}{2}$. Pela definição de $R(k, \ell - 1)$, o grafo G'' contém um clique de tamanho k ou contém um conjunto independente de tamanho $\ell - 1$. Note que se tal clique existir em G'', então ele é também um clique em G e não há nada mais a fazer. Caso G'' contenha um conjunto independente W'' de tamanho $\ell - 1$, então observamos que $W = W'' \cup \{x\}$ é um conjunto independente em G de tamanho ℓ.

Isto conclui a prova do Teorema 22. $\square$

Observação 23. A demonstração acima do Teorema 22 de fato implica que

$$R(k, \ell) \leq \binom{k + \ell - 2}{k - 1}. \tag{81}$$

De fato, a desigualdade (81) pode ser provada por indução usando-se (79) e (80).

Um problema numérico famoso relacionado ao teorema de Ramsey é o seguinte. Ponha

$$R(n) = R(n, n). \tag{82}$$

PROBLEMA 24. *Determine ou estime $R(n)$.*

Sabe-se o valor de $R(n)$ para valores pequenos de n. É trivial que $R(1) = 1$ e que $R(2) = 2$. Um exercício bem conhecido é provar que $R(3) = 6$. Já é mais difícil provar que $R(4) = 18$ (tente!). O que se sabe sobre $R(5)$ é que

$$43 \leq R(5) \leq 49.$$

Para mais detalhes sobre valores exatos dos números de Ramsey, veja a 'Resenha dinâmica' de Stanislaw Radziszowski [**62**].

O que podemos dizer sobre a ordem de grandeza de $R(n)$? Pela Observação 23, temos que

$$R(n) \leq \binom{2n-2}{n-1} \leq \frac{c}{\sqrt{n}} 4^n \tag{83}$$

para alguma constante positiva $c > 0$.

Como podemos limitar $R(n)$ por baixo? Claramente, provar que $R(n) > N$ significa provar que existe um grafo com N vértices que não contém nenhum clique de tamanho n nem contém nenhum conjunto independente de tamanho n. À primeira vista, pode ser surpreendente que este seja um problema difícil.

5.2.2. *O limitante exponencial de Erdős.* Um resultado influente de Erdős foi o seu limitante inferior exponencial [**19**] para os números de Ramsey $R(n)$, publicado em 1947. Embora a prova deste resultado seja muito simples, foi ela a demonstração definitiva de que o assim chamado *método probabilístico* é fundamental na combinatória.

TEOREMA 25. *Para todo $n \geq 2$, temos $R(n) > 2^{n/2}$.*

DEMONSTRAÇÃO. Podemos verificar por inspeção que $R(n) > 2^{n/2}$ de fato vale para $2 \leq n \leq 4$, de forma que podemos supor que $n \geq 5$.

Consideremos grafos G sobre $V = [N]$, onde

$$N = \lfloor 2^{n/2} \rfloor,$$

definidos da seguinte forma: para cada par de vértices distintos a e $b \in V$, lance uma moeda honesta e coloque a aresta $\{a, b\}$ em G se e só se a moeda der cara. Note que definimos assim um *grafo aleatório* G.

Mais formalmente, para cada $1 \leq a < b \leq N$, considere uma variável aleatória $X_{a,b}$ com

$$\mathbb{P}(X_{a,b} = 0) = \mathbb{P}(X_{a,b} = 1) = \frac{1}{2},$$

com todas as variáveis $X_{a,b}$ $(1 \leq a < b \leq N)$ independentes. A aresta $\{a, b\}$ pertence ao grafo aleatório G se e só se $X_{a,b} = 1$.

Qual é o número esperado de cliques de tamanho n em G? Para cada subconjunto $U \subset V$ de n vértices, escreva Y_U para a variável indicadora 0–1 que vale 1 se e só se U é um clique em G. Então

$$\mathbb{P}(Y_U = 1) = 2^{-\binom{|U|}{2}} = 2^{-\binom{n}{2}}. \tag{84}$$

O número total de cliques de tamanho n em G é $Y = \sum_U Y_U$, onde a soma é sobre todos os n-subconjuntos de V. Assim, o número esperado de cliques de tamanho n em G é, devido a (84),

$$\mathbb{E}(Y) = \mathbb{E}\Big(\sum_U Y_U\Big) = \sum_U \mathbb{E}(Y_U) = \sum_U \mathbb{P}(Y_U = 1) = \binom{N}{n} 2^{-\binom{n}{2}}, \tag{85}$$

onde usamos uma propriedade fundamental do valor esperado, a assim chamada *linearidade* (o valor esperado de uma soma de variáveis aleatórias é a soma dos valores esperados dessas variáveis). Analogamente, se Z é o número de conjuntos independentes em G, podemos deduzir que

$$\mathbb{E}(Z) = \binom{N}{n} 2^{-\binom{n}{2}}. \tag{86}$$

De (85) e (86), podemos deduzir que

$$\begin{aligned}(87)\quad \mathbb{E}(Y+Z) = 2\binom{N}{n}2^{-\binom{n}{2}} &\leq 2\left(\frac{eN}{n}\right)^n 2^{-n(n-1)/2} \\ &\leq 2\left(\frac{e2^{n/2}2^{-(n-1)/2}}{n}\right)^n = 2\left(\frac{e\sqrt{2}}{n}\right)^n < 1,\end{aligned}$$

onde usamos que $n \geq 5$ e que $\binom{a}{b} \leq (ea/b)^b$ (veja Lema 94 do Apêndice A)

O que podemos deduzir de (87)? O número esperado de cliques e conjuntos independentes de tamanho n em G é < 1. Claramente, algum grafo G gerado da forma acima precisa ser tal que o número de tais conjuntos é 0, pois caso contrário o número médio de tais conjuntos seria pelo menos 1! Daí segue que existe um grafo G com N vértices com $\omega(G) < n$ e $\alpha(G) < n$, e portanto $R(n) > N$. □

O argumento de Erdős, com um pouco mais de cuidado nas estimativas, fornece o seguinte resultado:

$$(88)\qquad R(n) \geq \frac{n}{e}2^{(n-1)/2}$$

para todo $n \geq 1$. Este limitante, entretanto, ainda pode ser melhorado levemente, usando-se técnicas mais avançadas da teoria de probabilidade. Usando o assim chamado *Lema Local de Lovász* [**26**], Spencer [**67**] provou que o limite inferior em (88) pode ser melhorado por um fator de 2, isto é, vale que

$$(89)\qquad R(n) \geq \frac{n}{e}2^{(n+1)/2}$$

A desigualdade (89) de 1975 é ainda o melhor resultado que se conhece nesta direção. Por outro lado, mais de 50 anos após o limitante superior (83) ter sido provado, Thomason e Rödl independentemente provaram limitantes superiores de ordem de grandeza menores que o lado direito de (83). O limitante superior mais forte que se conhece para $R(n)$ hoje é devido a Thomason [**70**], que diz que existe uma constante absoluta $c > 0$ para o qual temos

$$R(n) \leq n^{-1/2+c/\sqrt{\log n}} \binom{2n-2}{n-1}. \tag{90}$$

Note que o limitante de Thomason (90) é aproximadamente $n^{-1/2}$ menor que o limitante em (83). (O limitante de Rödl [**41**] para $R(n)$ era basicamente um fator de $\log\log n$ menor que o lado direito de (83).)

Para a grande frustração de todos os envolvidos, os seguintes problemas de Erdős, de 1947, persistem.

Conjectura 26. *O limite*

$$\lim_{n\to\infty} R(n)^{1/n} \tag{91}$$

existe.

Problema 27. *Encontre o valor do limite em* (91)*, caso ele exista.*

O que se sabe sobre o Problema 27 é que

$$\sqrt{2} \leq \liminf_{n\to\infty} R(n)^{1/n} \leq \limsup_{n\to\infty} R(n)^{1/n} \leq 4, \tag{92}$$

que é o que Erdős já sabia em 1947. Erdős ofereceu 100 dólares pela resolução da Conjectura 26, e ofereceu 250 dólares pela resolução do Problema 27.

Na Seção 5.3, exibiremos explicitamente um grafo que prova que $R(n)$ cresce pelo menos cubicamente em n. No Capítulo 2, Seção 5, exibiremos um grafo que prova que $R(n)$ cresce superpolinomialmente com n.

Será a teoria extremal dos conjuntos que nos dará informações sobre os cliques e sobre os conjuntos independentes dos grafos que vamos construir explicitamente na Seção 5.3 abaixo e na Seção 5 do Capítulo 2.

5.3. Construções explícitas. Considere as triplas do conjunto $[n]$ e defina um grafo G_n sobre elas, definindo como arestas exatamente os pares de triplas de têm exatamente um elemento em comum. Formalmente, o grafo G tem conjunto de vértices $V = \binom{[n]}{3}$ e conjunto de arestas

$$E = \left\{ \{A, B\} \in \binom{V}{2} : |A \cap B| = 1 \right\}.$$

Vamos provar que os cliques e conjuntos independentes de G_n são 'pequenos'.

TEOREMA 28. *Seja G_n o grafo definido acima. Então*

$$\omega(G_n),\ \alpha(G_n) \le n. \tag{93}$$

DEMONSTRAÇÃO. Suponha que $A_1, \ldots, A_\omega \in V$ formam um clique em G_n. Então temos uma família de subconjuntos de $[n]$ com cada par de conjuntos distintos intersectando em exatamente um elemento: o Teorema 17 implica que $\omega \le n$. Concluímos que $\omega(G_n) \le n$.

Suponha agora que $B_1, \ldots, B_\alpha \in V$ formam um conjunto independente em G_n. Então temos família de subconjuntos de $[n]$, todos de cardinalidade *ímpar*, com cada par de conjuntos distintos intersectando em 0 ou 2 elementos, isto é, em um número *par* de elementos: o Teorema 13 implica que $\alpha \le n$. Concluímos que $\alpha(G_n) \le n$. □

COROLÁRIO 29. *Para todo n, existe um grafo que pode ser explicitamente descrito que prova que $R(n+1) > \binom{n}{3}$.*

A construção de G_n acima é devida a Zsigmond Nagy (1972). Como mencionado anteriormente, veremos no Capítulo 2 uma construção explícita de um grafo que prova que $R(n)$ cresce mais rápido que qualquer polinômio em n.

5.4. O teorema de Ramsey para hipergrafos. Ramsey provou o seguinte resultado mais geral em seu trabalho original [**63**].

TEOREMA 30. *Sejam k, ℓ, e r inteiros positivos com $k \ge \ell$. Então existe um inteiro positivo $N_0 = N_0(k, \ell, r)$ para o qual vale a seguinte asserção: se $N \ge N_0$, então*

(*) *toda r-coloração dos ℓ-subconjuntos de $[N]$ colore todos os ℓ-subconjuntos de algum k-subconjunto de $[N]$ da mesma cor.*

Podemos enunciar a propriedade (*) do Teorema 30 mais formalmente da seguinte maneira. *Para toda r-coloração $\phi\colon \binom{[N]}{\ell} \to [r]$, existe $K \subset [N]$ com $|K| = k$ tal que $\phi \restriction \binom{K}{\ell}$ é constante.* A propriedade (*) é muitas vezes expressa da seguinte forma compacta:

$$N \to (k)^\ell_r. \tag{94}$$

O k-conjunto garantido em (*) é dito ser *monocromático.* O menor inteiro $N_0 = N_0(k, \ell, r)$ para o qual vale a conclusão do Teorema 30, ou, equivalentemente, o menor inteiro N para o qual vale (94), é conhecido como o *número de Ramsey* $R_r^{(\ell)}(k)$.

O leitor deve verificar que de fato o Teorema 30 generaliza o Teorema 22 (basta considerar o caso $r = 2$ no Teorema 30).

O Teorema 30 será particularmente importante na Seção 5 do Capítulo 3.

5.4.1. *Prova do Teorema 30.* A prova do Teorema 30 fica mais transparente se introduzimos a relação

$$N \to (k_1, \ldots, k_r)^\ell, \tag{95}$$

onde os $k_1, \ldots, k_r$ são inteiros positivos: vamos dizer que (95) vale se qualquer r-coloração $\phi\colon \binom{[N]}{\ell} \to [r]$ dos ℓ-subconjuntos de $[N]$ admitir um k_i-conjunto $K \subset [n]$ com $\phi \restriction \binom{K}{\ell}$ constante e igual a i, para algum $1 \le i \le r$. O menor inteiro N para o qual (95) vale será denotado por $R^{(\ell)}(k_1, \ldots, k_r)$. A desigualdade que generaliza (80) naturalmente é

$$R^{(\ell)}(k_1, \ldots, k_r) \le 1 + R^{(\ell-1)}(R_1, \ldots, R_r), \tag{96}$$

onde

$$\begin{aligned}
R_1 &= R^{(\ell)}(k_1 - 1, k_2, \ldots, k_r),\\
R_2 &= R^{(\ell)}(k_1, k_2 - 1, \ldots, k_r),\\
&\ \vdots\\
R_r &= R^{(\ell)}(k_1, k_2, \ldots, k_r - 1).
\end{aligned}$$

Deixamos a prova de (96) como um exercício para o leitor. (Sugestão: observe que se temos uma r-coloração ϕ dos ℓ-subconjuntos de $[N]$ então podemos temos uma r-coloração 'induzida' nos $(\ell-1)$-subconjuntos de $[N-1]$, a saber, aquela em que a cor de um $(\ell-1)$-subconjunto $X \subset [N-1]$ é a cor $\phi(X \cup \{N\})$ de $X \cup \{N\}$ na coloração original ϕ.)

O Teorema 30 segue de (96).

CAPÍTULO 2

A conjectura de Borsuk e o número cromático de $\mathbb{R}^n$

1. Introdução

Neste capítulo vamos discutir dois problemas clássicos de Geometria Combinatória, resolvidos recentemente por meio de técnicas de álgebra linear e teoria extremal dos conjuntos: a conjectura de Borsuk e o crescimento exponencial do número cromático de $\mathbb{R}^n$.

Em 1933 o famoso topólogo Karol Borsuk propôs um problema que ficou conhecido como a "Conjectura de Borsuk": É possível dividir um subconjunto limitado qualquer de $\mathbb{R}^d$ em $d+1$ conjuntos de diâmetro menor?

60 anos depois, Jeff Kahn e Gil Kalai [**47**] mostraram que a conjectura de Borsuk é espetacularmente falsa: se $f(d)$ é o menor número tal que qualquer subconjunto limitado de $\mathbb{R}^d$ pode ser dividido em $f(d)$ conjuntos de diâmetro menor então $f(d) \geq (1{,}1)^{\sqrt{d}}$, para d suficientemente grande. Vamos apresentar uma modificação desta prova devida a A. Nilli que implica que $f(d) \geq (1{,}2)^{\sqrt{d}}$ para d suficientemente grande, e uma outra modificação de A. Raigorodski e B. Weissbach, que fornece um contra-exemplo explícito em dimensão 561 (o atual recorde).

O número cromático de $\mathbb{R}^n$ é o menor k tal que é possível pintar os pontos de $\mathbb{R}^n$ usando k cores sem que haja dois pontos de mesma cor à distância 1. Não é difícil ver que o número cromático de $\mathbb{R}^n$ cresce no máximo como uma exponencial. Vamos mostrar um teorema de Frankl e Wilson [**34**] de 1981, que implica que o número cromático de $\mathbb{R}^n$ cresce exponencialmente, provando uma conjectura de 1972 de Larman e Rogers [**54**]: é maior que $(1{,}2)^n$ para n suficientemente grande. O trabalho de Frankl e Wilson introduziu as técnicas principais utilizadas neste capítulo. Nele é provado um pouco mais do que enunciamos: de fato, se dividimos $\mathbb{R}^n$ em menos que $(1{,}2)^n$ subconjuntos, em um desses subconjuntos todas as distâncias positivas são realizadas.

2. Espaços de polinômios

Nesta seção vamos provar alguns resultados técnicos que utilizam a noção de independência linear em certos espaços de polinômios. Esses resultados terão um papel fundamental nas seções seguintes sobre o número cromático de $\mathbb{R}^n$ e a conjectura de Borsuk. Começamos com um lema sobre independência linear:

LEMA 31. *Sejam $f_1, f_2, \dots, f_n \colon X \to \mathbb{Z}$ funções definidas num conjunto arbitrário X. Suponhamos que existe um número primo p e elementos $x_1, x_2, \dots, x_n \in X$ tais que $p \nmid f_i(x_i)$, $\forall\, i$ e $p \mid f_i(x_j)$, $\forall\, i \neq j$. Então $f_1, f_2, \dots, f_n$ são linearmente independentes sobre $\mathbb{Q}$, i.e., se uma combinação linear $\sum_{i=1}^n c_i f_i$ com coeficientes em $\mathbb{Q}$ é identicamente nula em X então $c_i = 0$ para todo i.*

DEMONSTRAÇÃO. Se existe uma combinação linear com coeficientes racionais $\sum_{i=1}^n c_i f_i$ que se anula em X, podemos supor que $c_i \in \mathbb{Z}$ para todo i (multiplicando pelo m.m.c. dos denominadores), e, talvez dividindo por um inteiro adequado, que $\operatorname{mdc}(c_1, c_2, \dots, c_n) = 1$. Em particular, existirá i tal que $p \nmid c_i$.

Teremos assim $\sum_{j=1}^n c_j f_j(x_i) = 0$, o que é um absurdo, pois $p \mid f_j(x_i)$, $\forall\, j \neq i$, mas p não divide c_i e não divide $f_i(x_i)$, donde p não divide $c_i f_i(x_i)$, e portanto também não divide $\sum_{j=1}^n c_j f_j(x_i)$. □

Vamos agora apresentar um lema que permite em determinadas situações substituir um polinômio em várias variáveis por um polinômio multilinear que assume os mesmos valores em certos conjuntos. Um *polinômio multilinear* é uma soma de monômios em que cada variável aparece com expoente 0 ou 1. O espaço dos polinômios multilineares com coeficientes racionais nas variáveis $x_1, x_2, \dots, x_n$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão 2^n, gerado pelos monômios $x_{(I)}$ $(I \subset \{1, 2, \dots, n\})$ definidos por $x_{(I)} = x_{i_1} x_{i_2} \dots x_{i_r}$ se $I = \{i_1, i_2, \dots, i_r\}$.

Se $k \leq n$, o espaço dos polinômios multilineares com coeficientes racionais nas variáveis $x_1, x_2, \ldots, x_n$ de grau menor ou igual a k é um espaço vetorial sobre $\mathbb{Q}$ de dimensão $\sum_{j=0}^{k} \binom{n}{j}$, gerado pelos monômios $x_{(I)}$, $I \subset \{1, 2 \ldots, n\}$ com $|I| \leq k$.

Lema 32. *Sejam $f(x_1, x_2, \ldots, x_n)$ um polinômio em n variáveis sobre $\mathbb{Q}$, $\Omega_1 = \{0,1\}^n \subset \mathbb{Q}^n$ e $\Omega_2 = \{-1,1\}^n \subset \mathbb{Q}^n$. Se f tem grau $\leq s$ então existem polinômios multilineares f_1 e f_2 de graus $\leq s$ tais que f_1 coincide com f em Ω_1 e f_2 coincide com f em Ω_2.*

Demonstração. Como $x_i^k = x_i$ se $x_i \in \{0,1\}$ e $k \geq 1$, para obter f_1 basta trocar todos os expoentes positivos na expansão de f por 1. Para obter f_2 usamos o fato que $x_i^2 = 1$ se $x_i \in \{-1,1\}$, e trocamos todos os expoentes pares na expansão de f por 0 e todos os expoentes ímpares por 1. □

Vamos agora provar um teorema de Deza, Frankl e Singhi [**17**] que limita o tamanho de famílias de subconjuntos de um conjunto finito dadas certas restrições (módulo p) sobre os tamanhos das interseções 2 a 2 desses conjuntos (a prova que apresentaremos é de Alon, Babai, e Suzuki [**3**]). No que segue, escrevemos $x \in L \pmod p$ se $x \equiv \ell \pmod p$ para algum $\ell \in L$.

Teorema 33. *Sejam p um número primo e L um conjunto de s números inteiros. Suponha que $\mathcal{F} = \{A_1, A_2, \ldots, A_m\}$ é uma família de subconjuntos de um conjunto de n elementos tal que*

(*i*) $|A_i| \notin L \pmod p \quad (1 \leq i \leq m)$;
(*ii*) $|A_i \cap A_j| \in L \pmod p \quad (1 \leq i < j \leq m)$.

Então

$$m \leq \sum_{j=0}^{s} \binom{n}{j}.$$

Demonstração. Vamos considerar o seguinte polinômio em $2n$ variáveis (x, y), $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$:

$$F(x,y) = \prod_{\ell \in L} (\langle x, y \rangle - \ell), \qquad \text{onde} \qquad \langle x, y \rangle = \sum_{i=1}^{n} x_i y_i.$$

Consideramos agora os polinômios em n variáveis $f_i(x) = F(x, v_i)$, onde $v_i \in \{0,1\}^n$ é o *vetor de incidência* do conjunto A_i, isto é, $v_i = (v_{i1}, v_{i2}, \ldots, v_{in})$, onde

$$v_{ij} = \chi_{A_i}(j) = \begin{cases} 1 \text{ se } j \in A_i \\ 0 \text{ se } j \notin A_i. \end{cases}$$

Pela definição de F e pelas hipóteses do teorema, $p \mid f_i(v_j)$ se $i \neq j$ e $p \nmid f_i(v_i)$, $\forall\, i$. Pelo Lema 32, podemos trocar os polinômios f_i por polinômios multilineares $\widetilde{f_i}$ de grau $\leq s$ que coincidem com f_i em $\{0,1\}^n$, e portanto nos vetores v_i. Pelo Lema 31, $\widetilde{f_1}, \widetilde{f_2}, \ldots, \widetilde{f_m}$ são linearmente independentes sobre $\mathbb{Q}$. Como a dimensão do espaço dos polinômios multilineares em n variáveis de grau $\leq s$ é $\sum_{j=0}^{s} \binom{n}{j}$, temos $m \leq \sum_{j=0}^{s} \binom{n}{j}$. $\square$

COROLÁRIO 34. *Seja p um primo e $\mathcal{F}$ uma família de subconjuntos com $2p-1$ elementos de um conjunto com $n > 2p$ elementos. Se a interseção de dois conjuntos da família nunca tem exatamente $p-1$ elementos então $|\mathcal{F}| \leq \sum_{j=0}^{p-1} \binom{n}{j}$.*

DEMONSTRAÇÃO. Tomamos $L = \{0, 1, \ldots, p-2\}$ e notamos que $\mathcal{F}$ satisfaz as hipóteses do Teorema 33. $\square$

PROPOSIÇÃO 35. *Sejam p um primo ímpar e $n = 4p - 2$. Seja*

$$Q = \{(x_1, x_2, \ldots, x_n) \in \{-1, 1\}^n \mid x_1 = 1 \textit{ e } |\{i \mid x_i = -1\}| \textit{ é par}\}.$$

Dizemos que dois elementos $x, y \in Q$ são quase-ortogonais se $|\langle x, y\rangle| = 2$. Se $Q' \subset Q$ não contém nenhum par de vetores quase-ortogonais então

$$|Q'| \leq \sum_{i=0}^{p-2} \binom{n}{i}.$$

OBSERVAÇÃO 36. Dados $x, y \in Q$, $\langle x, y\rangle = (4p-2) - 2|\{i \mid x_i \neq y_i\}|$ é sempre congruente a 2 módulo 4, pois, como x e y têm ambos um número par de coordenadas -1, a cardinalidade de $\{i \mid x_i \neq y_i\}$ é par. Assim, $|\langle x, y\rangle| \geq 2$, $\forall\, x, y \in Q$.

Prova da Proposição 35. Observemos inicialmente que, se $Q' \subset Q$ não contém nenhum par de vetores quase-ortogonais e $x, y \in Q'$ são tais que $\langle x, y\rangle \equiv \pm 2 \pmod p$ então $x = y$. De fato, $\langle x, y\rangle \notin \{-2, 2\}$, e, como $\langle x, y\rangle \equiv 2 \pmod 4$, teríamos $\langle x, y\rangle \equiv \pm 2 \pmod{4p}$, e como $-(4p-2) \leq \langle x, y\rangle \leq 4p-2$, devemos ter $\langle x, y\rangle \in \{-(4p-2), 4p-2\}$. Entretanto, como $x_1 = y_1$, não podemos ter $\langle x, y\rangle = -(4p-2)$. Portanto $\langle x, y\rangle = 4p-2$, donde $x = y$.

A cada $y \in Q'$ associamos o polinômio em n variáveis de grau $p-2$ dado por

$$F_y(x) = \prod_{\substack{j \in \{0,1,\ldots,p-1\} \\ j \notin \{2, p-2\}}} (\langle x, y\rangle - j), \qquad \text{onde} \qquad x = (x_1, x_2, \ldots, x_n).$$

As observações acima mostram que $p \mid F_y(x)$, $\forall\, x \neq y$ mas $p \nmid F_x(x)$, $\forall\, x$. Pelo Lema 32, podemos substituir os polinômios F_y por polinômios multilineares $\widetilde{F}_y$ de grau $\leq p-2$, que coincidem com F_y em $\{-1,1\}^n \supset Q'$. Pelo Lema 31, esses polinômios são linearmente independentes, donde o número deles, que é $|Q'|$, não excede a dimensão do espaço dos polinômios multilineares de grau $\leq p-2$ em n variáveis, que é $\sum_{i=0}^{p-2} \binom{n}{i}$. $\square$

Observação 37. A Proposição 35 também é válida para $p = 9$. Para mostrar isso, observamos inicialmente que a prova acima implica que se $x \neq y$, $\langle x, y\rangle \in \{0, 1, 3, 4, 5, 6, 8\} \pmod 9$, e, se $x = y$, $\langle x, y\rangle = 34 \equiv 7 \pmod 9$. Consideramos agora os polinômios

$$F_y(x) = \frac{1}{9} \prod_{j \in \{0,1,3,4,5,6,8\}} (\langle x, y\rangle - j),$$

associados aos elementos y de Q', e notamos que, se $x = y$, $3 \nmid F_y(x)$, e, se $x \neq y$, $3 \mid F_y(x)$. Pelo Lema 32, podemos substituir os polinômios F_y por polinômios multilineares $\widetilde{F}_y$, também de grau ≤ 7, que coincidem com F_y em $\{-1,1\}^{34} \supset Q'$. Aplicando o Lema 31 (com $p = 3$), concluímos que os polinômios $\widetilde{F}_y$ são linearmente independentes, donde $|Q'| \leq \sum_{i=0}^{7} \binom{34}{i} = 7055732$.

3. A conjectura de Borsuk é falsa

Teorema 38. *Sejam p um primo ímpar ou $p = 9$, $n = 4p - 2$ e $d = n(n-1)/2 = (2p-1)(4p-3)$. Então existe um conjunto $S \subset \{-1, 1\}^d$ de 2^{n-2} pontos em $\mathbb{R}^d$ tal que qualquer partição de S em subconjuntos de menor diâmetro tem pelo menos*

$$2^{n-2} \Big/ \sum_{j=0}^{p-2} \binom{n}{j}$$

partes.

Demonstração. A Proposição 35 da Seção 2 deste capítulo (e a Observação 37 subseqüente, para o caso $p = 9$) mostra que se

$$Q = \{x = (x_1, x_2, \ldots, x_n) \in \{-1, 1\}^n \mid x_1 = 1 \text{ e } |\{i \mid x_i = -1\}| \text{ é par}\},$$

então $|\langle x, y\rangle| \geq 2$, $\forall\, x, y \in Q$, e, se $Q' \subset Q$ não contém nenhum par de vetores quase-ortogonais (i.e., tais que $|\langle x, y\rangle| = 2$) então

$$|Q'| \leq \sum_{i=0}^{p-2} \binom{n}{i}.$$

Consideremos a função $h\colon \mathbb{R}^n \to \mathbb{R}^{n^2}$ que, a cada vetor

$$x = (x_1, \ldots, x_n) \in \mathbb{R}^n,$$

associa a matriz simétrica $(a_{ij})_{1 \leq i,j \leq n}$ onde $a_{ij} = x_i \cdot x_j$ (se olharmos x como um vetor coluna, $h(x) = x \cdot x^T$). Se $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$,

$$\begin{aligned}\langle h(x), h(y)\rangle &= \sum_{1 \leq i,j \leq n} (x_i x_j)(y_i y_j) \\ &= \Big(\sum_{1 \leq i \leq n} x_i y_i\Big)\Big(\sum_{1 \leq j \leq n} x_j y_j\Big) = \langle x, y\rangle^2,\end{aligned}$$

e

$$|h(x) - h(y)|^2 = |h(x)|^2 + |h(y)|^2 - 2\langle h(x), h(y)\rangle$$
$$= |x|^4 + |y|^4 - 2\langle x, y\rangle^2.$$

Em particular, se $x, y \in Q$, então

$$|h(x) - h(y)|^2 = 2n^2 - 2\langle x, y\rangle^2 \leq 2n^2 - 8,$$

valendo a igualdade se e somente se x e y são quase-ortogonais. Seja agora $g\colon \mathbb{R}^{n^2} \to \mathbb{R}^{n(n-1)/2}$ que leva cada matriz $n \times n$ nos termos abaixo da diagonal, isto é, $g((a_{ij})_{1\leq i,j\leq n}) = (a_{ij})_{1\leq i<j\leq n}$. Se $x, y \in \{-1, 1\}^n$, então $h(x)$ e $h(y)$ serão matrizes simétricas em cujas diagonais todos os termos são iguais a 1. Assim, $h(x) - h(y)$ é uma matriz simétrica cuja diagonal é nula, donde $|h(x) - h(y)|^2 = 2|g(h(x)) - g(h(y))|^2$. Assim, a restrição de g a

$$h(\{-1, 1\}^n) \supset h(Q)$$

preserva a ordem entre distâncias: $|h(x) - h(y)| \leq |h(z) - h(w)|$ se e somente se $|g(h(x)) - g(h(y))| \leq |g(h(z)) - g(h(w))|$.

Nosso conjunto S será $g(h(Q))$. Se dividirmos S em menos de

$$2^{n-2} \Big/ \sum_{j=0}^{p-2} \binom{n}{j}$$

partes, alguma dessas partes terá, assim como a parte correspondente em Q, mais de $\sum_{j=0}^{p-2} \binom{n}{j}$ elementos. Pela Proposição 35 da Seção 2, haverá dois vetores quase-ortogonais x e y na parte correspondente em Q, e portanto $|h(x) - h(y)|^2 = 2n^2 - 8$ e $|g(h(x)) - g(h(y))|^2 = n^2 - 4$ serão máximos, donde $|g(h(x)) - g(h(y))|$ é igual ao diâmetro de S. $\square$

O caso $p = 9$ fornece imediatamente um contra-exemplo para a conjectura de Borsuk em dimensão $d = 17 \times 33 = 561$: Precisamos de pelo menos

$$2^{32} \Big/ \sum_{j=0}^{7} \binom{34}{j} = \frac{2^{32}}{7055732} > 608$$

pedaços de diâmetro menor para cobrir o conjunto S, donde, na notação da introdução deste capítulo, $f(561) \geq 609 > 562$.

Vamos usar este teorema para provar o resultado enunciado na introdução deste capítulo. Primeiro enunciamos um lema simples que nos permite estimar fatoriais.

LEMA 39. *Para todo $n \geq 1$, temos*

$$e\left(\frac{n}{e}\right)^n \leq n! \leq ne\left(\frac{n}{e}\right)^n.$$

A prova do Lema 39 pode ser encontrada no Apêndice A.

OBSERVAÇÃO 40. Uma estimativa mais precisa é dada pela Fórmula de Stirling, segundo a qual

$$\lim_{n\to\infty} \frac{n!}{n^n e^{-n}\sqrt{2n\pi}} = 1.$$

Um esboço da prova da Fórmula de Stirling é dado no Apêndice A.

Um fato elementar mas importante sobre coeficientes binomiais é que somas de trechos iniciais da n-ésima linha do triângulo de Pascal podem ser limitados basicamente pelo maior dos termos sendo somados, desde que o trecho contenha $\leq cn$ termos, onde $c < 1/2$ (veja detalhes no Apêndice A). Aqui, usaremos o seguinte resultado.

LEMA 41. *Suponha que $0 \leq k \leq (n+1)/3$. Então*

$$\sum_{j=0}^{k} \binom{n}{j} < \binom{n}{k}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \dots\right) = 2\binom{n}{k}. \tag{97}$$

A prova simples do Lema 41 é dada no Apêndice A.

TEOREMA 42. *Se d é suficientemente grande existe um subconjunto finito de $\mathbb{R}^d$ que não pode ser dividido em menos de $(1{,}2)^{\sqrt{d}}$ partes de menor diâmetro.*

DEMONSTRAÇÃO. Sejam p o maior primo tal que $d' = (2p-1)(4p-3) \leq d$, e $n = 4p-2$. Identificando $\mathbb{R}^{d'}$ com $\mathbb{R}^{d'} \times \{0\} \subset \mathbb{R}^d$, obtemos, pelo Teorema 38, um conjunto finito $S \subset \mathbb{R}^{d'} \subset \mathbb{R}^d$ que não pode ser dividido em menos de

$$2^{n-2} \Big/ \sum_{j=0}^{p-2} \binom{n}{j}$$

partes de menor diâmetro.

Note que $p-2 \le (4p-1)/3$, de forma que o Lema 41 nos diz que

$$\sum_{j=0}^{p-2} \binom{n}{j} < \binom{n}{p-2}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \dots\right) = 2\binom{n}{p-2}.$$

Assim,

$$\begin{aligned} 2^{n-2} \Big/ \sum_{j=0}^{p-2} \binom{n}{j} &> 2^{n-3} \Big/ \binom{n}{p-2} \\ &= \frac{2^{4p-5}(p-2)!(3p)!}{(4p-2)!} > \frac{2^{4p-1}p!(3p)!}{(4p)!}, \end{aligned}$$

que, pelo Lema 39, é maior ou igual a

$$\begin{aligned} \frac{2^{4p-1}e^2(p/e)^p(3p/e)^{3p}}{4pe(4p/e)^{4p}} &= 2^{4p-3}\frac{e}{p}\left(\frac{27}{256}\right)^p \\ &= \frac{e}{8p}\left(\frac{27}{16}\right)^p = \left(\frac{27}{16}\right)^{p(1-o(1))}. \end{aligned}$$

Como, pelo teorema dos números primos, $d = d'(1+o(1))$, donde $p = \sqrt{\frac{d}{8}}(1-o(1))$, segue que

$$2^{n-2} \Big/ \sum_{j=0}^{p-2} \binom{n}{j} > \left(\frac{27}{16}\right)^{\sqrt{\frac{d}{8}}(1-o(1))} > (1{,}2)^{\sqrt{d}},$$

se d é suficientemente grande, pois $(27/16)^{\sqrt{1/8}} = 1{,}2032\cdots > 1{,}2$. □

Não é difícil ver que $f(d)$ é no máximo exponencial. De fato, se $X \subset \mathbb{R}^d$ tem diâmetro ℓ e $x \in X$, então X está contido na bola fechada $\overline{B(x,\ell)}$, de centro x e raio ℓ. Podemos supor sem perda de generalidade que X é compacto (se não substituímos X por seu fecho). Consideremos uma união disjunta maximal de bolas abertas

$$B(x_i, \ell/4) \quad (1 \le i \le m)$$

de raio $\ell/4$ com os centros x_i em $\overline{B(x,\ell)}$. Todas essas bolas estão contidas em $B(x, 5\ell/4)$, e, como são disjuntas, devemos ter

$$m \le \frac{\operatorname{vol}(B(x,5\ell/4))}{\operatorname{vol}(B(x_i,\ell/4))} = 5^d.$$

Por outro lado, as bolas abertas $B(x_i, \ell/2)$ cobrem $\overline{B(x,\ell)}$. De fato, se $y \in \overline{B(x,\ell)} \setminus \bigcup_{i=1}^m B(x_i, \ell/2)$ então $B(y,\ell/4) \cap B(x_i,\ell/4) = \emptyset$ para todo i, e poderíamos acrescentar $B(y,\ell/4)$ à nossa coleção de bolas abertas, contradizendo sua maximalidade. Como $\overline{B(x,\ell)}$ é um compacto contido na união de bolas abertas

$$\bigcup_{i=1}^m B\left(x_i, \frac{\ell}{2}\right) = \bigcup_{n=1}^\infty \left(\bigcup_{i=1}^m B\left(x_i, \frac{n\ell}{2(n+1)}\right)\right),$$

existe $n \in \mathbb{N}$ tal que

$$\overline{B(x,\ell)} \subset \bigcup_{i=1}^m B\left(x_i, \frac{n\ell}{2(n+1)}\right).$$

Como o diâmetro de $B\left(x_i, n\ell/2(n+1)\right)$ é $n\ell/(n+1) < \ell$ para todo i, e $m \le 5^d$, segue que $f(d) \le 5^d$, para todo d.

Observação 43. No final da Seção 4 veremos como decompor $\mathbb{R}^d$ como $\widetilde{A}_1 \cup \widetilde{A}_2 \cup \cdots \cup \widetilde{A}_k$, com os $\widetilde{A}_j$ fechados, $k < (3+o(1))^d$ e $x, y \in \widetilde{A}_j \Rightarrow |x-y| \ne 1$. Se $X \subset \mathbb{R}^d$ tem diâmetro ℓ então $X \subset \overline{X} = \bigcup_{j=1}^k (\ell\widetilde{A}_j \cap \overline{X})$. Como $\overline{X}$ tem diâmetro ℓ e $x, y \in \ell\widetilde{A}_j \Rightarrow |x-y| \ne \ell$, $\operatorname{diam}(\ell\widetilde{A}_j \cap \overline{X}) < \ell$, $\forall\, j$, donde $f(d) < (3+o(1))^d$.

A melhor estimativa conhecida para $f(d)$ é

$$f(d) < 5d\sqrt{d}(4 + \log d)\left(\frac{3}{2}\right)^{d/2} < (1{,}23)^d,$$

para d suficientemente grande, devida a Schramm [**66**].

É interessante observar que a conjectura de Borsuk é verdadeira para corpos convexos com fronteira suave (isto é, domínios compactos cuja fronteira é uma hiperfície de classe C^1), como foi provado por Hadwiger; descrevemos a seguir sua demonstração.

Observamos inicialmente que se a fronteira de um corpo convexo pode ser dividida em k subconjuntos de diâmetro menor, o mesmo vale para o corpo todo. Para ver isso basta tomar um ponto no interior do corpo e dividir o corpo como união dos cones com vértice no ponto e bases nos conjuntos em que a fronteira foi dividida.

Provamos agora que é possível dividir a bola unitária (e portanto também a esfera unitária) em $\mathbb{R}^n$ em $n+1$ pedaços de menor diâmetro. Podemos fazer isso por indução: se dividimos $\overline{B(0,1)} \subset \mathbb{R}^n$ como $A_1 \cup A_2 \cup \cdots \cup A_{n+1}$, com diam $A_i < 2$, $\forall\, i$, podemos dividir a bola unitária em $\mathbb{R}^{n+1}$, $B = \{(x_1, x_2, \ldots, x_{n+1}) \mid x_1^2 + \cdots + x_{n+1}^2 \leq 1\}$ como $\widetilde{A}_0 \cup \widetilde{A}_1 \cup \cdots \cup \widetilde{A}_{n+1}$ onde $\widetilde{A}_0 = \{(x_1, \ldots, x_{n+1}) \in B \mid x_{n+1} \geq \varepsilon\}$, onde $\varepsilon > 0$ é bem pequeno e, para $1 \leq i \leq n+1$, $\widetilde{A}_i = \{(x_1, \ldots, x_{n+1}) \in B \mid (x_1, \ldots, x_n) \in A_i \text{ e } x_{n+1} < \varepsilon\}$.

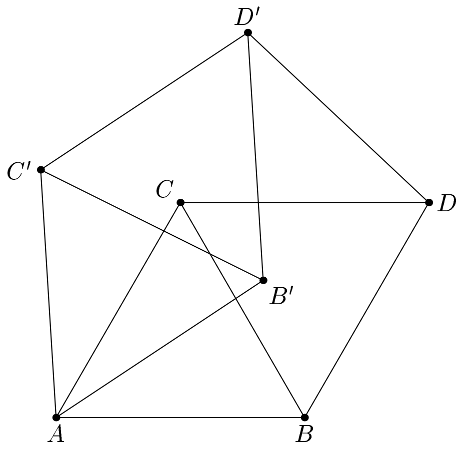
Seja agora $\Omega \subset \mathbb{R}^n$ um corpo convexo com fronteira suave, e seja M a sua fronteira. Seja agora $f\colon M \to S^{n-1}$ a *aplicação normal de Gauss*, isto é, a cada ponto de M associamos o vetor normal unitário que aponta para fora de Ω. Em outras palavras, $f(x)$ será um ponto na esfera unitária S^{n-1} tal que os planos tangentes a M em x e a S^{n-1} em $f(x)$ são paralelos, e M e S^{n-1} estão do mesmo lado desses hiperplanos.

Como Ω é convexo, f é uma bijeção (de fato um homeomorfismo). Dividimos agora S^{n-1} em $n+1$ conjuntos compactos $A_1, A_2, \ldots, A_{n+1}$ (não necessariamente disjuntos) de diâmetro menor que 2 (isto é, nenhum A_i contém nenhum par de pontos antípodas), e dividimos M nos $n+1$ conjuntos compactos $f^{-1}(A_1), f^{-1}(A_2), \ldots, f^{-1}(A_{n+1})$. Vamos ver que cada um desses conjuntos tem diâmetro menor que o diâmetro de M, o que pela observação inicial encerra a prova. Para isso, basta observar que se $x, y \in M$ são tais que $|x - y| = \text{diam}\, M$ então os planos tangentes a M em x e em y são paralelos, donde $f(x)$ e $f(y)$ são antípodas, logo x e y não podem pertencer a um mesmo conjunto $f^{-1}(A_i)$ de nossa decomposição. □

4. O número cromático de $\mathbb{R}^n$

Seja $c(n)$ o *número cromático* de $\mathbb{R}^n$, isto é, $c(n)$ é o menor inteiro positivo m tal que é possível decompor $\mathbb{R}^n$ como $A_1 \cup A_2 \cup \cdots \cup A_m$ de modo que, para todo i, temos $x, y \in A_i \Rightarrow |x - y| \neq 1$. Por exemplo, a configuração de 7 pontos no plano na Figura 1 mostra que $c(2) \geq 4$, isto é, o número cromático do plano é pelo menos 4. Naquela configuração, os triângulos ABC, BCD, $AB'C'$ e $B'C'D'$ são triânglos equiláteros de lado 1. Ademais, a distância entre D e D' é 1. Fica como um exercício fácil para o leitor verificar que de fato esta configuração prova que $c(2) \geq 4$.

Figura 1 $c(2) \geq 4$



Por outro lado, não é muito difícil provar que $c(2) \leq 7$ (exercício!). O valor exato de $c(2)$ não é conhecido. O melhor que se sabe é que

$$4 \leq c(2) \leq 7. \tag{98}$$

As cotas em (98) permanecem inalteradas por mais de 45 anos.

Nesta seção, estamos interessados em provar que $c(n)$ cresce exponencialmente com n (na verdade, vamos provar algo mais forte). A próxima proposição já mostra que o crescimento de $c(n)$ é pelo menos exponencial.

Proposição 44. *Sejam p um primo e $n > 2p$. Existe um conjunto com $\binom{n}{2p-1}$ elementos $A \subset \mathbb{R}^n$ tal que qualquer subconjunto de A com mais de $\sum_{j=0}^{p-1} \binom{n}{j}$ elementos contém dois pontos à distância 1.*

Demonstração. Tomaremos

$$A = \frac{1}{\sqrt{2p}} \Omega(n, 2p-1),$$

onde, para $k \leq n$, $\Omega(n,k) \subset \mathbb{R}^n$ é o conjunto dos vetores de incidência dos subconjuntos de k elementos de $[n] = \{1, 2, \ldots, n\}$; isto é, a cada um dos $\binom{n}{k}$ subconjuntos $B \subset [n]$ com k elementos, associamos o vetor $v_B = (x_1, x_2, \ldots, x_n) \in \Omega(n,k)$ dado por

$$x_i = \chi_B(i) = \begin{cases} 0 & \text{se } i \notin B \\ 1 & \text{se } i \in B. \end{cases}$$

Vamos provar que, se dividirmos $\Omega(n, 2p-1)$ em menos de $\binom{n}{2p-1} / \binom{n}{p-1}$ partes, alguma delas conterá um par de vetores à distância $\sqrt{2p}$.

Para isso, notemos que se $B_1, B_2 \subset [n]$ têm $2p-1$ elementos cada, o quadrado da distância entre seus vetores de incidência é $|v_{B_1} - v_{B_2}|^2 = 2(2p - 1 - |B_1 \cap B_2|)$, que é igual a $2p$ se e somente se $|B_1 \cap B_2| = p-1$. Assim, pelo Corolário 34, um subconjunto de $\Omega(n, 2p-1)$ que não contenha nenhum par de vetores à distância $\sqrt{2p}$ deve ter no máximo $\sum_{j=0}^{p-1} \binom{n}{j}$ elementos, o que implica o resultado. □

O próximo lema, devido a Larman e Rogers, permitirá provar que se dividirmos $\mathbb{R}^n$ em no máximo $(1{,}2)^n$ subconjuntos, então em um desses subconjuntos todas as distâncias serão realizadas, desde que n seja suficientemente grande.

Lema 45. *Se $X \subset \mathbb{R}^n$ é um conjunto finito com k elementos tal que qualquer subconjunto de X com mais de r elementos contém dois pontos* *à distância* 1 *então, se dividirmos* $\mathbb{R}^n$ *em menos de* k/r *subconjuntos, em algum deles todas as distâncias serão realizadas.*

DEMONSTRAÇÃO. Suponha por absurdo que $\mathbb{R}^n = A_1 \cup A_2 \cup \cdots \cup A_m$ onde $m < k/r$ e existem $\alpha_1, \alpha_2, \ldots, \alpha_m > 0$ tais que $x, y \in A_i \Rightarrow |x - y| \neq \alpha_i$. Tomamos conjuntos $Y_1, Y_2, \ldots, Y_m \subset \mathbb{R}^n$ congruentes respectivamente a $\alpha_1 X, \alpha_2 X, \ldots, \alpha_m X$ tais que

$$Y_1 + Y_2 + \cdots + Y_m = \{y_1 + y_2 + \cdots + y_m \mid y_i \in Y_i,\ 1 \leq i \leq m\}$$

tenha k^m elementos (ou seja, $y_1 + y_2 + \cdots + y_m = z_1 + z_2 + \cdots + z_m$ com $y_i, z_i \in Y_i$, $1 \leq i \leq m$, implica $y_i = z_i$, $1 \leq i \leq m$). Deixamos para o leitor a prova da existência de tais conjuntos Y_i (por exemplo, por indução em m: supomos que $Y_1 + \cdots + Y_{m-1}$ tem k^{m-1} elementos, e aplicamos uma isometria a $\alpha_m X$ para obter Y_m; use o fato que dados z e w em $Y_1 + \cdots + Y_{m-1}$, x e y em $\alpha_m X$, $x \neq y$, quase nenhuma isometria U satisfaz $Ux + z = Uy + w$).

Como $B = Y_1 + Y_2 + \cdots + Y_m = B \cap (A_1 \cup A_2 \cup \cdots \cup A_m) = (B \cap A_1) \cup (B \cap A_2) \cup \cdots \cup (B \cap A_m)$ tem k^m elementos, e $m < k/r$, existe $i \leq m$ tal que $B \cap A_i$ tem mais de $k^m/(k/r) = r \cdot k^{m-1}$ elementos. Por outro lado, B pode ser escrito como união disjunta de k^{m-1} translações de Y_i:

$$B = \bigcup_z (Y_i + z),$$

onde a união é sobre $z \in Y_1 \cup \cdots \cup Y_{i-1} \cup Y_{i+1} \cup \cdots \cup Y_m$, donde, para algum $z \in Y_1 \cup \cdots \cup Y_{i-1} \cup Y_{i+1} \cup \cdots \cup Y_m$, temos $|(Y_i + z) \cap A_i| > r$. Como $Y_i + z$ é congruente a $\alpha_i X$, existem, por hipótese, dois pontos de $(Y_i + z) \cap A_i$ à distância α_i, o que é uma contradição. $\square$

Podemos agora provar o

TEOREMA 46. *Se* n *é suficientemente grande e* $m \leq (1{,}2)^n$ *então, dada qualquer decomposição* $\mathbb{R}^n = A_1 \cup A_2 \cup \cdots \cup A_m$*, existe* $i \leq m$ *tal que, para todo* $d > 0$*, existem* $x, y \in A_i$ *com* $|x - y| = d$*.*

Demonstração. Combinando a proposição e o lema anteriores, concluímos que dado p primo com $2p < n$, se $m < \binom{n}{2p-1} / \sum_{j=0}^{p-1} \binom{n}{j}$, então vale que todas as distâncias são realizadas em algum A_i $(1 \leq i \leq m)$. Como podemos supor que $n \geq 3p - 4$, temos que $\sum_{j=0}^{p-1} \binom{n}{j} < 2\binom{n}{p-1}$, donde $\binom{n}{2p-1} / \sum_{j=0}^{p-1} \binom{n}{j} > \binom{n}{2p-1} / 2\binom{n}{p-1}$. Seja $a_k = \binom{n}{2k-1} / 2\binom{n}{k-1}$. Temos

$$\frac{a_{k+1}}{a_k} = \frac{(n-2k+1)(n-2k)k}{2k(2k+1)(n-k+1)} = \frac{(n-2k+1)(n-2k)}{2(2k+1)(n-k+1)}.$$

Se $k = \alpha n$, $0 < \alpha < \frac{1}{2}$, a razão a_{k+1}/a_k é aproximadamente

$$\frac{1-2\alpha)^2}{4\alpha(1-\alpha)} = \frac{1}{4\alpha(1-\alpha)} - 1,$$

que é uma função decrescente de $(0, \frac{1}{2})$ em $(0, \infty)$, e é maior que um se e somente se $0 < \alpha < \frac{2-\sqrt{2}}{4}$. Assim, para maximizar a_k, devemos tomar k próximo de $(\frac{2-\sqrt{2}}{4})n$. Seja então p o número primo mais próximo a $(\frac{2-\sqrt{2}}{4})n$.

Agora usamos que, fixado $\varepsilon > 0$, se $\alpha \in (\varepsilon, 1-\varepsilon)$ e $n \to \infty$, então

$$\binom{n}{\alpha n} = \left(\frac{1}{\alpha^\alpha (1-\alpha)^{1-\alpha}}\right)^{(1+o(1))n}$$

(veja Lema 95 no Apêndice A). No nosso caso, como $p - 1 = (\beta + o(1))n$ e $2p - 1 = (2\beta + o(1))n$, onde $\beta = \frac{2-\sqrt{2}}{4}$, segue que

$$\binom{n}{2p-1} \Big/ 2\binom{n}{p-1} = \left(\frac{\beta^\beta (1-\beta)^{1-\beta}}{(2\beta)^{2\beta}(1-2\beta)^{1-2\beta}}\right)^{(1+o(1))n}.$$

Para concluir a prova, basta observar que

$$\frac{\beta^\beta (1-\beta)^{1-\beta}}{(2\beta)^{2\beta}(1-2\beta)^{1-2\beta}} = 1{,}2071 \cdots > 1{,}2.$$

$\square$

O teorema anterior implica que o número cromático $c(n)$ do $\mathbb{R}^n$ satisfaz $c(n) > (1{,}2)^n$, para n suficientemente grande. Não é difícil ver que $c(n) \leq 9^n$ para todo n: consideramos uma união disjunta maximal de bolas abertas de raio 1 em $\mathbb{R}^n$, $\bigcup_{i=1}^{\infty} B(x_i, 1) \subset \mathbb{R}^n$. Devemos ter $\bigcup_{i=1}^{\infty} B(x_i, 2) = \mathbb{R}^n$, pois se $y \notin B(x_i, 2)$ para nenhum i, então $B(y, 1) \cap B(x_i, 1) \neq \emptyset$ para todo i, contradizendo a maximalidade de $\bigcup_{i=1}^{\infty} B(x_i, 1)$. Cobrimos agora $B(0, 2)$ por no máximo 9^n bolas de raio $\frac{1}{2}$ (consideramos uma coleção disjunta maximal de bolas de raio $\frac{1}{4}$ centradas em $B(0, 2)$ e dobramos seus raios), digamos $B(0, 2) \subset \bigcup_{j=1}^{m} B(y_j, \frac{1}{2})$, onde $m \leq 9^n$. Seja agora $A_j = \bigcup_{i=1}^{\infty} B(x_i + y_j, \frac{1}{2})$. É fácil ver que $A_1 \cup A_2 \cup \cdots \cup A_m = \mathbb{R}^n$ e $x, y \in A_j \Rightarrow |x - y| \neq 1$. Se quisermos os A_j disjuntos basta substituir A_j por $\widetilde{A}_j = A_j \setminus \bigcup_{i<j} A_i$, $1 \leq j \leq m$.

Vamos agora provar a melhor estimativa superior assintótica conhecida para $c(n)$, provada em 1972 por Larman e Rogers [**54**]:

Teorema 47. $c(n) < (3 + o(1))^n$.

Demonstração. Sejam $\mathbb{Z}^n$ o conjunto dos pontos de $\mathbb{R}^n$ com coordenadas inteiras, e $\mathbb{T}^n = \mathbb{R}^n/\mathbb{Z}^n$ o *toro n-dimensional* obtido como quociente de $\mathbb{R}^n$ pela relação de equivalência $\sim$ dada por $x \sim y \Leftrightarrow x - y \in \mathbb{Z}^n$. Dado $x \in \mathbb{R}^n$ denotamos por $\overline{x} \in \mathbb{T}^n$ sua classe de equivalência, e por $\pi \colon \mathbb{R}^n \to \mathbb{T}^n$ a projeção canônica dada por $\pi(x) = \overline{x}$. Dados $u, v \in \mathbb{T}^n$, definimos a distância $d(u, v)$ como $d(\pi^{-1}(u), \pi^{-1}(v)) = \min\{|x-y|,\ x \in \pi^{-1}(u), y \in \pi^{-1}(v)\}$, ou seja, $d(\pi(x), \pi(y)) = \min\{|x - y + z|,\ z \in \mathbb{Z}^n\}$. Dado $u \subset \mathbb{T}^n$ e $r > 0$, definimos a bola aberta $B(u, r) = \{v \in \mathbb{T}^n \mid d(u, v) < r\}$. Definimos também $\pi(x) + \pi(y) = \pi(x + y)$.

Consideremos uma união disjunta maximal de bolas abertas em $\mathbb{T}^n$ de raio $\frac{1}{4}$, digamos $\bigcup_{j=1}^{m} B(u_j, \frac{1}{4})$. Temos $\bigcup_{j=1}^{m} B(u_j, \frac{1}{2}) = \mathbb{T}^n$ (de fato, se $y \notin \bigcup_{j=1}^{m} B(u_j, \frac{1}{2})$, $B(y, \frac{1}{4})$ seria disjunto de $\bigcup_{j=1}^{m} B(u_j, \frac{1}{4})$, contradizendo a maximalidade).

Seja $P_j = \{v \in \mathbb{T}^n \mid d(v, u_j) \leq d(v, u_i),\ \forall\, i \neq j\}$ o *poliedro de Voronoi* em $\mathbb{T}^n$ associado a $u_j \in C = \{u_i,\ 1 \leq i \leq m\}$. Dado $x \in \pi^{-1}(u_j)$,

$$\pi^{-1}(P_j) = \bigcup_{v \in \mathbb{Z}^n} (\widetilde{P}_x + v), \tag{99}$$

onde $\widetilde{P}_x = \{y \in \mathbb{R}^n \mid |y-x| \leq |y-z|, \forall\, z \in \pi^{-1}(C)\}$ é um poliedro, o *poliedro de Voronoi* associado a $x \in \pi^{-1}(C) \subset \mathbb{R}^n$.

Note que a união (99) acima é uma união disjunta, pois, de $\mathbb{T}^n = \bigcup_{j=1}^m B(u_j, \frac{1}{2})$ segue que $P_j \subset B(u_j, \frac{1}{2})$, cujo diâmetro é menor que 1. Além disso, como as bolas $B(u_j, \frac{1}{4})$ são disjuntas, $P_j \supset B(u_j, \frac{1}{4})$.

Podemos então escrever $\widetilde{P}_x = x + Q_x$, onde Q_x é um poliedro convexo em $\mathbb{R}^n$ que contém $B(0, \frac{1}{4})$ e está contido em $B(0, \frac{1}{2})$, para cada $x \in \pi^{-1}(C)$. Fixamos $\delta > 0$ pequeno e definimos os conjuntos

$$\widetilde{A} = \bigcup_{x \in \pi^{-1}(C)} \left(x + \frac{1}{3+\delta} Q_x\right) = \bigcup_{x \in \pi^{-1}(C)} \left\{\frac{(2+\delta)x + y}{3+\delta},\, y \in \widetilde{P}_x\right\} \subset \mathbb{R}^n.$$

Temos que $y, z \in \widetilde{A} \Rightarrow |y-z| \neq \frac{1}{3}$. De fato, para cada $x \in \pi^{-1}(C)$, $Q_x \subset B(0, \frac{1}{2}) \Rightarrow x + \frac{1}{3+\delta} Q_x \subset B(x, \frac{1}{6+2\delta}) \Rightarrow |y-z| < \frac{1}{3}$, $\forall\, y, z \in x + \frac{1}{3+\delta} Q_x$. Por outro lado, dados dois pontos distintos $x_1, x_2 \in \pi^{-1}(C)$, $y_1 \in \widetilde{P}_{x_1}$, $y_2 \in \widetilde{P}_{x_2}$,

$$z_1 = \frac{(2+\delta)x_1 + y_1}{3+\delta} \in x_1 + \frac{1}{3+\delta} Q_{x_1}$$

e

$$z_2 = \frac{(2+\delta)x_2 + y_2}{3+\delta} \in x_2 + \frac{1}{3+\delta} Q_{x_2},$$

se α é o plano mediador de $\overline{x_1 x_2}$, x_1 e x_2 estão em lados opostos de α, y_1 está do mesmo lado de x_1 e y_2 do mesmo lado de x_2. Como $B(x_i, \frac{1}{4}) \subset \widetilde{P}_{x_i}$, $i = 1, 2$, segue que as distâncias de x_1 e x_2 ao plano α são maiores ou iguais a $\frac{1}{4}$, donde as distâncias de z_1 e z_2 ao plano α são maiores ou iguais a $\frac{2+\delta}{3+\delta} \cdot \frac{1}{4}$, e portanto a distância de z_1 a z_2 é pelo menos $\frac{2+\delta}{3+\delta} \cdot \frac{1}{2} > \frac{1}{3}$.

Vamos mostrar agora que é possível cobrir $\mathbb{R}^n$ com no máximo $(3 + 3\delta)^n$ translações de $\widetilde{A}$, se n é suficientemente grande. Isto encerrará a prova, pois nesse caso também seria possível cobrir $\mathbb{R}^n$ com no máximo $(3 + 3\delta)^n$ translações de $3\widetilde{A}$, e , numa translação de $3\widetilde{A}$, não há dois pontos à distância 1.

Para mostrar nossa afirmação, vamos provar que é possível cobrir $\mathbb{T}^n$ com no máximo $(3 + 3\delta)^n$ translações de $A = \pi(\widetilde{A})$. Como, para todo $u \in \mathbb{T}^n$ existe um único $x \in \pi^{-1}(u) \cap [0,1)^n$, dado um conjunto $X \subset \mathbb{T}^n$ podemos definir o volume de X (que denotaremos por $\mathrm{vol}(X)$) como o volume de $\pi^{-1}(X) \cap [0,1)^n$ em $\mathbb{R}^n$. Temos $\mathrm{vol}(\mathbb{T}^n) = 1$ e, como $\bigcup_{j=1}^m P_j = \mathbb{T}^n$, $\sum_{j=1}^m \mathrm{vol}(P_j) = 1$ (de fato, se $i \neq j$, $\mathrm{vol}(P_i \cap P_j) = 0$, pois $\pi^{-1}(P_i \cap P_j)$ está contido numa união enumerável de hiperplanos). Além disso, se $x \in \pi^{-1}(u_j)$,

$$\mathrm{vol}(P_j) = \mathrm{vol}\widetilde{P}_x = \mathrm{vol}\ Q_x,$$

e

$$\mathrm{vol}\left(x + \frac{1}{3+\delta} Q_x\right) = \frac{1}{(3+\delta)^n} \mathrm{vol}\ Q_x.$$

Dados $x_1, x_2 \in \pi^{-1}(u_j)$,

$$\pi\left(x_1 + \frac{1}{3+\delta} Q_{x_1}\right) = \pi\left(x_2 + \frac{1}{3+\delta} Q_{x_2}\right),$$

pois $Q_{x_1} = Q_{x_2}$. Assim, como

$$A = \pi\Big(\bigcup_{x \in \pi^{-1}(C)} \Big(x + \frac{1}{3+\delta} Q_x\Big)\Big) = \bigcup_{i=1}^m \widetilde{Q}_i,$$

com

$$\widetilde{Q}_i = u_i + \pi\left(\frac{1}{3+\delta} Q_{x_i}\right),$$

onde x_i é um elemento arbitrário de $\pi^{-1}(u_i)$, temos

$$\mathrm{vol}(A) = \frac{1}{(3+\delta)^n},$$

pois $\widetilde{Q}_i \cap \widetilde{Q}_j = \emptyset$ para todo $i \neq j$, e

$$\mathrm{vol}\ \widetilde{Q}_i = \frac{1}{(3+\delta)^n}\ \mathrm{vol}\ Q_{x_i} = \frac{1}{(3+\delta)^n}\ \mathrm{vol}\ (P_i).$$

Dados conjuntos $A', X \subset \mathbb{T}^n$ sempre existe uma translação de A', $A' + v \subset \mathbb{T}^n$, tal que $\mathrm{vol}((A' + v) \cap X) \geq \mathrm{vol}(A') \cdot \mathrm{vol}(X)$. De fato, a média de $\mathrm{vol}((A'+v) \cap X)$ para $v \in \mathbb{T}^n$ é igual a $\mathrm{vol}(A')\ \mathrm{vol}(X)$. Usando repetidamente este fato, concluímos que, para todo inteiro positivo k

existem $v_1, v_2, \ldots, v_k \in \mathbb{T}^n$ tais que

$$\operatorname{vol}\Big(\mathbb{T}^n \setminus \bigcup_{j=1}^{k}(A' + v_j)\Big) \leq (1 - \operatorname{vol}(A'))^k$$

(essa idéia, adaptada para conjuntos finitos, será muito usada no Capítulo 4).

Usaremos este fato com

$$A' = \pi\Bigg(\bigcup_{x \in \pi^{-1}(C)} \Big(x + \frac{1}{3+2\delta} Q_x\Big)\Bigg) \subset A,$$

para o qual

$$\operatorname{vol}(A') = \frac{1}{(3+2\delta)^n},$$

como antes, e $k = (3+3\delta)^n$, para obter $v_1, v_2, \ldots, v_k \in \mathbb{T}^n$ com

$$\operatorname{vol}\left(\mathbb{T}^n \Big\backslash \bigcup_{j=1}^{k}(A' + v_j)\right) \leq \left(1 - \frac{1}{(3+2\delta)^n}\right)^{(3+3\delta)^n} < e^{-(\frac{3+3\delta}{3+2\delta})^n}$$
$$< \left(\frac{\delta}{2(3+2\delta)\sqrt{n}}\right)^n < \operatorname{vol}\left(B\left(0, \frac{\delta}{4(3+2\delta)}\right)\right),$$

se n é suficientemente grande, donde, para todo $u \in \mathbb{T}^n$,

$$B\left(u, \frac{\delta}{4(3+2\delta)}\right)$$

intersecta $\bigcup_{j=1}^{k}(A' + v_j)$, e portanto existem $x \in \pi^{-1}(C)$ e $\widetilde{y} \in \frac{1}{3+2\delta} Q_x$ com

$$|u - (\pi(x + \widetilde{y}) + v_j)| < \frac{\delta}{4(3+2\delta)}.$$

Finalmente, se $Q \subset \mathbb{R}^n$ é convexo e $B(0,r) \subset Q$, se $y \in Q$, $0 < \lambda < 1$ e $|z - \lambda y| < r(1-\lambda)$ então $z \in Q$, pois, se

$$\widetilde{z} = \frac{z - \lambda y}{1 - \lambda},$$

temos

$$|\widetilde{z}| < \frac{r(1-\lambda)}{1-\lambda} = r,$$

donde $\widetilde{z} \in B(0,r) \subset Q$ e portanto $z = \lambda y + (1-\lambda)\widetilde{z} \in Q$. Assim, fazendo

$$Q = \frac{1}{3+\delta} Q_x, \quad \lambda = \frac{3+\delta}{3+2\delta}, \quad y = \frac{3+2\delta}{3+\delta}\widetilde{y} \quad \text{e} \quad r = \frac{1}{4},$$

temos

$$B\left(\widetilde{y}, \frac{\delta}{4(3+2\delta)}\right) \subset \frac{1}{3+\delta} Q_x$$

(pois $\widetilde{y} = \lambda y$), donde $|u - (\pi(x+\widetilde{y}) + v_j)| < \frac{\delta}{4(3+2\delta)}$ implica

$$u \in v_j + \pi\left(x + \frac{1}{3+\delta} Q_x\right).$$

Portanto, temos

$$\bigcup_{j=1}^{k} (A + v_j) = \bigcup_{j=1}^{k} \bigcup_{x \in \pi^{-1}(C)} \left(v_j + \pi\left(x + \frac{1}{3+\delta} Q_x\right)\right) = \mathbb{T}^n,$$

o que completa a prova. □

5. Uma construção explícita na teoria de Ramsey

O nosso objetivo nesta seção é expor uma construção de uma família de grafos, devida a Frankl e Wilson [**34**], que prova que os números de Ramsey diagonais $R(n)$ crescem superpolinomialmente com n (veja a Seção 5.3 do Capítulo 1).

Começamos provando um corolário do Teorema 33.

Corolário 48. *Seja $\mathcal{A} \subset \binom{[n]}{k}$ um sistema de k-conjuntos e L um conjunto de s inteiros. Suponha que, para todo A e $A' \in \mathcal{A}$ distintos, temos $|A \cap A'| \in L$. Então*

$$|\mathcal{A}| \le \sum_{0 \le j \le s} \binom{n}{j}. \tag{100}$$

Demonstração. Claramente, podemos supor que $L \subset [k-1]$. Suponha ainda que $\mathcal{A} = \{A_1, \ldots, A_m\}$, como no Teorema 33, e seja p um primo maior que k. Então as condições (i) e (ii) daquele teorema se aplicam. Concluímos que (100) vale. $\square$

Consideremos agora a seguinte construção de um grafo $G = G(n,p)$. Seja p um primo e n um inteiro positivo e ponha

$$V = \binom{[n]}{p^2-1}. \tag{101}$$

O nosso grafo G terá como conjunto de vértices o conjunto V acima. Dois vértices A e $B \in V$ serão adjacentes em G se e só se

$$|A \cap B| \equiv -1 \pmod{p}. \tag{102}$$

Observamos que se $p = 2$, então o grafo $G(n,p) = G(n,2)$ é exatamente o grafo construído por Nagy (veja Seção 5.3).

Vamos agora provar um limitante superior para $\alpha(G)$ e $\omega(G)$.

Teorema 49. *Para todo primo p e inteiro positivo n satisfazendo*

$$p - 1 \leq \frac{n+1}{3}, \tag{103}$$

temos

$$\alpha(G(n,p)),\ \omega(G(n,p)) < 2\binom{n}{p-1}. \tag{104}$$

Demonstração. Suponha que os vértices $A_1, \ldots, A_\omega$ formam um clique em $G = G(n,p)$. Note que o Corolário 48 aplica-se ao sistema $\mathcal{A} = \{A_i : 1 \leq i \leq \omega\}$ com $k = p^2 - 1$ e $L = \{p-1, 2p-1, \ldots, p^2-p-1\}$, de forma que $s = p - 1$. Daí segue que

$$\omega = |\mathcal{A}| \leq \sum_{0 \leq j \leq s} \binom{n}{j}. \tag{105}$$

Suponha que $B_1, \ldots, B_\alpha$ formam um conjunto independente em $G = G(n,p)$. Note que o Teorema 33 aplica-se ao sistema $\mathcal{B} = \{B_i : 1 \leq i \leq$

$\alpha\}$ com $L = \{0, 1, \ldots, p-2\}$, de forma que $s = p - 1$. Daí segue que

$$\alpha = |\mathcal{B}| \leq \sum_{0 \leq j \leq s} \binom{n}{j}. \tag{106}$$

Agora usamos o Lema 41 para estimar a soma que ocorre no lado direito de (105) e (106). A única hipótese do Lema 41 que temos de verificar é verdadeira aqui, pois já estamos supondo (103), de forma que

$$\sum_{0 \leq j \leq s} \binom{n}{j} < 2\binom{n}{s} = 2\binom{n}{p-1}. \tag{107}$$

O Teorema 49 segue de (105)–(107). □

O Teorema 49 fornece limitantes inferiores super-polinomiais para os números de Ramsey, através de grafos definidos explicitamente. Para verificar esta asserção, basta de escolher os parâmetros n e p de forma apropriada.

TEOREMA 50. *Para todo $\varepsilon > 0$, existe uma constante $t_0 = t_0(\varepsilon)$ para o qual vale o seguinte. Se $t \geq t_0$, então podemos definir explicitamente um grafo G_t com pelo menos*

$$\exp\left\{\left(\frac{1}{4} - \varepsilon\right)\frac{(\log t)^2}{\log\log t}\right\} \tag{108}$$

vértices e tal que $\alpha(G_t)$, $\omega(G_t) < t$. Em particular, este grafo mostra que

$$R(t) > \exp\left\{\left(\frac{1}{4} - \varepsilon\right)\frac{(\log t)^2}{\log\log t}\right\}. \tag{109}$$

DEMONSTRAÇÃO. Seja t um inteiro dado, que podemos supor ser convenientemente grande. No que segue, suporemos tacitamente que $t \geq t_0$ para uma constante t_0 convenientemente grande.

Seja p o maior primo satisfazendo

$$p \leq \frac{\log t}{2\log\log t}. \tag{110}$$

Pelo teorema dos números primos, sabemos que

$$p = \left(\frac{1}{2} - o(1)\right) \frac{\log t}{\log\log t}, \tag{111}$$

onde $o(1) \to 0$ conforme $t \to \infty$.

Note que, devido a esta escolha de p, temos

$$p + 2p \log p \leq \log t,$$

de onde segue que

$$(ep^2)^p \leq t. \tag{112}$$

Afirmamos agora que

$$2\binom{p^3}{p-1} \leq t. \tag{113}$$

De fato, note que

$$2\binom{p^3}{p-1} \leq 2\left(\frac{ep^3}{p-1}\right)^{p-1} \leq (ep^2)^p, \tag{114}$$

onde usamos que

$$\frac{2}{(1-1/p)^{p-1}} \leq 2e \leq ep^2.$$

A afirmação (113) decorre de (112) e (114).

Agora provamos que

$$\binom{p^3}{p^2-1} \geq \exp\left\{\left(\frac{1}{4} - \varepsilon\right) \frac{(\log t)^2}{\log\log t}\right\}, \tag{115}$$

desde que t seja suficientemente grande. Para verificar (115), use o Lema 94 do Apêndice A e observe que

$$\binom{p^3}{p^2-1} \geq \left(\frac{p^3}{p^2-1}\right)^{p^2-1} = \left(\frac{1}{1-1/p^2}\right)^{p^2-1} p^{p^2-1} \geq p^{p^2-1}. \tag{116}$$

Entretanto, temos

(117)
$$p^2 \log p = (1 - o(1)) \left(\frac{\log t}{2 \log\log t} \right)^2 \log\log t = \left(\frac{1}{4} - o(1) \right) \frac{(\log t)^2}{\log\log t},$$

onde $o(1) \to 0$ conforme $t \to \infty$. A desigualdade (115) segue de (116) e (117).

Agora estamos prontos para terminar a prova do Teorema 50. Naturalmente, tome para G_t o grafo $G(n, p)$ com p como acima e $n = p^3$. Então o número de vértices em G_t é, devido a (115), pelo menos o valor dado em (108). Ademais, as desigualdades (104) do Teorema 49 e (113) nos dizem que $G_t = G(n, p)$ é tal que

$$\alpha(G_t),\ \omega(G_t) < t.$$

O Teorema 50 está provado. $\square$

5.1. Grafos de Paley. Um grafo explicitamente definido que parece ser um bom candidato para provar limites inferiores exponenciais para os números de Ramsey $R(t)$ são os *grafos de Paley* Q_p. Suponha que p seja um primo com $p \equiv 1 \pmod 4$, de forma que -1 é um resíduo quadrático módulo p. Os vértices de Q_p são os inteiros módulo p e dois vértices distintos x, $y \in \mathbb{Z}/p\mathbb{Z}$ são adjacentes em Q_p se e só se $x - y$ é um resíduo quadrático módulo p. Como -1 é um resíduo quadrático, esta relação de adjacência é de fato simétrica e portanto temos um grafo bem definido.

Sabe-se que Q_p tem várias propriedades que o tornam parecido com o grafo aleatório G considerado na prova do Teorema 25 do Capítulo 1 (o limite inferior exponencial de Erdős para $R(t)$). Acredita-se que para valores esporádicos de p, os grafos Q_p podem ser tais que $\alpha(Q_p)$ e $\omega(Q_p)$ são pequenos.

No Capítulo 4, discutiremos brevemente uma construção de um sistema de conjuntos baseada em resíduos quadráticos.

CAPÍTULO 3

Teoria de Ramsey euclideana

1. Introdução

No começo da década de 70, um grupo de matemáticos ilustres, a saber, P. Erdős, R. L. Graham, P. Montgomery, B. L. Rothschild, J. Spencer, e E. G. Straus, iniciaram a investigação de um problema geométrico na teoria de Ramsey [**21, 22, 23**]. Basicamente falando, eles estavam interessados em saber quais configurações finitas de pontos, a menos de congruência, inevitavelmente ocorrem monocromaticamente em qualquer coloração de espaços euclideanos de dimensão suficientemente alta, se usamos um número fixo de cores. Em seu trabalho de 1973 [**21**], aqueles autores estabeleceram os fundamentos desse tópico da teoria de Ramsey, hoje conhecido como a *teoria de Ramsey euclideana*. Neste capítulo, vamos estudar alguns dos resultados básicos desta área. Os resultados das Seções 2 a 4.1 são todos deste trabalho que lançou este tópico de pesquisa. Nas seções seguintes, apresentamos alguns resultados mais recentes de Frankl, Rödl, e Křížž. Uma excelente resenha recente da área é [**40**].

Precisamos começar com algumas definições. Como usual, uma r-*coloração* de um conjunto X é simplesmente uma função $\phi\colon X \to C$, onde C é um conjunto com r elementos, chamados *cores*. Em geral, tomamos $C = [r] = \{1, \ldots, r\}$, de forma que nossas cores são os inteiros de 1 a r. No que segue, uma *configuração de pontos*, ou, simplesmente, uma *configuração*, é uma coleção finita de pontos em um espaço euclideano. Para enfatizar a finitude, usaremos às vezes o termo 'configuração finita'. No que segue, estamos interessados na estrutura de nossas configurações como objetos geométricos.

Seja K uma configuração finita. Vamos escrever $R(K, n, r)$ para a seguinte asserção:

(R) *Em qualquer r-coloração de $\mathbb{R}^n$, existe uma configuração $K' \subset \mathbb{R}^n$ congruente a K cujos pontos recebem todos a mesma cor.*

Podemos enunciar **(R)** mais formalmente como segue: para toda r-coloração $\phi\colon \mathbb{R}^n \to [r]$, existe uma isometria $\iota\colon K \hookrightarrow \mathbb{R}^n$ tal que se $K' = \iota(K) \subset \mathbb{R}^n$, então $\phi \restriction K'$ é constante (escrevemos $\phi \restriction K'$ para a função $K' \to [r]$ com $p \in K' \mapsto \phi(p)$, isto é, a *restrição* de ϕ a K').

Como usual, se os pontos de uma configuração K' estão todos coloridos de uma mesma cor, então dizemos que K' é *monocromática*. A asserção $R(K, n, r)$ diz que cópias monocromáticas de K são inevitáveis em r-colorações de $\mathbb{R}^n$. (Naturalmente, uma *cópia* de K é uma configuração congruente a K.)

Dizemos que uma configuração K é *Ramsey* se, para todo r, a asserção $R(K, n, r)$ vale para n suficientemente grande, isto é, existe $n_0 = n_0(K, r)$ tal que se $n \geq n_0$, então $R(K, n, r)$ vale. Note que se uma configuração K é Ramsey, então toda configuração semelhante a K também é Ramsey.

O princípio da casa do pombo mostra que se K é uma configuração com 2 pontos, digamos, à distância 1 (por exemplo, $K = \{0, 1\}$), então K é Ramsey. De fato, se $n \geq n_0(K, r) = r + 1$, então existem $r + 1$ pontos x_i $(1 \leq i \leq r + 1)$ em $\mathbb{R}^n$ com todos os pares $\{x_i, x_j\}$ $(1 \leq i < j \leq r + 1)$ à distância 1: basta tomar $x_i = (1/\sqrt{2})e_i$, onde os $e_i \in \mathbb{R}^n$ são os vetores da base canônica. Daí segue que $R(K, n, r)$ vale para $K = \{0, 1\}$ desde que $n \geq n_0(K, r) = r + 1$.

O leitor perceberá nesse ponto a relação entre o que estamos começando a discutir e tópicos que já discutimos: o número cromático do $\mathbb{R}^n$ é $> r$ se e só se $R(\{0, 1\}, n, r)$ vale. Traduzindo nossos resultados sobre o número cromático do $\mathbb{R}^n$ para este contexto, vemos que existem constantes c_1, $c_2 > 0$ para os quais $R(\{0, 1\}, n, r)$ vale se $r < 2^{c_1 n}$ e $R(\{0, 1\}, n, r)$ não vale se $r > 2^{c_2 n}$.

Neste capítulo, estamos tratando de configurações genéricas, mais ricas que dois pontos à distância 1. De fato, algumas delas têm tanta estrutura que é possível evitá-las em colorações com um número limitado de cores, mesmo que consideremos espaços de dimensão arbitrariamente alta. Por exemplo, a configuração $K = \{-1, 0, 1\} \subset \mathbb{R}$ não é Ramsey. Este é um bom exercício que o leitor pode tentar atacar agora, antes de ler este capítulo.

Quais configurações K são Ramsey? Esta é a pergunta central da teoria de Ramsey euclideana.

2. Um resultado de compacidade

Vamos começar com um lema básico. Para provar que se $|K| = 2$, então K é Ramsey, usamos uma configuração finita de pontos em $\mathbb{R}^n$ (a saber, $r+1$ pontos com todos os pares de pontos à mesma distância). O nosso primeiro lema diz que se uma configuração é Ramsey, então isto pode ser sempre provado considerando-se apenas configurações finitas de pontos de $\mathbb{R}^n$.

LEMA 51. *Seja K uma configuração Ramsey e $r \geq 1$ um inteiro. Então existe um configuração finita $L = L(K, r)$ tal que, em qualquer r-coloração de L, existe uma configuração $K' \subset L$ congruente a K cujos pontos recebem todos a mesma cor.*

Para provar o Lema 51, usaremos um argumento bem-conhecido de compacidade. Para tanto, precisamos de um resultado clássico da topologia, o teorema de Tychonov.

TEOREMA 52. *Seja X_λ $(\lambda \in \Lambda)$ uma família de espaços compactos. Então o espaço produto $Y = \prod_{\lambda \in \Lambda} X_\lambda$ é compacto.*

O leitor que não está familiarizado com o conceito de compacidade e o teorema de Tychonov deve acreditar no Lema 51 e continuar sua leitura mais adiante. Mencionamos ainda um exercício instrutivo para aqueles leitores: *suponha que a conclusão do Lema 51 seja falsa; mostre que então podemos encontrar uma r-coloração de $\mathbb{Q}^n$ sem cópias monocromáticas de K.* Para provar este fato, use o princípio da casa do pombo e o fato que $\mathbb{Q}^n$ é enumerável.

Provemos o Lema 51.

Demonstração do Lema 51. Seja K uma configuração Ramsey e $r \geq 1$ um inteiro dado. Suponha por contradição que nenhuma configuração finita L é tal que a conclusão do Lema 51 vale. Seja n um inteiro positivo arbitrário. Pela nossa hipótese, podemos r-colorir qualquer subconjunto finito de $\mathbb{R}^n$ sem criar uma cópia monocromática de K. Gostaríamos de provar que é possível 'colar' tais r-colorações em uma única r-coloração do $\mathbb{R}^n$ todo, sem criar cópias monocromáticas de K.

Se $L \subset \mathbb{R}^n$ é uma parte finita de $\mathbb{R}^n$ e $\phi\colon \mathbb{R}^n \to [r]$ é uma r-coloração de $\mathbb{R}^n$, vamos dizer que ϕ é *L-boa* se ϕ restrita a L não gera um cópia monocromática $K' \subset L$ congruente a K. Note que, para cada parte finita L de $\mathbb{R}^n$, sempre existe uma coloração ϕ que é L-boa.

Tome, para cada $p \in \mathbb{R}^n$, o espaço discreto $X_p = [r]$, que é compacto. Pelo Teorema 52, o espaço produto $Y = \prod_{p\in\mathbb{R}^n} X_p$ é compacto. Note que podemos identificar os pontos de Y com as r-colorações de $\mathbb{R}^n$. Para todo conjunto finito $L \subset \mathbb{R}^n$, ponha

$$F_L = \{\phi \in Y : \phi \text{ é } L\text{-boa}\}. \tag{118}$$

Claramente, F_L é fechado e não-vazio. Ademais, a intersecção finita de conjuntos da forma F_L ($L \subset \mathbb{R}^n$ finito) é não-vazia. Da compacidade de Y segue que

$$\bigcap_L F_L \neq \emptyset, \tag{119}$$

onde a interseção é tomada sobre todos os conjuntos finitos $L \subset \mathbb{R}^n$. Um ponto na interseção em (119) é uma r-coloração de $\mathbb{R}^n$ sem uma cópia monocromática de K. Como n era arbitrário, temos uma contradição com o fato de K ser Ramsey. Esta contradição termina a prova do Lema 51. □

2.1. Conjuntos infinitos. O que acontece se temos um conjunto infinito $Z \subset \mathbb{R}^d$? Pode valer a propriedade $R(Z, n, r)$ para algum n suficientemente grande e, digamos, $r = 2$? O seguinte resultado de Erdős *et al.* **[22]** mostra que isto não ocorre para nenhum Z infinito!

Teorema 53. *Seja Z qualquer subconjunto infinito de $\mathbb{R}^d$. Então $\mathbb{R}^d$ pode ser colorido com um número infinito de cores de forma que todas as configurações semelhantes a Z recebam todas as cores usadas.*

Mantendo uma das cores na coloração acima e identificando todas as outras, obtemos uma bi-coloração do $\mathbb{R}^d$ sem cópias semelhantes de Z monocromáticas.

Corolário 54. *Se Z é um conjunto infinito de pontos de um espaço euclideano, então a propriedade $R(Z, n, r)$ não vale para nenhum n e nenhum $r \geq 2$.*

3. O teorema do produto

Provaremos nesta seção um resultado que nos permite construir várias configurações Ramsey. Se $a = (a_i)^T \in \mathbb{R}^k$ e $b = (b_j)^T \in \mathbb{R}^\ell$, pomos

$$a * b = (a_1, \ldots, a_k, b_1, \ldots, b_\ell)^T \in \mathbb{R}^{k+\ell}. \tag{120}$$

Mais geralmente, se $A \subset \mathbb{R}^n$ e $B \subset \mathbb{R}^m$, pomos

$$A * B = \{a * b \colon a \in A \text{ e } b \in B\} \subset \mathbb{R}^{k+\ell}. \tag{121}$$

O resultado principal desta seção é o seguinte.

Teorema 55. *Se A e B são configurações Ramsey, então $A * B$ é uma configuração Ramsey.*

Demonstração. Suponha que A e B são Ramsey. Seja $L = L(A, r)$ uma configuração finita tal que qualquer r-coloração de L gera uma cópia monocromática de A. Tal configuração L existe devido ao Lema 51. Suponha que $L \subset \mathbb{R}^m$. Analogamente, seja $L' = L'(B, r')$ uma configuração tal que qualquer r'-coloração de L' gera uma cópia monocromática de B, onde

$$r' = r^{|L|}. \tag{122}$$

Suponha que $L' \subset \mathbb{R}^n$. Afirmamos que

(†) $L * L' \subset \mathbb{R}^{m+n}$ é tal que toda r-coloração de $L * L'$ gera uma cópia monocromática de $A * B$.

Para provar (†), fixe uma r-coloração $\psi\colon L * L' \to [r]$ de $L * L'$. Esta coloração ψ define naturalmente uma r'-coloração ϕ' de L', a saber, a coloração $\phi'\colon L' \to [r]^L$ com

$$\phi'(q) = (\psi(p * q))_{p \in L}.$$

Pela escolha de L', sabemos que existe uma cópia $B' \subset L'$ de B monocromática na coloração ϕ'. Esta cor comum dos pontos de B' define uma r-coloração $\phi\colon L \to [r]$, a saber, a coloração em que, para todo $p \in L$, temos

$$\phi(p) = \psi(p * q), \tag{123}$$

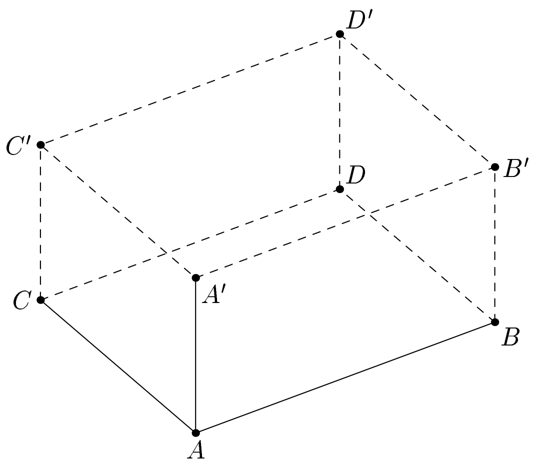
onde q é qualquer elemento de B' (como B' é monocromático, o lado direito de (123) é independente de q). Pela escolha de L, sabemos que existe uma cópia $A' \subset L$ de A que é monocromática na coloração ϕ.

É fácil ver que a coloração ψ é constante em $A' * B'$. Provamos portanto a validade de (†). O Teorema 55 segue imediatamente de (†). $\square$

Um *tijolo* é um conjunto da forma $I_i \times \cdots \times I_n \subset \mathbb{R}^n$ para algum n, onde os $I_i = [a_i, b_i] \subset \mathbb{R}$ são intervalos com $a_i < b_i$. Os *vértices* desse tijolo são os vetores da forma $(x_i)_{1 \leq i \leq n}$, onde cada x_i pertence a $\{a_i, b_i\}$. Veja a Figura 2. Pelo fato de configurações com 2 elementos ser Ramsey, segue do Teorema 55 que o conjunto de vértices de um tijolo é Ramsey. Naturalmente, todo subconjunto de um tal conjunto de vértices é também Ramsey.

As observações acima provam que o (conjunto de vértices) de um triângulo retângulo é Ramsey. Ademais, é um exercício de geometria simples (mas não deixe de fazer!) que o conjunto de vértices de todo triângulo *agudo* está contido no conjunto de vértices de um tijolo apropriado. Daí segue que todo triângulo agudo é também Ramsey. Temos ainda o seguinte resultado provado em 1986 por Frankl e Rödl **[35]**.

Figura 2 O belo tijolo $AB * AC * AA'$



Teorema 56. *Todo triângulo obtuso é Ramsey.*

A prova do Teorema 56 é um tanto delicada e fica para a Seção 5.2 abaixo.

Observação. Para ser mais preciso, o enunciado do Teorema 56 deveria ser que o conjunto de vértices de todo triângulo obtuso é Ramsey. Entretanto, será conveniente para nós identificarmos nossos triângulos com seus conjuntos de vértices. Ademais, muitas vezes identificaremos nossos tijolos com seus conjuntos de vértices também.

4. Conjuntos esféricos

Até agora, provamos resultados 'positivos' para a teoria de Ramsey, isto é, resultados que afirmam que certas configurações são Ramsey. Nesta seção, vamos discutir resultados 'negativos'. Comecemos com o seguinte resultado.

Teorema 57. *A configuração $K = \{-1, 0, 1\}$ não é Ramsey.*

Demonstração. Fixe $n \geq 1$. Vamos mostrar uma 4-coloração ϕ de $\mathbb{R}^n$ que não contém uma cópia monocromática de K. Pomos, para todo $x \in \mathbb{R}^n$,

$$\phi(x) = \lfloor \|x\|^2 \rfloor \bmod 4, \tag{124}$$

onde $\|x\| = \sqrt{\langle x, x\rangle}$ é a norma euclideana de x. Suponha que esta 4-coloração gera uma cópia monocromática K' de K. Sejam x e $u \in \mathbb{R}^n$ com $\|u\| = 1$ tais que $K' = \{x - u, x, x + u\}$. Pelo fato de K' ser monocromático, existem inteiros a_i $(i \in \{-1, 0, 1\})$, um inteiro $r \in \{0, 1, 2\}$, e reais $0 \leq \theta_i < 1$ $(i \in \{-1, 0, 1\})$, tais que

$$\|x - u\|^2 = 4a_{-1} + r + \theta_{-1}, \qquad \|x\|^2 = 4a_0 + r + \theta_0, \tag{125}$$

e

$$\|x + u\|^2 = 4a_1 + r + \theta_1. \tag{126}$$

Expandindo $\|x \pm u\|^2 = \langle x \pm u, x \pm u\rangle$ e usando (125) e (126), obtemos

$$1 + 2\langle x, u\rangle = 4(a_{-1} - a_0) + \theta_{-1} - \theta_0$$

e

$$1 - 2\langle x, u\rangle = 4(a_1 - a_0) + \theta_1 - \theta_0.$$

Daí segue que

$$2 = 4(a_{-1} + a_1 - 2a_0) + (\theta_{-1} + \theta_1 - 2\theta_0). \tag{127}$$

Entretanto $|\theta_{-1} + \theta_1 - 2\theta_0| < 2$, e portanto (127) não pode ocorrer. Este absurdo prova que a asserção $R(K, n, 4)$ não vale. Como n é arbitrário, concluímos que a configuração K não é Ramsey. $\square$

O resultado que fornece a condição necessária mais restritiva conhecida para uma configuração ser Ramsey é o seguinte. Dizemos que uma configuração K é *esférica* se alguma esfera contém uma cópia de K. Isto é, podemos encontrar uma cópia K' de K em algum $\mathbb{R}^n$ de forma que existe um ponto $w \in \mathbb{R}^n$ equidistante de todos os pontos em K'.

TEOREMA 58. *Toda configuração Ramsey é esférica.*

Claramente, o Teorema 58 implica o Teorema 57, pois a configuração $K = \{-1, 0, 1\}$ não pode ser imersa isometricamente em uma esfera. De fato, se $K' = \{x_{-1}, x_0, x_1\}$ é uma cópia de K em $\mathbb{R}^n$, por geometria elementar (planar) vemos que não há um ponto w equidistante de x_i para todo i.

Para provar o Teorema 58, usaremos o seguinte lema que caracteriza configurações esféricas.

Lema 59. *Uma configuração $K = \{x_0, x_1, \ldots, x_k\}$ não é esférica se e só se existem reais $c_1, \ldots, c_k$ não todos nulos tais que*

$$\sum_{1 \leq i \leq k} c_i(x_i - x_0) = 0 \tag{128}$$

e

$$\sum_{1 \leq i \leq k} c_i(\|x_i\|^2 - \|x_0\|^2) = b \neq 0. \tag{129}$$

Demonstração. Suponha que K seja esférico. Digamos que a configuração $K \subset \mathbb{R}^n$ esteja contida na esfera de centro $w \in \mathbb{R}^n$ e raio r. Suponha que existam reais $c_1, \ldots, c_k$ tais que (128) valha. Observe que

$$\|x_i\|^2 - \|x_0\|^2 = \|x_i - w\|^2 - \|x_0 - w\|^2 + 2\langle x_i - x_0, w\rangle = 2\langle x_i - x_0, w\rangle.$$

Assim, temos

$$\begin{aligned}\sum_{1 \leq i \leq k} c_i(\|x_i\|^2 - \|x_0\|^2) &= 2 \sum_{1 \leq i \leq k} c_i\langle x_i - x_0, w\rangle \\ &= 2\Big\langle \sum_{1 \leq i \leq k} c_i(x_i - x_0), w\Big\rangle = 0.\end{aligned}$$

Daí segue que de fato (128) e (129) não podem valer simultaneamente no caso de K ser esférico.

Suponha agora que K não seja esférico. Note que podemos supor que K é minimalmente não-esférico, isto é, todo subconjunto próprio de K é esférico.

Começamos observando que se K é *afim-independente*, isto é, se os vetores $x_i - x_0$ $(1 \leq i \leq k)$ são linearmente independentes, então K é esférico. (Para cada i, considere o hiperplano afim H_i que contém os pontos equidistantes a x_0 e a x_i. Estes hiperplanos se intersectam em pelo menos um ponto, que é equidistante de todos os x_i.)

Como estamos supondo que K não é esférico, podemos deduzir que existem reais $c_1, \ldots, c_k$, não todos nulos, para os quais (128) vale. Suponha que $c_k \neq 0$, e que a esfera que contém $\{x_0, \ldots, x_{k-1}\}$ tem centro w e raio r (lembre que K é minimalmente não-Ramsey). Então

$$\begin{aligned}\sum_{1\le i\le k} & c_i(\|x_i\|^2 - \|x_0\|^2) \\ &= \sum_{1\le i\le k} c_i\left(\|x_i - w\|^2 - \|x_0 - w\|^2\right) - 2\Big\langle \sum_{1\le i\le k} c_i(x_i - x_0), w\Big\rangle \\ &\qquad\qquad\qquad = c_k(\|x_k - w\|^2 - \|x_0 - w\|^2) \neq 0,\end{aligned}$$

e portanto (129) vale. Isto completa a prova do Lema 59. □

O nosso próximo lema é o ingrediente combinatório principal para a prova do Teorema 58.

Lema 60. *Sejam $c_1, \ldots, c_k$ e b números reais, com $b \neq 0$. Então existe um inteiro r e alguma r-coloração de $\mathbb{R}$ tal que toda solução da equação*

$$\sum_{1\le i\le k} c_i(y_i - y_0) = b \tag{130}$$

com $y_i \in \mathbb{R}$ $(1 \le i \le k)$ não é monocromática.

A prova do Lema 60 é delicada, e deixamos para mais adiante. Provemos agora o Teorema 58.

Demonstração do Teorema 58. Seja $K = \{x_0, \ldots, x_k\} \subset \mathbb{R}^n$ uma configuração Ramsey. Precisamos provar que ela é esférica. Suponha por contradição que ela não seja esférica, e considere reais $c_1, \ldots, c_k$, não todos nulos, e $b \neq 0$ satisfazendo (128) e (129) do Lema 59.

Fixe uma r-coloração ψ de $\mathbb{R}$ tal que a equação

$$\sum_{1\le i\le k} c_i(y_i - y_0) = b \tag{131}$$

não tenha nenhuma solução $y_1, \dots, y_k \in \mathbb{R}$ monocromática. Tal coloração existe pelo Lema 60. Definamos uma r-coloração ϕ de $\mathbb{R}^n$, pondo

$$\phi(x) = \psi(\|x\|^2). \tag{132}$$

Afirmamos que esta coloração não cria uma cópia monocromática de K. Como a única restrição que temos sobre n é que ele seja tal que $K \subset \mathbb{R}^n$, esta afirmação completará a prova do Teorema 58.

Para provarmos nossa afirmação, suponha que $K' = \{x'_0, \dots, x'_k\} \subset \mathbb{R}^n$ seja uma cópia monocromática de K na coloração ϕ. Ajuste a notação de forma que a aplicação $\iota\colon x_i \mapsto x'_i$ $(0 \le i \le k)$ se estenda a uma isometria de $\mathbb{R}^n$. Provemos inicialmente que

(**) as identidades (128) e (129) valem para os pontos x'_i $(0 \le i \le k)$ de K'.

Claramente, temos

$$\sum_{1 \le i \le k} c_i(x'_i - x'_0) = 0, \tag{133}$$

isto é, a identidade (128) vale para os x'_i $(0 \le i \le k)$. Por que a identidade (129) vale também para os x'_i $(0 \le i \le k)$? Suponha primeiro que a isometria ι preserve a origem. Então claramente $\|x'_i\|^2 = \|\iota(x_i)\|^2 = \|x_i\|^2$ para todo $0 \le i \le k$, e (129) vale nesse caso. Consideremos agora uma translação por $z \in \mathbb{R}^n$. Temos

$$\begin{aligned}\sum_{1 \le i \le k} c_i(\|x_i + z\|^2 - \|x_0 + z\|^2)& \\ &= \sum_{1 \le i \le k} c_i(\|x_i\|^2 - \|x_0\|^2) + 2\Big\langle z, \sum_{1 \le i \le k} c_i(x_i - x_0)\Big\rangle \\ &= \sum_{1 \le i \le k} c_i(\|x_i\|^2 - \|x_0\|^2) = b \neq 0.\end{aligned}$$

Como a configuração K' pode ser obtida a partir de K através da aplicação de uma isometria preservando a origem, seguida de uma translação, deduzimos que (129) vale também para os x_i' $(0 \leq i \leq k)$. Provamos (**).

Entretanto, o fato de K' ser monocromático de acordo com ϕ implica que se tomamos $y_i = \|x_i'\|^2$ $(0 \leq i \leq k)$, então temos uma solução monocromática de (131) de acordo com ψ. Isto contradiz a escolha de ψ e a nossa afirmação está provada. Isto completa a prova do Teorema 58.

□

4.1. Demonstração do Lema 60. Vamos de fato provar um resultado mais geral.

TEOREMA 61. *Sejam* $\mathbb{K}$ *um corpo de característica* 0 *e* $c_1, \ldots, c_k, b$ *elementos de* $\mathbb{K}$ *com* $b \neq 0$. *Então existe uma* $(2k)^k$*-coloração* ψ *de* $\mathbb{K}$ *tal que a equação*

$$\sum_{1 \leq i \leq k} c_i(y_i - y_i') = b \tag{134}$$

não tem nenhuma solução em $\mathbb{K}$ *com* $\psi(y_i) = \psi(y_i')$ *para todo* $1 \leq i \leq k$.

Claramente, o Teorema 61 implica o Lema 60. Antes de provar o Teorema 61, vamos provar um lema auxiliar.

LEMA 62. *Existe uma* $2k$*-coloração* ϕ *de* $\mathbb{R}$ *tal que a equação*

$$\sum_{1 \leq i \leq k} (x_i - x_i') = 1 \tag{135}$$

não tem nenhuma solução com $\phi(x_i) = \phi(x_i')$ *para todo* $1 \leq i \leq k$.

DEMONSTRAÇÃO. Para definir uma coloração ϕ como no enunciado, consideramos $\mathbb{R}/(2)$, os reais módulo 2. Podemos identificar $\mathbb{R}/(2)$ com o intervalo $[0, 2)$. Seja $r \in \mathbb{R} \mapsto \bar{r} \in \mathbb{R}/(2)$ a projeção canônica. (Concretamente, $\bar{r} = 2\{r/2\}$, onde escrevemos $\{x\}$ para a parte fracionária de x, isto é, $\{x\} = x - \lfloor x \rfloor$.)

Particione o intervalo $[0, 2)$ em $2k$ intervalos da forma $[a, b)$, todos de mesmo comprimento, isto é, com comprimento $1/k$ cada. Sejam I_i $(1 \leq i \leq 2k)$ estes intervalos. Ponha $\phi(r) = i$ onde i é tal que $\bar{r} \in I_i$.

Observe agora que se $\phi(x) = \phi(x')$, então $|x - x'| = 2m + \theta$ para algum inteiro m e algum θ real com $|\theta| < 1/k$. Suponha agora que (135) admite uma solução com $\phi(x_i) = \phi(x_i')$ para todo $1 \leq i \leq k$. Então, para todo i, temos $|x_i - x_i'| = 2m_i + \theta_i$ para um inteiro m_i e um real θ_i com $|\theta_i| < 1/k$. Segue que

$$\sum_{1\leq i\leq k}(x_i - x_i') = 2m + \theta \tag{136}$$

para algum m inteiro e θ satisfazendo $0 \leq |\theta| < 1$. Entretanto, nestas condições, não podemos ter (135), pois (135) e (136) conjuntamente nos dariam que

$$2m + \theta = 1,$$

o que é claramente impossível. O Lema 62 está provado. □

Vamos agora provar o Teorema 61.

Demonstração do Teorema 61. Consideremos $\mathbb{K}$ como um espaço vetorial sobre $\mathbb{Q}$. Fixe uma aplicação linear

$$T\colon \mathbb{K} \to \mathbb{Q}$$

tal que $T(b) = 1$. Fixe também uma $2k$-coloração ϕ de $\mathbb{R}$ como no Lema 62.

No que segue, estaremos apenas interessados nos valores de ϕ nos racionais $\mathbb{Q} \subset \mathbb{R}$ (porque estaremos interessados na imagem de T, que é $\mathbb{Q}$). Por outro lado, o leitor poderá facilmente verificar que, no caso em que $\mathbb{K} = \mathbb{R}$, podemos simplesmente tomar $T(y) = y/b$ ($y \in \mathbb{R}$) e usar que ϕ está definida sobre toda a reta $\mathbb{R}$.

Para cada $r \in \mathbb{K}$, ponha

$$\psi(r) = (\phi(T(c_ir)))_{1\leq i\leq k} = (\phi(T(c_1r)), \ldots, \phi(T(c_kr))) \in [2k]^k. \tag{137}$$

Temos assim uma $(2k)^k$-coloração ψ de $\mathbb{K}$. Suponha que temos uma solução de (134) com

$$\psi(y_i) = \psi(y_i') \text{ para todo } 1 \leq i \leq k. \tag{138}$$

Aplicando T a (134), obtemos

$$\sum_{1\leq i\leq k}(T(c_iy_i)-T(c_iy_i'))=1. \tag{139}$$

Ponha $x_i = T(c_iy_i)$ e $x_i' = T(c_iy_i')$. A condição (138) implica, em particular, que, para todo $1 \leq i \leq k$, a i-ésima coordenada de $\psi(y_i)$, a saber $\phi(T(c_iy_i)) = \phi(x_i)$, coincide com a i-ésima coordenada de $\psi(y_i')$, a saber $\phi(T(c_iy_i')) = \phi(x_i')$. Isto é,

$$\phi(x_i)=\phi(x_i') \text{ para todo } 1\leq i\leq k, \tag{140}$$

o que contradiz a escolha de ϕ. Esta contradição completa a prova do Teorema 61. □

5. Triângulos e polígonos regulares

Discutimos nesta seção alguns resultados mais avançados. Inicialmente, discutiremos como o teorema de Ramsey clássico pode ser usado para provar que certas configurações específicas são Ramsey. Na seção seguinte, provamos o Teorema 56. Na Seção 5.3, discutimos o caso dos polígonos regulares.

5.1. Preliminares. Recordemos o teorema de Ramsey para hipergrafos (veja Teorema 30 da Seção 5.4 do Capítulo 1): *Sejam k, ℓ, e r inteiros positivos com $k \geq \ell$. Então, existe um inteiro positivo $N_0 = N_0(k, \ell, r)$ para o qual vale a seguinte asserção: se $N \geq N_0$, então*

(*) *toda r-coloração dos ℓ-subconjuntos de $[N]$ colore todos os ℓ-subconjuntos de algum k-subconjunto de $[N]$ da mesma cor.*

Lembre que escrevemos

$$N\to(k)^{\ell}_{r}. \tag{141}$$

se a propriedade (*) é verificada.

Como podemos usar o teorema original de Ramsey acima na teoria de Ramsey euclideana? O seguinte exemplo mostra que podemos construir configurações Ramsey de forma muito simples, devido ao Teorema 30.

EXEMPLO 63. Considere $A = (-1, 1, 0)^T$, $B = (-1, 0, 1)^T$, e $C = (0, -1, 1)^T \in \mathbb{R}^3$. O triângulo ABC é isósceles obtuso: os lados de ABC têm comprimento $a = \sqrt{2}$, $b = \sqrt{6}$ e $c = \sqrt{2}$, de forma que $a^2 + c^2 < b^2$. Entretanto, ABC é Ramsey. De fato, podemos aplicar o teorema de Ramsey da seguinte forma para provar esta asserção.

Ponha $K = \{A, B, C\}$ e seja dado um inteiro positivo r. Vamos provar que $R(K, n, r)$ vale se

$$n \to (3)^2_r. \tag{142}$$

Considere todos os vetores $y = (y_i)_{1 \leq i \leq n}$ de $\mathbb{R}^n$ que têm exatamente duas coordenadas não-nulas e que, ademais, são tais que estas duas coordenadas são -1 e 1 'nesta ordem', isto é, se y_i e $y_j \neq 0$ e $i < j$, então $y_i = -1$ e $y_j = 1$ (os demais y_k, $k \notin \{i, j\}$, são todos nulos). Denotaremos por $y(P)$ o vetor y que acabamos de descrever, onde $P = \{i, j\}$.

Seja ϕ uma r-coloração de $\mathbb{R}^n$. Então temos também uma r-coloração dos vetores $y(P)$ acima. Afirmamos que há, dentre estes $y(P)$, uma cópia monocromática de ABC.

Note que a r-coloração dos $y(P)$ ($P \in \binom{[n]}{2}$) induz uma r-coloração dos conjuntos $P \in \binom{[n]}{2}$. Usando (142), podemos supor, sem perda de generalidade, que os pares P contidos em $\{1, 2, 3\}$ são todos da mesma cor. Entretanto, isto significa que os pontos $y(P)$, com $P \in \binom{[3]}{2}$, receberam todos a mesma cor em ϕ. Como estes 3 pontos formam um triângulo congruente a ABC, provamos $R(K, n, r)$.

A técnica que acabamos de ver pode ser incrementada para provar que todos os triângulos obtusos são Ramsey. Vamos provar este resultado na próxima seção.

5.2. Triângulos. O objetivo desta seção é provar o Teorema 56, de Frankl e Rödl [**35**]. Para ilustrarmos a técnica, começamos provando que certos triângulos específicos são Ramsey.

Lema 64. *Seja $t \geq 2$ um inteiro. O triângulo ABC de lados $\sqrt{2t}$, $\sqrt{2t}$ e $\sqrt{8t-6}$ é Ramsey.*

Demonstração. Fixe r um inteiro positivo arbitrário. Seja n tal que $n \to (2t+1)_r^{2t-1}$, ou, em palavras, seja n tal que toda r-coloração dos $(2t-1)$-subconjuntos de $[n]$ necessariamente contém um $(2t+1)$-conjunto monocromático. Vamos provar que a propriedade $R(ABC, n, r)$ vale.

Ponha $x_i = i$ para todo $1 \leq i \leq t$ e $x_i = 2t - i$ para todo $t < i \leq 2t-1$. Para cada $P = \{j_1 < j_2 < \cdots < j_{2t-1}\} \subset [n]$, definimos $y = y(P) = (y_j)_{1 \leq j \leq n} \in \mathbb{R}^n$ colocando $y_{j_i} = x_i$ para todo $1 \leq i \leq 2t-1$ e $y_j = 0$ para todos os demais $j \in [n]$.

Seja ϕ uma r-coloração de $\mathbb{R}^n$. Esta r-coloração induz uma r-coloração dos $y(P)$ ($P \subset [n]$, $|P| = 2t-1$) e, conseqüentemente, uma r-coloração dos $P \subset [n]$ com $|P| = 2t-1$. Pela definição de n, sabemos que existe um $(2t+1)$-subconjunto de $[n]$ que é monocromático nesta coloração. Suponha que este $(2t+1)$-subconjunto seja

$$Q = \{k_1 < \cdots < k_{2t+1}\} \subset [n].$$

Se

$$P_1 = \{k_1 < \cdots < k_{2t-1}\}, \qquad P_2 = \{k_2 < \cdots < k_{2t}\}$$

e

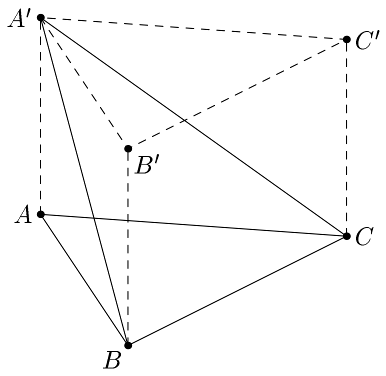
$$P_3 = \{k_3 < \cdots < k_{2t+1}\},$$

então $y(P_1)$, $y(P_2)$ e $y(P_3)$ formam uma cópia monocromática de ABC, e a prova do nosso lema está completa. □

Note que o triângulo ABC do Lema 64 é isósceles e o seu maior ângulo tende a π conforme $t \to \infty$. O Lema 64 e o teorema do produto, Teorema 55, implicam que qualquer triângulo isósceles é Ramsey, como mostra o argumento a seguir.

Seja $A'BC$ um triângulo isósceles com $A'B = A'C$. Vamos considerar uma construção em $\mathbb{R}^3$. Seja H um plano que contém o segmento BC e tal que a projeção ortogonal A de A' em H seja tal que o triângulo ABC seja um triângulo semelhante a um triângulo como do Lema 64. Claramente, $A'BC \subset ABC * AA'$. O Teorema 55 e o Lema 64 implicam que $A'BC$ é Ramsey (veja a Figura 3).

Figura 3 $A'BC \subset ABC * AA'$



A construção acima prova um resultado um pouco mais geral, como segue.

LEMA 65. *Sejam ABC e $A'B'C'$ dois triângulos. Sejam α, β e γ, e α', β' e γ' os ângulos destes triângulos em A, B e C, e em A', B' e C', respectivamente. Suponha que*

$$\alpha' \leq \alpha \qquad e \qquad \frac{\tan\beta}{\tan\gamma} = \frac{\tan\beta'}{\tan\gamma'}. \tag{143}$$

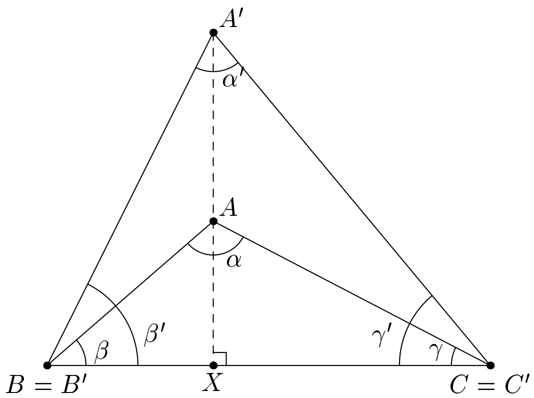
Se ABC é Ramsey, então $A'BC$ é Ramsey.

DEMONSTRAÇÃO. Podemos supor que $BC = B'C'$; de fato, supomos que $B = B'$ e $C = C'$. Ademais, suponha que ABC esteja contido no plano H. Devido à hipótese (143), podemos supor que ABC é obtido pela projeção ortogonal de $A'B'C' = A'BC$ em H (o ponto A é a projeção ortogonal de A' em H). Veja a Figura 4; observe que a razão entre as tangentes em (143) é CX/BX.

Se ABC é Ramsey, então $A'BC = A'B'C' \subset ABC * AA'$ é Ramsey, devido ao Teorema 55. $\square$

Podemos generalizar o Lema 64 da seguinte forma.

Figura 4 Triângulos satisfazendo (143)



Lema 66. *Sejam p e q inteiros positivos e $\varepsilon > 0$ um número real. Então existe um triângulo ABC que é Ramsey e que satisfaz as seguintes propriedades: se β e γ são os ângulos em B e C de ABC, então (i) $\beta + \gamma < \varepsilon$ e (ii) $|\tan\beta/\tan\gamma - p/q| \leq \varepsilon$.*

Demonstração. Seguiremos os mesmos passos da prova do Lema 64, e portanto seremos breves em certas partes do argumento.

Seja r um inteiro positivo. Usaremos os x_i $(1 \leq i \leq 2t-1)$ da prova do Lema 64. Desta vez, escolhemos n tal que

$$n \to (2t + p + q - 1)_r^{2t-1}.$$

Consideremos os pontos $y(P) \in \mathbb{R}^n$ $(P \subset [n],\ |P| = 2t-1)$ como na prova do Lema 64. Suponha dada uma r-coloração de $\mathbb{R}^n$, e considere a r-coloração induzida por esta coloração nos $(2t-1)$-subconjuntos de $[n]$ através dos $y(P)$. Suponha que

$$Q = \{k_1 < \cdots < k_{2t+p+q-1}\}$$

seja um $(2t+p+q-1)$-subconjunto monocromático de $[n]$. Considere

$$P_1 = \{k_1 < \cdots < k_{2t-1}\}, \qquad P_2 = \{k_{p+1} < \cdots < k_{2t+p-1}\},$$

e

$$P_3 = \{k_{p+q+1} < \cdots < k_{2t+p+q-1}\},$$

e ponha $A_i = y(P_i)$ $(i \in \{1,2,3\})$. Seja α_i o ângulo de A_i no triângulo $A_1A_2A_3$. Uma conta um pouco entediante mostra que $\alpha_1 + \alpha_3 \to 0$ e $\tan\alpha_1/\tan\alpha_3 \to p/q$ se fazemos $t \to \infty$. □

Podemos agora provar o Teorema 56. Na demonstração abaixo, escrevemos $T_{p,q,t}$ para o triângulo $A_1A_2A_3$ que ocorre na demonstração do Lema 66. Abaixo, vamos dizer que um triângulo T é *equivalente no sentido do Lema 65 a* $T_{p,q,t}$ se pudermos deduzir que T é Ramsey por aquele lema e pelo fato de $T_{p,q,t}$ ser Ramsey, por valerem as relações (143) entre T e $T_{p,q,t}$.

Demonstração do Teorema 56. Seja ABC um triângulo obtuso. Suponha que α, β e γ sejam os ângulos de ABC em A, B e C. Suponha que $\alpha \geq \beta, \gamma$ (note que $\alpha > \pi/2$).

Consideraremos uma construção em $\mathbb{R}^3$. Seja H o plano que contém ABC. Aplique uma *rotação de* θ em ABC, em torno do eixo AB, e seja C'_θ a imagem de C por esta rotação. Seja C_θ a projeção ortogonal de C'_θ no plano H. Note que C_θ percorre o segmento $CC_{\pi/2}$ ao fazermos θ variar de 0 a $\pi/2$. Este segmento é perpendicular à reta determinada por A e B. Ademais, $C_{\pi/2}$ pertence a esta reta mas não pertence ao segmento AB.

Consideremos o triângulo $ABC_\theta \subset H$. Sejam $\alpha(\theta)$, $\beta(\theta)$ e $\gamma(\theta)$ os ângulos deste triângulo em A, B e C_θ. Veja a Figura 5. É fácil ver que

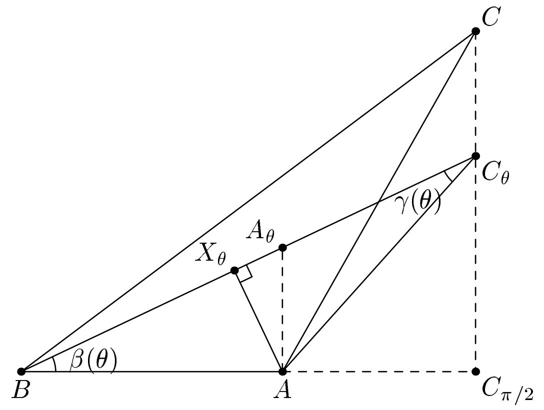
$$\frac{\tan\beta(\theta)}{\tan\gamma(\theta)} = \frac{C_\theta X_\theta}{BX_\theta} > \frac{A_\theta C_\theta}{A_\theta B} = \frac{AC_{\pi/2}}{AB},$$

para todo $0 \leq \theta < \pi/2$ e, ainda,

$$\lim_{\theta\to\pi/2} \frac{\tan\beta(\theta)}{\tan\gamma(\theta)} = \frac{AC_{\pi/2}}{AB}. \tag{144}$$

Seja ϱ o quociente no lado direito de (144) e escolha p e $q \geq 1$ inteiros tais que $\varrho < p/q < \tan\beta(0)/\tan\gamma(0) = \tan\beta/\tan\gamma$. Um argumento de continuidade implica que existe um $\bar\theta$ para o qual vale que $ABC_{\bar\theta}$ é

Figura 5 O argumento para o Teorema 56



equivalente no sentido do Lema 65 a algum $T_{p,q,t}$, e portanto $ABC_{\bar{\theta}}$ é Ramsey.

Note agora que $ABC \subset ABC_{\bar{\theta}} * C_{\bar{\theta}}C'_{\bar{\theta}}$, onde, recordamos, $C'_{\bar{\theta}}$ é a imagem de C pela rotação de ABC em torno do eixo AB pelo ângulo $\bar{\theta}$ e $C_{\bar{\theta}}$ é a projeção ortogonal de $C'_{\bar{\theta}}$ em H. Como $ABC_{\bar{\theta}}$ é Ramsey, segue do Teorema 55 que ABC é Ramsey. Isto completa a prova do Teorema 56. □

COROLÁRIO 67. *Todo triângulo é Ramsey.*

O leitor pode achar interessante o contraste entre o Teorema 57 e o Corolário 67: embora todo triângulo seja Ramsey (Corolário 67), a configuração $K = \{-1, 0, 1\}$, que pode ser considerada como um triângulo degenerado, não é Ramsey (Teorema 57).

5.3. Polígonos regulares. O objetivo desta seção é provar o seguinte resultado, devido a Křížž [**52**].

TEOREMA 68. *Todo polígono regular é Ramsey.*

Na realidade, Křížž provou resultados mais gerais em seu artigo, mas a prova que veremos do Teorema 68 contém várias das idéias usadas em [**52**], além de evitar algumas tecnicalidades necessárias para demonstrar tais resultados mais gerais. Cabe mencionar que o problema de decidir se o pentágono regular é Ramsey ficou aberto por 20 anos.

5.3.1. *Configurações E-Ramsey e o teorema do produto.* Precisamos refinar o conceito de uma configuração ser Ramsey. Para tanto, consideraremos configurações K nas quais temos uma relação de equivalência E definida. Diremos que K é 'E-Ramsey' se, para todo r, toda r-coloração de um $\mathbb{R}^n$ com n suficientemente grande resulta em uma cópia de K em que vértices E-equivalentes sempre têm a mesma cor. Apresentemos esta definição formalmente.

Seja K uma configuração e $E \subset K \times K$ uma relação de equivalência sobre K. Esta relação E particiona K em *classes de equivalência*; denotaremos a coleção destas classes de equivalência por K/E. Vamos escrever $R_E(K, n, r)$ para a seguinte asserção:

(ER) *Em qualquer r-coloração de $\mathbb{R}^n$, existe uma configuração $K' \subset \mathbb{R}^n$ congruente a K com cada uma das classes de equivalência em K'/E monocromática.*

Por exemplo, se K/E é unitário (temos apenas uma classe de equivalência), então a asserção $R_E(K, n, r)$ coincide com a asserção $R(K, n, r)$. Por outro lado, a asserção $R_E(K, n, r)$ vale trivialmente se $|K/E| = |K|$ (isto é, se cada ponto de K forma uma classe de equivalência por si só).

Formalmente, podemos enunciar **(ER)** como segue: para toda r-coloração $\phi\colon \mathbb{R}^n \to [n]$, existe uma isometria $\iota\colon K \hookrightarrow \mathbb{R}^n$ tal que, pondo $K' = \iota(K)$ e $E' = \iota(E) = \{(\iota(x), \iota(y))\colon xEy\}$, temos que $\phi \restriction C$ é constante para toda classe de equivalência $C \in K'/E'$. No enunciado informal acima, identificamos E' com E da forma natural; no que segue, quando temos uma relação E sobre uma configuração K e K' é congruente a K, muitas vezes denotaremos também por E a relação sobre K' naturalmente definida por E e a congruência entre K e K'.

Suponha agora que K seja uma configuração e que E seja uma relação de equivalência sobre K. Dizemos que K é *E-Ramsey* se, para todo inteiro $r \geq 1$, existe $n_0 = n_0(K, E, r)$ tal que se $n \geq n_0$, então $R_E(K, n, r)$ vale.

Sejam A e B configurações dadas, e suponha que E e F são relações de equivalência sobre A e B. Definimos a relação $E \times F$ sobre $A \times B$

colocando

$$(a,b)(E\times F)(a',b')$$

se e só se aEa' e bFb'.

Deixamos para o leitor a prova da seguinte generalização do teorema do produto, Teorema 55.

Teorema 69. *Suponha que temos relações de equivalência E e F sobre configurações A e B. Se A é E-Ramsey e B é F-Ramsey, então $A*B$ é $E\times F$-Ramsey.*

No que segue, teremos uma configuração fixa K e uma relação de equivalência E sobre K. Usaremos então que se K é E-Ramsey, então $K^m = K*\cdots*K$ (m fatores) é E^m-Ramsey, onde $E^m = E*\cdots*E$ (m fatores).

5.3.2. *Demonstração do Teorema 68.* Suponha que K seja o conjunto de vértices de um polígono regular com t lados. Digamos $K = \{x_0,\dots,x_{t-1}\}$, com a notação de tal forma que as arestas de K são x_0x_1, x_1x_2, etc. No que segue, os índices dos x_i são *sempre tomados módulo* t.

Usamos abaixo a isometria $b\colon K\to K$ dada por $b(x_i) = x_{i+1}$ para todo i, que corresponde a uma rotação de $2\pi/t$ em torno do centro de K. Sejam $E_0,\dots,E_{t-1}$ as seguintes relações de equivalência sobre K: em E_n $(0\le n<t)$, as classes de equivalência são

$$\{x_0,\dots,x_n\},\ \{x_{n+1}\},\ \{x_{n+2}\},\ \dots\ ,\{x_{t-1}\}. \tag{145}$$

Vamos provar a seguinte asserção por indução em n:

(‡) *K é E_n-Ramsey.*

Claramente, a prova do Teorema 68 estará completa se provarmos (‡) para $n = t-1$.

Começamos observando que a base de nossa indução é trivial, pois as classes de equivalência relativas a E_0 são todas unitárias. Suponha agora que $1\le n<t$ e que K seja E_{n-1}-Ramsey.

Afirmação 70. *A configuração K é E_n-Ramsey.*

Demonstração. Para provarmos esta afirmação, fixe um inteiro $r \geq 1$. Seja m um inteiro tal que

$$m \to (t)^{t-1}_{r^n}. \tag{146}$$

Como estamos supondo que K é E_{n-1}-Ramsey, o Teorema 69 implica que K^m é E^m_{n-1}-Ramsey.

Sabemos que se N é suficientemente grande, então em toda r-coloração de $\mathbb{R}^N$ temos uma cópia $\widetilde{K}$ de K^m em $\mathbb{R}^N$ tal que cada uma das classes de equivalência em $\widetilde{K}/E^m_{n-1}$ é monocromática. Afirmamos que existe uma cópia K' de $t^{1/2}K$ em $\mathbb{R}^N$ tal que cada uma das classes de equivalência em K'/E_n é monocromática. De fato, vamos encontrar K' dentro de $\widetilde{K}$.

No parágrafo acima, escrevemos $t^{1/2}K$ para a configuração

$$\{t^{1/2}x_i \colon 0 \leq i < t\}.$$

Claramente, se conseguirmos encontrar $K' \subset \widetilde{K}$ como descrito acima, a Afirmação 70 estará provada, pois K' é congruente a $t^{1/2}K$ e este último é semelhante a K.

Suponha que ϕ seja uma r-coloração de $\widetilde{K} \subset \mathbb{R}^N$ tal que

(††) cada uma das classes de equivalência em $\widetilde{K}/E^m_{n-1}$ é monocromática.

No que segue, queremos encontrar $K' \subset \widetilde{K}$ como acima. Por simplicidade, identificamos $\widetilde{K}$ com K^m, de forma que procuramos $K' \subset K^m$ congruente a $t^{1/2}K$ com cada $C \in K'/E_n$ monocromática.

Para cada $P = \{i_1 < \cdots < i_{t-1}\} \in \binom{[m]}{t-1}$, vamos definir n pontos

$$u^{(0)}(P), \ldots, u^{(n-1)}(P)$$

em $\widetilde{K} = K^m$. Para cada $0 \leq j < n$, pomos

$$u^{(j)}(P) = \Big(u^{(j)}_k(P)\Big)_{1 \leq k \leq m} = \Big(u^{(j)}_1(P), \ldots, u^{(j)}_m(P)\Big) \in \widetilde{K} = K^m,$$

onde

$$u_k^{(j)}(P) = \begin{cases} x_j & \text{se } k \notin P \\ b^\alpha(x_j) = x_{j+\alpha} & \text{se } k = i_\alpha \in P \ (1 \leq \alpha < t). \end{cases} \tag{147}$$

A r-coloração ϕ de $\widetilde{K} = K^m$ induz uma r^n-coloração ψ dos $(t-1)$-subconjuntos P de $[m]$ através dos $u^{(j)}(P) \in \widetilde{K} = K^m$ $(0 \leq j < n)$. De fato, colocamos

$$\psi(P) = \big(\phi(u^{(j)}(P))\big)_{0 \leq j < n} = \big(\phi(u^{(0)}(P)), \ldots, \phi(u^{(n-1)}(P))\big) \in [r]^n$$

para todo $P \in \binom{[m]}{t-1}$. Pela escolha de m (veja (146)), existe um t-subconjunto monocromático M de $[m]$ nesta r^n-coloração ψ. Suponha que

$$M = \{k_0 < \cdots < k_{t-1}\}. \tag{148}$$

Considere a aplicação $\iota \colon K \to \widetilde{K} = K^m$ tal que

$$\iota(x) = (y_k)_{1 \leq k \leq m} = (y_1, \ldots, y_m) \in \widetilde{K} = K^m, \tag{149}$$

onde

$$y_k = \begin{cases} x_0 & \text{se } k \notin M \\ b^\alpha(x) & \text{se } k = k_\alpha \in M \ (0 \leq \alpha < t). \end{cases} \tag{150}$$

Pomos

$$K' = \iota(K) \subset \widetilde{K} = K^m, \tag{151}$$

e afirmamos que

$$K' \text{ é congruente a } t^{1/2} K \tag{152}$$

e

(153)

ϕ é constante em cada uma das classes de equivalência em K'/E_n.

Note que as asserções (152) e (153) completam a prova da Afirmativa 70.

A asserção (152) é fácil ver: de fato, basta observar que a aplicação $\iota\colon K \to \widetilde{K} = K^m$ aumenta distâncias por um fator de $t^{1/2}$, pois b é uma isometria. Ponha agora

$$x'_j = \iota(x_j) \in \widetilde{K} = K^m \qquad (0 \le j < t).$$

Para provar (153), precisamos simplesmente provar que

$$\phi(x'_0) = \cdots = \phi(x'_n).$$

Provemos que

$$\phi(x'_{i-1}) = \phi(x'_i) \text{ para todo } 1 \le i \le n. \tag{154}$$

Seja x''_{i-1} o vetor em K^m que coincide com x'_{i-1} nas coordenadas em M, e que, em todas as coordenadas fora de M, é constante e igual a x_{i-1}. Note também que $x'_{i-1} = \iota(x_{i-1})$ é constante e igual x_0 fora de M (veja (149) e (150)). Como $x_0 E_{n-1} x_{i-1}$, pois $i \le n$, temos $x'_{i-1} E^m_{n-1} x''_{i-1}$. Devido à hipótese (††) sobre ϕ, temos que

$$\phi(x'_{i-1}) = \phi(x''_{i-1}). \tag{155}$$

Lembre agora que $k_0 = \min M$ e $k_{t-1} = \max M$ (veja (148)). Observe agora que, na verdade, temos $u^{(i-1)}(M \setminus \{k_0\}) = x''_{i-1}$. Ademais,

$$\phi(u^{(i-1)}(M \setminus \{k_0\})) = \phi(u^{(i-1)}(M \setminus \{k_{t-1}\})), \tag{156}$$

pois M é monocromático em relação à coloração ψ. Note agora que $x'_i = \iota(x_i) \in K^m$ coincide com $u^{(i-1)}(M \setminus \{k_{t-1}\})$ nas coordenadas em M, e que, em todas as coordenadas fora de M, este vetor é constante e igual a x_0. Como $x_0 E_{n-1} x_{i-1}$, pois $i \le n$, temos $u^{(i-1)}(M \setminus \{k_{t-1}\}) E^m_{n-1} x'_i$. Devido à hipótese (††) sobre ϕ, temos que

$$\phi(u^{(i-1)}(M \setminus \{k_{t-1}\})) = \phi(x'_i). \tag{157}$$

Assim, concluímos de (155)–(157) que (154) vale.

Isto completa a prova de (153) e portanto a Afirmação 70 está provada. □

A Afirmação 70 completa o passo de indução de nossa prova indutiva de (‡). Como já mencionado anteriormente, isto prova o Teorema 68.

6. Alguns resultados mais avançados

Discutimos nesta breve seção alguns resultados mais avançados.

6.1. Resultados envolvendo a teoria dos grupos. Como mencionado anteriormente, Kříž [**52**] deduziu que polígonos regulares são Ramsey a partir de um resultado mais geral. Nesta seção, enunciamos dois resultados de [**52**], sem prova.

Seja K uma configuração, e suponha que G seja um grupo de isometrias de K. Escrevemos E_G para a relação de equivalência sobre K em que xE_Gy se e só se $g(x) = y$. Claramente, as classes de equivalência desta relação são as *órbitas da ação de G em K*: dado $x \in K$, a sua *órbita* por G é

$$\mathrm{Orb}_G(x) = \{y\colon \text{ existe } g \in G \text{ tal que } g(x) = y\}.$$

A órbita de x coincide com a classe de equivalência de x na relação E_G.

Teorema 71. *Suponha que K seja uma configuração e que G seja um grupo de isometrias de K. Se G é solúvel, então K é E_G-Ramsey.*

Claramente, no caso de um polígono regular de t lados, podemos tomar como G o grupo cíclico de ordem t.

Abaixo, dizemos que uma configuração K é *transitiva* se para todo x e $y \in K$ existe uma isometria g de K tal que $g(x) = y$. Equivalentemente, a configuração K é transitiva se existe uma única órbita na ação do grupo de isometrias de K.

Teorema 72. *Seja K uma configuração transitiva. Se K admite um grupo solúvel de isometrias com no máximo duas órbitas, então K é Ramsey.*

Kříž observa que com o teorema do produto (Teorema 55) e o Teorema 72, podemos deduzir que todos os cinco sólidos platônicos são Ramsey (exercício!).

6.2. Configurações super-Ramsey. Já observamos a relação óbvia entre a propriedade da configuração $K = \{0, 1\}$ ser Ramsey e o fato do número cromático do $\mathbb{R}^n$ tender a infinito conforme $n \to \infty$. No Capítulo 2, provamos que o número cromático do $\mathbb{R}^n$ é exponencial em n, e portanto podemos deduzir que existem constantes c_1, $c_2 > 0$ para os quais $R(\{0, 1\}, n, r)$ vale se $r < 2^{c_1 n}$ e $R(\{0, 1\}, n, r)$ não vale se $r > 2^{c_2 n}$. A grosso modo, o 'limiar' para o número de cores r para a validade da propriedade $R(\{0, 1\}, n, r)$ é exponencial em n.

Surpreendentemente, não é apenas no caso de configurações simples como $K = \{0, 1\}$ que este limiar é exponencial. Na realidade, para toda configuração K que hoje sabemos ser Ramsey, este limiar é exponencial. De fato, toda configuração Ramsey que conhecemos hoje é também o que chamamos 'super-Ramsey'.

Seja K uma configuração. Dizemos que K é *super-Ramsey* se existem constantes $C > 1$, $\varepsilon > 0$, e $n_0 = n_0(K)$ tais que, para todo $n \geq n_0$, existe uma configuração $X = X_n \subset \mathbb{R}^n$ tal que

(*i*) $|X| \leq C^n$,

(*ii*) se $Y \subset X$ não contém uma cópia de K, então

$$|Y| < |X|/(1 + \varepsilon)^n.$$

Note que, em particular, se K é super-Ramsey com constantes C e ε como acima, então a asserção $R(K, n, r)$ vale para todo $r \leq (1 + \varepsilon)^n$, desde que n seja suficientemente grande.

Frankl e Rödl provaram o seguinte resultado [**33**].

LEMA 73. *Todo tijolo é super-Ramsey.*

O resultado acima é apenas o lema inicial da prova de que todo simplexo não-degenerado é super-Ramsey, um resultado de Frankl e Rödl [**33**], publicado no *Journal of American Mathematical Society.*

Teorema 74. *Suponha que K seja uma coleção de $d+1$ pontos afim-independentes em $\mathbb{R}^d$. Então K é super-Ramsey.*

A demonstração do Teorema 74 envolve argumentos sofisticados da teoria extremal dos conjuntos e geometria.

Observações finais. Existem ainda dois conceitos relacionados à propriedade de ser Ramsey. Uma configuração K pode ser o que se chama 'esfera-Ramsey' e, ainda, 'hiper-Ramsey'.

Seja K uma configuração finita. Seja $S^n(\varrho) \subset \mathbb{R}^{n+1}$ a esfera de raio ϱ em $\mathbb{R}^{n+1}$ e centro 0. Vamos escrever $S(K, \varrho, n, r)$ para a seguinte asserção:

- **(S)** *Em qualquer r-coloração de $S^n(\varrho)$, existe uma configuração $K' \subset S^n(\varrho)$ congruente a K cujos pontos recebem todos a mesma cor.*

Dizemos que uma configuração K é *esfera-Ramsey* se, para todo r, existe um real ϱ e um inteiro n para o qual a asserção $S(K, \varrho, n, r)$ é verdadeira. Uma configuração K é *hiper-Ramsey* se ela admitir configurações esféricas $X \subset S^n(\varrho)$ satisfazendo (i) e (ii) da definição de configurações super-Ramsey e, ademais, podemos escolher ϱ arbitrariamente próximo do 'circunraio' ϱ_0 de K, isto é, o raio da menor esfera contendo K (estamos sendo deliberadamente concisos nesta definição).

Graham [**38**] provou que tijolos são esfera-Ramsey. Matoušek e Rödl [**59**] provaram que simplexos não-degenerados são esfera-Ramsey. A prova deste último resultado depende de certos argumentos que foram primeiro usados na teoria de espaços de Banach. Finalmente, Frankl e Rödl [**31**] provaram que simplexos não-degenerados são hiper-Ramsey.

7. Problemas em aberto

Há vários problemas em aberto nesta área. O mais importante é a seguinte conjectura de Graham, que oferece 1.000 dólares pela sua resolução (veja, por exemplo, [**39**]).

Conjectura 75. *Todo conjunto esférico é Ramsey.*

O primeiro caso ainda em aberto da Conjectura 75 é aquele em que temos uma configuração genérica de 4 pontos em um círculo. Sabe-se que se os 4 pontos no círculo determinam um trapézio (dois de seus lados são paralelos), então eles formam uma configuração Ramsey. Este resultado, que generaliza o Corolário 67, é devido a Kříž [**53**].

No outro extremo do espectro, temos problemas bastante específicos que ainda estão em aberto, como o seguinte problema de 1979 de Erdős [**28**].

PROBLEMA 76. *Seja T um triângulo não equilátero. Vale então a propriedade $R(T,2,2)$?*

O caso do triângulo equilátero precisa ser excluído. Considere a coloração do plano com duas cores, em que (x,y) é colorido da cor $\lfloor 2x/\sqrt{3}\rfloor \bmod 2$. Um argumento geométrico simples mostra que, nesta coloração, não há um triângulo equilátero de lado 1 monocromático.

Um problema mais modesto que o Problema 76, sugerido por Rödl, é o seguinte: é verdade que existe uma constante absoluta n_0 para o qual todo triângulo T é tal que $R(T,n_0,2)$ vale? Para apreciar este problema ainda mais, o leitor deve recordar o contraste já observado entre o Teorema 57 (o 'triângulo degenerado' $K=\{-1,0,1\}$ não é Ramsey) e o Corolário 67 (todo triângulo é Ramsey).

CAPÍTULO 4

Coberturas e empacotamentos em hipergrafos

1. Introdução

Um *hipergrafo* é uma família de subconjuntos finitos de um conjunto dado, todos com o mesmo número de elementos, isto é, dado um conjunto A e um inteiro positivo r, um hipergrafo (ou r-hipergrafo) sobre A é um subconjunto H de $\binom{A}{r}$ (usualmente o que se chama de hipergrafo é o par (A, H), $H \subset \binom{A}{r}$, mas neste capítulo será conveniente identificar hipergrafos e famílias de subconjuntos). Costumamos chamar os elementos de H de *hiperarestas* de H.

Dado um hipergrafo H sobre um conjunto finito A, e um elemento $x \in A$, definimos o *grau de x em H* $\mathrm{gr}_H(x) = |\{C \in H \mid x \in C\}|$. Um hipergrafo H é dito regular se $\mathrm{gr}_H(x)$ não depende de x, isto é, se existe b tal que $\mathrm{gr}_H(x) = b$ para todo $x \in A$. Nesse caso, dizemos que H é b-regular. Dados dois elementos $x, y \in H$, definimos $\mathrm{gr}_H(x, y) = |\{C \in H \mid \{x, y\} \subset C\}|$.

Neste capítulo estaremos interessados em dois parâmetros extremais associados a hipergrafos, relativos a *coberturas* e *empacotamentos* optimais em H. Definimos $\alpha(A, H) = \min\{k \in \mathbb{N} \mid \exists\, C_1, C_2, \ldots, C_k \in H$ tais que $A = \bigcup_{j=1}^{k} C_j\}$ (o tamanho mínimo de uma cobertura de A por elementos de H), e $\beta(A, H) = \max\{k \in \mathbb{N} \mid \exists\, C_1, C_2, \ldots, C_k \in H$ com $C_i \cap C_j = \emptyset, \forall\, i \neq j\}$ (o tamanho máximo de um empacotamento em H). Estaremos particularmente interessados em estimar esses parâmetros no caso de hipergrafos regulares.

Se $|A| = n$ e $H \subset \binom{A}{r}$ é um hipergrafo sobre A, é fácil ver que $\beta(A, H) \leq \frac{n}{r} \leq \alpha(A, H)$. Por outro lado, se $\alpha(A, H)$ estiver próximo de $\frac{n}{r}$ então $\beta(A, H)$ também estará. Mais precisamente, se $\alpha(A, H) < \frac{n}{r}(1 + \tau)$ então $\beta(A, H) > \frac{n}{r}(1 - \tau r)$. De fato, se $m < \frac{n}{r}(1 + \tau)$, e

$C_1, C_2, \ldots, C_m \in H$ são tais que $A = \bigcup_{j=1}^{m} C_j$, se definimos, para cada $x \in A$, $d(x) = |\{1 \le j \le m \mid x \in C_j\}|$, teremos $\sum_{x\in A} d(x) = \sum_{x\in A}\sum_{j=1}^{m} \chi_{C_j}(x) = \sum_{j=1}^{m}\sum_{x\in A} \chi_{C_j}(x) = rm < n(1+\tau)$. Assim, se para cada $x \in A$ retiramos $d(x)-1$ elementos de $\{C_1, C_2, \ldots, C_m\}$ que contêm x, retiramos no máximo $\sum_{x\in A}(d(x)-1) = rm - n < n\tau$ elementos de $\{C_1, \ldots, C_m\}$, obtendo assim um empacotamento com mais de $m - n\tau \ge \frac{n}{r} - n\tau = \frac{n}{r}(1 - r\tau)$ elementos. Este fato será importante na próxima seção.

Em geral pouco pode ser dito sobre estimativas gerais de $\beta(A, H)$ e $\alpha(A, H)$ (por exemplo, se dois elementos de H sempre se intersectam, $\beta(A, H) = 1$, e se a união dos elementos de H não é igual a A, $\alpha(A, H)$ não está definido). Entretanto, para hipergrafos regulares (ou "quase" regulares) vamos mostrar resultados gerais sobre estimativas desses parâmetros extremais (por exemplo, $\alpha(A, H) < \frac{n}{r}(\log r + 1)$ e $\beta(A, H) \ge n/r^2$ para todo r-hipergrafo regular H sobre um conjunto A de n elementos). Mostraremos também que essas estimativas não podem ser assintoticamente melhoradas sem hipóteses adicionais (veja a Seção 3).

Um marco do assim chamado *método probabilístico* foi a demonstração devida a Rödl [**64**] de uma conjectura de Erdős e Hanani [**24**] de 1963, sobre empacotamento e coberturas, que ficou em aberto por 22 anos. De fato, Rödl mostrou que, em certas condições, $\alpha(A, H)$ e $\beta(A, H)$ são assintoticamente iguais a n/r. O método de Rödl pode ser visto como o resultado de um refinamento de algumas idéias já presentes em um trabalho de Ajtai, Komlós, e Szemerédi [**2**], onde esses autores lidam com um certo problema da teoria dos grafos com o objetivo de atacar um problema da teoria combinatória dos números. Uma versão 'abstrata' do método de Rödl foi desenvolvida por Frankl e Rödl [**32**]; veremos neste capítulo a versão de Pippenger (veja, por exemplo, [**37**]).

O método de Rödl, às vezes chamado de *Rödl nibble* ou o método *semi-aleatório*, mostrou-se capaz de lidar com uma grande gama de problemas e é hoje uma das ferramentas probabilísticas indispensáveis da combinatória contemporânea.

Descrevemos agora a conjectura de Erdős e Hanani (a prova desta conjectura será apresentada na Seção 2). Dados $n \geq k \geq t \geq 1$ inteiros, dizemos que um k-hipergrafo $H \subset \binom{[n]}{k}$ sobre $[n] = \{1, 2, \ldots, n\}$ é um (n, k, t)-empacotamento se $|C \cap C'| < t$, $\forall\, C, C' \in H$, $C \neq C'$. Definimos $P(n, k, t)$ como a maior cardinalidade possível de um (n, k, t)-empacotamento. Um tal hipergrafo H é dito uma (n, k, t)-cobertura se para todo $B \subset \binom{[n]}{t}$ existe $C \in H$ tal que $B \subset C$. Definimos $C(n, k, t)$ como a menor cardinalidade de uma (n, k, t)-cobertura. É fácil ver que $P(n, k, t) \leq \binom{n}{t}/\binom{k}{t} \leq C(n, k, t)$. A conjectura de Erdős e Hanani diz que, para k e t fixos, $\lim_{n\to\infty} P(n, k, t)\binom{k}{t}/\binom{n}{t} = \lim_{n\to\infty} C(n, k, t)\binom{k}{t}/\binom{n}{t} = 1$. Assim, num jogo como a loto ou a sena, com n números, cujo objetivo é acertar os t números que são sorteados (no caso da loto, $n = 100$ e $t = 5$, e, no caso da sena, $n = 50$ e $t = 6$), se k e t estão fixos e n é grande, então o número mínimo de cartões de k números que devemos jogar para garantir que acertaremos os t números sorteados é $(1 + o(1))\binom{n}{t}/\binom{k}{t}$.

2. O teorema de Rödl

Vamos mostrar a seguir a versão de Pippenger do teorema de Rödl:

Teorema 77. *Dados $r \geq 2$ inteiros e K, $\varepsilon > 0$ reais, existe $\delta > 0$ para o qual vale o seguinte. Suponha que H é um r-hipergrafo sobre um conjunto F com $|F| = n$ e existe d satisfazendo as seguintes condições:*

(i) $\mathrm{gr}_H(x) < Kd$ *para todo* $x \in F$*,*
(ii) $(1-\delta)d < \mathrm{gr}_H(x) < (1+\delta)d$ *para pelo menos* $(1-\delta)n$ *elementos* $x \in F$*,*
(iii) $\mathrm{gr}_H(x, y) < \delta d$ *para todo* $x \neq y$*.*

Então $\alpha(F, H) < (1 + \varepsilon)\frac{n}{r}$ *e* $\beta(F, H) > (1 - \varepsilon)\frac{n}{r}$.

Antes de provar o teorema, vamos ver como ele implica a conjectura de Erdős e Hanani, enunciada na introdução deste capítulo:

Dados $n \geq k \geq t \geq 1$, construímos um $\binom{k}{t}$-hipergrafo sobre $\binom{[n]}{t}$, $H(n, k, t) = \{\binom{B}{t},\ B \in \binom{[n]}{k}\}$. Como cada subconjunto de t elementos de $[n]$ está contido em $\binom{n-t}{k-t}$ subconjuntos de k-elementos de $[n]$, temos

$\mathrm{gr}_{H(n,k,t)}(X) = \binom{n-t}{k-t}$, para todo $X \in \binom{[n]}{t}$. Por outro lado, dados $X, Y \in \binom{[n]}{t}$, $X \neq Y$, temos $s = |X \cup Y| \geq t+1$, donde $\mathrm{gr}_{H(n,k,t)}(X,Y) = \binom{n-s}{k-s} \leq \binom{n-t-1}{k-t-1}$. Fixados k e t, temos

$$\lim_{n\to\infty} \binom{n-t-1}{k-t-1} \Big/ \binom{n-t}{k-t} = \lim_{n\to\infty} \frac{k-t}{n-t} = 0.$$

Portanto, dado $\delta > 0$, se k e t são fixos e n é suficientemente grande, as condições do teorema são verificadas, com $d = \binom{n-t}{k-t}$. Isso mostra que

$$\lim_{n\to\infty} \frac{\binom{k}{t}}{\binom{n}{t}} \alpha\left(\binom{[n]}{t}, H(n,k,t)\right) = \lim_{n\to\infty} \frac{\binom{k}{t}}{\binom{n}{t}} \beta\left(\binom{[n]}{t}, H(n,k,t)\right) = 1.$$

Por outro lado, é fácil ver que

$$\alpha\left(\binom{[n]}{t}, H(n,k,t)\right) = C(n,k,t),$$

e

$$\beta\left(\binom{[n]}{t}, H(n,k,t)\right) = P(n,k,t),$$

o que encerra a prova.

A prova do Teorema 77 utiliza o método probabilístico de maneira fundamental. As condições (i), (ii) e (iii) do enunciado são condições de regularidade fraca, ou melhor, de regularidade com tolerância δ. O seguinte lema mostra que, se escolhermos aleatoriamente um subconjunto pequeno de hiperarestas de um hipergrafo fracamente regular com tolerância pequena e retirarmos os vértices cobertos por essas hiperarestas, obtemos, com alta probabilidade, um hipergrafo fracamente regular com tolerância ainda pequena, e permite estimar os parâmetros desse novo hipergrafo.

Lema 78. *Sejam dados r, α, e $K > 0$. Dado $\delta' > 0$ existem $\delta = \delta(r, \delta', \alpha, K)$, $n_0 = n_0(r, \delta', \alpha, K)$ e $d_0 = d_0(r, \delta', \alpha, K) > 0$ para os quais vale o seguinte. Suponha que H é um r-hipergrafo sobre F, $|F| = n > n_0$, e existe $d > d_0$ satisfazendo as seguintes condições:*

(i) $\mathrm{gr}_H(x) < Kd$ *para todo* $x \in F$,

(ii) $(1-\delta)d < \mathrm{gr}_H(x) < (1+\delta)d$ *para pelo menos* $(1-\delta)n$ *elementos* $x \in F$,

(iii) $\mathrm{gr}_H(x,y) < \delta d$ *para todo* $x \neq y$.

Então existe $X \subset H$ *tal que, se* $F' = F \setminus \left(\bigcup_{A\in X} A\right)$ *e* $H' = \{A \in H \mid A \subset F'\}$, *temos:*

(a) $(1-\delta')\alpha \cdot \frac{n}{r} < |X| < (1+\delta')\alpha \cdot \frac{n}{r}$

(b) $(1-\delta')e^{-\alpha}n < |F'| < (1+\delta')e^{-\alpha}n$

(c) $(1-\delta')e^{-\alpha(r-1)}d < \mathrm{gr}_{H'}(x) < (1+\delta')e^{-\alpha(r-1)}d$ *para pelo menos* $(1-\delta')|F'|$ *elementos* $x \in F'$.

Antes de provar o lema, vamos ver como ele implica o Teorema 77:

Prova do Teorema 77. Seja $\alpha \in (0,1)$ tal que $\frac{\alpha\cdot e^{\alpha^2}}{1-e^{\alpha^2-\alpha}} < 1 + \frac{\varepsilon}{2r}$ (todo α suficientemente pequeno satisfaz isso, pois $\lim_{\alpha\to 0} \frac{\alpha\, e^{\alpha^2}}{1-e^{\alpha^2-\alpha}} = 1$), e seja k um inteiro positivo tal que $e^{k(\alpha^2-\alpha)} < \frac{\varepsilon}{2r^2}$. Definimos $\delta_0 = 1-e^{-\alpha^2} < e^{\alpha^2}-1$ e, para $1 \le j \le k$, $\delta_j = \min\{1-e^{-\alpha^2}, \delta'(r,\delta_{j-1},\alpha,\widetilde{K})\}$, onde $\widetilde{K} = Ke^{k\alpha(r-1)}$. Afirmamos que, se n e d são suficientemente grandes (o que é automático se δ é suficientemente pequeno) e $\delta = \delta_k$ então valem as conclusões do teorema.

De fato, aplicando k vezes o Lema 78, obtemos conjuntos $X_1,\dots,X_k$ de arestas de H e subconjuntos $F_0, F_1, F_2, \dots, F_k$ de F com $F_0 = F$, $e^{-\alpha-\alpha^2}|F_j| < |F_{j+1}| < e^{\alpha^2-\alpha}|F_j|$, para $0 \le j \le k-1$ (donde $e^{j(-\alpha-\alpha^2)}n < |F_j| < e^{j(\alpha^2-\alpha)}n$, para todo $j \le k$) e $|X_{j+1}| < e^{\alpha^2}\cdot\alpha\cdot\frac{|F_j|}{r} < e^{\alpha^2}\cdot\frac{\alpha}{r}\cdot e^{j(\alpha^2-\alpha)}n$, para todo $j \le k-1$ tais que $F_{j+1} = F_j \setminus (\bigcup_{A\in X_j} A)$, $0 \le j \le k-1$.

Temos então $|F_k| < e^{k(\alpha^2-\alpha)}n < \frac{\varepsilon}{2r^2}\cdot n$, donde podemos, usando uma hiperaresta de H para cada elemento de F_k, cobrir F_k com no máximo $\frac{\varepsilon}{2r^2}\cdot n$ hiperarestas. Por outro lado, $\bigcup_{j=1}^k X_j$ cobre $F\setminus F_k$, e $|\bigcup_{j=1}^k X_j| < e^{\alpha^2}\cdot\frac{\alpha}{r}\cdot n\sum_{j=0}^{k-1} e^{j(\alpha^2-\alpha)} < \frac{n}{r}\cdot\frac{\alpha e^{\alpha^2}}{1-e^{\alpha^2-\alpha}} < \frac{n}{r}(1+\frac{\varepsilon}{2r})$, donde podemos cobrir F com menos de $\frac{n}{r}(1+\frac{\varepsilon}{2r}) + \frac{\varepsilon}{2r^2}\cdot n = \frac{n}{r}(1+\frac{\varepsilon}{r})$ hiperarestas de H, ou seja, $\alpha(F,H) < (1+\frac{\varepsilon}{r})\frac{n}{r} < (1+\varepsilon)\frac{n}{r}$. Por outro lado, como vimos após a definição de $\beta(F,H)$, $\alpha(F,H) < \frac{n}{r}(1+\frac{\varepsilon}{r})$ implica $\beta(F,H) > \frac{n}{r}(1-r\cdot\frac{\varepsilon}{r}) = (1-\varepsilon)\frac{n}{r}$. □

Antes de provarmos o Lema 78, vamos recordar algumas noções de probabilidade em conjuntos finitos. Dado um conjunto finito Ω, uma *probabilidade* em Ω pode ser vista como uma função $\mathbb{P}\colon \Omega \to [0,1]$ tal que $\sum_{x\in\Omega} \mathbb{P}(x) = 1$. Dado $A \subset \Omega$, definimos $\mathbb{P}(A) = \sum_{x\in A} \mathbb{P}(x)$. Dois eventos $A, B \subset \Omega$ são ditos *independentes* se $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$. Uma variável aleatória em Ω é uma função $\xi\colon \Omega \to \mathbb{R}$. Definimos o *valor esperado* de ξ por $\mathbb{E}(\xi) = \sum_{x\in\Omega} \mathbb{P}(x)\xi(x)$, a *variância* de ξ por $V(\xi) = \sum_{x\in\Omega} \mathbb{P}(x)(\xi(x) - \mathbb{E}(\xi))^2$, e *desvio padrão* de ξ por $D(\xi) = \sqrt{V(\xi)}$.

Uma ferramenta importante para a prova do lema é a desigualdade de Chebyshev:

$$\mathbb{P}(|\xi - \mathbb{E}(\xi)| > \lambda D(\xi)) \leq \frac{1}{\lambda^2}, \qquad \text{para todo} \qquad \lambda > 0.$$

De fato, se

$$A = \{x \in \Omega \mid |\xi(x) - \mathbb{E}(\xi)| > \lambda D(\xi)\},$$

então

$$\begin{aligned} V(\xi) = \mathbb{E}(\xi)^2 = \sum_{x\in\Omega} \mathbb{P}(x)(\xi(x) - \mathbb{E}(\xi))^2 &\geq \sum_{x\in A} \mathbb{P}(x)(\xi(x) - \mathbb{E}(\xi))^2 \\ &\geq (\lambda D(\xi))^2 \sum_{x\in A} \mathbb{P}(x) = \lambda^2 V(\xi)\mathbb{P}(A), \end{aligned}$$

donde $\mathbb{P}(A) \leq \frac{1}{\lambda^2}$.

Em particular, se $D(\xi) = o(|\mathbb{E}(\xi)|)$, tomando $\lambda = \sqrt{|\mathbb{E}(\xi)|/D(\xi)}$, a desigualdade de Chebyshev mostra que $\mathbb{P}(\xi(x) = (1 + o(1))\mathbb{E}(\xi))$ é $1 - o(1)$.

Prova do Lema 78. Vamos mostrar que se δ é suficientemente pequeno (isto é, se $\delta = o(1)$) e d e n são suficientemente grandes então vale o resultado. Para isso escolheremos aleatoriamente o conjunto $X \subset H$ de hiperarestas a serem retiradas: para cada $C \in H$, a probabilidade de termos $C \in X$ será sempre igual a $p = \alpha/d$, sendo esses eventos mutuamente independentes (a rigor nosso espaço amostral será $\Omega = \mathcal{P}(H)$, e, para cada $X \subset H$, teremos $\mathbb{P}(X) = p^{|X|}(1-p)^{|H|-|X|}$).

Temos

$$|H| = \frac{1}{r}\sum_{x\in F} \mathrm{gr}_H(x) = \frac{1}{r}(n(1-o(1))d(1+o(1))+Kd\cdot o(n)) = \frac{nd}{r}(1+o(1)).$$

O valor esperado de $|X|$ é $p|H| = \frac{\alpha n}{r}(1+o(1))$. Por outro lado, a variância de $|X|$ é $p(1-p)|H|$. De fato, definindo

$$f(x) = \sum_{s=0}^{m} \binom{m}{s} x^s (1-p)^{m-s} = (x+1-p)^m,$$

temos

$$f'(x) = \sum_{s=0}^{m} s\binom{m}{s} x^{s-1}(1-p)^{m-s} = m(x+1-p)^{m-1},$$

e

$$f''(x) = \sum_{s=0}^{m} s(s-1)\binom{m}{s} x^{s-2}(1-p)^{m-s} = m(m-1)(x+1-p)^{m-2},$$

e portanto, se $m = |H|$,

$$\mathbb{E}(|X|) = \sum_{s=0}^{m} s\binom{m}{s} p^s(1-p)^{m-s} = pf'(p) = pm = p|H|,$$

e

$$\begin{aligned} V(|X|) = \mathbb{E}(|X|^2) - \mathbb{E}(|X|)^2 &= \left(\sum_{s=0}^{m} s^2\binom{m}{s} p^s(1-p)^{m-s}\right) - (p|H|)^2 \\ &= (p^2 f''(p) + pf'(p)) - (p|H|)^2 = p^2 m(m-1) + pm - p^2m^2 \\ &= p(1-p)m = p(1-p)|H|. \end{aligned}$$

Assim,

$$V(|X|) = p(1-p)|H| < p|H| = \mathbb{E}(|X|),$$

donde

$$D(|X|) = \sqrt{V(|X|)} = o(\mathbb{E}(|X|)),$$

e, pela desigualdade de Chebyshev, com probabilidade $1 - o(1)$ teremos $|X| = (1 + o(1))\mathbb{E}(|X|) = (1 + o(1))\frac{\alpha n}{r}$, o que implica a condição (a), se n é suficientemente grande.

Vamos agora mostrar que a condicão (b) vale com probabilidade $1 - o(1)$. Para isso, para cada $x \in F$, consideramos a variável aleatória ξ_x definida por

$$\xi_x = \begin{cases} 1 \text{ se } x \notin \bigcup_{C \in X} C \\ 0 \text{ caso contrário.} \end{cases}$$

Seja $\xi = \sum_{x \in F} \xi_x$. Note que $\xi = |F \setminus \bigcup_{C \in X} C| = |F'|$. Temos $\mathbb{E}(\xi_x) = \mathbb{P}(x \in C \in H \Rightarrow C \notin X) = (1-p)^{\mathrm{gr}_H(x)}$. Assim, se

$$\mathrm{gr}_H(x) = (1 + o(1))d, \quad \mathbb{E}(\xi_x) = \Big(1 - \frac{\alpha}{d}\Big)^{d(1+o(1))} = e^{-\alpha} + o(1)$$

(isso acontece para $(1 - o(1))n$ elementos x de F). Como sempre temos $0 \leq \mathbb{E}(\xi_x) \leq 1$,

$$\begin{aligned}\mathbb{E}(|F'|) = \mathbb{E}(\xi) &= \sum_{x \in F} \mathbb{E}(\xi_x) = (1 - o(1))n(e^{-\alpha} + o(1)) + o(n) \\ &= ne^{-\alpha} + o(n) = ne^{-\alpha}(1 + o(1)).\end{aligned}$$

Vamos agora estimar

$$\begin{aligned} V(|F'|) = V(\xi) &= \mathbb{E}((\xi - \mathbb{E}(\xi))^2) = \mathbb{E}((\sum_{x \in F}(\xi_x - \mathbb{E}(\xi_x)))^2) \\ &= \sum_{x \in F} \mathbb{E}((\xi_x - \mathbb{E}(\xi_x))^2) + \sum_{\substack{x,y \in F \\ x \neq y}} \mathbb{E}((x_x - \mathbb{E}(\xi_x))(\xi_y - \mathbb{E}(\xi_y)) \\ &= \sum_{x \in F} \mathbb{E}((\xi_x - \mathbb{E}(\xi_x))^2) + \sum_{\substack{x,y \in F \\ x \neq y}} (\mathbb{E}(\xi_x \xi_y) - \mathbb{E}(\xi_x)\mathbb{E}(\xi_y)). \end{aligned}$$

Por outro lado,

$$\mathbb{E}((\xi_x - \mathbb{E}(\xi_x))^2) = \mathbb{E}(\xi_x^2) - \mathbb{E}(\xi_x)^2 \leq \mathbb{E}(\xi_x^2) = \mathbb{E}(\xi_x)$$

(pois $\xi_x^2 = \xi_x$), e, se $x, y \in F$, $x \neq y$, $\mathbb{E}(\xi_x\xi_y) = \mathbb{P}(C \cap \{x,y\} = \emptyset, \forall\, C \in X) = (1-p)^{\mathrm{gr}_H(x)+\mathrm{gr}_H(y)-\mathrm{gr}_H(x,y)}$, donde

$$\begin{aligned}\mathbb{E}(\xi_x\xi_y) - \mathbb{E}(\xi_x)\mathbb{E}(\xi_y) &= (1-p)^{\mathrm{gr}_H(x)+\mathrm{gr}_H(y)-\mathrm{gr}_H(x,y)} - (1-p)^{\mathrm{gr}_H(x)+\mathrm{gr}_H(y)}\\ &\leq (1-p)^{-\,\mathrm{gr}_H(x,y)} - 1 = (1-\frac{\alpha}{d})^{-o(d)} - 1\\ &= (1+o(1)) - 1 = o(1).\end{aligned}$$

Assim,

$$V(|F'|) \leq \sum_{x\in F}\mathbb{E}(\xi_x) + \sum_{\substack{x,y\in F\\ x\neq y}} o(1) \leq n + o(n^2) = o(n^2),$$

donde

$$D(|F'|) = \sqrt{V(|F'|)} = o(n) = o(\mathbb{E}(|F'|)),$$

e portanto

$$|F'| = \mathbb{E}(|F'|)(1+o(1)) = ne^{-\alpha}(1+o(1))$$

com probabilidade $1-o(1)$, o que mostra que a condição (b) vale com probabilidade $1-o(1)$.

Por fim, vamos mostrar que a condição (c) também vale com probabilidade $1-o(1)$. Para isso, é suficiente mostrar que

$$\sum_{x\in F}\mathbb{P}(x \notin F' \text{ ou } \mathrm{gr}_{H'}(x) = (1+o(1))e^{-\alpha(r-1)}d) = (1-o(1))n.$$

De fato, essa soma é o valor esperado da variável aleatória $|B|$ onde

$$B = (F\setminus F') \cup \{x \in F' \mid \mathrm{gr}_{H'}(x) = (1+o(1))e^{-\alpha(r-1)}d\}.$$

Como

$$V(|B|) = \mathbb{E}(|B|^2) - \mathbb{E}(|B|)^2 \leq n^2 - ((1-o(1))n)^2 = o(n^2),$$

temos

$$D(|B|) = \sqrt{V(|B|)} = o(n) = o(\mathbb{E}(|B|)),$$

donde, com probabilidade $1 - o(1)$, $|B| = (1 + o(1))\mathbb{E}(|B|) = (1 - o(1))n = n - o(n) = n - o(|S|)$.

Como

$$\begin{aligned}&\mathbb{P}(x \notin F' \text{ ou } \operatorname{gr}_{H'}(x) = (1+o(1))e^{-\alpha(r-1)}d)\\&\quad = \mathbb{P}(x \notin F') + \mathbb{P}(x \in F')\mathbb{P}(\operatorname{gr}_{H'}(x) = (1+o(1))e^{-\alpha(r-1)}d \mid x \in F'),\end{aligned}$$

basta provar que

$$\sum_{x\in F} \mathbb{P}(\operatorname{gr}_{H'}(x) = (1+o(1))e^{-\alpha(r-1)}d \mid x \in F') = (1-o(1))n.$$

Dizemos que $y \in F$ é razoável se $(1-\delta)d < \operatorname{gr}_H(y) < (1+\delta)d$, e que y é ruim caso contrário. Dizemos que uma hiperaresta $C \in H$ é boa se, para todo $y \in C$, y é razoável. Temos

$$\begin{aligned}|\{C \in H \mid C \text{ não é boa }\}| &\leq \sum_{C\in H} |\{y \in C \mid y \text{ é ruim }\}|\\&= \sum_{\substack{y\in F\\ y \text{ é ruim}}} |\{C \in H \mid y \in C\}|\\&\leq \delta n \cdot Kd = o(nd).\end{aligned}$$

Dizemos que $x \in F$ é ótimo se x é razoável e

$$|\{C \in H \mid x \in C \text{ e } C \text{ não é boa}\}| \leq \sqrt{\delta} \cdot d = o(d).$$

Temos

$$\begin{aligned}\sum_{x\in F} |\{C \in H \mid x \in C \text{ e } C \text{ não é boa}\}| &= \sum_{C\in H} |\{x \in F \mid x \in C\}|\\&= r|\{C \in H \mid C \text{ não é boa}\}| \leq rK\delta nd = o(nd),\end{aligned}$$

donde

$$|\{x \in F \mid x \text{ não é ótimo}\}| \leq \delta n + \frac{rK\delta nd}{\sqrt{\delta}d} = n(\delta + rK\sqrt{\delta}) = o(n).$$

Basta provar então que, para todo $x \in F$ ótimo,

$$\mathbb{P}(\mathrm{gr}_{H'}(x) = (1 + o(1))e^{-\alpha(r-1)}d \mid x \in F') = (1 - o(1)).$$

Se $x \in F$ é ótimo então $\{C \in H \mid x \in C\} = \{C_1, C_2, \ldots, C_k\}$, onde $k = d(1 + o(1))$, e C_j é boa, $\forall\, j$. Assim, como $\mathrm{gr}_H(y, z) = o(d)$, $\forall\, y, z \in F$, $y \neq z$, para todo j temos

$$|\{C \in H \mid x \notin C \text{ e } C \cap C_j \neq \emptyset\}| = (1 + o(1))(r - 1)d.$$

A probabilidade condicional $\mathbb{P}(\,\cdot \mid x \in F')$ pode ser vista como uma probabilidade em $\mathcal{P}(H \setminus \{C_1, C_2, \ldots, C_k\})$ onde escolhemos um conjunto $\widetilde{X} \subset H \setminus \{C_1, \ldots, C_k\}$ de hiperarestas a serem retiradas: para cada $C \in H \setminus \{C_1, \ldots, C_k\}$, a probabilidade de termos $C \in \widetilde{X}$ será sempre igual a $p = \frac{\alpha}{d}$, sendo esses eventos mutuamente independentes. De agora em diante trabalharemos com essa probabilidade.

Sejam ξ_j, $1 \leq j \leq k$, as variáveis aleatórias definidas por

$$\xi_j = \begin{cases} 0 \text{ se existe } C \in \widetilde{X} \text{ com } C \cap C_j \neq \emptyset \\ 1 \text{ caso contrário,} \end{cases}$$

e $\xi = \sum_{j=1}^{k} \xi_j$. Temos

$$\xi = \mathrm{gr}_{H'}(x),$$

e

$$\mathbb{E}(\xi_j) = \left(1 - \frac{\alpha}{d}\right)^{(1+o(1))(r-1)d} = e^{-\alpha(r-1)} + o(1)$$

para todo j, donde

$$\mathbb{E}(\xi) = k(1 + o(1))e^{-\alpha(r-1)} = d(1 + o(1))e^{-\alpha(r-1)}.$$

Assim, para encerrar a prova, basta mostrar que $D(\xi) = o(d)$. Temos

$$V(\xi) = \sum_{j=1}^{k}(\mathbb{E}(\xi_j^2) - \mathbb{E}(\xi_j)^2) + \sum_{i=1}^{k}\sum_{\substack{j=1 \\ j \neq i}}^{k}(\mathbb{E}(\xi_i \xi_j) - \mathbb{E}(\xi_i)\mathbb{E}(\xi_j)),$$

como antes. Temos $\mathbb{E}(\xi_j^2) - \mathbb{E}(\xi_j)^2 \leq \mathbb{E}(\xi_j^2) \leq 1$. Por outro lado, como C_i é boa, $|\{C \in H \mid |C \cap C_i| \geq 2\}| = o(d)$, donde $|\{1 \leq j \leq k \mid C_i \cap C_j \neq \{x\}\}| = o(d)$. Além disso, se $C_i \cap C_j = \{x\}$, como $|\{C \in H \backslash \{C_1, \ldots, C_k\} \mid C \cap C_i \neq \emptyset \text{ ou } C \cap C_j \neq \emptyset\}| = (1+o(1))(2r-2)d$, $\mathbb{E}(\xi_i \xi_j) = (1 - \frac{\alpha}{d})^{(1+o(1))(2r-2)d}$, e portanto $\mathbb{E}(\xi_i \xi_j) - \mathbb{E}(\xi_i)\mathbb{E}(\xi_j) = o(1)$. Assim,

$$V(\xi) \leq k + o(kd) + o(k^2) = o(d^2),$$

donde

$$D(\xi) = \sqrt{V(\xi)} = o(d).$$

Portanto, as três condições (a), (b) e (c) valem com probabilidade $1 - o(1)$, o que encerra a prova. $\square$

3. Coberturas e empacotamentos optimais

O nosso objetivo desta seção é investigar estimativas para coberturas e empacotamentos optimais.

3.1. Preliminares. Nesta seção provaremos estimativas gerais sobre o tamanho de coberturas e empacotamentos optimais em hipergrafos (quase) regulares, e mostramos exemplos onde essas estimativas são assintoticamente ótimas.

Estendemos a definição dos parâmetros α e β para famílias quaisquer de subconjuntos de um conjunto finito F: dado $\mathcal{C} \subset \mathcal{P}(F)$, definimos

$$\alpha(F, \mathcal{C}) = \min\{k \in \mathbb{N} \mid \exists\, C_1, C_2, \ldots, C_k \in \mathcal{C} \text{ tais que } F = \bigcup_{j=1}^{k} C_j\}$$

e

$$\beta(F, \mathcal{C}) = \max\{k \in \mathbb{N} \mid \exists\, C_1, C_2, \ldots, C_k \in \mathcal{C} \text{ com } C_i \cap C_j = \emptyset,\ \forall\, i \neq j\}.$$

Além disso, dado $x \in \mathcal{C}$, definimos $\mathrm{gr}_{\mathcal{C}}(x) = |\{C \in \mathcal{C} \mid x \in C\}|$.

Apesar de alguns dos resultados desta seção se referirem a famílias gerais de subconjuntos de um dado conjunto finito, nosso foco principal continua sendo em hipergrafos regulares. Vamos dar alguns exemplos de hipergrafos regulares que aparecem naturalmente em certos problemas, e de aplicações de resultados desta seção nesses casos:

Se F admite uma métrica d, e r é um número real tal que $|B(x,r)| = |\{y \in F \mid d(x,y) \leq r\}|$ não depende de x, então $\mathcal{C} = \{B(x,r) \mid x \in F\}$ é um hipergrafo regular. De fato, se $|B(x,r)| = a$, para todo $x \in F$, dado $x_0 \in F$, $\{C \in \mathcal{C} \mid x_0 \in C\}| = \{x \in F \mid d(x,x_0) \leq r\}| = |B(x_0,r)| = a$, donde $\mathcal{C}$ é um a-hipergrafo a-regular. Em particular, se G é um grafo regular, e d é a distância usual em G, dada por $d(x,y) = \min\{k \in \mathbb{N} \mid \exists\, x_1, x_2, \ldots, x_k \in V(G)$ tais que $\{x_i, x_{i+1}\} \in e(G), \forall\, i < k\}$ (onde $V(G)$ é o conjunto dos vertices de G e $e(G)$ é o conjunto das arestas de G), a condição acima é satisfeita com $r = 1$. De fato, se G é a-regular então $|B(x,1)| = a+1$, para todo $x \in G$. Portanto, o Corolário 81 mostra que existe $X \subset V(G)$ com no máximo $\frac{|V(G)|}{a+1}(\log(a+2)+\gamma)$ elementos tal que, para todo $x \in V(G)$, $x \in X$ ou existe $y \in X$ com $\{x,y\} \in e(G)$.

Outro exemplo é o caso $F = I_1 \times I_2 \times \cdots \times I_m$ onde os I_j são conjuntos finitos, $1 \leq j \leq m$, e d é a *distância de Hamming*, dada por $d((a_1,\ldots,a_m),(b_1,\ldots,b_m)) = |\{1 \leq j \leq m \mid a_j \neq b_j\}|$. Nesse caso, dado $r \geq 0$, temos

$$|B(x,r)| = |B(x,\lfloor r\rfloor)| = 1 + \sum_{k=1}^{\lfloor r\rfloor} \sum_{1 \leq j_1 < j_2 < \cdots < j_k \leq m} \prod_{i=1}^{k} (|I_{j_i}| - 1),$$

que não depende de x. No caso em que existe a tal que $|I_j| = a$ para $1 \leq j \leq m$, temos $|B(x,r)| = \sum_{k=0}^{\lfloor r\rfloor} \binom{m}{k}(a-1)^k$, e $|F| = a^m$. Podemos pensar em F como o conjunto de possíveis cartões numa loteria exportiva generalizada com m jogos, em que há a possíveis resultados para cada jogo (na loteria esportiva usual, $m = 13$ e $a = 3$: cada jogo pode terminar em vitória, empate ou derrota do time que tem o mando de campo). Se $x_0 \in F$ for o resultado da loteria numa dada semana, para cada $r \geq 0$, $B(x,r)$ é o conjunto dos cartões que erram no máximo r resultados, ou seja, que fazem pelo menos $m - r$ pontos. Se $h(a,m,r) = \alpha(F,\mathcal{C})$, onde, como antes, $\mathcal{C} = \{B(x,r), x \in F\}$, então $h(a,m,m-p)$ é a responta à seguinte pergunta: Numa tal loteria, quantos cartões (no mínimo) devem ser jogados de modo a garantir que, em pelo menos um deles, vamos fazer pelo mesno p pontos. Esta pergunta (o problema da loteria esportiva) motivou o nosso interesse pelo assunto deste capítulo.

Se $b = \sum_{k=0}^{m-p} \binom{m}{k}(a-1)^k$, o Corolário 81 mostra que $\frac{a^m}{b} < h(a,m,m-p) < \frac{a^m}{b}(\log(b+1)+\gamma)$. Por outro lado, se $p \le \lceil m/a \rceil$, bastam a cartões para garantir os p pontos (isto é, $h(a,m,m-p) \le a$). De fato, se no cartão j marcamos a opção j em todos os jogos, para $1 \le j \le a$, garantimos que, em um dos cartões faremos pelo menos $\lceil m/a \rceil$ pontos.

Estes fatos, junto com as estimativas do Lema 92 do Apêndice A mostram que, dados $a \in \mathbb{N}$ e $\alpha \in (0,1)$, se m é grande e $p = (\alpha + o(1))m$ então $h(a,m,m-p) = (g_a(\alpha) + o(1))^m$, onde

$$g_a(\alpha) = \begin{cases} 1 & \text{se } \alpha \le 1/a \\ a\alpha^\alpha \left(\frac{1-\alpha}{a-1}\right)^{1-\alpha} & \text{se } \alpha \ge 1/a \end{cases}$$

Se a e $r = m - p$ estão fixos e m é grande então é possível dar estimativas melhores para $h(a,m,r)$. De fato, temos a

Proposição 79. *Existe $c = c(a,r)$ tal que $h(a,m,r) < c \cdot \frac{a^m}{b}$, onde, como antes, $b = \sum_{k=0}^{r} \binom{m}{k}(a-1)^k$.*

Antes de provar isso, vamos fazer uma digressão sobre espaços projetivos, que serão úteis nessa prova e nas estimativas sobre empacotamentos no fim deste capítulo. Para toda potência de primo q, existe um único corpo (a menos de isomorfismos) com q elementos, que denotaremos por $\mathbb{F}_q$. Se q é primo, $\mathbb{F}_q$ é simplesmente o corpo $\mathbb{Z}/q\mathbb{Z}$. Dado um inteiro positivo n, o *espaço projetivo de dimensão* n sobre $\mathbb{F}_q$ que denotaremos por $\mathbb{P}^n(\mathbb{F}_q)$, é o quociente $(\mathbb{F}_q^{n+1})^*/\mathbb{F}_q^*$ de $(\mathbb{F}_q^{n+1})^* = \mathbb{F}_q^{n+1} \setminus \{0\}$ pela relação de equivalência $\sim$ dada por $u \sim v \Leftrightarrow \exists\, \lambda \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ tal que $v = \lambda u$. Temos $|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}$. Se $n = 2$, $\mathbb{P}^n(\mathbb{F}_q)$ é o *plano* projetivo sobre $\mathbb{F}_q$. Em geral, denotamos os elementos de $\mathbb{P}^n(\mathbb{F}_q)$ por $(a_0 : a_1 : \cdots : a_n)$, onde $(a_0, a_1, \ldots, a_n) \in \mathbb{F}_q^{n+1} \setminus \{0\}$. Temos $(b_0 : b_1 : \cdots : b_n) = (a_0 : a_1 : \cdots : a_n)$ se e somente se existe $\lambda \in \mathbb{F}_q^*$ tal que $b_i = \lambda a_i$, para $1 \le i \le n$. A cada elemento

$u = (a_0 : a_1 : a_2) \in \mathbb{P}^2(\mathbb{F}_q)$ associamos a *reta em* $\mathbb{P}^2(\mathbb{F}_q)$

$$\ell_u = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{F}_q) \mid a_0x_0 + a_1x_1 + a_2x_2 = 0\}.$$

Não é difícil mostrar que $|\ell_u| = q+1$ para todo u, se $u \neq v$, $|\ell_u \cap \ell_v| = 1$, e que, dado $w = (x_0 : x_1 : x_2)$ em $\mathbb{P}^2(\mathbb{F}_q)$, $|\{u \in \mathbb{P}^2(\mathbb{F}_q) \mid w \in \ell_u\}| = |\ell_w| = q+1$.

Vamos agora provar a Proposição 79.

Prova da Proposição 79. Mostraremos inicialmente que, se q é uma potência de primo, n é um inteiro positivo e

$$m = \frac{q^{n+1}-1}{q-1},$$

então $h(q,m,1) = \frac{q^m}{b}$, onde $b = 1+m(q-1) = q^{n+1}$ (essa é uma das raras situações onde há *coberturas perfeitas*, isto é, coberturas que também são empacotamentos). Para isso seja A uma matriz $(n+1)\times m$ cujas colunas $v_1, v_2, \ldots, v_m$ são vetores em $\mathbb{F}_q^{n+1}$ cujas classes de equivalência cobrem todo o espaço projetivo $\mathbb{P}^n(\mathbb{F}_q)$, ou seja, dado qualquer $w \in \mathbb{F}_q^{n+1}$, existem $\lambda \in \mathbb{F}_q$ e $1 \leq j \leq m$ com $w = \lambda v_j$. Seja $X \subset \mathbb{F}_q^m$ o conjunto dos vetores $u \in \mathbb{F}_q^m$ tais que $A \cdot u = 0$. Note que, como A tem posto $n+1$, X é um subespaço de $\mathbb{F}_q^m$ de codimensão $n+1$, e portanto tem $q^{m-n-1} = \frac{q^m}{b}$ elementos. Afirmamos que $\mathbb{F}_q^m = \bigcup_{u\in X} B(u,1)$. De fato, dado $\widetilde{u} \in \mathbb{F}_q^m$, teremos $A \cdot \widetilde{u} = \widetilde{v} \in \mathbb{F}_q^{n+1}$. Pela construção, existem $1 \leq j \leq m$ e $\lambda \in \mathbb{F}_q$ com $\widetilde{v} = \lambda v_j$, logo $A(\widetilde{u} - \lambda e_j) = A\cdot\widetilde{u} - \lambda A \cdot e_j = \widetilde{v} - \lambda v_j = 0$, onde e_j é o j-ésimo vetor da base canônica de $\mathbb{F}_q^m$, donde $\widetilde{u} - \lambda e_j \in X$. Como $d(\widetilde{u} - \lambda e_j, \widetilde{u}) \leq 1$, isso prova a afirmação. Tais subespaços X são conhecidos como *Códigos de Hamming*.

Mais geralmente, fixado $r \geq 1$, se $\widetilde{m} = rm = r\left(\frac{q^{n+1}-1}{q-1}\right)$ então $h(q,\widetilde{m},r) \leq \frac{q^{\widetilde{m}}}{b^r}$. De fato,

$$\widetilde{X} = \{(w_1, w_2, \ldots, w_r) \in \mathbb{F}_q^{mr} = (\mathbb{F}_q^m)^r \mid w_j \in X,\ 1 \leq j \leq r\}$$

é tal que

$$|\widetilde{X}| = |X|^r = \frac{q^{mr}}{b^r},$$

e

$$\mathbb{F}_q^{mr} = \bigcup_{\widetilde{w}\in\widetilde{X}} B(\widetilde{w}, r).$$

Note que, se $\widetilde{m} \geq 2r$,

$$\begin{aligned}\widetilde{b} = \sum_{j=0}^{r} \binom{\widetilde{m}}{j}(q-1)^j \leq (r+1)\binom{\widetilde{m}}{r}(q-1)^r \leq (r+1)\frac{\widetilde{m}^r}{r!}(q-1)^r \\ = \frac{(r+1)r^r}{r1}(m(q-1))^r \leq \frac{(r+1)r^r}{r!}\cdot b^r,\end{aligned}$$

donde

$$h(q,\widetilde{m},r) \leq \frac{(r+1)r^r}{r!}\cdot\frac{q^{\widetilde{m}}}{\widetilde{b}}.$$

Por outro lado, se $X \subset I_1 \times \cdots \times I_k$ é tal que $I_1 \times \cdots \times I_k = \bigcup_{v\in X} B(v,r)$ então, se $x > k$, $Y = X \times I_{l+1} \times \cdots \times I_s$ é tal que

$$|Y| = |X||I_{k+1} \times \cdots \times I_s|$$

e

$$I_1 \times \cdots \times I_k \times I_{k+1} \times \cdots \times I_s = \bigcup_{w\in Y} B(w,r).$$

Assim, no caso geral, dado $a > 1$, escolhemos uma potência de primo q, $q \mid a$, e escrevemos os conjuntos I_j de a elementos como $\mathbb{F}_q \times J$, onde $|J| = a/q$. Assim, dado m, escrevemos $I_1 \times \cdots \times I_m = \mathbb{F}_q^m \times J^m$. Tomamos ainda o maior ineiro n tal que $\widetilde{m} = r\left(\frac{q^{n+1}-1}{q-1}\right) \leq m$ (temos portanto $\widetilde{m} \geq \frac{m}{q+1}$), e portanto $I_1 \times \cdots \times I_m = \mathbb{F}_q^{\widetilde{m}} \times \mathbb{F}_q^{m-\widetilde{m}} \times J^m$, donde, como é possível cobrir $\mathbb{F}_q^{\widetilde{m}}$ por $\frac{q^{\widetilde{m}}}{b_0^r}$ bolas de raio r, onde $b_0 = q^{n+1}$, pela observação acima é possível cobrir $\mathbb{F}_q^{\widetilde{m}} \times \mathbb{F}_q^{m-\widetilde{m}} \times J^m$ por $\frac{a^m}{b_0^r}$ bolas de raio r. Se $m \geq 2r$, temos

$$\begin{aligned}b := \sum_{k=0}^{r} \binom{m}{k}(a-1)^k \leq (r+1)\binom{m}{r}(a-1)^r \leq (r+1)\frac{m^r}{r!}(a-1)^r \\ \leq (r+1)\frac{(q+1)^r}{r!}\cdot\widetilde{m}^r(a-1)^r \\ < (r+1)\frac{(q+1)^r}{r!}\left(\frac{rb_0}{q-1}\right)^r(a-1)^r\end{aligned}$$

$$\leq (r+1)\frac{(3r)^r}{r!}(a-1)^r \cdot b_0^r,$$

donde

$$\frac{a^m}{b_0^r} < c(a,r)\frac{a^m}{b},$$

onde

$$c(a,r) = (r+1)\frac{(3r(a-1))^r}{r!}.$$

□

Um interessante problema em aberto é determinar se, de fato,

$$h(a,m,r) = (1+o(1))\frac{a^m}{b}.$$

Isso não é conhecido nem no caso $a = 2$ (mas é verdade se $a = 2$ e $r = 1$). Veja o Capítulo 12 de [**13**].

O restante deste capítulo corresponde ao trabalho [**14**].

3.2. Cotas superiores para coberturas. Vamos incialmente provar uma versão ligeiramente melhorada de resultados clássicos de Johnson, Stein e Lovász (veja [**46, 69, 56**]).

Dizemos que uma família $\mathcal{C}$ de subconjuntos de um conjunto F é (a,b)-*semiregular* se $|C| \leq a$ para todo $C \in \mathcal{C}$ e $\mathrm{gr}_{\mathcal{C}}(x) \geq b$ para todo $x \in F$. Ocasionalmente, chamamos a-hipergrafos b-regulares de famílias *(a,b)-regulares.*

Proposição 80. *Sejam a e b inteiros positivos e suponha que $\mathcal{C}$ é uma família semiregular de subconjuntos de um conjunto F de n elementos. Seja $n = |\mathcal{C}|$. Então, para todo inteiro positivo ℓ',*

$$\frac{n}{a} \leq \frac{\log(m\ell'/bn)}{\log(1-b/m)} + \frac{m}{b}\sum_{1\leq j\leq \ell'}\frac{1}{j}.$$

Em particular, se $\ell = \lceil \frac{bn}{m} \rceil$*, temos* $\alpha(F, C) \le f(a, b, m, n)$*, onde*

$$f(a,b,m,n) = \begin{cases} \dfrac{n}{\ell} + \dfrac{m}{b}\displaystyle\sum_{j=2}^{\ell}\dfrac{1}{j} & \text{se } b \le m/\sqrt{n} \\ \dfrac{m}{b}\left(\log\left(\dfrac{bn}{m}\right) + \gamma\right) \\ \qquad\qquad -\dfrac{1}{2}\log\left(\dfrac{b^2 n}{m^2}\right) + \dfrac{1}{2} & \text{se } b > m/\sqrt{n}. \end{cases} \tag{158}$$

Além disso, se $b \le m/\sqrt{n}$*, temos*

$$f(a,b,m,n) \le \frac{n}{a} + \frac{m}{b}\sum_{2 \le r \le a}\frac{1}{r} \le \frac{m}{b}(\log(a+1) + \gamma), \tag{159}$$

onde $\gamma = 0.5772156649\ldots$ *é a constante de Euler.*

Vamos provar a Proposição 80 na seção abaixo.

Corolário 81. *Seja* F *um conjunto de* n *elementos e* $\mathcal{C}$ *um* a*-hipergrafo* b*-regular sobre* F*. Seja ainda* $\ell = \min\{a, \lceil n/a \rceil\}$*. Então*

$$\left\lceil \frac{n}{a} \right\rceil \le \alpha(F, \mathcal{C}) \le \frac{\log(a/\ell)}{\log \dfrac{1}{1 - a/n}} + \frac{n}{a}\sum_{r=1}^{\ell}\frac{1}{r} \tag{160}$$
$$< \frac{n}{a}\big(\log(a+1) + \gamma\big) - \frac{1}{2}\log\frac{a}{\ell} + \frac{1}{2}.$$

Nosso resultado principal desta seção, apresentado na Seção 3 (ver Proposição 6), mostra que as estimativas para $\alpha(F, \mathcal{C})$ acima são assintoticamente ótimas para certos hipergrafos regulares.

3.3. Prova da Proposição 80. Inicialmente enunciamos e provamos dois lemas auxiliares. Para o resto desta subseção, fixamos uma família (a, b)-semiregular $\mathcal{C}$ de subconjuntos de um conjunto finito F, onde a e b são inteiros positivos. Sejam $n = |F|$ e $m = |\mathcal{C}|$. Nosso primeiro lema segue de um argumento de contagem dupla:

Lema 82. *Temos* $am \ge bn$*. Além disso, dado qualquer* $A \subset F$*, existe* $C \in \mathcal{C}$ *tal que* $|C \cap A| \ge (b/m)|A|$*.*

Demonstração. De fato, para cada $B \subset F$ temos

$$ma \geq \sum_{C \in \mathcal{C}} |C \cap B| = \sum_{C \in \mathcal{C}} \sum_{x \in B} \chi_C(x)$$
$$= \sum_{x \in B} \sum_{C \in \mathcal{C}} \chi_C(x) = \sum_{x \in B} \mathrm{gr}_{\mathcal{C}}(x) \geq b|B|,$$

onde, como sempre, χ_C é a função característica do conjunto C, isto é, $\chi_C(x) = 1$ se $x \in C$ e $\chi_C(x) = 0$ caso contrário. Tomando $B = F$, obtemos $am \geq bn$, o que prova a primeira desigualdade no nosso lema. Tomando $B = A$, deduzimos que $\sum_{C \in \mathcal{C}} |C \cap A| \geq b|A|$, o que implica que existe um conjunto $C \in \mathcal{C}$ para o qual $|C \cap A| \geq (b/|\mathcal{C}|)|A|$, como afirmamos.

$\square$

Um corolário imediato do Lema 82 é o seguinte:

Corolário 83. *Para cada inteiro positivo k, existem $C_1, \ldots, C_k \in \mathcal{C}$ tais que*

$$\left| F \setminus \bigcup_{1 \leq i \leq k} C_i \right| \leq n \left(1 - \frac{b}{m}\right)^k. \tag{161}$$

Um corolário mais fino do Lema 82 é o

Corolário 84. *É possível cobrir qualquer $A \subset F$ com no máximo*

$$\frac{r}{\ell} + \frac{m}{b} \sum_{2 \leq j \leq \ell} \frac{1}{j} \leq \frac{m}{b} \sum_{1 \leq j \leq \ell} \frac{1}{j} \tag{162}$$

membros de $\mathcal{C}$, onde $\ell = \lceil br/m \rceil$ e $r = |A|$.

Demonstração. Podemos cobrir A por $C_1, C_2, \ldots \in \mathcal{C}$ tais que, para cada i, a cardinalidade de $C_i \cap (A \setminus \bigcup_{1 \leq j < i} C_j)$ é a maior possível, dados $C_1, \ldots, C_{i-1}$. Para $1 \leq s \leq A$, seja k_s o número de conjuntos C_i nessa cobertura tais que $|C_i \cap (A \setminus \bigcup_{1 \leq j < i} C_j)| = s$. É fácil ver que o

Lema 82 implica

$$k_1 \leq \frac{m}{b},\ k_1 + 2k_2 \leq \frac{2m}{b},\ \dots\ ,\ k_1 + 2k_2 + \cdots + sk_s \leq \frac{ms}{b} \tag{163}$$

para todo s. Além disso, obviamente

$$k_1 + 2k_2 + \cdots + sk_s \leq r \tag{164}$$

para todo s, e

$$k_1 + 2k_2 + \cdots + ak_a = r. \tag{165}$$

Notemos também que $a \geq \ell$. De (163)–(165) segue que

$$\begin{aligned} k_1 + \cdots + k_a \\ &= \frac{1}{a}(k_1 + 2k_2 + \cdots + ak_a) + \sum_{1 \leq j < a} \frac{1}{j(j+1)}(k_1 + 2k_2 + \cdots + jk_j) \\ &\leq \frac{r}{a} + \frac{m}{b} \sum_{1 \leq j < \ell} \frac{1}{j+1} + r \sum_{\ell \leq j < a} \frac{1}{j(j+1)} \\ &= \frac{r}{\ell} + \frac{m}{b} \sum_{1 \leq j < \ell} \frac{1}{j+1} \leq \frac{m}{b} \sum_{1 \leq j \leq \ell} \frac{1}{j}, \end{aligned}$$

como afirmamos. □

Podemos finalmente provar a Proposição 80.

Prova da Proposição 80. No caso $b \leq m/\sqrt{n}$, o resultado em (158) segue do Corolário 84 tomando $r = n$. A primeira desigualdade em (159) segue de

$$\frac{n}{\ell} = \frac{n}{a} + \sum_{\ell \leq j < a} \frac{n}{j(j+1)} \leq \frac{n}{a} + \frac{m}{b} \sum_{\ell \leq j < a} \frac{\ell}{j(j+1)} \leq \frac{n}{a} + \frac{m}{b} \sum_{\ell \leq j < a} \frac{1}{j+1},$$

e portanto

$$\frac{n}{\ell} + \frac{m}{b} \sum_{2 \leq j \leq \ell} \frac{1}{j} \leq \frac{n}{a} + \frac{m}{b} \sum_{2 \leq r \leq a} \frac{1}{r}.$$

A segunda desigualdade em (159) é evidente.

Em geral, dado um inteiro positivo ℓ', tomamos $r = m\ell'/b$, e aplicamos o Corolário 83 com o menor k que faz o lado direito de (161) ficar menor ou igual a r. A partir daí, aplicamos o Corolário 84. Isso nos dá a estimativa

$$\alpha(F, \mathcal{C}) \leq \frac{\log(r/n)}{\log(1 - b/m)} + \frac{m}{b} \sum_{1 \leq j \leq \ell'} \frac{1}{j}.$$

Para provar a desigualdade $\alpha(F, \mathcal{C}) \leq f(a, b, m, n)$ no caso $b > m/\sqrt{n}$, basta tomar $\ell' = \lfloor m/b \rfloor$ e aplicar a desigualdade acima.

Alguns cálculos (que deixamos como exercício) completam a prova. Os dois ingredientes principais desses cálculos são as desigualdades

$$\sum_{1 \leq r \leq k} \frac{1}{r} - \log k - \gamma < \frac{1}{2k} - \frac{1}{12k(k+1)},$$

que vale para todo inteiro positivo k e

$$-\frac{1}{\log(1-x)} < \frac{1}{x} - \frac{1}{2},$$

válida para $0 < x < 1$. □

4. Cotas inferiores para coberturas

Trabalharemos com famílias de translações de subconjuntos de a elementos de $\mathbb{Z}/n\mathbb{Z}$.

Se $A = \{\bar{0}, \bar{1}, \ldots, \overline{a-1}\} \subset \mathbb{Z}/n\mathbb{Z}$ e $\mathcal{C} = \{A + t \mid t \in \mathbb{Z}/n\mathbb{Z}\}$, onde $A + t = \{x + t \mid x \in A\}$, então $\alpha(\mathbb{Z}/n\mathbb{Z}, \mathcal{C}) = \lceil n/a \rceil$.

Na outra direção, temos o seguinte resultado:

Proposição 85. *Existe $a_0 \in \mathbb{N}$ tal que se $n > a \geq a_0$ então, para algum $A \subset F := \mathbb{Z}/n\mathbb{Z}$ com $|A| = a$, a família $\mathcal{C} = \{A + t \mid t \in \mathbb{Z}/n\mathbb{Z}\}$ é tal que*

$$\alpha(F, \mathcal{C}) > k_0 = \left(1 - \frac{12 \log\log a}{\log a}\right) \frac{\log a}{\log \dfrac{1}{1 - a/n}} \tag{166}$$

$$> \left(1 - \frac{12 \log\log a}{\log a}\right)\left(\frac{n}{a} - 1\right)\log a.$$

Um aspecto interessante da Proposição 85 é que ela implica a existência de hipergrafos regulares com α grande. Além disso, os parâmetros $n > a$ são livres e (166) fornece boas estimativas independente da relação entre n e a. Convidamos o leitor a comparar as cotas em (160) e (166) para os casos em que (i) $a \sim \log n$ (ii) $a \sim n/\log n$ e (iii) $a \sim n/2$. Ao responder uma pergunta de Tuza, Alon [**4**] obteve cotas precisas para o caso (ii), embora, a rigor, as famílias em [**4**] não fossem hipergrafos (seus elementos têm cardinalidade média a). Observamos também que, na Proposição 85 acima, por simplicidade, nós nos restringimos a a-hipergrafos b-regulares com $a = b$.

4.1. Prova da cota inferior. Vamos provar a Proposição 85. A prova será dividida em dois casos, de acordo com o tamanho de a. Vamos considerar inicialmente o caso em que a é grande; o outro caso requer uma idéia adicional.

4.1.1. *a grande.* Vamos supor que $a \geq n/(\log n)^3$. Consideramos todos os subconjuntos de a elementos de $\mathbb{Z}/n\mathbb{Z}$, tomados com igual probabilidade. Vamos estimar a probabilidade de que um tal conjunto A tenha k translações que cobrem F, onde k é um inteiro positivo dado, i.e., vamos estimar a probabilidade $p(n, a, k)$ de que existam $t_1, \ldots, t_k \in \mathbb{Z}/n\mathbb{Z}$ tais que $(A+t_1) \cup \cdots \cup (A+t_k) = \mathbb{Z}/n\mathbb{Z}$. Note que $1 - p(n, a, k)$ é a probabilidade de que $(A + t_1) \cup \cdots \cup (A + t_k) \neq \mathbb{Z}/n\mathbb{Z}$ para quaisquer $t_1, \ldots, t_k \in \mathbb{Z}/n\mathbb{Z}$, i.e., $(A^c + t_1) \cap \cdots \cap (A^c + t_k) \neq \emptyset$ para quaisquer $t_1, \ldots, t_k \in \mathbb{Z}/n\mathbb{Z}$. Observe que, dados $t_1, \ldots, t_k \in \mathbb{Z}/n\mathbb{Z}$, temos $(A^c + t_1) \cap \cdots \cap (A^c + t_k) \neq \emptyset$ se e somente se existe $x \in \mathbb{Z}/n\mathbb{Z}$ tal que $\{x - t_1, \ldots, x - t_k\} \subset A^c$.

Fixemos $T = \{t_1, \ldots, t_k\} \subset \mathbb{Z}/n\mathbb{Z}$.

AFIRMAÇÃO 86. *Seja* $r = \lceil n/k^2 \rceil$. *Existem* $x_1, \ldots, x_r \in \mathbb{Z}/n\mathbb{Z}$ *tais que os conjuntos* $B_i = x_i - T = \{x_i - t_1, \ldots, x_i - t_k\}$ $(1 \leq i \leq r)$ *são dois a dois disjuntos.*

Demonstração. Tomamos $x_1 = 0$. Suponhamos que já escolhemos $x_1, \dots, x_s$, com $s < n/k^2$, tais que $B_1, \dots, B_s$ são dois a dois disjuntos. Como $s < n/k^2$, claramente $U = \bigcup_{1 \le i \le s}(x_i - T)$ tem menos que n/k elementos. Portanto, a cardinalidade média da interseção de U com $x - T$, para $x \in \mathbb{Z}/n\mathbb{Z}$, é estritamente menor que 1, donde existe $x_{s+1} \in \mathbb{Z}/n\mathbb{Z}$ tal que $x_{s+1} - T$ é disjunto de U. A afirmação segue por indução. (Veja também a Seção 3.) □

Vamos agora provar a nossa proposição. Para qualquer conjunto fixo $T = \{t_1, \dots, t_k\}$, a probabilidade de que $x - T \subset A^c$ para algum $x \in \mathbb{Z}/n\mathbb{Z}$ é maior ou igual à probabilidade de que $x_j - T \subset A^c$ para algum $j \in [r] := \{1, \dots, r\}$, onde os x_j $(1 \le j \le r)$ são dados pela afirmação anterior. Esta última probabilidade é $1 - \widetilde{p}(n, a, k, r)$, onde $\widetilde{p}(n, a, k, r)$ é a probabilidade de termos $x_j - T \not\subset A^c$ para cada $j \in [r]$. Para estimar $\widetilde{p}(n, a, k, r)$, consideramos subconjuntos aleatórios $\tilde{A} \subset \mathbb{Z}/n\mathbb{Z}$ construídos da seguinte forma: fazemos $y \in \tilde{A}$ com probabilidade a/n, independentemente para cada $y \in \mathbb{Z}/n\mathbb{Z}$. A probabilidade de que $\tilde{A}$ tenha m elementos é $\binom{n}{m}(a/n)^m(1 - a/n)^{n-m}$, que é maximal para $m = a$, donde a probabilidade de termos $|\tilde{A}| = a$ é pelo menos $1/(n+1)$. Com essa distribuição de probabilidade, os eventos $B_j = x_j - T \not\subset \tilde{A}^c$ $(j \in [r])$ são independentes (pois os conjuntos B_j são dois a dois disjuntos), e a probabilidade de cada um desses eventos é $1 - (1 - a/n)^k$. Assim, a probabilidade de $B_j \not\subset \tilde{A}^c$ para todo $j \in [r]$ é $(1 - (1 - a/n)^k)^r$. Logo, temos

$$\begin{aligned}\widetilde{p}(n, a, k, r) &= \mathbb{P}\left(\forall j \in [r] \text{ temos } x_j - T \not\subset \tilde{A}^c \;\middle|\; |\tilde{A}| = a\right)\\ &\le (n+1)\mathbb{P}(\forall j \in [r] \text{ we have } x_j - T \not\subset \tilde{A}^c)\\ &= (n+1)\left(1 - \left(1 - \frac{a}{n}\right)^k\right)^r,\end{aligned}$$

e assim $p(n, a, k)$ é no máximo

$$(167)\qquad \binom{n}{k}\widetilde{p}(n, a, k, r) \le \binom{n}{k}(n+1)\left(1 - \left(1 - \frac{a}{n}\right)^k\right)^r$$

$$\leq n^{k+1}\left(1-\left(1-\frac{a}{n}\right)^k\right)^r.$$

Seja $k = -\beta \log a/\log(1-a/n) \leq \beta(n/a)\log n$, onde $\beta \leq 1$. O lado direito de (167) é $n^{k+1}\left(1-a^{-\beta}\right)^r$, que é menor que

$$n^{1+\beta\log^4 n}\exp\left(-\frac{a^{-\beta}n}{k^2}\right) < \exp\left(-\frac{a^{2-\beta}}{\beta^2 n\log^2 n}+\log n\left(1+\log^4 n\right)\right).$$

Se $\beta \leq (1-12(\log\log a)/\log a)$, então $a^{2-\beta}/\beta^2 n\log^2 n \geq \log^6 n$ para n suficientemente grande.

Como $\log^6 n \gg \log n(1+\log^4 n)$, temos $p(n,a,k) \ll 1$. Portanto existe $A \subset \mathbb{Z}/n\mathbb{Z}$ com $|A| = a$ tal que $(A+t_1)\cup\cdots\cup(A+t_k) \neq \mathbb{Z}/n\mathbb{Z}$ para quaisquer $t_1,\ldots,t_k \in \mathbb{Z}/n\mathbb{Z}$. Isso implica que, para algum $A \subset \mathbb{Z}/n\mathbb{Z}$ com $|A| = a$, temos $\alpha(F,\mathcal{C}) > k_0$, onde k_0 é dado em (166). Isso completa a prova da Proposição 85 no caso $a \geq n/(\log n)^3$.

4.1.2. *a pequeno.* Vamos agora tratar do caso em que a é “pequeno”, isto é, $a < n/(\log n)^3$. Sejam

$$b = \lceil a(\log a+1)\rceil, \quad r = \lceil \log a\rceil, \quad \varepsilon = \frac{1}{r}, \quad \delta = \frac{10\log\log a}{\log a}, \tag{168}$$

e

$$k = \left\lceil \frac{1-\delta}{1+\varepsilon} r(\log a)^2\right\rceil. \tag{169}$$

Vamos usar a seguinte afirmação, que provaremos a seguir.

Afirmação 87. *Existem $0 \leq y_i < b$ $(1 \leq i \leq a)$ tais que se $A_0 = \{\overline{y}_1,\ldots,\overline{y}_a\} \subset \{\overline{0},\overline{1},\ldots,\overline{b-1}\} \subset \mathbb{Z}/rb\mathbb{Z}$, então*

$$(A_0+t_1)\cup\cdots\cup(A_0+t_k) \neq \mathbb{Z}/rb\mathbb{Z}$$

para quaisquer $t_1,\ldots,t_k \in \mathbb{Z}/rb\mathbb{Z}$.

Vamos agora provar a Proposição 85 para $a < n/(\log a)^3$ assumindo a Afirmação 87. Seja $\ell = \lfloor n/(r+1)b\rfloor$, e sejam y_i $(1 \leq i \leq a)$ como na Afirmação 87. Seja $A_0 = \{\overline{y}_1,\ldots,\overline{y}_a\} \subset \mathbb{Z}/rb\mathbb{Z}$, e seja $A = \{y_1 \bmod$

$n, \ldots, y_a \bmod n\} \subset \mathbb{Z}/n\mathbb{Z}$. Afirmamos que

$$(A + s_1) \cup \cdots \cup (A + s_m) = \mathbb{Z}/n\mathbb{Z} \tag{170}$$

implica $m \geq \ell(k+1)$. Para provar isso, suponha que (170) vale para certos $s_1, \ldots, s_m \in \mathbb{Z}/n\mathbb{Z}$. Para $0 \leq j < \ell$, sejam

$$B_j = \{jb(r+1) + q \mid 0 \leq q < rb\}$$

e

$$I_j = \{i \leq m \mid (A + s_i) \cap B_j \neq \emptyset\}.$$

Os conjuntos I_j são dois a dois disjuntos, pois o diâmetro de $A + s_i$ é no máximo b, e a distância entre B_j e B_{j+1} é $b+1$. Além disso, cada I_j dever ter pelo menos $k+1$ elementos, pois

$$\bigcup_{i \in I_j} (A + s_i) \supset B_j$$

implica que

$$\bigcup_{i \in I_j} (A_0 + \overline{s}_i) = \mathbb{Z}/rb\mathbb{Z},$$

o que, pela escolha de $A_0 = \{\overline{y}_1, \ldots, \overline{y}_a\}$, implica que $|I_j| > k$.

Para encerrar a prova, basta notar que

$$\begin{aligned}
\ell(k+1) &= \left\lfloor \frac{n}{(r+1)b} \right\rfloor \left(\left\lceil \frac{1-\delta}{1+\varepsilon} r (\log a)^2 \right\rceil + 1 \right) \\
&> \left(\frac{n}{(r+1)b} - 1 \right) \frac{1-\delta}{1+\varepsilon} (\log a)^3 \\
&> \frac{n}{b(r+1)} (\log a)^3 \left(1 - \frac{11 \log\log a}{\log a} \right) \\
&> \frac{n}{a} (\log a) \left(1 - \frac{12 \log\log a}{\log a} \right) \\
&\geq \left(1 - \frac{12 \log\log a}{\log a} \right) \frac{\log a}{\log \dfrac{1}{1 - a/n}},
\end{aligned}$$

para a suficientemente grande. $\square$

Prova da Afirmação 87. Consideraremos um subconjunto aleatório A_0 de $\{\overline{0}, \overline{1}, \dots, \overline{b-1}\}$, em que cada elemento pertence a A_0 com probabilidade a/b, independentemente. A probabilidade de que A_0 tenha m elementos é $\frac{b}{m}(a/b)^m(1-a/b)^{b-m}$, que é maximal para $m = a$. Assim, a probabilidade de que um tal conjunto A_0 tenha a elementos é pelo menos $1/(b+1)$. Como antes, vamos estimar probabilidades condicionais em relação ao evento $|A| = a$.

Fixemos $t_1, \dots, t_k$. Vamos estimar por cima a probabilidade de que

$$(A_0 + t_1) \cup \dots \cup (A_0 + t_k) = \mathbb{Z}/rb\mathbb{Z}. \tag{171}$$

Seja $T = \{t_1, \dots, t_k\}$. Observemos que (171) ocorre se e somente se para todo $x \in \mathbb{Z}/rb\mathbb{Z}$, , o conjunto $x - T = \{x - t_1, \dots, x - t_k\}$ intersecta A_0. Sejam

$$s = \left\lceil \frac{\varepsilon}{1+\varepsilon} rb \right\rceil \quad \text{e} \quad s_0 = \left\lceil \frac{s}{k^2} \right\rceil. \tag{172}$$

Provaremos agora os seguintes fatos (veja a Afirmação 86):

(*) Existem $x_1, \dots, x_s$ tal que, para cada i, temos:

$$|(x_i - T) \cap \{\overline{0}, \overline{1}, \dots, \overline{b-1}\}| \leq (1+\varepsilon)\frac{k}{r}.$$

(**) Existem $\widetilde{x}_1, \dots, \widetilde{x}_{s_0} \in \{x_1, \dots, x_s\}$ tais que os conjuntos $\widetilde{x}_j - T$ $(1 \leq j \leq s_0)$ são dois a dois disjuntos.

Para provar (*), basta observar que o número médio de elementos em $(x - T) \cap \{\overline{0}, \overline{1}, \dots, \overline{b-1}\}$ $(x \in \mathbb{Z}/rb\mathbb{Z})$ é k/r. A prova de (**) é similar à prova da afirmação: suponhamos já ter escolhido $\widetilde{x}_1, \dots, \widetilde{x}_{s_1} \in \{x_1, \dots, x_s\}$ tais que os conjuntos $\widetilde{x}_j - T$ $(1 \leq j \leq s_1)$ são dois a dois disjuntos, mas $s_1 < s/k^2$. Então

$$\Big| \bigcup_{1 \leq j \leq s_1} (\widetilde{x}_j - T) \Big| = s_1 k < \frac{s}{k}. \tag{173}$$

Se escolhermos $x_i \in \{x_1, \ldots, x_s\}$ aleatoriamente, a probabilidade de que um elemento dado $z \in \mathbb{Z}/rb\mathbb{Z}$ pertença a $x_i - T$ é no máximo k/s, pois $k = |T|$ translações de T contêm z. Por causa de (173), a cardinalidade esperada de

$$(x_i - T) \cap \bigcup_{1 \leq j \leq s_1} (\widetilde{x}_j - T)$$

é estritamente menor que 1. Portanto, a seqüência $\widetilde{x}_1, \ldots, \widetilde{x}_{s_1}$ pode ser estendida com um novo elemento $x_i \in \{x_1, \ldots, x_s\}$. Isso completa a prova de (**).

No resto da prova, vamos concentrar nossa atenção nos $\widetilde{x}_j$ em (**). Podemos verificar facilmente que a probabilidade de que $(\widetilde{x}_j - T) \cap A_0 \neq \emptyset$ para todo $1 \leq j \leq s_0$ é no máximo

$$\left(1 - \left(1 - \frac{a}{b}\right)^{(1+\varepsilon)k/r}\right)^{s_0}.$$

Portanto, a probabilidade de que, para algum $T = \{t_1, \ldots, t_k\} \subset \mathbb{Z}/rb\mathbb{Z}$, tenhamos $(\widetilde{x}_j - T) \cap A_0 \neq \emptyset$ para todo $1 \leq j \leq s_0$, dado que $|A_0| = a$, é no máximo

$$(b+1)(rb)^k \left(1 - \left(1 - \frac{a}{b}\right)^{(1+\varepsilon)k/r}\right)^{s_0}. \tag{174}$$

Vamos estimar (174) por partes. Nos cálculos abaixo, vamos assumir tacitamente que a é grande. Como $1 - a/b \geq 1 - 1/(\log a + 1)$,

$$\left(1 - \frac{a}{b}\right)^{(1+\varepsilon)k/r} \geq \exp\left(-(1+\varepsilon)\frac{k}{r(\log a)}\right). \tag{175}$$

Temos

$$(1+\varepsilon)\frac{k}{r(\log a)} \geq (1-\delta)\log a. \tag{176}$$

Juntando (175) e (176), temos

$$\left(1 - \left(1 - \frac{a}{b}\right)^{(1+\varepsilon)k/r}\right)^{s_0} \leq \left(1 - a^{-1+\delta}\right)^{s_0} \tag{177}$$

$$\leq \exp\left(-a^{-1+\delta}\frac{\varepsilon rb}{(1+\varepsilon)k^2}\right).$$

Com bastante folga, temos $rb/k^2 \geq a/3(\log a)^4$, e portanto

$$a^{-1+\delta}\frac{\varepsilon rb}{(1+\varepsilon)k^2} \geq \frac{a^\delta}{7(\log a)^5}. \tag{178}$$

Por outro lado, temos

$$(b+1)(rb)^k \leq \exp\left(4(\log a)^4\right). \tag{179}$$

Juntando (177), (178), e (179), vemos que a expressão (174) é limitada por cima por

$$\exp\left(-\frac{a^\delta}{7(\log a)^5} + 4(\log a)^4\right). \tag{180}$$

Pela nossa escolha de δ (veja (168)), temos $a^\delta = (\log a)^{10} \gg (\log a)^9$, e portanto a expressão (180) é menor que q para a suficientemente grande. Concluímos que a probabilidade de que A_0 satisfaça as condições da Afirmação 87 é positiva, o que implica o resultado. □

4.2. Cotas inferiores construtivas. Lembre que provamos a existência de sistemas $\mathcal{C}$ com $\alpha(F,\mathcal{C})$ grande tomando $F = \mathbb{Z}/n\mathbb{Z}$ e considerando transladados $A+t$ ($t \in \mathbb{Z}/n\mathbb{Z}$) para conjuntos aleatórios apropriados $A \subset \mathbb{Z}$. Lembre também que na Seção 5.1 do Capítulo 2 mencionamos que os conjuntos dos quadrados em corpos finitos podem ser usados para 'simular' (muito vagamente falando) subconjuntos aleatórios (os vizinhos de 0 no grafo de Paley são justamente os quadrados; veja a Seção 5.1 do Capítulo 2). Nesta seção, vamos ver que os quadrados em um corpo finito formam um bom conjunto explícito A para a nossa construção do sistema $\mathcal{C}$.

De fato, como já observado por Alon **[4]**, se tomamos para n uma potência de primo q e tomamos para $A \subset F = \mathbb{F}_q$ o conjunto dos quadrados em $\mathbb{F}_q$, então

$$\mathcal{C} = \{A + t \mid t \in \mathbb{F}_q\}$$

é um sistema (a,a)-regular com $a=(q-1)/2$ e

$$\alpha(F,\mathcal{C}) \geq \left(\frac{1}{2}-o(1)\right)\lg q, \tag{181}$$

onde escrevemos lg para o logaritmo na base 2. O limite em (181) segue do resultado abaixo de [**10**] (veja Lema 9, Capítulo 13), que citamos sem prova. Seja χ o caracter quadrático em $\mathbb{F}_q$, de forma que $\chi(x)=x^{(q-1)/2}$ $(x\in\mathbb{F}_q)$. Temos $\chi(x)\in\{\pm1,0\}$, com $\chi(x)=0$ se $x=0$ e $\chi(x)=1$ se e só se x é um quadrado em $\mathbb{F}_q\setminus\{0\}$.

Lema 88. *Se $T\subset\mathbb{F}_q$ e $k=|T|$, então*

$$\left|q-\sum_{x\notin T}\prod_{t\in T}(1-\chi(x-t))\right| \leq \left((k-2)2^{k-1}+1\right)q^{1/2}+k2^{k-1}. \tag{182}$$

O Lema 88 é de fato uma conseqüência de uma estimativa bem conhecida de Weil para somas de caracteres (veja [**10**]). Este resultado de Weil foi uma de suas ferramentas importantes para a sua demonstração da *Hipótese de Riemann para curvas sobre corpos finitos*. Uma referência acessível é a monografia de Schmidt [**65**].

Para deduzir (181) do Lema 88, seja $T\subset\mathbb{F}_q$ um conjunto arbitrário com $k=|T|=\lfloor(1/2)\lg q-\lg\lg q\rfloor$. O elemento $x\in\mathbb{F}_q$ não será coberto pelos transladados $A+t$ $(t\in T)$ se e só se $x-T$ não encontra A, isto é, $x-t$ não é um quadrado para nenhum $t\in T$. Agora, o número de tais x é

$$2^{-k}\sum_{x\notin T}\prod_{t\in T}(1-\chi(x-t)).$$

Como, pela escolha de k, temos

$$2^{-k}q>\frac{1}{2}(k-2)q^{1/2}+2^{-k}q^{1/2}+\frac{k}{2},$$

a existência de tal x segue de (182).

Finalmente, observemos que nosso limite inferior k_0 na Proposição 85 para o caso em que $a=n/2$ (onde supomos que n é par por simplicidade) é

$$k_0 = \left(1 - \frac{12 \log\log n}{\log n}\right) \lg n.$$

Ademais, o limite superior para $\alpha(F, \mathcal{C})$ no Corolário 81 para este caso é $\lg n + 1$. Assim, a construção de Alon fornece um limite que difere do 'valor correto' por um fator de 2 apenas.

5. Empacotamentos

Disctutimos brevemente o problema de se encontrar empacotamentos grandes em famílias regulares. Suponha que $\mathcal{C}$ seja uma família de subconjuntos de um conjunto F. Seja $\beta(F, \mathcal{C})$ o maior inteiro r para o qual existem conjuntos $C_1, \dots, C_r \in \mathcal{C}$ dois a dois disjuntos.

PROPOSIÇÃO 89. *Suponha que $\mathcal{C}$ seja uma família (a, b)-regular sobre um conjunto F de n elementos. Então*

$$\frac{n}{a^2} \le \beta(F, \mathcal{C}) \le \frac{n}{a}. \tag{183}$$

A Proposição 89 segue do lema abaixo.

LEMA 90. *Seja $\mathcal{C}$ um sistema (a, b)-regular sobre um conjunto F. Dada uma subfamília $\widetilde{\mathcal{C}} \subset \mathcal{C}$ com r elementos, existe uma subfamília $\mathcal{B} \subset \widetilde{\mathcal{C}}$ de conjuntos dois a dois disjuntos com pelo menos r/ab membros.*

Para provar a Proposição 89 a partir do Lema 90, observe que se $\mathcal{C}$ é como no enunciado daquela proposição, então podemos tomar $\widetilde{\mathcal{C}} = \mathcal{C}$ no Lema 90. Note que então $r = |\widetilde{\mathcal{C}}| = |\mathcal{C}| = bn/a$, e portanto $r/ab = n/a^2$, e o limite inferior em (183) segue. O limite superior em (183) é óbvio.

Agora provamos o Lema 90.

DEMONSTRAÇÃO DO LEMA 90. Seja s a cardinalidade máxima de uma família de membros de $\widetilde{\mathcal{C}}$ dois a dois disjuntos. Suponha por contradição que $s < r/ab$, e seja $C_1, \dots, C_s \in \widetilde{\mathcal{C}}$ uma tal família de cardinalidade máxima. Seja $A = \bigcup_{1 \le j \le s} C_j$. Temos que $|A| = as$, e portanto o número de membros de $\widetilde{\mathcal{C}}$ que encontram A é no máximo $abs < r = |\widetilde{\mathcal{C}}|$. Portanto existe $C_{s+1} \in \widetilde{\mathcal{C}}$ que é disjunto de todos os C_j $(1 \le j \le s)$, o que contradiz a maximalidade de $C_1, \dots, C_s$. $\square$

5.1. Um exemplo. O nosso objetivo agora é mostrar que os limites na Proposição 89 não podem ser substancialmente melhorados sem hipóteses adicionais. De fato, dada uma potência de primo q podemos tomar para F o conjunto dos pontos do plano projetivo finito canônico sobre o corpo $\mathbb{F}_q$ e para $\mathcal{C}$ a coleção das linhas desse plano projetivo (lembre que discutimos planos projetivos na Seção 3.1). Então $|F| = q^2 + q + 1$, o sistema de conjuntos $\mathcal{C}$ é $(q+1, q+1)$-regular, e $\beta(F, \mathcal{C}) = 1$. Note que o limite inferior em (183) nos diz que $\beta(F, \mathcal{C}) \geq (q^2 + q + 1)/(q + 1)^2$, que tende a 1 conforme $q \to \infty$.

Mais geralmente, dado um inteiro positivo r, podemos tomar $F_r = F \times \{1, 2, \ldots, r\}$ e $\mathcal{C}_r = \{L \times \{j\} \mid L \in \mathcal{C},\ 1 \leq j \leq r\}$ (isto é, F_r é a união disjunta dos pontos de r cópias disjuntas do plano projetivo finito sobre $\mathbb{F}_q$ e $\mathcal{C}_r$ é a coleção de linhas destas cópias). Temos que $|F_r| = r(q^2 + q + 1)$, o sistema $\mathcal{C}_r$ é $(q + 1, q + 1)$-regular, e $\beta(F, \mathcal{C}) = r$, o que é próximo do limite inferior $r(q^2 + q + 1)/(q + 1)^2$ dado por (183), desde que q seja grande. Podemos usar estes exemplos para mostrar que, dadas seqüências de inteiros (a_k) e (n_k), com $a_k \to \infty$ e $n_k/a_k^2 \to \infty$ conforme $k \to \infty$, existem seqüências $(\tilde{a}_k)$ e $(\tilde{n}_k)$ tais que $\tilde{a}_k/a_k$ e $\tilde{n}_k/n_k$ tendem a 1 conforme $k \to \infty$, e para os quais existem $F^{(k)}$ e $\mathcal{C}^{(k)}$ tais que $\mathcal{C}^{(k)}$ é uma família $(\tilde{a}_k, \tilde{a}_k)$-regular de conjuntos sobre $F^{(k)}$, onde $|F^{(k)}| = \tilde{n}_k$, e

$$\lim_{k\to\infty} \beta(F^{(k)}, \mathcal{C}^{(k)}) \left(\frac{\tilde{n}_k}{\tilde{a}_k^2}\right)^{-1} = 1$$

(aqui usamos o fato que sempre existe um primo entre x e $(1 + o(1))x$, que decorre do teorema dos números primos).

6. Observações finais

Se a é um inteiro positivo, ponha

$$\alpha(a, n) = \max \alpha(F, \mathcal{C}),$$

onde o máximo é tomado sobre todas as famílias (a, b)-regulares de conjuntos $\mathcal{C}$ sobre um conjunto F de n elementos, e $b \geq 1$ é arbitrário.

Ponha

$$f(a) = \limsup_{n\to\infty} \frac{a}{n}\alpha(a,n).$$

Nossos resultados implicam que, para cada a fixo, temos

$$\log a - 10\log\log a \leq f(a) \leq \sum_{1\leq k\leq a} \frac{1}{k} = \log a + \gamma + O\left(\frac{1}{a}\right). \tag{184}$$

Considere o caso em que $a = 2$, isto é, o caso dos grafos regulares. Não é difícil mostrar que $(2/n)\alpha(2,n) = 4/3 + o(1)$ conforme $n \to \infty$, de forma que $f(2) = 4/3$. De fato, para o limite inferior, basta tomar para $\mathcal{C}$ uma coleção de, digamos, k triângulos disjuntos nos vértices sobre um conjunto F de cardinalidade $3k$. Então $\alpha(F,\mathcal{C}) = 2k$ e concluímos que $f(2) \geq 4/3$.

Para provar o limite superior, mostramos que qualquer grafo b-regular G $(b > 0)$ necessariamente contém um emparelhamento que cobre pelo menos $2/3$ de seus vértices. Lembramos que um *emparelhamento* em um grafo é simplesmente uma coleção de suas arestas que são duas a duas disjuntas. Um vértice v é *coberto* por um emparelhamento M se algum membro de M contém v.

Provemos a asserção acima sobre grafos b-regulares G. Seja M um emparelhamento máximo em G, e suponha que U é o conjunto de vértices cobertos por M. Suponha por contradição que $|U| < (2/3)n$, onde $n = |V(G)|$. Ponha $W = U^c = V(G) \setminus U$. O *$W$-grau* $\mathrm{gr}_W(u)$ de um vértice u em U é o número de vizinhos de u em W. O W-grau médio de um vértice em U é

$$|W|b/|U|. \tag{185}$$

De fato, para ver isto, primeiro observe que as b arestas incidentes a um vértice em W têm seus outros extremos em U, pois M é um emparelhamento máximo (não pode haver uma aresta contida em W). Desta observação segue que o número de arestas entre W e U é $|W|b$, e portanto o W-grau médio de um vértice em U é de fato dado por (185). Mas daí segue que existe uma aresta $e \in M$ cujos extremos x e y são tais que

$$\mathrm{gr}_W(x) + \mathrm{gr}_W(y) \geq 2|W|b/|U| > b. \tag{186}$$

Note que $\mathrm{gr}_W(x)$, $\mathrm{gr}_W(y) < b$ (por causa da aresta $e = \{x, y\} \subset U$). Portanto (186) implica que $\mathrm{gr}_W(x)$, $\mathrm{gr}_W(y) \geq 2$. Mas então existem vértices distintos x', $y' \in W$, com x' adjacente a x e y' adjacente a y'. Observe agora que $M \setminus \{e\} \cup \{xx', yy'\}$ é um emparelhamento maior que M, o que contradiz a maximalidade de $|M|$. Esta contradição mostra que M de fato cobre pelo menos $(2/3)n$ vértices de G, e portanto $\alpha(F, \mathcal{C}) \leq 2n/3$. Isto implica que $f(2) \leq 4/3$.

Problema 91. *Determine ou estime $f(a)$ precisamente para todo $a \geq 3$ fixo.*

Ademais, observamos que seria muito interessante melhorar as cotas inferiores que podemos obter através de construções explícitas (veja Seção 4.2).

APÊNDICE A

Estimativas para fatoriais e coeficientes binomiais

1. Fatoriais

O seguinte lema elementar dá uma estimativa para fatoriais que é correta a menos de um fator polinomial pequeno.

LEMA 92. *Para todo $n \geq 1$, temos*

$$e\left(\frac{n}{e}\right)^n \leq n! \leq ne\left(\frac{n}{e}\right)^n.$$

DEMONSTRAÇÃO. Para $n = 1$ as duas desigualdades são igualdades. Se $a_n = e(n/e)^n$ e $b_n = ne(n/e)^n$ temos, para todo $n \geq 1$,

$$\begin{aligned}(187)\qquad \frac{a_{n+1}}{a_n} = \frac{(n+1)}{e}\left(\frac{n+1}{n}\right)^n &\leq n+1 = \frac{(n+1)!}{n!} \\ &\leq \frac{(n+1)}{e}\left(\frac{n+1}{n}\right)^{n+1} = \frac{b_{n+1}}{b_n},\end{aligned}$$

e o resultado segue facilmente por indução. A desigualdade que usamos em (187), a saber, $((n+1)/n)^n \leq e \leq ((n+1)/n)^{n+1}$, segue de

$$\frac{\varepsilon}{1+\varepsilon} \leq \log(1+\varepsilon) \leq \varepsilon,$$

válida para todo $\varepsilon \geq 0$. $\square$

Como é bem conhecido, uma estimativa mais precisa para fatoriais é dada pela Fórmula de Stirling.

TEOREMA 93 (Fórmula de Stirling). *Temos*

$$\lim_{n\to\infty} \frac{n!}{n^n e^{-n}\sqrt{2n\pi}} = 1.$$

Esboço de prova. Notemos inicialmente que

$$\int_1^n \log x\, dx = n \log n - n + 1.$$

Por outro lado, essa integral é

$$\sum_{j=1}^{n-1} b_j$$

onde

$$b_k = \int_k^{k+1} \log x\, dx.$$

Ponha

$$a_k = \frac{1}{2}(\log k + \log(k+1)) \quad \text{e} \quad c_k = \log\left(k + \frac{1}{2}\right).$$

É fácil ver que $a_k < b_k < c_k$ para todo k. Temos ainda

$$\sum_{j=1}^{n-1} a_j = \log \frac{n!}{\sqrt{n}}.$$

Por outro lado,

$$c_k - a_k = \frac{1}{2}\log\left(1 + \frac{1}{4k(k+1)}\right) < \frac{1}{8k(k+1)},$$

cuja série converge, e portanto

$$\sum_{j=1}^{n-1}(b_j - a_j) = \log\left(e n^n e^{-n} \frac{\sqrt{n}}{n!}\right)$$

converge. Isso mostra que existe uma constante positiva c tal que

$$n! = (c + o(1)) \left(\frac{n}{e}\right)^n \sqrt{n}.$$

É possivel mostrar que $c = \sqrt{2\pi}$ calculando

$$I_n = \int_0^{\pi/2} (\cos x)^n\, dx$$

através da recorrência $I_n = (1 - 1/n)I_{n-2}$ $(n > 2)$, com valores iniciais $I_0 = \pi/2$ e $I_1 = 1$, e usando o fato que

$$\frac{I_{n+1}}{I_n} \to 1$$

quando $n \to \infty$. □

2. Coeficientes binomiais

A seguinte estimativa elementar para coeficientes binomiais é muito útil.

Lema 94. *Sejam $a \geq b$ inteiros positivos. Então*

$$\left(\frac{a}{b}\right)^b \leq \binom{a}{b} \leq \left(\frac{ea}{b}\right)^b. \tag{188}$$

Demonstração. Temos

$$\binom{a}{b} = \frac{(a)_b}{b!}, \tag{189}$$

onde $(a)_b = a(a-1)\dots(a-b+1)$. Como $a \geq b$, temos $(a-i)/(b-i) \geq a/b$ para todo $0 \leq i < b$, e a primeira desigualdade segue. Para a segunda desigualdade, apresentamos um argumento elementar de Babai [**6**]. Lembre que $1 + x \leq e^x$ para todo $x \in \mathbb{R}$ (compare, por exemplo, os gráficos). Assim, para todo $x > 0$, temos

$$\binom{a}{b}x^b \leq \sum_{0\leq k\leq a} \binom{a}{k}x^k = (1 + x)^a \leq e^{ax}. \tag{190}$$

Tomando $x = b/a$, temos

$$\binom{a}{b}\left(\frac{b}{a}\right)^b \leq e^b,$$

que é equivalente a (188). □

Podemos estimar coeficientes binomiais da forma $\binom{a}{b}$ com b um fator constante de a como no lema a seguir.

Lema 95. *Seja* $0 < \alpha < 1$ *uma constante. Então*

$$\binom{n}{\lfloor \alpha n \rfloor} = (1+o(1))\sqrt{\frac{1}{2\pi\alpha(1-\alpha)n}}\left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)^n. \tag{191}$$

Em particular,

$$\binom{n}{\lfloor \alpha n \rfloor} = \left(\frac{1}{\alpha^\alpha(1-\alpha)^{1-\alpha}}\right)^{(1+o(1))n}. \tag{192}$$

Em (191) *e* (192) *acima,* $o(1)$ *denota um termo que tende a* 0 *quando* $n \to \infty$.

Demonstração. Provemos (192). Vamos ignorar os $\lfloor \quad \rfloor$. Temos

$$\binom{n}{\alpha n} = \frac{n!}{(\alpha n)!((1-\alpha)n)!}. \tag{193}$$

Pelo Lema 92, deduzimos que (193) está entre

$$\frac{n^n}{e\alpha(1-\alpha)n^2(\alpha n)^{\alpha n}((1-\alpha)n)^{(1-\alpha)n}} > \frac{1}{en^2(\alpha^\alpha(1-\alpha)^{(1-\alpha)})^n}$$

e

$$\frac{n\cdot n^n}{e(\alpha n)^{\alpha n}((1-\alpha)n)^{(1-\alpha)n}} = \frac{n}{e(\alpha^\alpha(1-\alpha)^{1-\alpha})^n},$$

donde (191) segue. Para provar (191), basta usar a Fórmula de Stirling (Teorema 93) em vez do Lema 92. □

É freqüente encontrarmos somas da forma

$$\sum_{j=0}^{k}\binom{n}{j}, \tag{194}$$

onde $k \leq cn$ com $c < 1/2$. É também comum estarmos interessados em estimar a soma em (194) a menos de fatores constantes. Nestes casos, podemos estimar esta soma pela maior parcela que ocorre nela, pois os coeficientes binomiais $\binom{n}{j}$ decrescem geometricamente se $|j-n/2|$ é uma fração positiva de n.

Um caso que usamos várias vezes nestas notas é dado no lema a seguir.

LEMA 96. *Suponha que* $0 \leq k \leq (n+1)/3$. *Então*

$$\sum_{j=0}^{k} \binom{n}{j} < \binom{n}{k}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \dots\right) = 2\binom{n}{k}. \tag{195}$$

DEMONSTRAÇÃO. Note que $\binom{n}{j}/\binom{n}{j-1} = (n-j+1)/j \geq 2$ se $1 \leq j \leq (n+1)/3$. Portanto, a primeira desigualdade em (195) de fato vale e o nosso lema está provado. □

Em geral, temos o seguinte lema.

LEMA 97. (*i*) *Para toda constante* $0 < c < 1/2$, *existe uma constante* $B = B(c)$ *tal que se* $0 \leq k \leq cn$, *então*

$$\sum_{j=0}^{k} \binom{n}{j} \leq B\binom{n}{k}. \tag{196}$$

(*ii*) *Seja* b *uma constante positiva fixa. Então, quando* $n \to \infty$, *temos*

$$\sum_{|j-n/2| \leq b} \binom{n}{j} = (1+o(1))b^* \sqrt{\frac{2}{\pi n}}\, 2^n, \tag{197}$$

onde b^* *é o número de parcelas presentes na soma no lado esquerdo de* (197).

Finalmente, vamos enunciar um resultado que nos diz onde está o 'peso' em cada linha do triângulo de Pascal: naturalmente, temos

$$\sum_{0 \leq k \leq n} \binom{n}{k} = 2^n, \tag{198}$$

mas onde está concentrada a 'massa' na soma do lado esquerdo de (198)?

LEMA 98. *Seja $\omega = \omega(n)$ uma função com $\omega \to \infty$ conforme $n \to \infty$. Então*

$$\sum\nolimits_k^* \binom{n}{k} = (1 + o(1))2^n, \tag{199}$$

onde $\sum_k^*$ indica soma sobre todos os k satisfazendo

$$\left|k - \frac{n}{2}\right| \leq \omega\sqrt{n}. \tag{200}$$

Ademais, se para alguma constante $c_1 \geq 0$ temos $\omega = \omega(n) \to c_1$ quando $n \to \infty$, então

$$\sum\nolimits_k^* \binom{n}{k} = (c_2 + o(1))2^n, \tag{201}$$

para uma constante $c_2 = c_2(c_1)$. Temos $c_2(0) = 0$.

O Lema 98 pode ser provado com as cotas para coeficientes binomiais que discutimos acima. Devido ao Lema 98, podemos dizer que a soma em (198) está concentrada em uma faixa de largura da ordem de $\sqrt{n} \ll n$ em torno de $k = n/2$.

O valor da constante c_2 no Lema 98 é dado por

$$c_2 = c_2(c_1) = \frac{1}{\sqrt{2\pi}} \int_{-2c_1}^{2c_1} e^{-x^2/2}\, dx. \tag{202}$$

Referências Bibliográficas

1. Rudolf Ahlswede e Levon H. Khachatrian, *The complete intersection theorem for systems of finite sets*, European J. Combin. **18** (1997), no. 2, 125–136.
2. Miklós Ajtai, János Komlós, e Endre Szemerédi, *A dense infinite Sidon sequence*, European J. Combin. **2** (1981), no. 1, 1–11.
3. N. Alon, L. Babai, e H. Suzuki, *Multilinear polynomials and Frankl–Ray-Chaudhuri–Wilson type intersection theorems*, J. Combin. Theory Ser. A **58** (1991), no. 2, 165–180.
4. Noga Alon, *Transversal numbers of uniform hypergraphs*, Graphs Combin. **6** (1990), no. 1, 1–4.
5. Ian Anderson, *Combinatorics of finite sets*, The Clarendon Press Oxford University Press, New York, 1987.
6. László Babai, *An anti-Ramsey theorem*, Graphs Combin. **1** (1985), no. 1, 23–28.
7. László Babai e Peter Frankl, *Linear algebra methods in combinatorics, with applications to geometry and computer science* (*Preliminary version 2*), 1992, University of Chicago.
8. F. Behrend, *On sequences of numbers not divisible one by another*, Journal of the London Mathematical Society **10** (1935), 42–44.
9. B. Bollobás, *On generalized graphs*, Acta Math. Acad. Sci. Hungar **16** (1965), 447–452.
10. Béla Bollobás, *Random graphs*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London, 1985.
11. ______, *Combinatorics*, Cambridge University Press, Cambridge, 1986, Set systems, hypergraphs, families of vectors and combinatorial probability.
12. R. C. Bose, *A note on Fisher's inequality for balanced incomplete block designs*, Ann. Math. Statistics **20** (1949), 619–620.
13. Gérard Cohen, Iiro Honkala, Simon Litsyn, e Antoine Lobstein, *Covering codes*, North-Holland Publishing Co., Amsterdam, 1997.
14. Carlos Gustavo T. de A. Moreira e Yoshiharu Kohayakawa, *Bounds for optimal coverings*, submetido, 2001, 14pp.
15. Carlos Gustavo Tamm de Araújo Moreira, *O teorema de Ramsey*, Eureka! **6** (1999), 23–29.

16. N. G. de Bruijn e P. Erdös, *On a combinatorial problem*, Nederl. Akad. Wetensch., Proc. **51** (1948), 1277–1279 = Indagationes Math. **10**, 421–423 (1948).
17. M. Deza, P. Frankl, e N. M. Singhi, *On functions of strength t*, Combinatorica **3** (1983), no. 3-4, 331–339.
18. P. Erdős, *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. **51** (1945), 898–902.
19. ______, *Some remarks on the theory of graphs*, Bull. Amer. Math. Soc. **53** (1947), 292–294.
20. ______, *Some recent problems and results in graph theory, combinatorics and number theory*, Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing (Louisiana State Univ., Baton Rouge, La., 1976) (Winnipeg, Man.), Utilitas Math., 1976, pp. 3–14. Congressus Numerantium, No. XVII.
21. P. Erdős, R. L. Graham, P. Montgomery, B. L. Rothschild, J. Spencer, e E. G. Straus, *Euclidean Ramsey theorems. I*, J. Combinatorial Theory Ser. A **14** (1973), 341–363.
22. ______, *Euclidean Ramsey theorems. II*, Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. I, North-Holland, Amsterdam, 1975, pp. 529–557. Colloq. Math. Soc. János Bolyai, Vol. 10.
23. ______, *Euclidean Ramsey theorems. III*, Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. I, North-Holland, Amsterdam, 1975, pp. 559–583. Colloq. Math. Soc. János Bolyai, Vol. 10.
24. P. Erdős e H. Hanani, *On a limit theorem in combinatorial analysis*, Publ. Math. Debrecen **10** (1963), 10–13.
25. P. Erdős, Chao Ko, e R. Rado, *Intersection theorems for systems of finite sets*, Quart. J. Math. Oxford Ser. (2) **12** (1961), 313–320.
26. P. Erdős e L. Lovász, *Problems and results on 3-chromatic hypergraphs and some related questions*, Infinite and finite sets (Colloq., Keszthely, 1973; dedicated to P. Erdős on his 60th birthday), Vol. II, North-Holland, Amsterdam, 1975, pp. 609–627. Colloq. Math. Soc. János Bolyai, Vol. 10.
27. P. Erdős, A. Sárközy, e E. Szemerédi, *On a theorem of Behrend*, J. Austral. Math. Soc. **7** (1967), 9–16.
28. Paul Erdős, *Combinatorial problems in geometry and number theory*, Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978), Amer. Math. Soc., Providence, R.I., 1979, pp. 149–162.

29. P. Frankl, *The Erdős-Ko-Rado theorem is true for* $n = ckt$, Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976), Vol. I, North-Holland, Amsterdam, 1978, pp. 365–375.
30. P. Frankl e Z. Füredi, *Solution of the Littlewood-Offord problem in high dimensions*, Ann. of Math. (2) **128** (1988), no. 2, 259–270.
31. P. Frankl e V. Rödl, *Strong Ramsey properties of simplices*, to appear.
32. ______, *Near perfect coverings in graphs and hypergraphs*, European J. Combin. **6** (1985), no. 4, 317–326.
33. ______, *A partition property of simplices in Euclidean space*, J. Amer. Math. Soc. **3** (1990), no. 1, 1–7.
34. P. Frankl e R. M. Wilson, *Intersection theorems with geometric consequences*, Combinatorica **1** (1981), no. 4, 357–368.
35. Peter Frankl e Vojtěch Rödl, *All triangles are Ramsey*, Trans. Amer. Math. Soc. **297** (1986), no. 2, 777–779.
36. ______, *Forbidden intersections*, Trans. Amer. Math. Soc. **300** (1987), no. 1, 259–286.
37. Zoltán Füredi, *Matchings and covers in hypergraphs*, Graphs Combin. **4** (1988), no. 2, 115–206.
38. R. L. Graham, *Euclidean Ramsey theorems on the* n*-sphere*, J. Graph Theory **7** (1983), no. 1, 105–114.
39. ______, *Recent trends in Euclidean Ramsey theory*, Discrete Mathematics **136** (1994), no. 1–3, 119–127.
40. ______, *Euclidean ramsey theory*, Handbook of discrete and computational geometry (Jacob E. Goodman e Joseph O'Rourke, eds.), CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1997, pp. 153–166.
41. R. L. Graham e V. Rödl, *Numbers in Ramsey theory*, Surveys in combinatorics 1987 (New Cross, 1987), Cambridge Univ. Press, Cambridge, 1987, pp. 111–153.
42. Ronald L. Graham, Bruce L. Rothschild, e Joel H. Spencer, *Ramsey theory*, second ed., John Wiley & Sons Inc., New York, 1990, A Wiley-Interscience Publication.
43. Heini Halberstam e Klaus Friedrich Roth, *Sequences*, second ed., Springer-Verlag, New York, 1983, MR83m:10094.
44. G. H. Hardy e E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.
45. J. R. Isbell, *An inequality for incidence matrices*, Proc. Amer. Math. Soc. **10** (1959), 216–218.

46. David S. Johnson, *Approximation algorithms for combinatorial problems*, J. Comput. System Sci. **9** (1974), 256–278, Fifth Annual ACM Symposium on the Theory of Computing (Austin, Tex., 1973).
47. Jeff Kahn e Gil Kalai, *A counterexample to Borsuk's conjecture*, Bull. Amer. Math. Soc. (N.S.) **29** (1993), no. 1, 60–62.
48. Gy. Katona, *On a conjecture of Erdős and a stronger form of Sperner's theorem*, Studia Sci. Math. Hungar **1** (1966), 59–63.
49. Daniel J. Kleitman, *On a lemma of Littlewood and Offord on the distribution of certain sums*, Math. Z. **90** (1965), 251–259.
50. ———, *On a lemma of Littlewood and Offord on the distributions of linear combinations of vectors*, Advances in Math. **5** (1970), 155–157 (1970).
51. ———, *Some new results on the Littlewood-Offord problem*, J. Combinatorial Theory Ser. A **20** (1976), no. 1, 89–113.
52. Igor Kříž, *Permutation groups in Euclidean Ramsey theory*, Proc. Amer. Math. Soc. **112** (1991), no. 3, 899–907.
53. ———, *All trapezoids are Ramsey*, Discrete Math. **108** (1992), no. 1-3, 59–62, Topological, algebraical and combinatorial structures. Frolík's memorial volume.
54. D. G. Larman e C. A. Rogers, *The realization of distances within sets in Euclidean space*, Mathematika **19** (1972), 1–24.
55. J. E. Littlewood e A. C. Offord, *On the number of real roots of a random algebraic equation. III*, Rec. Math. [Mat. Sbornik] N.S. **12(54)** (1943), 277–286.
56. L. Lovász, *On the ratio of optimal integral and fractional covers*, Discrete Math. **13** (1975), no. 4, 383–390.
57. D. Lubell, *A short proof of Sperner's lemma*, J. Combinatorial Theory **1** (1966), 299.
58. Kulendra N. Majumdar, *On some theorems in combinatorics relating to incomplete block designs*, Ann. Math. Statistics **24** (1953), 377–389.
59. Jiří Matoušek e Vojtěch Rödl, *On Ramsey sets in spheres*, J. Combin. Theory Ser. A **70** (1995), no. 1, 30–44.
60. L. D. Meshalkin, *A generalization of Sperner's theorem on the number of subsets of a finite set (in Russian)*, Teor. Probab. Ver. Primen. **8** (1964), 219–220, English translation in *Theory of Probab. and its Applications* **8** (1964), 204–205.
61. S. S. Pillai, *On numbers which are not multiples of any other in the set*, Proc. Indian Acad. Sci., Sect. A. **10** (1939), 392–394.
62. Stanisław P. Radziszowski, *Small Ramsey numbers*, Electron. J. Combin. **1** (1994), Dynamic Survey 1, 30 pp. (electronic).
63. F. P. Ramsey, *On a problem of formal logic*, Proceedings of the London Mathematical Society **30** (1930), 264–286.

64. Vojtěch Rödl, *On a packing and covering problem*, European J. Combin. **6** (1985), no. 1, 69–78.
65. Wolfgang M. Schmidt, *Equations over finite fields. An elementary approach*, Springer-Verlag, Berlin, 1976, Lecture Notes in Mathematics, Vol. 536.
66. Oded Schramm, *Illuminating sets of constant width*, Mathematika **35** (1988), no. 2, 180–189.
67. Joel Spencer, *Ramsey's theorem—a new lower bound*, J. Combinatorial Theory Ser. A **18** (1975), 108–115.
68. E. Sperner, *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. **27** (1928), 544–548.
69. S. K. Stein, *Two combinatorial covering theorems*, J. Combinatorial Theory Ser. A **16** (1974), 391–397.
70. Andrew Thomason, *An upper bound for some Ramsey numbers*, J. Graph Theory **12** (1988), no. 4, 509–517.
71. Koichi Yamamoto, *Logarithmic order of free distributive lattice*, J. Math. Soc. Japan **6** (1954), 343–353.