

# PICME/IME/USP COMBINATÓRIA

## NOTAS - 2010

YOSHIHARU KOHAYAKAWA E GUILHERME MOTA (IME/USP)

### 1. $(n, d, \lambda)$ -GRAFOS

01/03/2010

O objeto de estudo desta seção é um tópico bastante estudado por Noga Alon. Sobre este assunto, o leitor pode encontrar uma boa palestra deste pesquisador em

<http://www.pims.math.ca/resources/multimedia>.

Seja  $G$  um grafo com conjunto de vértices  $V(G) = [n] = \{1, \dots, n\}$  e conjunto de arestas  $E$ . A matriz de adjacência  $A = (a_{i,j})_{1 \leq i,j \leq n}$  de  $G$  é a matriz em que  $a_{i,j} = 1$ , caso  $(i, j) \in E$  e  $a_{i,j} = 0$ , caso contrário.

**Definição 1.** Dizemos que  $\lambda$  é autovalor de uma matriz  $A$  se existe um vetor não nulo  $x$  tal que  $Ax = \lambda x$ . Dizemos que  $x$  é um autovetor associado ao autovalor  $\lambda$ .

Como a matriz de adjacência  $A$  é real e simétrica, possui  $n$  autovalores reais, denotados por  $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ , onde estamos considerando  $\lambda_0 \geq \lambda_1 \geq \dots \geq \lambda_{n-1}$  (as vezes supõe-se que  $|\lambda_0| \geq |\lambda_1| \geq \dots \geq |\lambda_{n-1}|$ ) e  $\underline{x}_0, \underline{x}_1, \dots, \underline{x}_{n-1}$  são os autovetores associados, respectivamente, a  $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$ . Ademais, podemos supor que os vetores  $\underline{x}_0, \underline{x}_1, \dots, \underline{x}_{n-1}$  formam uma base ortonormal de  $\mathbb{R}^n$ , isto é,  $\langle \underline{x}_i, \underline{x}_j \rangle = 1$ , se  $i = j$  e  $\langle \underline{x}_i, \underline{x}_j \rangle = 0$ , caso contrário.

Se  $O = [\underline{x}_0 \mid \dots \mid \underline{x}_{n-1}]$ , então  $O^t O = O O^t = I_n$  (matriz identidade). Se  $D$  é a matriz  $O^t A O$ , temos que  $D = \text{diag}(\lambda_0, \lambda_1, \dots, \lambda_{n-1})$ . Portanto,  $A = O D O^t$ , isto é,

$$A = \left( \sum_{i=0}^{n-1} \lambda_i \underline{x}_i \underline{x}_i^t \right),$$

pois  $(\sum_{i=0}^{n-1} \lambda_i \underline{x}_i \underline{x}_i^t) \underline{x}_j = \sum_{i=0}^{n-1} \lambda_i \underline{x}_i (\underline{x}_i^t \underline{x}_j) = \lambda_j \underline{x}_j = A \underline{x}_j$ .

Deste ponto em diante, vamos considerar  $G$  como sendo um grafo  $d$ -regular.

**Fato 2.** *Todo autovalor  $\lambda$  de  $G$  satisfaz  $|\lambda| \leq d$ .*

*Demonstração.* Seja  $\underline{x} = (x_i)^n$  um autovetor associado a  $\lambda$ . Assim,  $A\underline{x} = \lambda\underline{x}$ . Suponha que  $x_p$  seja tal que  $|x_p| \geq |x_i|$ , para todo  $i$ . Então,

$$|\lambda||x_p| = |(\lambda\underline{x})_p| = |(A\underline{x})_p| = \left| \sum_{j=1}^n a_{pj}x_j \right| \leq \sum_{j=1}^n a_{pj}|x_p| = d|x_p|.$$

Como  $\underline{x} \neq \underline{0}$ , então  $|x_p| > 0$ . Portanto,  $|\lambda| \leq d$ . □

Observe que, com a notação que estamos utilizando,  $\lambda_0 = d$ . Ademais,  $\underline{x}_0 = (1, \dots, 1)/\sqrt{n}$ .

**Definição 3.** *Um grafo  $G$  é um  $(n, d, \lambda)$ -grafo se é  $d$ -regular, tem  $n$  vértices e seus autovalores satisfazem  $|\lambda_i| \leq \lambda$ , para  $i = 1, \dots, n-1$ .*

**Fato 4.** *Seja  $G$  um  $(n, d, \lambda)$ -grafo. Se  $d \leq (1 - \varepsilon)n$ , então  $\lambda \geq \sqrt{\varepsilon d}$ .*

*Demonstração.* Seja  $A$  a matriz de adjacência de  $G$ . Assim,  $A^2$  tem autovalores  $\lambda_0^2, \lambda_1^2, \dots, \lambda_{n-1}^2$ , onde  $\lambda_0, \lambda_1, \dots, \lambda_{n-1}$  são os autovalores de  $A$ . Ademais,  $nd = \text{tr}(A^2) = \sum_{i=0}^{n-1} \lambda_i^2$ , onde  $\text{tr}(A)$  é a soma dos elementos da diagonal principal de  $A$ . Portanto,  $nd = \lambda_0^2 + \sum_{i=1}^{n-1} \lambda_i^2 \leq d^2 + (n-1)\lambda^2$ . Concluimos que  $\lambda^2(n-1) \geq nd - d^2 = d(n-d) \geq \varepsilon nd$ , logo  $\lambda^2 \geq \varepsilon d$ . □

Existem construções determinísticas de  $(n, d, \lambda)$ -grafos. Duas importantes construções foram feitas por Lubotzky, Phillips e Sarnak [14] e Margulis [15]. Os grafos obtidos nestas construções são tais que  $\lambda = 2\sqrt{d-1}$ . Estes grafos são chamados *grafos de Ramanujan*.

**Definição 5.** *Seja  $G = (V, E)$  um grafo. Denotamos por  $e(U, W)$  a quantidade de arestas com uma extremidade em  $U$  e a outra em  $W$ , onde as arestas que possuem as duas extremidades em  $U \cap W$  são contadas duas vezes. Isto é,  $e(U, W) = |\{(u, w) : u \in U, w \in W \text{ e } \{u, w\} \in E(G)\}|$ .*

**Teorema 6** (*Expander Mixing Lemma*). *Seja  $G$  um  $(n, d, \lambda)$ -grafo. Então, para todo  $U, W \subset V(G)$ , temos que*

$$\left| e(U, W) - \frac{d|U||W|}{n} \right| \leq \lambda\sqrt{|U||W|}.$$

*Observação 1.* Se  $U = W$ , temos que  $|e(U, U) - d|U|^2/n| \leq \lambda|U|$ . Ademais,  $e(U, U)$  é igual a duas vezes o número de arestas induzidas por  $U$ , que denotamos por  $e(U)$ . Portanto, temos que  $|2e(U) - d|U|^2/n| \leq \lambda|U|$ , isto é,  $|e(U) - d|U|^2/2n| \leq (\lambda/2)|U|$ .

*Observação 2.*  $\alpha(G) = \max_I |I|$ , onde o máximo é tomado sobre os conjuntos  $I \subset V(G)$  que são independentes (estáveis), isto é, que não induzem nenhuma aresta. Se  $I \subset V(G)$  é independente,

então  $e(I) = 0$ . O Teorema 6 diz que  $d|I|^2/2n \leq (\lambda/2)|I|$ , isto é,  $|I| \leq (n/d)\lambda$ . Portanto, concluímos que  $\alpha(G) \leq \lambda(n/d)$  para todo  $(n, d, \lambda)$ -grafo.

*Observação 3.* Se  $G$  é um  $(n, d, \lambda)$ -grafo, então

$$\chi(G) \geq \frac{n}{\alpha(G)} \geq \frac{n}{\frac{\lambda n}{d}} = \frac{d}{\lambda}.$$

*Demonstração do Teorema 6.* Fixe  $U, W \subset V(G)$ . Sejam  $\chi_U = (\chi_{U,i})^n$  e  $\chi_W$  os vetores característicos de  $U$  e  $W$ , isto é,  $\chi_{U,i} = 1$ , se  $i \in U$  e  $\chi_{U,i} = 0$ , caso contrário (analogamente para  $\chi_W$ ). Temos que  $e(U, W) = \chi_U^t A \chi_W$ . Lembre que  $A = \sum_{i=0}^{n-1} \lambda_i \underline{x}_i \underline{x}_i^t = \lambda_0 \underline{x}_0 \underline{x}_0^t + \sum_{i=1}^{n-1} \lambda_i \underline{x}_i \underline{x}_i^t$ , onde dizemos que  $A_0 = \lambda_0 \underline{x}_0 \underline{x}_0^t$  (termo principal) e  $E = \sum_{i=1}^{n-1} \lambda_i \underline{x}_i \underline{x}_i^t$  (termo de erro). Temos  $\chi_U = \sum_{i=0}^{n-1} \alpha_i \underline{x}_i$  e  $\chi_W = \sum_{i=0}^{n-1} \beta_i \underline{x}_i$ , onde  $\alpha_i = \langle \chi_U, \underline{x}_i \rangle = \chi_U^t \underline{x}_i$  e  $\beta_i = \langle \chi_W, \underline{x}_i \rangle = \chi_W^t \underline{x}_i$ .

Observe que  $A_0$  é a matriz com todas as posições tendo valor  $d/n$ , pois  $\underline{x}_0 = (1, \dots, 1)/\sqrt{n}$  e  $\lambda_0 = d$ . Assim, fica fácil ver que  $\chi_U^t A_0 \chi_W = d|U||W|/n$ . Ademais

$$\begin{aligned} \chi_U^t E \chi_W &= \left( \sum_{i=0}^{n-1} \alpha_i \underline{x}_i^t \right) \left( \sum_{j=1}^{n-1} \lambda_j \underline{x}_j \underline{x}_j^t \right) \left( \sum_{k=0}^{n-1} \beta_k \underline{x}_k \right) \\ &= \left( \sum_{i=0}^{n-1} \alpha_i \underline{x}_i^t \right) \left( \sum_{k=1}^{n-1} \lambda_k \beta_k \underline{x}_k \right) \\ &= \left( \sum_{k=1}^{n-1} \lambda_k \alpha_k \beta_k \right). \end{aligned}$$

Com isso, temos que  $|\chi_U^t E \chi_W| \leq \sum_{k=1}^{n-1} |\lambda_k| |\alpha_k| |\beta_k|$ . Utilizando a desigualdade de Cauchy–Schwarz,

$$\begin{aligned} |\chi_U^t E \chi_W| &\leq \lambda \sum_{k=0}^{n-1} |\alpha_k| |\beta_k| \\ &\leq \lambda \left( \sum_{k=0}^{n-1} \alpha_k^2 \right)^{1/2} \left( \sum_{k=0}^{n-1} \beta_k^2 \right)^{1/2} \\ &= \lambda \sqrt{|U|} \sqrt{|W|}. \end{aligned}$$

Assim,  $e(U, W) = \chi_U^t A \chi_W = (d/n)|U||W| + O_1(\lambda \sqrt{|U||W|})$ , onde  $O_1(x)$  denota um valor  $y$  tal que  $|y| \leq x$ . □

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

1. Suponha que  $G = (X, Y; E)$  seja um grafo bipartido. Mostre que, se  $\lambda$  é um autovalor de  $G$ , então  $-\lambda$  também o é.
2. Considere um grupo com  $n$  pessoas. Suponha que, para quaisquer duas pessoas  $x$  e  $y$  do grupo, exista uma terceira pessoa  $z$  tal que  $x$  e  $y$  conhecem  $z$ . Prove que existe uma pessoa do grupo que conhece todas as outras.

08/03/2010

Intuitivamente, dizemos que um grafo  $G$  é *expansor* se todo conjunto  $U \subset V(G)$  possui muitos vizinhos.

**Definição 7.** Considere um grafo  $G = (V, E)$  e  $U \subset V$ . Dizemos que  $\Gamma_G(U)$  é a vizinhança de  $U$  em  $G$ , isto é,  $\Gamma_G(U) = \{w \in V(G) : \{v, w\} \in E(G), v \in U\}$ . Quando é claro qual o grafo em questão, podemos simplesmente utilizar  $\Gamma(U)$ .

**Definição 8.** Um grafo  $G$  é um  $(b, f)$ -expansor se  $|\Gamma(U)| \geq f|U|$ , para todo  $U \subset V(G)$  tal que  $|U| \leq b$ .

Claramente, se  $\Delta(G)$  denota o grau máximo de um vértice em  $G$ , então  $|\Gamma(U)| \leq \Delta|U|$ .

Vamos provar que qualquer subgrafo  $H$  de um  $(n, d, \lambda)$ -grafo é expansor, desde que  $\delta(H)$  (grau mínimo de um vértice em  $H$ ) seja limitado inferiormente.

**Teorema 9.** Seja  $G$  um grafo. Se  $H$  é um subgrafo de  $G$  tal que  $\delta(H) \geq \delta d$ , com  $0 < \delta \leq 1$ , então  $H$  é um  $((1 - \eta)\delta n/f, f)$ -expansor, onde  $f = (n\delta d/\lambda)^2$ , para todo  $0 < \eta < 1$ .

*Demonstração.* Suponha, por contradição, que  $H$  não seja um  $((1 - \eta)\delta n/f, f)$ -expansor, isto é, existe um subconjunto  $U$  de vértices de  $H$  tal que  $|U| \leq (1 - \eta)\delta n/f$  e  $|\Gamma_H(U)| < f$ . Observe que  $\delta d|U| \leq e_H(U, \Gamma_H(U)) \leq e_G(U, \Gamma_H(U))$ . Pelo Teorema 6, temos que

$$\begin{aligned} \delta d|U| &\leq \frac{d}{n}|U||\Gamma_H(U)| + \lambda\sqrt{|U||\Gamma_H(U)|} \\ &\leq \frac{d}{n}|U|(f|U|) + \lambda\sqrt{|U||\Gamma_H(U)|} \\ &\leq \frac{d}{n}|U|(1 - \eta)\delta n + \lambda\sqrt{|U||\Gamma_H(U)|}. \end{aligned}$$

Assim,  $\eta\delta d|U| < \lambda\sqrt{|U||\Gamma_H(U)|}$ . Portanto,  $|\Gamma_H(U)| > (\eta\delta d/\lambda)^2|U| = f|U|$ . Mas isto contradiz a escolha de  $U$ . □

Enunciamos a seguir um importante lema obtido por Lajos Pósa.

**Lema 10** (Lema de Pósa). *Sejam  $G$  um grafo não vazio e  $b$  um inteiro positivo tal que, para todo  $X \subset V(G)$ , com  $|X| \leq b$ , temos  $|\Gamma(X) \setminus X| \geq 2|X| - 1$ . Então  $G$  contém um  $p^{3b-1}$  (caminho com  $3b - 1$  vértices).*

É um bom exercício provar o lema acima.

### 3. GRAFOS EXPANSORES - PARTE II

15/03/2010

Inicialmente, vamos relembrar algumas definições.

**Definição 11.** O número de Ramsey é dado por  $R(n) = \min\{N: K^N \rightarrow (K^n, K^n)\}$ , onde a notação  $G \rightarrow (H_1, H_2)$  significa que ao colorir as arestas do grafo  $G$  com as cores azul e vermelho, existe, em  $G$ , uma cópia de  $H_1$  somente com arestas azuis ou uma cópia de  $H_2$  somente com arestas vermelhas.

Observe que podemos generalizar o conceito de números de Ramsey.

**Definição 12.** O número de Ramsey generalizado é dado por  $r(H) = \min\{N: K^N \rightarrow (H, H)\}$ .

O seguinte teorema nos dá uma cota superior para o número de Ramsey generalizado.

**Teorema 13** (Chvátal–Rödl–Szemerédi–Trotter [3]). *Para todo  $\Delta > 0$ , existe um  $c > 0$  tal que se  $H$  é um grafo com  $n$  vértices e grau máximo  $\Delta(H) \leq \Delta$ , então  $r(H) \leq cn$ .*

Podemos definir também o número de Ramsey relativo às arestas de um grafo. Definimos tal número por  $r_a(H) = \min\{e(G): G \rightarrow (H, H)\}$ .

*Observação.* Se  $\Delta(H) \leq \Delta$ , então, utilizando o Teorema 13, temos que

$$r_a(H) \leq \binom{r(H)}{2} \leq \binom{cn}{2} \leq \frac{1}{2}(cn)^2 = c'n^2.$$

Paul Erdős fez a seguinte pergunta (oferecendo \$ 100,00 para quem resolvesse): É verdade que  $r_a(P^n) \ll \binom{n}{2}$ ? József Beck forneceu a resposta a esta questão mostrando que  $r_a(P^n) \leq cn$ , para algum  $c > 0$ , porém, através de uma prova não construtiva [2]. Em 1988, Noga Alon e Fan Chung deram uma prova construtiva utilizando  $(n, d, \lambda)$ -grafos [1]. Abaixo mostramos um esboço da prova de Alon e Chung.

Seja  $G^N$  um  $(N, d, \lambda)$ -grafo com  $\lambda \ll d = O(1)$  (lembre-se que tais grafos existem [14, 15]). Fixe  $H \subset G$  com  $e(H) \geq e(G)/2$ . Afirmamos que se  $N, d$  e  $\lambda$  forem escolhidos apropriadamente, então  $H \supset P^n$ . De fato, basta que consigamos  $d = O(1)$  e  $N = O(n)$ . Isto prova o resultado.

Observe que  $H$  contém um subgrafo  $H'$  com  $\delta(H') \geq d/4$ . De fato, seja inicialmente  $H' = H$ . Eliminamos vértices de  $H'$ , sucessivamente, enquanto houver vértices com grau menor que  $d/4$ . Se exaurirmos o conjunto de vértices, temos menos que  $Nd/4 = e(G)/2$  arestas em  $H$ , uma contradição com a escolha de  $H$ . Logo, ao término deste processo temos o grafo  $H'$  desejado.

Com isso, sabemos que  $H'$  é um  $(b, f)$ -expansor, para todo  $0 < f \leq (d/(8\lambda))^2$  e  $b = N/8f$  (para obter tais valores, faça  $\delta = 1/4$  e  $\eta = 1/2$  no Teorema 9). Suponha que  $(d/(8\lambda))^2 \geq 3$ . Então, temos que  $H'$  é um  $(N/24, 3)$ -expansor.

Tomando  $b = \lfloor N/24 \rfloor$ , temos que se  $X \subset V(H')$  com  $|X| \leq \lfloor N/24 \rfloor$ , então  $|\Gamma(X)| \geq 3|X|$ . Portanto,  $|\Gamma(X) \setminus X| \geq 2|X| \geq 2|X| - 1$ . Pelo Lema 10 (Lema de Pósa), sabemos que  $H' \supset P^{3b-1}$ , mas  $3b - 1 = 3\lfloor N/24 \rfloor - 1 \geq 3(N/24 - 1) - 1 = N/8 - 4$ . Portanto, escolhendo  $N \geq 8n + 32$ , temos que  $3b - 1 \geq n$ . Assim,  $H' \supset P^n$ , concluindo a esboço da prova.

Vamos agora provar o Lema de Pósa (Lema 10).

**Definição 14.** Dado um grafo  $G = (V, E)$ , seja  $P$  um caminho entre vértices  $x$  e  $y$  em  $G$ . Se  $z$  é um vizinho de  $y$  que está em  $P$  mas não é o vizinho de  $y$  em  $P$ , existe um vizinho  $z'$  de  $z$ , de modo que podemos gerar um novo caminho  $P'$  de mesmo tamanho que  $P$  adicionando a aresta  $\{y, z\}$  e removendo a aresta  $\{z, z'\}$  (veja Figura 1). Chamamos esta transformação de troca de caminho.

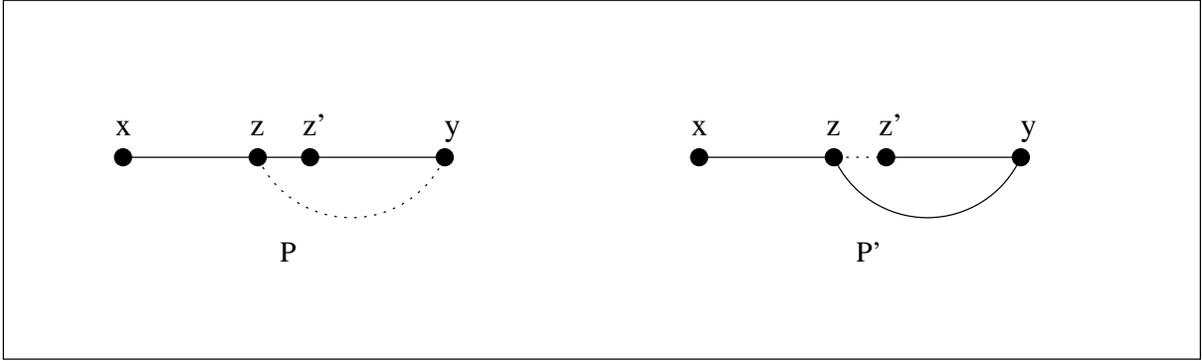


FIGURA 1. Troca de caminho de  $P$  para  $P'$ .

*Demonstração do Lema de Pósa.* Seja  $P$  um caminho máximo no grafo  $G$  e  $\mathcal{P}$  o conjunto de todos os caminhos obtidos a partir de  $P$  através de troca de caminhos. Se  $X$  é o conjunto dos extremos de caminhos em  $\mathcal{P}$ , defina  $X^-$  e  $X^+$  como os conjuntos de vértices que, respectivamente, antecedem e sucedem imediatamente os elementos de  $X$  em  $P$ .

Mostraremos inicialmente que  $\Gamma(X) \subset X^- \cup X \cup X^+$ . Considere um caminho  $P' \in \mathcal{P}$  que começa em um vértice  $x \in X$  (tal caminho existe, pela definição de  $X$ ) e seja  $y \in V(G) \setminus X^- \cup X \cup X^+$ . Se  $y \in V(G) \setminus V(P)$ , então, como  $P'$  é máximo,  $x$  e  $y$  não são adjacentes. Suponha agora que  $y \in V(P) \setminus X^- \cup X \cup X^+$ . Assim,  $y$  possui os mesmos vizinhos em qualquer caminho de  $\mathcal{P}$ , pois uma troca de caminhos que torna  $y$  não adjacente a algum desses vizinhos faria com que  $y$  ou tal vizinho pertencesse a  $X$ , uma contradição, pois  $y \notin X^- \cup X \cup X^+$ . Portanto, uma troca de

caminhos aplicada em  $P'$  faria com que  $y$  fosse vizinho de um elemento em  $X$ , uma contradição. Logo,  $x$  e  $y$  não podem ser adjacentes, de onde concluímos que todos os vizinhos de vértices em  $X$  estão em  $X^- \cup X \cup X^+$ .

Sabendo que  $\Gamma(X) \subset X^- \cup X \cup X^+$ , considere um caminho máximo  $P$  em  $G$ . Assim, temos que  $\Gamma(X) \setminus X \subset X^- \cup X^+$ , de onde concluímos que  $|\Gamma(X) \setminus X| \leq 2|X| - 2$ . Pela hipótese no enunciado do Lema de Pósa,  $|X| > b$ . Logo, existe  $X' \subset X$  tal que  $|X'| = b$  e, portanto, temos  $|\Gamma(X') \setminus X'| \geq 2|X'| - 1$ . Mas, como  $X' \cup \Gamma(X') \subset V(P)$ , temos que

$$|V(P)| \geq |X' \cup \Gamma(X')| = |X'| + |\Gamma(X') \setminus X'| \geq 3|X'| - 1 = 3b - 1.$$

Portanto, existe um  $P^{3b-1}$  em  $G$ . □

22/03/2010

**Definição 15.** Dado um grafo  $G$ , um emparelhamento é um subconjunto de arestas não adjacentes de  $G$ . Ademais, dizemos que  $M$  cobre  $U \subset V(G)$  se todo vértice de  $U$  é extremo de alguma aresta em  $M$ .

**Teorema 16** (Teorema de Hall [11]). *Seja  $B = (U, W; E)$  um grafo bipartido. Se, para todo  $U' \subset U$ , temos que  $|\Gamma_B(U')| \geq |U'|$ , então  $B$  possui um emparelhamento que cobre  $U$ .*

*Demonstração (Rado [18]).* Remova as arestas de  $B$  até que a hipótese seja satisfeita de forma minimal, isto é, se removermos qualquer outra aresta de  $B$ , a hipótese falha. Se  $B$  não contém vértices  $u_1, u_2 \in U$  e  $w \in W$  tais que  $\{u_1, w\}, \{u_2, w\} \in E$ , então, claramente, existe um emparelhamento que cobre  $U$ . Portanto, supomos que existem tais vértices  $u_1, u_2$  e  $w$ . Como removemos arestas de forma que a hipótese seja válida minimalmente, existem  $U_1, U_2 \subset U$  (com  $u_1 \in U_1$  e  $u_2 \in U_2$ ) tais que a hipótese falha para  $B_i = B - \{u_i, w\}$ , com  $i = \{1, 2\}$ . Assim,  $|\Gamma_B(U_i)| = |U_i|$ , para  $i = \{1, 2\}$ . Ademais,  $w \notin \Gamma_B(U_1 \setminus \{u_1\})$  e  $w \notin \Gamma_B(U_2 \setminus \{u_2\})$ . Concluimos então que

$$w \cup (\Gamma_B(U_1 \setminus \{u_1\}) \cap \Gamma_B(U_2 \setminus \{u_2\})) \subset (\Gamma_B(U_1) \cap \Gamma_B(U_2)),$$

onde  $w \notin \Gamma_B(U_1 \setminus \{u_1\}) \cap \Gamma_B(U_2 \setminus \{u_2\})$ . Portanto,

$$\begin{aligned} |\Gamma_B(U_1) \cap \Gamma_B(U_2)| &\geq |\Gamma_B(U_1 \setminus \{u_1\}) \cap \Gamma_B(U_2 \setminus \{u_2\})| + 1 \\ &\geq |\Gamma_B(U_1 \setminus \{u_1\}) \cap U_2 \setminus \{u_2\}| + 1 \\ &= |\Gamma_B(U_1 \cap U_2)| + 1. \end{aligned}$$

Podemos então concluir que

$$\begin{aligned} |\Gamma_B(U_1 \cup U_2)| &= |\Gamma_B(U_1) \cup \Gamma_B(U_2)| = |\Gamma_B(U_1)| + |\Gamma_B(U_2)| - |\Gamma_B(U_1) \cap \Gamma_B(U_2)| \\ &\leq |\Gamma_B(U_1)| + |\Gamma_B(U_2)| - (|\Gamma_B(U_1 \cap U_2)| + 1) \\ &= |U_1| + |U_2| - |\Gamma_B(U_1 \cap U_2)| - 1 \\ &\leq |U_1| + |U_2| - |U_1 \cap U_2| - 1 \\ &= |U_1 \cup U_2| - 1, \end{aligned}$$

uma contradição. □

Provaremos agora um resultado de Friedman e Pippenger [9] sobre contenção de árvores em certos grafos com propriedades de expansão. Para isso, precisamos de algumas definições.

**Definição 17.** *Seja  $G$  um grafo,  $T$  uma árvore e  $n, d$  inteiros positivos. Dizemos que uma árvore  $T$  é  $(n, d)$ -pequena, ou simplesmente pequena se  $|V(T)| \leq n$  e  $\Delta(T) \leq d$ .*

Lembre-se que um grafo  $G$  é dito  $(b, f)$ -expansor se  $|\Gamma(X)| \geq f|X|$ , para todo  $X \subset V(G)$  tal que  $|X| \leq b$ . No Teorema 19, denotamos um  $(2n - 2, d + 1)$ -expansor simplesmente por *expansor*.

**Definição 18.** *Uma imersão de um grafo  $H$  em um grafo  $G$  é uma função injetiva  $f : V(H) \rightarrow V(G)$  com  $\{f(x), f(y)\} \in E(G)$  para todo  $\{x, y\} \in E(H)$ , isto é,  $f$  preserva adjacências.*

**Teorema 19** (Friedman–Pippenger [9]). *Fixe  $n, d > 0$ . Todo grafo expansor não vazio  $G$  contém toda árvore  $(n, d)$ -pequena  $T$ .*

*Demonstração.* Fixe  $f : V(T) \rightarrow V(G)$  uma imersão de  $T$  em  $G$ . Definimos:

1. Para todo  $x \in V(G)$ , defina  $J_f(x) = \deg_T(f^{-1}(x))$ , se  $x \in f(V(T))$ , e 0, caso contrário.
2.  $A_f(X) = |\Gamma_G(X) \setminus f(V(T))|$ , onde  $X \subset V(G)$ .
3.  $B_f(X) = \sum_{x \in X} B_f(x)$ , onde  $B_f(x) = d - J_f(x)$  e  $X \subset V(G)$ .
4.  $C_f(X) = A_f(X) - B_f(X)$ , onde  $X \subset V(G)$ .

Dizemos que um conjunto  $X \subset V(G)$  é *solvente* se  $C_f(X) \geq 0$ , é *crítico* se  $C_f(X) = 0$  e é *falido* se  $C_f(X) < 0$ . Uma imersão é dita *boa* se todo  $X \subset V(G)$ , com  $|X| \leq 2n - 2$ , é solvente. Vamos provar as seguintes proposições.

$P_1$ . Se  $|V(T)| = 1$ , então qualquer imersão  $f : V(T) \rightarrow V(G)$  é boa.

$P_2$ . Seja  $v$  uma folha de  $T$  e  $S = T - v$ . Se  $f : V(S) \rightarrow V(G)$  é uma imersão boa, então existe uma extensão  $g : V(T) \rightarrow V(G)$  que é boa.

Observe que isso prova o resultado. □

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

Nos exercícios abaixo, dado um grafo  $G$ , denote por  $r(G)$  o número máximo de arestas em uma floresta (grafo acíclico) contida em  $G$ .

1. Suponha que  $F_1, F_2, \dots, F_n$  sejam  $n$  florestas com conjunto de vértices  $[n]$ . Imaginemos que  $F_i$  seja *colorido* com a cor  $i$ , para  $i = 1, \dots, n$ . Suponha que, para todo  $I \subset [n - 1]$ , temos  $r(\bigcup_{i \in I} F_i) \geq |I|$ . Mostre que  $\bigcup_{i=1}^{n-1} F_i$  contém uma árvore geradora (floresta com  $n - 1$  arestas) multicolorida, isto é, onde todas suas arestas têm cores diferentes.

2. Seja  $V$  um espaço vetorial de dimensão finita. Considere  $F_i \subset (V)$ , para  $i = 1, \dots, N$ . Suponha que, para todo  $I \subset [N]$ , temos  $r(\bigcup_{i \in I} F_i) \geq |I|$ , onde  $r(X) = \dim \langle X \rangle$ . Mostre que existe  $T = (t_i)^N$ , com  $t_i \in F_i$  para todo  $i = 1, \dots, N$  e  $t_1, \dots, t_N$  linearmente independentes.
3. Seja  $B = (U, W; E)$  um grafo bipartido e  $k \in \mathbb{N}$  fixo. Suponha que, para todo  $U' \subset U$ , temos  $|\Gamma(U')| \geq k|U'|$ . Prove que existe  $H \subset B$  tal que, para todo  $u \in U$ , vale  $d_H(u) = 3$  e, para todo  $w \in W$ , vale  $d_H(w) \leq 1$ .
4. Demonstre a proposição  $P_1$  na prova do Teorema 19.

05/04/2010

Dando continuidade à prova do Teorema 19 sobre contenção de árvores *pequenas* em expansores, precisamos provar a proposição  $P_2$  enunciada na seção anterior. Dados  $n, d > 0$ , seja  $G$  um  $(2n - 2, d + 1)$ -expansor (por simplicidade, chamemos somente de *expansor*) e  $T$  uma árvore pequena ( $|V(T)| \leq n$  e  $\Delta(T) \leq d$ ). Relembrando:

$P_2$ . Seja  $v$  uma folha de  $T$  e  $S = T - v$ . Se  $f : V(S) \rightarrow V(G)$  é uma imersão boa, então existe uma extensão  $g : V(T) \rightarrow V(G)$  que é boa.

Nos três lemas abaixo, que nos permitiram provar a proposição  $P_2$ , considere um expansor  $G$ , uma árvore pequena  $T$  e  $S = T - v$ , onde  $v$  é uma folha de  $T$ .

**Lema 20.** *Seja  $X \subset V(G)$ . Se  $C_f(X) = 0$  e  $|X| \leq 2n - 2$ , então  $|X| \leq n - 1$ .*

*Demonstração.* Observe que  $|\Gamma_G(X)| \geq (d + 1)|X|$ . Assim,

$$A_f(X) \geq (d + 1)|X| - |f(V(S))| = d|X| + |X| - (n - 1).$$

Ademais,  $B_f(X) \leq d|X|$ . Portanto,  $0 = C_f(X) \geq d|X| + |X| - n + 1 - d|X|$ , isto é,  $|X| \leq n - 1$ .  $\square$

**Definição 21.** *Seja  $Z$  um conjunto. Dizemos que uma função  $\varphi : \mathcal{P}(Z) \rightarrow \mathbb{R}$  é submodular se, para todos  $A, B \subset Z$ , temos que  $\varphi(A \cup B) + \varphi(A \cap B) \leq \varphi(A) + \varphi(B)$ .*

**Lema 22.** *Prove que  $C_f(X)$  é submodular.*

*Demonstração.* Exercício 2.

**Lema 23.** *Seja  $f$  uma imersão boa e  $X, Y \subset V(G)$  tais que  $C_f(X), C_f(Y) = 0$  e  $|X|, |Y| \leq n - 1$ . Assim, temos que  $C_f(X \cup Y) = 0$  e  $|X \cup Y| \leq n - 1$ .*

*Demonstração.* Temos que  $|X \cup Y|, |X \cap Y| \leq 2n - 2$ . Como  $f$  é boa e  $C_f(X)$  é submodular (pelo Lema 22), temos que

$$0 \leq C_f(X \cup Y) + C_f(X \cap Y) \leq C_f(X) + C_f(Y) = 0.$$

Portanto,  $C_f(X \cup Y), C_f(X \cap Y) = 0$ . Pelo Lema 20,  $|X \cup Y| \leq n - 1$ .  $\square$

*Demonstração da proposição  $P_2$ .* Seja  $T$  uma árvore pequena e  $S$  a árvore obtida através da remoção de uma folha  $v$  de  $T$  e a aresta  $\{v, w\}$  incidente a  $v$ . Considere  $\xi$  o conjunto das imersões que são

extensões de  $F$  para  $T$ . Tome  $Y = \Gamma_G(f(w)) \setminus f(V(S))$ . O mapeamento  $g \mapsto g(v)$  é, claramente, uma bijeção entre  $\xi$  e  $Y$ .

Suponha, por contradição, que nenhuma extensão  $g \in \xi$  é boa. Assim, para cada  $g \in \xi$ , existe um conjunto  $X_g \subset V(G)$  com  $|X_g| \leq 2n - 2$  tal que

$$(1) \quad C_g(X_g) < 0.$$

Como  $f$  é uma imersão boa, temos que

$$(2) \quad C_f(X_g) \geq 0.$$

Temos que  $g(V(T)) = (\text{im } f) \cup \{g(v)\} = f(V(S)) \cup \{g(v)\}$ . Ademais,  $A_g(X) = |\Gamma_G(X) \setminus g(V(T))|$ , isto é,  $A_g(X) = A_f(X) - [g(v) \in \Gamma_G(X)]$ , onde  $[p] = 1$  se  $p$  é válido e  $[p] = 0$  se  $p$  é falso. Observe que, como  $E(T) = E(S) \cup \{v, w\}$ , temos  $B_g(X) = B_f(X) - [f(w) \in X] - [g(v) \in X]$ . Assim, temos que  $C_g(X) = C_f(X) - [g(v) \in \Gamma_G(X)] + [f(w) \in X] + [g(v) \in X]$ .

Por (1) e (2), deduzimos que, para toda extensão  $g \in \xi$ , valem as seguintes quatro afirmações:

- 1)  $C_f(X_g) = 0$ .
- 2)  $g(v) \in \Gamma_G(X_g)$ .
- 3)  $f(w) \in X_g$ .
- 4)  $g(v) \notin X_g$ .

Ponha  $X^* = \bigcup_{g \in \xi} X_g$ . Pelo Lema 20,  $|X_g| \leq n - 1$ , para todo  $g \in \xi$ . Assim, por indução e pelo Lema 23, temos que  $C_f(X^*) = 0$  e  $|X^*| \leq n - 1$ . Ponha agora  $X' = X^* \cup \{f(w)\}$ . Temos que  $|X'| \leq n$ . Como  $f$  é boa,  $C_f(X') \geq 0$ .

Sabemos que  $g(v) \in \Gamma_G(X_g)$  para toda extensão  $g \in \xi$ . Assim,  $Y \subset \Gamma_G(X^*)$ . Portanto,

$$\begin{aligned} A_f(X') &= A_f(X^* \cup f(w)) \\ &= \Gamma_G(X^* \cup f(w)) \setminus f(V(S)) \\ &= \Gamma_G(X^*) \setminus f(V(S)) \\ &= A_f(X^*). \end{aligned}$$

Temos  $f(w) \notin X_g$  para toda extensão  $g \in \xi$ . Portanto,  $f(w) \notin X^*$ . Portanto, temos que  $B_f(X') = B_f(X^*) + B_f(f(w)) = B_f(X^*) + d - J_f(f(w)) > B_f(X^*)$ . Logo, podemos concluir que  $0 \leq C_f(X') = A_f(X') - B_f(X') < A_f(X^*) - B_f(X^*) = C_f(X^*) = 0$ , uma contradição.

□

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

1. Seja  $G$  um grafo e  $X \subset V(G)$ . Mostre que  $\varphi(X) = |\Gamma_G(X)|$  é submodular.
2. Prove o Lema 22.

12/04/2010

**Definição 24.** Um hipergrafo  $l$ -uniforme (ou  $l$ -grafo) é um par  $(X, \mathcal{M})$  com  $\mathcal{M} \subset \binom{X}{l}$ , onde temos que  $\binom{X}{l} = \{U \subset X : |U| = l\}$ .

**Definição 25.** Um hipergrafo  $G = (X, \mathcal{M})$  é dito  $a$ -partido se existe uma partição  $\{X_1, X_2, \dots, X_a\}$  de  $X$  em que cada aresta de  $\mathcal{M}$  contém no máximo um vértice de cada classe de vértices da partição.

*Observação.* Um grafo é um 2-grafo.

**Definição 26.** Um circuito de tamanho  $p$  em um hipergrafo  $(X, \mathcal{M})$  é uma sequência  $M_1, \dots, M_p$  de arestas diferentes de  $\mathcal{M}$  onde existem diferentes vértices  $x_i \in M_i \cap M_{i+1}$ , com  $i \in \{1, 2, \dots, p-2\}$  e  $x_p \in M_1 \cap M_p$ .

**Definição 27.** A cintura  $g(G)$  de um hipergrafo  $G$  é o comprimento do menor circuito em  $G$ .

Apresentamos, nesta seção, uma prova construtiva da existência de hipergrafos com número cromático e cintura arbitrariamente grandes. Formalmente, provamos o seguinte resultado.

**Teorema 28** (Nešetřil–Rödl [17]). *Para quaisquer inteiros positivos  $l, n, p$ , existe um  $l$ -grafo  $(X, \mathcal{M})$  tal que*

- 1) *Todos os circuitos de  $(X, \mathcal{M})$  tem tamanho maior que  $p$ .*
- 2)  $\chi(X, \mathcal{M}) > n$ .

Antes de provar o Teorema 28, precisamos definir uma operação entre certos hipergrafos. Dados

- $((X_i), \mathcal{M})$  um  $l$ -grafo  $a$ -partido, onde  $(X_i)$  é a partição  $\{X_1, X_2, \dots, X_a\}$  de um conjunto  $X$  e  $|X_r| = k$  para um  $r \in [1, a]$  fixo,
- $(Y, \mathcal{N})$  um  $k$ -grafo,

dizemos que  $(Y, \mathcal{N}) *_r ((X_i), \mathcal{M})$  é o  $l$ -grafo  $a$ -partido  $((X'_i), \mathcal{M}')$ , onde os vértices desse hipergrafo são definidos por

- $X'_i = X_i \times \mathcal{N}$ , para  $i \neq r$ ,
- $X'_r = Y$ ,

e uma hiperaresta  $M'$  pertence a  $\mathcal{M}'$  se e somente se existem  $N \in \mathcal{N}$  e  $M \in \mathcal{M}$  tais que

- $M' \cap X'_i = (M \cap X_i, N)$ , para  $i \neq r$ ,
- $M' \cap X'_r = \iota_N(M \cap X_r)$ ,

---

<sup>1</sup>Os resultados desta seção foram apresentados pelo aluno Marcelo Matheus Gauy.

onde  $\iota_N: X_r \rightarrow N$  é uma bijeção, para  $N \in \mathcal{N}$ . Denotados uma hiperaresta  $M' \in \mathcal{M}'$  por um par  $(M, N)$ . Na Figura 2, temos um exemplo mostrando o que acontece com uma aresta que contém interseção com  $X_r$  quando realizamos esta operação.

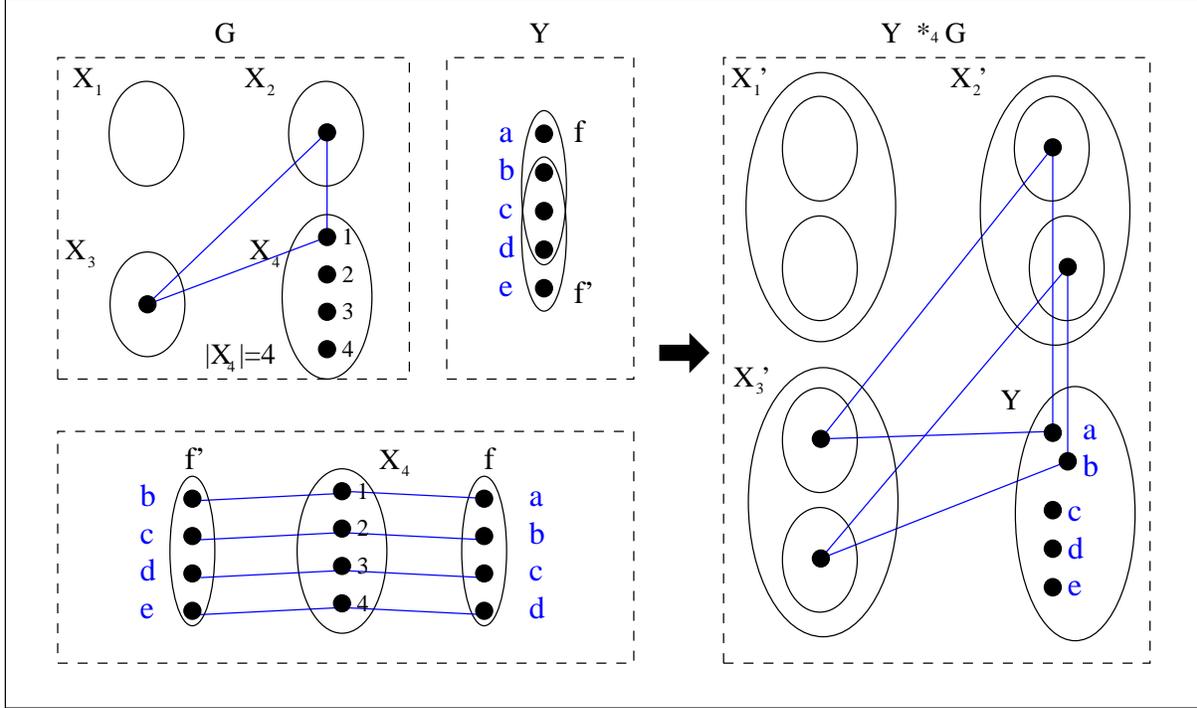


FIGURA 2. Resultado da operação  $Y *_4 G$  em um 4-grafo  $Y$  e um 3-grafo  $G$  com partição  $\{X_1, X_2, X_3, X_4\}$ , onde  $|X_4| = 4$ . Do lado esquerdo temos os hipergrafos  $G$  e  $Y$  e as bijeções  $\iota_f$  e  $\iota_{f'}$ . Do lado direito temos o resultado da operação.

*Demonstração do Teorema 28.* Fixe  $n, l$ . Provamos o resultado utilizando indução em  $p$ . Se  $p = 1$ , o resultado é válido, pois não temos restrição alguma quanto ao tamanho dos circuitos. Tome  $p > 1$  e suponha que o resultado é válido para  $1 \leq p' < p$ . Seja  $a = (l - 1)n + 1$  e considere o  $l$ -grafo  $a$ -partido  $((X_i^1), \mathcal{M}^1)$  onde, para cada conjunto de  $l$  partes  $\omega \subset [1, a]$  com  $|\omega| = l$ , existe uma aresta  $M \in \mathcal{M}^1$  onde  $M \cap X_i^1 \neq \emptyset$  para todo  $i \in \omega$ . Claramente,  $((X_i^1), \mathcal{M}^1)$  pode ser escolhido de modo a não conter circuitos de tamanho menor ou igual a  $p$ , pois podemos utilizar quantos vértices forem necessários em cada  $X_i$ .

Indutivamente, definimos  $l$ -grafos  $a$ -partidos  $((X_i^t), \mathcal{M}^t)$ , onde  $t \in [2, a + 1]$ . Se  $((X_i^{t-1}), \mathcal{M}^{t-1})$  é um  $l$ -grafo  $a$ -partido tal que  $|X_{t-1}^{t-1}| = k_{t-1}$ , então, pela hipótese indutiva, sabemos que existe um  $k_{t-1}$ -grafo  $(Y^{t-1}, \mathcal{N}^{t-1})$  sem circuitos de tamanho menor que  $p$  e com número cromático maior que  $n$ . Assim, fazemos  $((X_i^t), \mathcal{M}^t) = (Y^{t-1}, \mathcal{N}^{t-1}) *_t ((X_i^{t-1}), \mathcal{M}^{t-1})$ . Mostraremos que

o  $l$ -grafo  $((X_i^{a+1}), \mathcal{M}^{a+1})$  não possui circuitos com tamanho menor ou igual a  $p$  e tem número cromático maior que  $n$ .

Utilizando indução em  $j$ , mostramos agora que  $((X_i^j), \mathcal{M}^j)$  não contém circuitos de tamanho menor ou igual a  $p$  para  $j \in [1, a+1]$ . Suponha, por contradição, que  $((X_i^j), \mathcal{M}^j)$  não contém circuitos de tamanho menor ou igual a  $p$ , mas  $((X_i^{j+1}), \mathcal{M}^{j+1})$  contém tal circuito  $C = \{M'_1, \dots, M'_q\}$ , com  $q \leq p$ . Assim, as arestas  $M'_1, \dots, M'_q$  podem ser denotadas por  $(M_1, N_1), \dots, (M_q, N_q)$ . Mas veja que  $N_1, \dots, N_q$  não podem ser todos iguais, pois teríamos um circuito de tamanho  $q$  em  $((X_i^j), \mathcal{M}^j)$ . Ademais, pela definição de  $((X_i^{j+1}), \mathcal{M}^{j+1})$ , temos que  $N_1, \dots, N_q$  também não podem ser todos diferentes. Mas como  $C$  é um circuito,  $N_1, \dots, N_q$  contém um circuito de tamanho no máximo  $q-1$  em  $(Y^j, \mathcal{N}^j)$ , uma contradição com a escolha de  $(Y^j, \mathcal{N}^j)$ .

Resta mostrar que  $\chi((X_i^{a+1}), \mathcal{M}^{a+1}) > n$ . Suponha, por contradição, que  $\chi((X_i^{a+1}), \mathcal{M}^{a+1}) \leq n$ . Seja  $c$  uma coloração com  $n$  cores dos vértices de  $((X_i^{a+1}), \mathcal{M}^{a+1}) = (Y^a, \mathcal{N}^a) *_{a-1} ((X_i^a), \mathcal{M}^a)$ . Lembrando que  $\chi(Y^a, \mathcal{N}^a) > n$ , existe  $N^a \in \mathcal{N}^a$  tal que  $|c(N^a)| = 1$ . Considere tal coloração aplicada a  $(X_{a-1}^a; N^a) = \{(x, N^a) : x \in X_{a-1}^a\}$ . Mas  $((X_i^a), \mathcal{M}^a) = (Y^{a-1}, \mathcal{N}^{a-1}) *_{a-1} ((X_i^{a-1}), \mathcal{M}^{a-1})$  e  $\chi(Y^{a-1}, \mathcal{N}^{a-1}) > n$ , assim, existe  $N^{a-1} \in \mathcal{N}^{a-1}$  tal que  $|c(N^{a-1}; N^a)| = 1$ . Repetindo o processo, temos uma aresta  $N^i \in \mathcal{N}^i$  tal que  $|c(N^i; N^{i+1}, \dots, N^a)| = 1$  para  $i \in [1, a]$ . Definindo  $Z_i = \{(x, N^i; N^{i+1}, \dots, N^a) : |c(x, N^i; N^{i+1}, \dots, N^a)| = 1\}$ , temos que  $Z_i \subset X_i^{a+1}$ . Pela definição de  $((X_i^{a+1}), \mathcal{M}^{a+1})$ , o subhipergrafo de  $((X_i^{a+1}), \mathcal{M}^{a+1})$  formado por  $\bigcup_{i=1}^a Z_i$  contém uma cópia de  $((X_i^1), \mathcal{M}^1)$ . Assim, como  $a = (l-1)n + 1$ , existe  $\omega \subset [1, a]$  com  $|\omega| = l$  tal que  $|c(\bigcup_{i \in \omega} Z_i)| = 1$ . Mas, lembrando da definição de  $((X_i^1), \mathcal{M}^1)$ , existe uma aresta monocromática  $M \in \mathcal{M}^1$  tal que  $M \subset \bigcup_{i \in \omega} Z_i$ . Portanto, temos uma contradição.

□

19/04/2010

## TEOREMA DA AMIZADE

**Teorema 29** (Teorema da Amizade (Erdős–Rényi–Sós [7])). *Se  $G$  é um grafo em que quaisquer dois vértices distintos possuem um único vizinho, então  $G$  tem um vértice que é vizinho de todos os outros vértices.*

*Demonstração.* Seja  $G = (V, E)$  um grafo. Suponha, por contradição, que não existe um vértice que é vizinho de todos os outros vértices. Seja  $k$  o maior grau de um vértice em  $G$  e  $v$  um vértice de grau  $k$ . Sejam  $w_1, \dots, w_k$  os vizinhos de  $v$  e seja  $x$  um vértice qualquer que não é vizinho de  $v$  (ele existe, pela suposição que fizemos no início da prova). Claramente,  $x$  só pode ser vizinho de um único elemento em  $\{w_1, \dots, w_k\}$ , pois caso contrário  $x$  e  $v$  teriam dois vizinhos em comum. Seja  $z_i$  um vizinho em comum de  $x$  e  $w_i$ , onde  $\{x, w_i\} \notin E$  (ele existe, pois a distância entre  $x$  e  $w_i$  é dois). Sabemos que tal  $z_i$  está à distância dois de  $v$ , pois não pode ser um dos elementos de  $\{w_1, \dots, w_k\}$  e qualquer par de vértices está à distância dois em  $G$ . Observe agora que cada  $z_i$  é único, pois caso contrário  $x$  e  $w_i$  teriam dois vizinhos em comum. Assim, concluímos que  $\deg(x) = k$ , o grau máximo de  $G$ . Repetindo o mesmo procedimento (com  $x$  fazendo o papel de  $v$ ), obtemos que todo vértice possui grau  $k$ . Portanto,  $G$  é  $k$ -regular, de modo que possui  $1 + k + k(k - 2)$  vértices.

Seja  $A$  a matriz de adjacência de  $G$ . A matriz  $A^2 = (a_{i,j})$  é tal que  $a_{i,j}$  contém a quantidade de caminhos de tamanho dois entre os vértices  $i$  e  $j$ . Temos que  $\det(A^2 - \lambda I) = (k^2 - \lambda)(k - 1 - \lambda)^{k^2 - k}$ , logo  $k^2$  é autovalor de  $A^2$  e  $k - 1$  é autovalor de  $A^2$  com multiplicidade  $k^2 - k$ . Assim, temos que os autovalores de  $A$  são  $k$ ,  $\sqrt{k - 1}$  e  $-\sqrt{k - 1}$ . Se  $r$  a multiplicidade de  $\sqrt{k - 1}$  e  $s$  a multiplicidade de  $-\sqrt{k - 1}$ , então  $k + r\sqrt{k - 1} - s\sqrt{k - 1} = 0$ . Desta forma,  $k^2 = (s - r)^2(k - 1)$ . Portanto, temos que  $k - 1 | k^2$ , que implica  $k - 1 | k$  e assim,  $k - 1 | 1$ . Assim, temos que  $k = 2$ , um absurdo, pois  $G$  seria um triângulo (todos os vértices são vizinhos de todos os outros).  $\square$

## FUNÇÕES LIMIARES

**Definição 30.** *Dada uma variável aleatória  $X$ . A variância de  $X$  é dada por*

$$\text{var}(X) = \mathbb{E}((X - \mathbb{E}(X))^2) = \mathbb{E}(X^2) - \mathbb{E}(X)^2.$$

<sup>1</sup>Os resultados desta seção foram apresentados pelo aluno Thiago da Silva Pinheiro.

**Definição 31.** Dadas duas variáveis aleatórias  $X$  e  $Y$ . A covariância de  $(X, Y)$  é dada por

$$\text{cov}(X, Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y).$$

Se  $X \geq 0$  e  $\lambda > 0$ , a seguinte desigualdade é válida.

$$(3) \quad \Pr(X \geq \lambda) \leq \frac{\mathbb{E}(X)}{\lambda}.$$

Fazendo  $X = (Y - \mathbb{E}(Y))^2$  e  $\lambda = \omega^2$  em (3), temos  $\Pr((Y - \mathbb{E}(Y))^2 \geq \omega^2) \leq \text{var}(Y)/\omega^2$ . Logo,

$$(4) \quad \Pr(|Y - \mathbb{E}(Y)| \geq \omega) \leq \frac{\text{var}(Y)}{\omega^2}.$$

Fazendo  $\lambda = 1$  em (3) temos que

$$(5) \quad \Pr(X \geq 1) \leq \mathbb{E}(X).$$

Fazendo  $\omega = \mathbb{E}(Y)$  em (4) temos que

$$(6) \quad \Pr(Y = 0) \leq \frac{\text{var}(Y)}{\mathbb{E}(Y)^2}.$$

**Definição 32.** Dizemos que uma função  $f(n) \ll g(n)$  quando  $\lim_{n \rightarrow \infty} f(n)/g(n) = 0$ .

**Definição 33.** Dizemos que  $G_{n,p}$  é um grafo com  $n$  vértices onde cada par de vértices define uma aresta do grafo independentemente com probabilidade  $p$ .

**Definição 34.** Considere o grafo  $G_{n,p}$ . Dizemos que  $f(n)$  é função limiar para um evento  $A$  se temos as seguintes afirmações.

- a) Se  $p \gg f(n)$ , então  $\lim_{n \rightarrow \infty} \Pr(A) = 1$  (1-afirmação);
- b) Se  $p \ll f(n)$ , então  $\lim_{n \rightarrow \infty} \Pr(A) = 0$  (0-afirmação).

**Teorema 35.** A função  $n^{-2/3}$  é limiar para o evento  $K^4 \subset G_{n,p}$ .

*Demonstração.* Seja  $S$  um conjunto de quatro vértices. Definimos a variável aleatória indicadora  $X_S$  como sendo 1 caso  $S$  induza um  $K^4$  em  $G_{n,p}$  e 0 caso contrário. Assim, se  $X$  representa a quantidade de cópias de  $K^4$  em  $G_{n,p}$ , temos que  $X = \sum_S X_S$ . Desta forma, sabemos que  $\mathbb{E}(X) = \sum_S \mathbb{E}(X_S)$ , portanto,  $\mathbb{E}(X) = O(n^4 p^6)$ .

Mostramos agora a 0-afirmação. Suponha que  $p \ll n^{-2/3}$ . Pela desigualdade (5) podemos concluir que  $\Pr(X \geq 1) \leq \mathbb{E}(X) = O(n^4 p^6) \ll 1$ . Assim, quando  $n \rightarrow \infty$ , temos que  $\Pr(X \geq 1)$  tende a zero, isto é,  $G_{n,p}$  não contém cópias de  $K^4$ .

A 1-afirmação requer um pouco mais de esforço. Suponha que  $p \gg n^{-2/3}$ . Vamos mostrar que  $\Pr(X = 0)$  tende a zero quando  $n \rightarrow \infty$ . Observe que

$$\begin{aligned} \mathbb{E}(X^2) &= \sum_S \mathbb{E}(X_S^2) + \sum_{(S,T), S \neq T} \mathbb{E}(X_S X_T). \\ \mathbb{E}(X)^2 &= \left( \mathbb{E} \left( \sum_S X_S \right) \right)^2 = \left( \sum_S \mathbb{E}(X_S) \right)^2 \\ &= \sum_S \mathbb{E}(X_S)^2 + \sum_{(S,T), S \neq T} \mathbb{E}(X_S) \mathbb{E}(X_T). \end{aligned}$$

Assim, temos que

$$\begin{aligned} \text{var}(X) &= \mathbb{E}(X^2) - \mathbb{E}(X)^2 \\ &= \sum_S (\mathbb{E}(X_S^2) - \mathbb{E}(X_S)^2) + \sum_{(S,T), S \neq T} \mathbb{E}(X_S X_T) - \sum_{(S,T), S \neq T} \mathbb{E}(X_S) \mathbb{E}(X_T) \\ &= \sum_S \text{var}(X_S) + \sum_{(S,T), S \neq T} \text{cov}(X_S, X_T). \end{aligned}$$

Para utilizarmos a desigualdade (6) e obter o resultado que estamos procurando, precisamos limitar superiormente o valor de  $\text{var}(X)$ . Observe que  $\text{var}(X_S) = \mathbb{E}(X_S^2) - \mathbb{E}(X_S)^2 \leq \mathbb{E}(X_S^2)$ . Mas como  $X_S$  é uma variável indicadora, temos  $\text{var}(X_S) \leq \mathbb{E}(X_S) = p^6$ . Logo,  $\sum_S \text{var}(X_S) = O(n^4 p^6)$ .

Resta limitarmos superiormente a covariância de  $X_S$  e  $X_T$  quando  $S \neq T$ . Se  $|S \cap T| \leq 1$ , então  $\text{cov}(X_S, X_T) = 0$ . Se  $|S \cap T| = 2$ , como  $\text{cov}(X_S, X_T) \leq \mathbb{E}(X_S X_T)$ , temos que  $\text{cov}(X_S, X_T) \leq p^{11}$ , de onde concluímos que  $\sum \text{cov}(X_S, X_T) = O(n^6 p^{11})$ , onde a soma é sobre os pares  $(S, T)$  tais que  $|S \cap T| = 2$ . Por fim, se  $|S \cap T| = 3$ , como  $\text{cov}(X_S, X_T) \leq \mathbb{E}(X_S X_T)$ , temos  $\text{cov}(X_S, X_T) \leq p^9$ , de onde concluímos que  $\sum \text{cov}(X_S, X_T) = O(n^5 p^9)$ , onde a soma é sobre os pares  $(S, T)$  tais que  $|S \cap T| = 3$ . Desta forma, podemos calcular um limitante superior para  $\text{var}(X)$ .

$$\begin{aligned}\text{var}(X) &= \sum_S \text{var}(X_S) + \sum_{(S,T), S \neq T} \text{cov}(X_S, X_T) \\ &= O(n^4 p^6 + n^6 p^{11} + n^5 p^9).\end{aligned}$$

Sabemos que  $\mathbb{E}(X) = O(n^4 p^6)$ . Portanto, temos todos os ingredientes para aplicar a desigualdade (6).

$$\begin{aligned}\Pr(X = 0) &= O\left(\frac{n^4 p^6}{n^8 p^{12}} + \frac{n^6 p^{11}}{n^8 p^{12}} + \frac{n^5 p^9}{n^8 p^{12}}\right) \\ &= O(n^{-4} p^{-6} + n^{-2} p^{-1} + n^{-3} p^{-3}) \\ &\ll 1,\end{aligned}$$

onde a última relação segue pela escolha de  $p$ . Assim, quando  $n \rightarrow \infty$ , temos que  $\Pr(X = 0)$  tende a zero, isto é,  $G_{n,p}$  contém pelo menos uma cópia de  $K^4$ .  $\square$

Vimos que se  $p \ll n^{-2/3}$ , então  $\Pr(K_4 \subset G_{n,p})$  tende a zero quando  $n$  tende a infinito. Vimos também que se  $p \gg n^{-2/3}$ , então  $\Pr(K_4 \subset G_{n,p})$  tende a infinito quando  $n$  tende a infinito. Portanto, é natural perguntar o que acontece quando  $p = cn^{-2/3}$ , onde  $c$  é uma constante. É um bom exercício tentar estimar  $\lim_{n \rightarrow \infty} \Pr(K_4 \not\subset G_{n,p})$ , onde  $p = cn^{-2/3}$ .

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

Dizemos que  $G \xrightarrow{\text{ind}} H$  se, colorindo as arestas de  $G$  com duas cores, necessariamente existe um subgrafo  $H'$  induzido de  $G$  tal que  $H' \sim H$  e  $H'$  é monocromático.

1. Encontre um grafo  $G$  tal que
  - (i)  $G \xrightarrow{\text{ind}} C^4$ .
  - (ii)  $G \xrightarrow{\text{ind}} C^5$ .
2. Encontre um grafo  $G$  tal que
  - (i)  $G \rightarrow K^3$  e  $G \not\rightarrow K_4$ .
  - (ii)  $G \rightarrow K^3$  e  $G \not\rightarrow K_5$ .
  - (iii)  $G \rightarrow K^3$  e  $G \not\rightarrow K_6$ .

26/04/2010

**Definição 36.** Seja  $\mathbb{E}^d$  o espaço euclidiano  $d$ -dimensional. Dizemos que  $\mathcal{P} \subset \mathbb{E}^d$  determina o ângulo  $\alpha$  se existem  $a, b, c \in \mathcal{P}$  tal que  $\sphericalangle abc = \alpha$ .

**Definição 37.** Seja  $\mathcal{P}$  finito. Pomos  $\alpha_d(\mathcal{P}) = \max\{0 \leq \alpha \leq \pi : \mathcal{P} \text{ determina } \alpha\}$ . Ademais, pomos também  $\alpha_d(n) = \inf_{\mathcal{P} \subset \mathbb{E}^d} \{\alpha_d(\mathcal{P}) : |\mathcal{P}| = n\}$ .

Observe que, por exemplo,  $\alpha_2(3) = \pi/3$ . De fato, se  $\mathcal{P}$  é um conjunto de três pontos formando um triângulo equilátero, então obtemos  $\alpha_2(3) \leq \pi/3$ . Sabemos também que, como quaisquer três pontos não colineares no plano formam um triângulo, todo conjunto  $\mathcal{P}$  determina um ângulo maior ou igual a  $\pi/3$ , de onde concluímos que  $\alpha_2(3) \geq \pi/3$ .

**Definição 38.** Pomos  $f(d) = \max_{\mathcal{P} \subset \mathbb{E}^d} \{|\mathcal{P}| : \mathcal{P} \text{ determina somente ângulos agudos}\}$ .

Veja que, por exemplo,  $f(2) = 3$ . De fato, se  $\mathcal{P}$  é um conjunto de três pontos formando um triângulo equilátero, então obtemos  $f(2) \geq 3$ . Observe que, se  $|\mathcal{P}| \geq 4$ , então o fecho convexo de  $\mathcal{P}$  é um quadrilátero ou um triângulo que contém pontos em seu interior. Em ambos os casos, existe um ângulo que não é agudo. Portanto,  $f(2) \leq 3$ .

Considere a seguinte invariante  $f'(d) = \max_{\mathcal{P} \subset \mathbb{E}^d} \{|\mathcal{P}| : \mathcal{P} \text{ determina somente ângulos } \leq \pi/2\}$ . Temos que  $f'(d) \geq 2^d$  (construa um hipercubo de dimensão  $d$ ). Danzer e Grünbaum [4] provaram o seguinte resultado sugerido por Erdős [8]:  $f'(d) \leq 2^d$  (Exercício 8.1.3).

Erdős e Füredi sugeriram que existe uma constante absoluta  $\varepsilon > 0$  tal que  $\alpha_d(2^d + 1) \geq \pi/2 + \varepsilon$ . Conjeturava-se que  $f(d) \leq 2d - 1$ . Porém, Erdős e Füredi [6] provaram que  $f(d) \geq (1.18\dots)^d$ , sempre que  $d \geq d_0$ , para algum  $d_0 > 0$ . Um resultado que encontra-se em aberto até os dias de hoje é mostrar que  $f(d) \leq (2 - \varepsilon)^d$  para algum  $\varepsilon > 0$ . Ademais, será que  $f(d) \leq 2^d - 1$ ?

Usaremos o método probabilístico para obter cotas inferiores exponenciais para  $f(d)$ . Escolha aleatoriamente  $m$  pontos do hipercubo em  $\mathbb{E}^d$ , isto é,  $\underline{x}_1, \dots, \underline{x}_m \in \{0, 1\}^d$ , com cada  $\underline{x}_i$  sendo escolhido uniformemente de forma independente dentre os  $2^d$  possíveis. Afirmamos que a probabilidade de  $\sphericalangle \underline{x}_A \underline{x}_B \underline{x}_C = \pi/2$  é  $(3/4)^d$ . Isto segue do seguinte lema.

**Lema 39.** Sejam  $A, B, C \subset [d]$  e  $\underline{x}_A \underline{x}_B \underline{x}_C \in \{0, 1\}^d$  os respectivos vetores característicos. Temos que  $\sphericalangle \underline{x}_A \underline{x}_B \underline{x}_C = \pi/2$  se e somente se  $(A \cap C) \subset B \subset (A \cup C)$ .

*Demonstração.* Exercício 8.1.4. □

Observe que, dada qualquer tripla formada pelos pontos escolhidos, o ângulo que ela determina é menor ou igual a  $\pi/2$  (pois escolhemos pontos do hipercubo). Seja  $X$  o número de triplas  $(i, j, k)$  tal que  $\sphericalangle \underline{x}_A \underline{x}_B \underline{x}_C = \pi/2$ . Desta forma, podemos observar que  $\mathbb{E}(X) = m(m-1)(m-2)(3/4)^d$ . Se  $\mathbb{E}(X) < 1$ , então existe um experimento tal que todos os ângulos são menores que  $\pi/2$ , de onde concluímos que, neste caso,  $f(d) \geq m$ . Pondo  $m < (1, 1)^d$ , temos que  $\mathbb{E}(X) < 1$ . Portanto, provamos que  $f(d) \geq (1, 1)^d$ .

É possível melhorar o resultado anterior através do *Método da Alteração*. Escolha  $m$  de modo que  $(2m)_3(3/4)^d < m$ . Assim, temos que  $m = \lfloor (2/\sqrt{3})^d / (2\sqrt{2}) \rfloor = (1, 15 \dots)^d / (2\sqrt{2})$ . Geramos  $\underline{x}_1, \dots, \underline{x}_{2m}$  como antes. Como  $\mathbb{E}(X) = (2m)_3(3/4)^d < m$ , existe uma configuração com  $2m$  pontos tal que  $X < m$ . Então, existe uma configuração  $\mathcal{P}$  com mais que  $2m - m = m$  pontos tal que todos os ângulos são menores que  $\pi/2$ . Portanto, obtemos o seguinte resultado.

**Teorema 40** (Erdős–Füredi[6]).

$$f(d) > \frac{1}{2\sqrt{2}} \left( \frac{2}{\sqrt{3}} \right)^d.$$

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

1. Prove que  $f(3) = 5$ .
2. É fácil ver que  $f(d) \geq d + 1$ . Prove a seguinte cota:  $f(d) \geq 2d - 1$ .
3. Prove que  $f'(d) \leq 2^d$ . Observe que isto é o mesmo que provar  $\alpha_d(2^d + 1) > \pi/2$ .
4. Prove o Lema 39.
5. Prove que, para todo  $\varepsilon > 0$ , existe  $\delta > 0$  tal que existem pelo menos  $(1 + \delta)^d$  pontos em  $\mathbb{E}^d$  que determinam apenas ângulos agudos menores que  $\pi/3 + \varepsilon$ .

03/05/2010

## FUNÇÕES GERADORAS

**Definição 41.** Dado um polinômio  $f(z)$ , denotamos por  $[z^n]f(z)$  o coeficiente de  $z^n$  em  $f(z)$ .

**Definição 42.** Seja  $\langle g_n \rangle_{n \in \mathbb{N}}$  uma sequência em  $\mathbb{C}$ . Dizemos que  $G(z)$  é função geradora de  $\langle g_n \rangle$  se  $[z^n]G(z) = g_n$ . Isto é,  $G(z) = \sum_{n=0}^{\infty} g_n z^n$ .

Considere as funções geradoras  $F(z)$  e  $G(z)$  para as sequências  $\langle f_n \rangle_{n \in \mathbb{N}}$  e  $\langle g_n \rangle_{n \in \mathbb{N}}$ , respectivamente. Temos que  $\alpha F(z) + \beta G(z) = \alpha \sum_{n=0}^{\infty} f_n z^n + \beta \sum_{n=0}^{\infty} g_n z^n = \sum_{n=0}^{\infty} (\alpha f_n + \beta g_n) z^n$ . Portanto,  $\alpha F(z) + \beta G(z)$  é a função geradora da sequência  $\langle \alpha f_n + \beta g_n \rangle_{n \in \mathbb{N}}$ .

De agora em diante,  $F(z)$  e  $G(z)$  sempre representarão funções geradoras de sequências  $\langle f_n \rangle_{n \in \mathbb{N}}$  e  $\langle g_n \rangle_{n \in \mathbb{N}}$ , respectivamente. A derivada de  $G(z)$  com relação a  $z$  é dada por

$$G'(z) = \sum_{n=0}^{\infty} (n+1)g_{n+1}z^n.$$

Desta forma, temos

$$zG'(z) = \sum_{n=1}^{\infty} n g_n z^n.$$

Multiplicando  $F(z)$  e  $G(z)$ , obtemos

$$F(z)G(z) = \sum_{n=0}^{\infty} \left( \sum_{k=0}^n f_k g_{n-k} \right) z^n.$$

**Definição 43.** Dada uma variável aleatória  $X$  que assume valores inteiros não negativos, dizemos que  $G_X(z)$  é a função geradora de probabilidade de  $X$  se  $G_X(z) = \sum_{k=0}^{\infty} \Pr(X = k)z^k$ .

*Observação.* Temos que  $G_X(1) = 1$ .

Funções geradoras de probabilidade tornam simples os cálculos de valor esperado e variância. Considere uma variável aleatória  $X$  que assume valores inteiros não negativos. Para o cálculo do

<sup>1</sup>Os resultados desta seção foram apresentados pelos alunos Eric Ossami Endo e Renato dos Santos Nunes.

<sup>2</sup>O conteúdo desta seção foi baseado em [10].

valor esperado, temos

$$\begin{aligned}
 \mathbb{E}(X) &= \sum_{k=0}^{\infty} k \Pr(X = k) \\
 (7) \qquad &= \sum_{k=0}^{\infty} k \Pr(X = k) z^{k-1} \Big|_{z=1} \\
 &= G'_X(1).
 \end{aligned}$$

Para o cálculo da variância, sabemos que  $\text{var}(X) = \mathbb{E}(X^2) - \mathbb{E}(X)^2$ . Mas observe que

$$\begin{aligned}
 \mathbb{E}(X^2) &= \sum_{k=0}^{\infty} k^2 \Pr(X = k) \\
 &= \sum_{k=0}^{\infty} \left( k(k-1)z^{k-2} + kz^{k-1} \right) \Big|_{z=1} \Pr(X = k) \\
 &= G''_X(1) + G'_X(1).
 \end{aligned}$$

Assim, temos que

$$(8) \qquad \text{var}(X) = G''_X(1) + G'_X(1) - G'_X(1)^2.$$

Considere agora que as variáveis aleatórias  $X$  e  $Y$  sejam independentes. Desta forma,

$$\begin{aligned}
 G_{X+Y}(z) &= \sum_{n=0}^{\infty} \Pr(X + Y = n) z^n \\
 &= \sum_{n=0}^{\infty} \sum_{k=0}^n \Pr(X = k \text{ e } Y = n - k) z^n \\
 &= \sum_{n=0}^{\infty} \sum_{k=0}^n \Pr(X = k) \Pr(Y = n - k) z^n \\
 &= G_X(z) G_Y(z).
 \end{aligned}$$

Observe que  $\mathbb{E}(X + Y) = (G_X(z)G_Y(z))' \Big|_{z=1} = G'_X(1)G_Y(1) + G_X(1)G'_Y(1)$ . Mas sabemos que  $G_X(1) = G_Y(1) = 1$ , portanto,  $\mathbb{E}(X + Y) = \mathbb{E}(X) + \mathbb{E}(Y)$ . Calculemos agora a variância de  $X + Y$ . Para isto, precisamos calcular  $G''_{X+Y}(1)$  e  $G'_{X+Y}(1)$ .

$$G'_{X+Y}(1) = G'_X(1)G_Y(1) + G_X(1)G'_Y(1) = G'_X(1) + G'_Y(1).$$

Ademais,

$$\begin{aligned} G''_{X+Y}(1) &= G''_X(1)G_Y(1) + 2G'_X(1)G'_Y(1) + G_X(1)G''_Y(1) \\ &= G''_X(1) + 2G'_X(1)G'_Y(1) + G''_Y(1). \end{aligned}$$

Assim, como  $\text{var}(X + Y) = G''_{X+Y}(1) + G'_{X+Y}(1) - G'_{X+Y}(1)^2$ , temos que

$$\begin{aligned} \text{var}(X + Y) &= (G''_X(1) + G'_X(1) - G'_X(1)^2) + (G''_Y(1) + G'_Y(1) - G'_Y(1)^2) \\ &= \text{var}(X) + \text{var}(Y). \end{aligned}$$

#### LANÇANDO MOEDAS

Consideremos agora o lançamento de uma moeda onde a probabilidade de dar cara é  $p$  e a probabilidade de dar coroa é  $q = 1 - p$ ; Se  $X$  é a variável aleatória representando a quantidade de caras após um lançamento, temos que a função de probabilidade de  $X$  é dada por  $H_X(z) = q + pz$ . Se  $Y$  representa a quantidade de caras em  $n$  lançamentos independentes,  $Y$  é gerada por

$$H_Y(z) = H_X(z)^n = \sum_{k=0}^n \binom{n}{k} p^k q^{n-k} z^k.$$

A sequência de probabilidades  $\langle \binom{n}{k} p^k q^{n-k} \rangle_{k=1}^n$  é chamada de *distribuição binomial*. Observe que, por (7), temos  $\mathbb{E}(Y) = (H'_Y(1)) = (H_X(z)^n)'|_{z=1} = (nH_X(z)^{n-1}H'_X(z))|_{z=1} = nH'_X(1) = np$ , como era esperado. Por (8), temos que

$$\begin{aligned} \text{var}(Y) &= (H_X(z)^n)''|_{z=1} + (H_X(z)^n)'|_{z=1} = \mathbb{E}(Y)^2 \\ &= (n(n-1)p^2) + (np) - n^2p^2 \\ &= np(1-p). \end{aligned}$$

Vamos agora considerar o processo de lançar moedas independentemente até que apareça a primeira cara. Seja  $X$  a variável aleatória representando a quantidade de lançamentos realizados até o aparecimento da primeira cara. Claramente,  $X$  é gerada por

$$G_X(z) = \sum_{k=0}^{\infty} q^k p z^{k+1} = \frac{pz}{1-qz}.$$

Repetindo esse processo até o aparecimento de  $n$  caras, temos

$$(9) \quad G_X(z)^n = \frac{p^n z^n}{(1-qz)^n} = p^n z^n (1-qz)^{-n}.$$

Seja  $(n)_k = n(n-1)\dots(n-k+1)$ . Assim, se  $n$  é um inteiro positivo, temos que

$$\begin{aligned} \binom{-n}{k} &= \frac{(-n)_k}{k!} \\ &= \frac{(-1)^k (n+k-1)_k}{k!} \\ &= (-1)^k \binom{n+k-1}{k}. \end{aligned}$$

Desta forma, por (9), temos

$$\begin{aligned} G_X(z)^n &= p^n z^n \sum_{k=0}^n \binom{-n}{k} (-1)^k q^k z^k \\ &= p^n z^n \sum_{k=0}^n \binom{n+k-1}{k} q^k z^k. \end{aligned}$$

Dividindo por  $z^n$  dos dois lados, obtemos

$$\frac{p^n}{(1-qz)^n} = \sum_{k=0}^n \binom{n+k-1}{k} p^n q^k z^k,$$

que é a função geradora para a chamada *distribuição binomial negativa*.

Seja  $Y$  uma variável aleatória com distribuição binomial negativa como acima. Uma maneira fácil de calcular o valor esperado e a variância de  $Y$  é através da chamada *função geradora recíproca*  $I(z) = (1-qz)/p = 1/p - (q/p)z$ . Observe que, apesar de  $I(z)$  não ser uma função geradora de probabilidade,  $I(1) = 1$  (podemos ver  $I(z)^{-n}$  gerando uma distribuição binomial com parâmetros  $-n$  e  $-q/p$ ). Assim,  $\mathbb{E}(Y) = (-n)(-q/p) = nq/p$  e  $\text{var}(Y) = (-n)(-q/p)(1/p) = nq/p^2$ .

Vamos considerar agora o experimento de lançar moedas independentemente até que duas caras apareçam seguidamente. Veja que o espaço de probabilidades deste experimento é dado por  $\Omega = \{HH, THH, TTHH, HTHH, \dots\}$ , onde  $H$  representa que o resultado do lançamento foi cara e  $T$  que o resultado do lançamento foi coroa. Trocando  $H$  por  $p$  e  $T$  por  $q$ , obtemos a probabilidade de uma dada sequência ser obtida. Se  $X$  é a variável aleatória representando a quantidade de lançamentos até a ocorrência de duas caras seguidas, então  $X$  é gerada pela seguinte função geradora de probabilidade.

$$G_X(z) = p^2 z^2 + qp^2 z^3 + q^2 p^2 z^4 + qp^3 z^4 + \dots$$

A soma acima é obtida trocando  $H$  por  $pz$  e  $T$  por  $qz$  para todo elemento de  $\Omega$  e somando-os.

Podemos dividir os elementos de  $\Omega$  pela quantidade de  $T$ 's que possuem. Vamos ver com qual valor, os elementos de  $\Omega$  que possuem  $n$  termos  $T$ , contribuem com a soma  $G_X(z)$ . Como não pode haver duas caras seguidas (a menos das últimas), existem  $\binom{n}{k}/k!$  elementos com  $k + 2$  caras e  $n$  coroas. Cada um desses elementos contribui com  $p^{k+2}q^n z^{n+k+2}$ . Assim,

$$\begin{aligned} G_X(z) &= \sum_{n=0}^{\infty} \left( \sum_{k=0}^n \binom{n}{k} p^{k+2} q^n z^{n+k+2} \right) \\ &= p^2 z^2 \sum_{n=0}^{\infty} \left( \sum_{k=0}^n \binom{n}{k} (pqz^2)^k (qz)^{n-k} \right) \\ &= p^2 z^2 \sum_{n=0}^{\infty} (pqz^2 + qz)^n \\ &= \frac{p^2 z^2}{1 - pqz^2 - qz} \end{aligned}$$

Desta forma, utilizaremos a função  $F(z) = z^2/G_X(z) = (1 - pqz^2 - qz)/p^2$  para calcular o valor esperado e a variância de  $X$ . Simples cálculos são suficientes para mostrar que  $F'(1) = -p^{-2} - p^{-1} + 2$  e  $F''(1) = -p^{-4} - 2p^{-3} + 2p^{-2} + p^{-1}$ . Mas, como  $G_X(z)F(z) = z^2$ , temos que

$$\begin{aligned} \mathbb{E}(X) &= 2 - (-p^{-2} - p^{-1} + 2) \\ &= p^{-1} + p^{-2}. \end{aligned}$$

Ademais,

$$\begin{aligned} \text{var}(X) &= 0 - (-p^{-4} - 2p^{-3} + 2p^{-2} + p^{-1}) \\ &= p^{-4} + 2p^{-3} - 2p^{-2} - p^{-1}. \end{aligned}$$

10. LANÇAMENTO DE MOEDAS

10/05/2010

Vamos considerar o experimento onde realizamos lançamentos independentes de uma moeda, parando quando uma determinada sequência de caras e coroas apareça pela primeira vez. Seja  $p$  a probabilidade de dar cara e  $q = 1 - p$  a probabilidade de dar coroa em qualquer dos lançamentos. Por exemplo, se considerarmos a sequência  $THTTH$ , o espaço de probabilidades desse evento é dado por  $\Omega = \{THTTH, HTHTTH, TTHTTH, HHTHTTH, HTTHTTH, \dots\}$ . Se  $X$  é a variável aleatória representando a quantidade de lançamentos até a ocorrência da sequência em questão, então  $X$  é gerada pela seguinte função geradora de probabilidade.

$$G_X(z) = p^2q^3z^5 + qp^3q^3z^6 + p^2q^4z^6 + p^4q^3z^7 + \dots$$

Trocando  $pz$  por  $H$  e  $qz$  por  $T$ , podemos, para clarear as idéias, representar a expressão acima como a soma  $S = THTTH + HTHTTH + TTHTTH + HHTHTTH + \dots$ . Dizemos que  $S$  é a soma das sequências vencedoras para  $THTTH$ . Da mesma maneira, considere  $N$  como a soma das sequências em que  $THTTH$  não ocorre, onde 1 representa a sequência vazia. Assim, temos que

$$(10) \quad 1 + N(H + T) = N + S.$$

$$(11) \quad NTHTTH = S + STTH.$$

Por (10), temos que  $(1 - S)(1 - (H + T))^{-1} = N$ . Assim, por (11), temos

$$(1 - S)(1 - (H + T))^{-1}THTTH = S(1 + TTH).$$

Portanto,

$$(1 - G_X(z))(1 - z)^{-1}p^2q^3z^5 = G_X(z)(1 + pq^2z^3).$$

Logo,

$$G_X(z) = \frac{p^2q^3z^5}{p^2q^3z^5 + (1 + pq^2z^3)(1 - z)}.$$

Faça  $G_X(z) = z^5/F_X(z)$ . Assim, com alguns cálculos, obtemos  $F'_X(1) = 5 - (1 + pq^2)/(p^2q^3)$  e  $F''_X(1) = 20 - (6pq^2)/(p^2q^3)$ . Com isso, podemos calcular o valor esperado e a variância de  $X$ .

<sup>1</sup>Os resultados desta seção foram apresentados pelos alunos Eric Ossami Endo e Renato dos Santos Nunes.

<sup>2</sup>O conteúdo desta seção foi baseado em [10].

Valor esperado:

$$\begin{aligned}\mathbb{E}(X) &= G'_X(1) \\ &= 5 - F'_X(1) \\ &= p^{-2}q^{-3} + p^{-1}q^{-1}.\end{aligned}$$

Variância:

$$\begin{aligned}\text{var}(X) &= G''_X(1) + G'_X(1) - G'_X(1)^2 \\ &= -(F''_X(1) + F'_X(1) - F'_X(1)^2) \\ &= \mathbb{E}(X)^2 - 9p^{-2}q^{-3} - 3p^{-1}q^{-1}.\end{aligned}$$

Pensaremos agora sobre o que ocorre no caso de considerarmos uma sequência qualquer. Seja  $A$  tal sequência de caras e coroas de tamanho  $m$ . Seja  $S$  a sequência das sequências vencedoras para  $A$ , e  $N$  a soma das sequências onde  $A$  não aparece. Note que a igualdade (10) continua válida. Defina  $A^{(k)}$  e  $A_{(k)}$ , respectivamente, como os  $k$  últimos caracteres e os  $k$  primeiros caracteres de  $A$ . Assim, temos que

$$(12) \quad NA = S \left( 1 + \sum_{k=1}^{m-1} A^{(k)} \left[ A_{(m-k)} = A^{(m-k)} \right] \right),$$

lembrando que  $[p] = 1$  se  $p$  é válido e  $[p] = 0$  se  $p$  é falso.

Vamos calcular o valor esperado e a variância de  $X$ , onde  $X$  representa a quantidade de lançamentos da moeda até que a sequência  $A$  ocorra pela primeira vez. Substituindo (10) em (12), obtemos

$$S = \frac{A}{A + \left( 1 + \sum_{k=1}^{m-1} A^{(k)} \left[ A_{(m-k)} = A^{(m-k)} \right] \right) (1 - H - T)}.$$

Fazendo  $\tilde{A}_{(k)}$  o valor resultante da substituição de  $H$  por  $p^{-1}$  e  $T$  por  $q^{-1}$  em  $A_{(k)}$ . Considere também  $\hat{A}_{(k)} = \tilde{A}_{(k)}^{-1}$ . Assim,

$$G_X(z) = \frac{\hat{A}_{(m)}z^m}{\hat{A}_{(m)}z^m + \left( 1 + \sum_{k=1}^{m-1} \hat{A}_{(k)} \left[ A_{(m-k)} = A^{(m-k)} \right] \right) (1 - z)}.$$

Portanto, fazendo  $F_X(z) = z^m/G_X(z)$  e observando que  $\hat{A}_{(k)}/\hat{A}_{(m)} = \tilde{A}_{(m-k)}$ , temos que

$$F_X(z) = z^m + \left( \sum_{k=1}^m \tilde{A}_{(k)}z^{(m-k)} \left[ A_{(k)} = A^{(k)} \right] \right) (1 - z).$$

Assim,

$$F'_X(1) = m - \sum_{k=1}^m \tilde{A}_{(k)} \left[ A_{(k)} = A^{(k)} \right].$$

Ademais,

$$F''_X(1) = (m-1)m - 2 \sum_{k=1}^m (m-k) \tilde{A}_{(k)} \left[ A_{(k)} = A^{(k)} \right].$$

Desta forma, podemos facilmente calcular o valor esperado e a variância de  $X$ .

Valor esperado:

$$\mathbb{E}(X) = G'_X(1) = m - F'(1) = \sum_{k=1}^m \tilde{A}_{(k)} \left[ A_{(k)} = A^{(k)} \right].$$

Variância:

$$\begin{aligned} \text{var}(X) &= G''_X(1) + G'_X(1) - G'_X(1)^2 \\ &= -(F''_X(1) + F'_X(1) - F'_X(1)^2) \\ &= \mathbb{E}(X)^2 - \sum_{k=1}^m (2k-1) \tilde{A}_{(k)} \left[ A_{(k)} = A^{(k)} \right]. \end{aligned}$$

Vamos considerar agora o jogo conhecido por “Penney ante”. Neste jogo existem os jogadores 1 e 2 e cada um deles escolhe uma configuração de caras e coroas, respectivamente,  $A$  e  $B$ , da maneira que quiserem. Uma moeda honesta é lançada repetidas vezes até que  $A$  apareça ou  $B$  apareça. A configuração que aparecer primeiro dá a vitória ao jogador correspondente. Considere  $S_A$  e  $S_B$  como sendo as somas das sequências vencedoras para  $A$  e  $B$ , respectivamente, onde  $|A| = l$  e  $|B| = m$ , e seja  $N$  a soma das sequências que não são vencedoras nem para  $A$  nem para  $B$ .

Observe que temos

$$(13) \quad 1 + N(H + T) = N + S_A + S_B.$$

$$(14) \quad \begin{aligned} NA &= S_A \sum_{k=1}^l A^{(l-k)} \left[ A^{(k)} = A_{(k)} \right] + S_B \sum_{k=1}^{\min\{l,m\}} A^{(l-k)} \left[ B^{(k)} = A_{(k)} \right]. \\ NB &= S_B \sum_{k=1}^m B^{(m-k)} \left[ B^{(k)} = B_{(k)} \right] + S_A \sum_{k=1}^{\min\{l,m\}} B^{(m-k)} \left[ A^{(k)} = B_{(k)} \right]. \end{aligned}$$

Como a moeda que estamos considerando no jogo é honesta, (14) nos diz que

$$(15) \quad \begin{aligned} N &= S_A \sum_{k=1}^l 2^k [A^{(k)} = A_{(k)}] + S_B \sum_{k=1}^{\min\{l,m\}} 2^k [B^{(k)} = A_{(k)}]. \\ N &= S_B \sum_{k=1}^m 2^k [B^{(k)} = B_{(k)}] + S_A \sum_{k=1}^{\min\{l,m\}} 2^k [A^{(k)} = B_{(k)}]. \end{aligned}$$

Defina agora a operação  $A : B$  como segue, onde  $A$  pode ser igual a  $B$ .

$$A : B = \sum_{k=1}^{\min\{l,m\}} 2^{k-1} [A^{(k)} = B_{(k)}].$$

Assim, igualando as expressões em (15), obtemos uma igualdade bem simples.

$$\frac{S_A}{S_B} = \frac{B : B - B : A}{A : A - A : B}.$$

Vale ressaltar que a relação de vitória entre os padrões escolhidos neste jogo não são transitivas. Por exemplo, suponha que jogadores 1, 2 e 3 escolheram as sequências  $HHTH$ ,  $HTHH$  e  $THHH$ , respectivamente. Temos que o jogador 1 vence o jogador 2 com probabilidade  $3/2$  e o jogador 2 vence o jogador 3 com probabilidade  $7/5$ , porém, o jogador 3 vence o jogador 1 com probabilidade  $7/5$ . De fato, se o jogador 1 escolheu a sequência  $\tau_1, \dots, \tau_l$ , o jogador 2 sempre ganhará se escolher a sequência  $\bar{\tau}_2\tau_1, \tau_2, \dots, \tau_{l-1}$  (veja o exercício 10.1.1).

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

1. Seja  $\tau_1, \dots, \tau_l$  a sequência escolhida pelo jogador 1 no jogo “Penney ante”.

(i) Mostre que o jogador 2 sempre vencerá caso escolha a sequência  $\bar{\tau}_2\tau_1, \tau_2, \dots, \tau_{l-1}$ .

(i) A sequência  $\bar{\tau}_2\tau_1, \tau_2, \dots, \tau_{l-1}$  é a melhor escolha para o jogador 2 (isto é, a que lhe dá a maior probabilidade de vitória)?

11. TEORIA PROBABILÍSTICA DOS NÚMEROS

17/05/2010

Nesta seção utilizaremos a seguinte forma da desigualdade de Chebyshev.

$$(16) \quad \Pr \left( |X - \mathbb{E}(X)| \geq \omega \sqrt{\text{var}(X)} \right) \leq \frac{1}{\omega^2},$$

onde  $\omega$  é um número positivo qualquer. O seguinte lema também será necessário.

**Lema 44.**

$$\sum_{p \leq x} \frac{1}{p} = \ln \ln x + O(1).$$

*Demonstração do limite inferior.* Lembre que, para qualquer  $n$  inteiro, podemos escrevê-lo de maneira única na forma  $n = mq^2$ , onde  $m$  é livre de quadrados, isto é,  $m$  não é divisível por nenhum quadrado perfeito. Assim, temos que

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &= \sum_{m \leq x} \left( \frac{1}{m} \sum_{q \leq \sqrt{x/m}} \frac{1}{q^2} \right) \\ &\leq 2 \sum_{m \leq x} \frac{1}{m} \\ &= 2 \prod_{p \leq x} \left( 1 + \frac{1}{p} \right). \end{aligned}$$

Mas

$$\begin{aligned} \sum_{n \leq x} \frac{1}{n} &\geq \sum_{n \leq x} \int_n^{n+1} \frac{1}{t} dt \\ &\geq \log x. \end{aligned}$$

Portanto,  $\log x \leq 2 \prod_{p \leq x} (1 + 1/p) \leq 2 \prod_{p \leq x} e^{1/p} = 2e^{\sum_{p \leq x} 1/p}$ . Assim,

$$\sum_{p \leq x} 1/p \geq \ln \ln x + O(1)$$

□

**Definição 45.** Denotamos por  $v(n)$  o número de primos positivos que dividem  $n$ .

<sup>1</sup>Os resultados desta seção foram apresentados pelo aluno Thiago da Silva Pinheiro.

O seguinte teorema nos diz, de forma grosseira, que quase todo número  $n$  possui uma quantidade de fatores primos muito próxima de  $\ln \ln n$ .

**Teorema 46** (Hardy–Ramanujan [12]). *Seja  $\omega$  uma função qualquer tal que  $\omega = \omega(n) \rightarrow \infty$ . A quantidade de elementos  $x \in [n]$  tais que  $|v(x) - \ln \ln n| > \omega \sqrt{\ln \ln n}$  é  $o(n)$ .*

*Demonstração (feita por Turán [19]).* Utilizaremos o método do segundo momento. Tome  $x \in [n]$  escolhido aleatoriamente com distribuição uniforme. Para  $p$  primo, denotamos  $X_p = 1$  se  $p|x$  e  $X_p = 0$  caso contrário. Fazendo  $m = n^{1/10}$ , dizemos que  $X = X(x) = \sum_{p \leq m} X_p$ , onde este somatório é sobre todos os primos menores que  $m$ . Observe que  $X(x)$  representa a quantidade de primos não maiores que  $m$  que dividem  $x$ . Ademais, podemos notar que não existem mais que 10 elementos maiores que  $m$  que dividem  $x$ . Assim, temos que  $v(x) - 10 \leq X(x) \leq v(x)$ .

Podemos calcular o valor esperado de  $X$ . Temos  $\mathbb{E}(X_p) = \lfloor n/p \rfloor / n = 1/p + O(1/n)$ , onde a última igualdade segue do fato de  $x - 1 \leq \lfloor x \rfloor \leq x$ . Portanto,

$$\begin{aligned} \mathbb{E}(X(x)) &= \sum_{p \leq m} \mathbb{E}(X_p) \\ &= \sum_{p \leq m} (1/p + O(1/n)) \\ &= \left( \sum_{p \leq m} 1/p \right) + O(1) \\ &= \ln \ln n + O(1), \end{aligned}$$

onde a última igualdade segue do Lema 44.

Precisamos agora calcular a variância de  $X(x)$ . Vimos em seções anteriores que se  $X = \sum_S X_S$ , então temos que  $\text{var}(X) = \sum_S \text{var}(X_S) + \sum_{(S,T), S \neq T} \text{cov}(X_S, X_T)$ . Assim, precisamos saber os valores de  $\text{var}(X_p)$  e  $\text{cov}(X_p, X_q)$  para  $p \neq q$ .

$$\begin{aligned} \text{var}(X_p) &= \mathbb{E}(X_p^2) - \mathbb{E}(X_p)^2 \\ &= \mathbb{E}(X_p) - \mathbb{E}(X_p)^2 \\ &= \mathbb{E}(X_p)(1 - \mathbb{E}(X_p)) \\ &= \left( \frac{1}{p} + O\left(\frac{1}{n}\right) \right) \left( 1 - \frac{1}{p} + O\left(\frac{1}{n}\right) \right) \\ &= \frac{1}{p} \left( 1 - \frac{1}{p} \right) + O\left(\frac{1}{n}\right). \end{aligned}$$

Portanto,

$$\begin{aligned}
\sum_{p \leq m} \text{var}(X_p) &= \sum_{p \leq m} \left( \frac{1}{p} \left( 1 - \frac{1}{p} \right) + O\left(\frac{1}{n}\right) \right) \\
&= \left( \sum_{p \leq m} \frac{1}{p} \right) + O(1) \\
&= \ln \ln n + O(1),
\end{aligned}$$

onde a última igualdade segue do Lema 44. Para a covariância, temos

$$\begin{aligned}
\text{cov}(X_p, X_q) &= \mathbb{E}(X_p X_q) - \mathbb{E}(X_p) \mathbb{E}(X_q) \\
&= \frac{\lfloor n/pq \rfloor}{n} - \frac{\lfloor n/p \rfloor}{n} \frac{\lfloor n/q \rfloor}{n} \\
&\leq \frac{1}{pq} - \left( \frac{1}{p} - \frac{1}{n} \right) \left( \frac{1}{q} - \frac{1}{n} \right) \\
&\leq \frac{1}{n} \left( \frac{1}{p} + \frac{1}{q} \right).
\end{aligned}$$

Portanto,

$$\begin{aligned}
\sum_{p \neq q} \text{cov}(X_p X_q) &\leq \frac{1}{n} \sum_{p \neq q} \left( \frac{1}{p} + \frac{1}{q} \right) \\
&\leq \frac{2m}{n} \sum_{p \leq m} \frac{1}{p} \\
&= 2n^{-9/10} (\ln \ln n + O(1)) \\
&= o(1).
\end{aligned}$$

Com isso, vemos que a covariância não tem nenhum efeito sobre a variância de  $X(x)$ . Logo,

$$\begin{aligned}
\text{var}(X(x)) &= \sum_{p \leq m} \text{var}(X_p) + \sum_{p \neq q} \text{cov}(X_p X_q) \\
&= \ln \ln n + O(1).
\end{aligned}$$

Utilizando a desigualdade (16) e lembrando que  $v(x) - 10 \leq X \leq v(x)$ , temos que

$$\Pr \left( |v(x) - \ln \ln n| > \omega \sqrt{\ln \ln n} \right) < \omega^{-2},$$

onde  $\omega = \omega(n)$  tende a infinito quando  $n$  tende a infinito. Isto completa a prova.  $\square$

O seguinte teorema mostra um importante resultado, obtido por Erdős e Kac em 1940, que relaciona a quantidade de fatores primos de um número  $n$  com a distribuição normal.

**Teorema 47** (Erdős–Kac [5]). *Para todo  $t \in \mathbb{R}$ , se  $x \in [n]$  é escolhido aleatoriamente com distribuição uniforme, então*

$$\lim_{n \rightarrow \infty} \Pr \left( \frac{v(x) - \ln \ln n}{\sqrt{\ln \ln n}} \geq t \right) = \frac{1}{\sqrt{2\pi}} \int_t^{\infty} e^{-s^2/2} ds.$$

24/05/2010

Provaremos agora o Lema 44, isto é, mostraremos que  $\sum_{p \leq x} 1/p = \ln \ln x + O(1)$ . Para isto, precisaremos utilizar alguns resultados.

**Lema 48** (Soma de Abel). *É verdade que*

$$\sum_{s < r \leq t} a(r)f(r) = A(t)f(t) - A(s)f(s) - \int_s^t A(\theta)f'(\theta) d\theta,$$

onde  $A(\theta) = \sum_{s < r \leq \theta} a(r)$ .

*Demonstração.* Consideramos, nesta prova,  $s$  e  $t$  inteiros, porém, o mesmo resultado é válido sem esta restrição (veja o exercício 12.1.1). Sabemos que

$$\begin{aligned} \int_k^{k+1} A(\theta)f'(\theta) d\theta &= \int_k^{k+1} A(k)f'(\theta) d\theta \\ &= A(k) \int_k^{k+1} f'(\theta) d\theta \\ &= A(k)(f(k+1) - f(k)). \end{aligned}$$

Assim,

$$\begin{aligned} \int_s^{s+1} A(\theta)f'(\theta) d\theta &= A(s)(f(s+1) - f(s)). \\ \int_{s+1}^{s+2} A(\theta)f'(\theta) d\theta &= A(s+1)(f(s+2) - f(s+1)). \\ &\vdots \\ \int_{t-1}^t A(\theta)f'(\theta) d\theta &= A(t-1)(f(t) - f(t-1)). \end{aligned}$$

---

<sup>1</sup>Os resultados desta seção foram apresentados pelo aluno Thiago da Silva Pinheiro.

Portanto,

$$\begin{aligned}
\int_s^t A(\theta)f'(\theta) d\theta &= -A(s)f(s) \\
&\quad - f(s+1)(A(s+1) - A(s)) \\
&\quad - f(s+2)(A(s+2) - A(s+1)) \\
&\quad \quad \quad \vdots \\
&\quad - f(t-1)(A(t-1) - A(t-2)) \\
&\quad + A(t-1)f(t) + (f(t)a(t) - f(t)a(t)).
\end{aligned}$$

Mas, como  $A(k+1) - A(k) = a(k)$ , temos que

$$\int_s^t A(\theta)f'(\theta) d\theta = -A(s)f(s) - \sum_{s < r \leq t} a(r)f(r) + A(t)f(t).$$

Assim, o resultado segue. □

O seguinte lema também será necessário.

**Lema 49.** *A igualdade  $\sum_{p \leq x} (\ln p)/p = \ln x + O(1)$  é válida, onde  $x \in \mathbb{R}$  e a soma é sobre os primos não maiores que  $x$ .*

*Demonstração.* Estimaremos o valor de  $\ln x!$  de duas maneiras distintas. Primeiro, observe que

$$\begin{aligned}
(17) \quad \ln x! &= \sum_{p \leq x} \left( \left( \left\lfloor \frac{x}{p} \right\rfloor + \left\lfloor \frac{x}{p^2} \right\rfloor + \dots \right) \ln p \right) \\
&= \sum_{p \leq x} \left( \left\lfloor \frac{x}{p} \right\rfloor \ln p \right) + \sum_{p \leq x} \left( \left( \left\lfloor \frac{x}{p^2} \right\rfloor + \left\lfloor \frac{x}{p^3} \right\rfloor + \dots \right) \ln p \right) \\
&< \sum_{p \leq x} \left( \left\lfloor \frac{x}{p} \right\rfloor \ln p \right) + x \sum_{p \leq x} \left( \left( \frac{1}{p^2} + \frac{1}{p^3} \dots \right) \ln p \right) \\
&= \sum_{p \leq x} \left( \left\lfloor \frac{x}{p} \right\rfloor \ln p \right) + x \sum_{p \leq x} \frac{\ln p}{p(p-1)} \\
&= \sum_{p \leq x} \left( \left\lfloor \frac{x}{p} \right\rfloor \ln p \right) + O(x).
\end{aligned}$$

Mas veja que  $0 \leq \int_x^{x+1} \ln t dt - \ln x = \int_x^{x+1} \ln(t/x) dt \leq \int_x^{x+1} (t/x - 1) dt = 1/2x$ . Assim,

$$\sum_{n \leq x-1} \left( \int_n^{n+1} \ln t dt - \ln n \right) = O(\ln x),$$

de onde concluímos que

$$\int_1^x \ln t \, dt - \sum_{n \leq x-1} \ln n = O(\ln x).$$

Logo, temos que  $x \ln x - x + 1 - \sum_{n \leq x-1} \ln n = O(\ln x)$ . Portanto,

$$\sum_{n \leq x} \ln n = x \ln x + O(x).$$

Desta forma,  $\ln x! = x \ln x + O(x)$ . Isto, juntamente com (17), nos diz que

$$(18) \quad \sum_{p \leq x} \left( \left\lfloor \frac{x}{p} \right\rfloor \ln p \right) = x \ln x + O(x).$$

Observando que  $\sum_{p \leq x} (\lfloor x/p \rfloor \ln p) = \sum_{p \leq x} (x/p + O(1)) \ln p$ , obtemos

$$(19) \quad \sum_{p \leq x} \left( \left\lfloor \frac{x}{p} \right\rfloor \ln p \right) = \sum_{p \leq x} \left( \frac{x}{p} \ln p \right) + O(\pi(x) \ln x),$$

onde  $\pi(x)$  denota a quantidade de primos não maiores que  $x$ . Dividindo (18) e (19) por  $x$ , temos

$$\sum_{p \leq x} \left( \frac{\ln p}{p} \right) = \ln x + O(1) + O\left( \frac{\pi(x)}{x/\ln x} \right).$$

Mas é verdade que  $\pi(x) = \theta(x/\ln x)$  (Este fato será provado na próxima seção). Com isto, completamos a prova, pois

$$\sum_{p \leq x} \left( \frac{\ln p}{p} \right) = \ln x + O(1).$$

□

Vamos à prova do Lema 44, isto é, provaremos que  $\sum_{p \leq x} 1/p = \ln \ln x + O(1)$ .

*Demonstração do Lema 44.* Tomando  $f(r) = 1/\ln r$  e fazendo  $a(r) = (\ln p)/p$  se  $r = p$  para  $p$  primo e  $a(r) = 0$  caso contrário, obtemos a seguinte relação ao aplicar o Lema 48 (Soma de Abel).

$$\sum_{p \leq x} \frac{1}{p} = \frac{A(x)}{\ln x} + \int_2^x \frac{A(t)}{t(\ln t)^2} \, dt.$$

Mas como  $A(x) = \sum_{p \leq x} (\ln p)/p$ , obtemos, pelo Lema 49,

$$\begin{aligned}\sum_{p \leq x} \frac{1}{p} &= 1 + O(1) + \int_2^x \frac{\ln t + O(1)}{t(\ln t)^2} dt \\ &= 1 + O(1) + \int_2^x \frac{1}{t \ln t} + \int_2^x \frac{O(1)}{t(\ln t)^2} dt \\ &= \ln \ln x + O(1) + \int_2^x \frac{O(1)}{t(\ln t)^2} dt \\ &= \ln \ln x + O(1).\end{aligned}$$

□

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

1. Prove o Lema 48 sem a suposição de que  $s$  e  $t$  sejam inteiros.

13. TEORIA ADITIVA DOS NÚMEROS

31/05/2010

Em uma carta endereçada a Euler, Goldbach propôs, em 1742, a seguinte conjectura.

**Conjectura 50** (Goldbach). *Para todo  $n \geq 2$  par, existem primos  $p, q$  tal que  $p + q = n$ .*

Computacionalmente já foi verificado que tal conjectura é válida para  $n \leq 4 \times 10^{11}$ . Os seguintes resultados dizem respeito a esta conjectura.

**Teorema 51** (Lagrange). *Todo natural pode ser escrito como soma de no máximo quatro quadrados.*

**Teorema 52** (Fermat). *Todo primo  $p \equiv 1 \pmod{4}$  pode ser escrito como soma de dois quadrados.*

**Teorema 53** (Vinogradov). *Todo inteiro ímpar suficientemente grande pode ser escrito como soma de no máximo três primos.*

**Teorema 54** (Shnirelman). *Existe uma constante  $h$  tal que todo inteiro  $n \geq 2$  pode ser escrito como soma de no máximo  $h$  primos.*

Provaremos o Teorema 54. Para tal, considere o conjunto  $A = \{0 < a_1 < a_2 < \dots\} \subset \mathbb{N}$  e seja  $A(x) = \max\{k: a_k \leq x\}$  a quantidade de elementos de  $A$  não maiores que  $x$ . Definimos a *densidade de Shnirelman* como  $\sigma(A) = \inf_{n \geq 1} A(n)/n$ . Podemos observar os seguintes fatos sobre a densidade de Shnirelman.

- (i) Se  $1 \notin A$ , então  $\sigma(A) = 0$ .
- (ii) Se  $a_k = 1 + (k - 1)d$ , para  $k = 1, 2, \dots$ , então  $\sigma(A) = 1/d$ .
- (iii) Se  $a_n = \lfloor (1 + \alpha)^n \rfloor$ , para  $\alpha > 0$ , então  $\sigma(A) = 0$ .
- (iv) Se  $a_n = n^2$ , para  $n \geq 1$ , então  $\sigma(\alpha) = 0$ .
- (v) Se  $1 \in A$  mas  $\sigma(A) = 0$ , então, para todo  $\varepsilon > 0$ , existe  $m$  arbitrariamente grande tal que  $A(m) \leq \varepsilon m$ .
- (vi)  $\sigma(A) = 1$  se e somente se  $\{1, 2, \dots\} \subset A$ .

Dados  $A, B \subset \mathbb{N}$ , definimos  $A + B = \{a + b: a \in A, b \in B\}$ . Em geral, para  $A_1, \dots, A_h \subset \mathbb{N}$ , temos que  $A_1 + \dots + A_h = \{a_1 + \dots + a_h: a_i \in A_i \text{ para todo } i\}$ . Considere também os seguintes conjuntos.

- 1)  $S = \{0, 1, 4, 9, 16, \dots\}$ , o conjunto de todos os quadrados perfeitos.
- 2)  $(4\mathbb{N} + 1) = \{x \in \mathbb{N}: x = 1 \pmod{4}\}$ .
- 3)  $\mathcal{P} = \{p_1 < p_2 < \dots\}$ , o conjunto de todos os primos.

4)  $\mathcal{P}_0 = \mathcal{P} \cup \{0\}$ .

Podemos reescrever a Conjectura de Goldbach e os teoremas enunciados anteriormente com base nesses conjuntos.

**Conjectura 50** (Goldbach).  $2\mathcal{P} \supset \{n > 2: n \in \mathbb{N} \text{ par}\}$ .

**Teorema 51** (Lagrange)  $4S \supset \mathbb{N}$ .

**Teorema 52** (Fermat)  $2S \supset \mathcal{P} \cap (4\mathbb{N} + 1)$ .

**Teorema 53** (Vinogradov) Existe  $n_0$  tal que  $3\mathcal{P}_0 \supset \{n \in \mathbb{N}: n \geq n_0, n \text{ ímpar}\}$ .

**Teorema 54** (Shnirelman) Existe  $h \in \mathbb{N}$  tal que  $h\mathcal{P}_0 \supset \mathbb{N} \setminus \{1\}$ .

A seguinte definição será importante.

**Definição 55.** Dizemos que  $A \subset \mathbb{N}$  é uma base de ordem  $h$  de  $\mathbb{N}$  se  $hA \supset \mathbb{N}$ . Ademais, se existe  $h$  tal que  $A$  é base de ordem  $h$ , então dizemos que  $A$  é uma base de ordem finita.

Os seguintes resultados compõem a prova do Teorema 54 (Shnirelman).

**Teorema 56.** Se  $0 \in A \subset \mathbb{N}$  e  $\sigma(A) > 0$ , então  $A$  é base de ordem finita.

**Lema 57.** Se  $A = 2\mathcal{P} + \{0, 1\}$ , então  $\sigma(A) > 0$ .

**Teorema 58.** O Teorema 56 e o Lema 57 implicam o Teorema 54.

*Demonstração do Teorema 58.* Seja  $A$  como no Lema 57. Pelo Teorema 58,  $A$  é base de ordem  $h$ , para algum  $h$ . Seja  $N \geq 2$ . Como  $A$  é base de ordem  $h$ , temos que  $0 \leq N - 2 = a_1 + \dots + a_h$ , com  $a_i \in A$  para todo  $i$ . Sem perda de generalidade, temos  $N - 2 = k + (p_1 + q_1) + \dots + (p_l + q_l)$ , onde  $k + l \leq h$  e  $\{p_i, q_i\} \in \mathcal{P}$  para todo  $i$ . Se  $k = 0$ , então podemos escrever  $N$  da seguinte forma:  $N = 2 + p_1 + q_1 + \dots + p_l + q_l$ , isto é, como soma de  $2l + 1 \leq 2h$  primos. Suponha que temos  $0 < k = 2m + r$ , com  $r \in \{0, 1\}$ . Se  $r = 0$ , então  $N = 2(m + 1) + \sum_{i=1}^l (p_i + q_i)$ . Assim,  $N$  é soma de  $m + 1 + 2l \leq 3h$  primos. Se  $r = 1$ , então  $N = 3 + 2m + \sum_{i=1}^l (p_i + q_i)$ . Logo,  $N$  é soma de  $2m + 1 + 2l \leq 3h$  primos. Concluimos que  $(3h)\mathcal{P}_0 \supset \{2, 3, \dots\}$ .  $\square$

A fim de provar o Teorema 56, precisamos provar alguns lemas e corolários.

**Lema 59.** Suponha que  $0 \in A \subset \mathbb{N}$  e  $0 \in B \subset \mathbb{N}$ . Se  $h \geq 0$  e  $A(n) + B(n) \geq n$ , então  $n \in A + B$ .

*Demonstração.* Se  $n \in A$  ou  $n \in B$ , então  $n \in A + B$ . Portanto, podemos considerar  $n \notin A \cup B$ . Assim, temos  $A(n - 1) + B(n - 1) = A(n) + B(n) \geq n$ . Suponha  $A \cap [n - 1] = \{a_1 < a_2 < \dots < a_r\}$

e  $B \cap [n-1] = \{b_1 < b_2 < \dots < b_s\}$ . Considere  $A$  e  $n - (B \cap [n-1]) = \{n - b_s < \dots < n - b_1\}$ . Como  $r + s = A(n-1) + B(n-1) \geq n$ , segue que existem  $i, j$  tais que  $a_i = n - b_j$ . Portanto, temos  $n = a_i + b_j$ .  $\square$

**Corolário 60.** *Seja  $0 \in A \subset \mathbb{N}$  e  $0 \in B \subset \mathbb{N}$ . Se  $\sigma(A) + \sigma(B) \geq 1$ , então  $n \in A + B$  para todo  $n \geq 0$ .*

*Demonstração.* Fixado  $n$ , temos que  $A(n) + B(n) \geq n\sigma(A) + n\sigma(B) \geq n$ . Pelo Lema 59, temos que  $n \in A + B$ .  $\square$

**Corolário 61.** *Se  $0 \in A$  e  $\sigma(A) \geq 1/2$ , então  $A$  é uma base de ordem 2, isto é,  $2A \supset \mathbb{N}$ .*

**Lema 62.** *Se  $0 \in A \subset \mathbb{N}$  e  $0 \in B \subset \mathbb{N}$ , então  $\sigma(A + B) \geq \sigma(A) + \sigma(B) - \sigma(A)\sigma(B)$ , isto é,  $1 - \sigma(A + B) \leq (1 - \sigma(A))(1 - \sigma(B))$ .*

*Observação.* Mann provou um resultado melhor que o apresentado no lema acima, onde concluiu que  $\sigma(A + B) \geq \sigma(A) + \sigma(B)$ .

Por indução em  $h$ , podemos provar o seguinte resultado.

**Corolário 63.** *Se  $0 \in A_i \subset \mathbb{N}$  para  $i = 1, \dots, h$ , então  $1 - \sigma(A_1 + \dots + A_h) \leq \prod_{i=1}^h (1 - \sigma(A_i))$ .*

Finalmente estamos aptos a provar o Teorema 56.

*Demonstração do Teorema 56.* Seja  $A \subset \mathbb{N}$  com  $0 \in A$  e  $\sigma(A) > 0$ . Então  $1 - \sigma(A) < 1$  e portanto existe  $k$  tal que  $(1 - \sigma(A))^k < 1/2$ . Assim, pelo Corolário 63, temos que  $1 - \sigma(kA) \leq (1 - \sigma(A))^k \leq 1/2$ . Assim,  $kA$  é tal que  $\sigma(kA) \geq 1/2$ . Pelo Corolário 61, temos que  $kA$  é base de ordem 2. Segue que  $A$  é base de ordem  $h = 2k$ .  $\square$

Nos resta mostrar a validade do Lema 57. Seja  $r(N)$  a quantidade de maneiras de escrever  $N$  como soma de dois primos (por exemplo,  $r(5) = 2$ ). Os seguintes dois lemas, quando combinados, implicam o Lema 57.

**Lema 64.** *Existem  $x_0$  e  $c > 0$  tais que  $\sum_{N=1}^x r(N) \geq cx^2/(\log x)^2$  para todo  $x \geq x_0$ .*

O lema acima segue do fato de  $\pi(x) \geq c''x/\log x$  para uma certa constante positiva  $c''$ .

**Lema 65.** *Existem  $x'_0$  e  $c' > 0$  tais que  $\sum_{N=1}^x r(N)^2 \leq c'x^3/(\log x)^4$  para todo  $x \geq x'_0$ .*

*Demonstração do Lema 57.* Por Cauchy-Schwarz,  $(\sum_{N=1}^x r(N))^2 \leq (\sum_{N=1}^x 1)(\sum_{n \leq x} r(N)^2)$ . Assim,

$$\begin{aligned} \left( \sum_{N=1}^x r(N) \right)^2 &\leq (2\mathcal{P})(x) \sum_{N=1}^x r(N)^2 \\ &\leq A(x) \sum_{N \leq x} r(N)^2. \end{aligned}$$

Portanto,

$$\begin{aligned} A(x) &\geq \frac{(\sum_{N=1}^x r(N))^2}{\sum_{N=1}^x r(N)^2} \\ &\geq \left( \frac{c}{c'} \right) x, \end{aligned}$$

onde a última desigualdade é válida quando  $x > \max\{x_0, x'_0\}$ . Desta forma, como  $1 \in A$ , segue que  $\sigma(A) \geq \min\{1/\max\{x_0, x'_0\}, c/c'\} > 0$ . Portanto, estamos feitos.  $\square$

Para maiores detalhes sobre o assunto, veja o livro de Khinchin [13].

14. UM PROBLEMA GEOMÉTRICO DE ERDŐS E FÜREDI - CONTINUAÇÃO

7/6/2010

Na seção 8 vimos um problema geométrico abordado por Erdős e Füredi em 1983 [6]. Dizemos que  $\mathcal{P}$  determina  $\sphericalangle abc = \alpha$  se  $a, b, c \in \mathcal{P}$ . Lembre que  $\alpha_n(\mathcal{P}) = \max\{0 \leq \alpha \leq \pi : \mathcal{P} \text{ determina } \alpha\}$ , onde  $\mathcal{P} \subset \mathbb{R}^n$  com  $\mathcal{P}$  finito. Erdős e Füredi mostraram que existe  $c > 1$  tal que existe  $\mathcal{P} \subset \mathbb{R}^n$  onde  $|\mathcal{P}| \geq c^n$  e  $\alpha_n(\mathcal{P}) < \pi/2$  (Observe que não podemos ter limite  $\pi/3$ , pois quaisquer três pontos determinam um ângulo não menor que  $\pi/3$ ).

Tome  $f_{\alpha}^{\leq}(n) = \max\{|\mathcal{P}| : \mathcal{P} \subset \mathbb{R}^n, \alpha_n(\mathcal{P}) \leq \alpha\}$ . Considerando o simplexo regular de dimensão  $n$ , observamos que  $f_{\pi/3}^{\leq}(n) \geq n + 1$ . Mas é verdade que  $f_{\pi/3}^{\leq}(n) \leq n + 1$ ?

Um bom exercício é pensar no seguinte problema.

**Problema 66.** *Fixe  $\varepsilon > 0$ . Prove que  $f_{\pi/3+\varepsilon}^{\leq}(n) \geq e^{cn}$  para algum  $c = c(\varepsilon) > 0$ .*

14/6/2010

O postulado de Bertrand diz que todo intervalo  $(n, 2n]$ , com  $n \geq 1$ , contém pelo menos um primo. Apresentamos nesta seção uma prova elegante de um resultado que implica uma versão mais fraca do postulado de Bertrand, a saber, para cada  $\varepsilon > 0$ , existe  $n_0 = n_0(\varepsilon)$  tal que se  $n \geq n_0$ , então o intervalo  $(n, (2 + \varepsilon)n]$  contém pelo menos um primo. O seguinte teorema é o resultado principal desta seção.

**Teorema 67.** *Para  $n \geq 4$ , temos que*

$$(\ln 2) \frac{n}{\log n} \leq \pi(n) \leq \left( \ln 4 + \frac{8 \ln \ln n}{\ln n} \right) \frac{n}{\ln n}.$$

Para provarmos o limite superior, vamos precisar da seguinte estimativa.

**Teorema 68.** *Para  $n \geq 1$ , temos*

$$\prod_{p \leq n} p \leq 4^n.$$

Com a estimativa dada pelo Teorema 68, observe que, para todo  $1 \leq t \leq n$ , temos

$$t^{\pi(n) - \pi(t)} \leq \prod_{t < p \leq n} p \leq 4^n.$$

Assim, aplicando o logaritmo natural dos dois lados, obtemos

$$\pi(n) \leq \frac{n \ln 4}{\ln t} + t.$$

Fazendo  $t = n/(\ln n)^2$ , temos que

$$\pi(n) \leq \left( \ln 4 + \frac{8 \ln \ln n}{\ln n} \right) \frac{n}{\ln n},$$

desde que  $n \geq 4$  (exercício).

Antes de provarmos o limite inferior, vamos à prova do Teorema 68.

*Demonstração do Teorema 68.* Utilizamos indução em  $n$  e supomos  $n \geq 3$ . Se  $n$  é par, o resultado segue por indução, uma vez que  $n$  não é primo. Portanto, considere  $n$  ímpar e faça  $n = 2m + 1$ . Observe que, como  $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ , então este coeficiente aparece duas vezes na expansão binomial de  $(1 + 1)^{2m+1}$ . Portanto,

$$\binom{2m+1}{m} \leq \frac{2^{2m+1}}{2} = 4^m.$$

Mas é fácil ver que

$$\left( \prod_{m+1 < p \leq 2m+1} p \right) \mid \binom{2m+1}{m} \leq 4^m.$$

Pela hipótese indutiva, temos que

$$\begin{aligned} \prod_{p \leq n} p &= \prod_{p \leq m+1} p \prod_{m+1 < p \leq 2m+1} p \\ &\leq 4^{m+1} 4^m \\ &= 4^n. \end{aligned}$$

□

Para completar a prova (provar o limite inferior), considere  $d_n$  o mínimo múltiplo comum dos números  $1, 2, \dots, n$ . Dizemos que  $p^v \mid x$  se  $p^v \mid x$  e  $p^{v+1}$  não divide  $x$ . Assim, se  $p^v \mid n$ , então existe  $m \leq n$  tal que  $p^v \mid m$ , de onde concluímos que  $p^v \leq n$ . Portanto,

$$\begin{aligned} d_n &= \prod_{p \leq n, p^v \mid d_n} p^v \\ &\leq \prod_{p \leq n} n \\ &= n^{\pi(n)}. \end{aligned}$$

Aplicando logaritmo dos dois lados da desigualdade acima, obtemos  $\pi(n) \geq \ln d_n / \ln n$ . O teorema abaixo completa a prova do Teorema 67.

**Teorema 69** (Nair [16]). *Para  $n \geq 7$ , temos que  $d_n \geq 2^n$ .*

*Demonstração.* Para começar, definimos, para  $1 \leq m \leq n$ ,

$$I(m, n) = \int_0^1 x^{m-1} (1-x)^{n-m} dx.$$

Através da expansão binomial de  $(1-x)^{n-m}$ , obtemos

$$I(m, n) = \sum_{j=0}^{n-m} (-1)^j \binom{n-m}{j} \frac{1}{m+j}.$$

Assim, é fácil ver que  $I(m, n)$  é um número racional cujo denominador divide  $d_n$ , uma vez que  $d_n$  é o mínimo múltiplo comum dos números  $1, 2, \dots, n$ . Mas note que, para todo  $0 \leq y \leq 1$ , temos a

seguinte igualdade.

$$\begin{aligned} \sum_{m=1}^n \binom{n-1}{m-1} y^{m-1} I(m, n) &= \int_0^1 (1-x+xy)^{n-1} dx \\ &= \frac{1}{n} \sum_{m=1}^n y^{m-1}. \end{aligned}$$

Desta forma, para  $1 \leq m \leq n$ , temos que

$$I(m, n) = \frac{1}{n \binom{n-1}{m-1}} = \frac{1}{m \binom{n}{m}}.$$

Com isso, temos que  $m \binom{n}{m} | d_n$  para  $1 \leq m \leq n$ . Portanto, podemos concluir que  $n \binom{2n}{n} | d_{2n} | d_{2n+1}$  e  $(n+1) \binom{2n+1}{n} = (2n+1) \binom{2n}{n} | d_{2n+1}$ . Mas como  $n$  e  $2n+1$  são números primos entre si, temos que  $n(2n+1) \binom{2n}{n} | d_{2n+1}$ . Assim, podemos concluir que

$$d_{2n+1} \geq n4^n, \quad n \geq 1.$$

$$d_{2n+1} \geq 2 \cdot 4^n = 2^{2n+1}, \quad n \geq 2.$$

$$d_{2n+2} \geq d_{2n+1} \geq 4^n + 1, \quad n \geq 4.$$

Temos então o resultado desejado,  $d_n \geq 2^n$ , para  $n \geq 9$ . Para  $n = 7$  e  $n = 8$ , o resultado pode ser facilmente verificado. □

## REFERÊNCIAS

- [1] N. Alon and F. R. K. Chung, *Explicit construction of linear sized tolerant networks*, Proceedings of the First Japan Conference on Graph Theory and Applications (Hakone, 1986), vol. 72, 1988, pp. 15–19.
- [2] J. Beck, *On size Ramsey number of paths, trees, and circuits. I*, J. Graph Theory **7** (1983), no. 1, 115–129.
- [3] C. Chvatál, V. Rödl, E. Szemerédi, and W. T. Trotter, Jr., *The Ramsey number of a graph with bounded maximum degree*, J. Combin. Theory Ser. B **34** (1983), no. 3, 239–243.
- [4] L. Danzer and B. Grünbaum, *Über zwei Probleme bezüglich konvexer Körper von P. Erdős und von V. L. Klee*, Math. Z. **79** (1962), 95–99.
- [5] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, Amer. J. Math. **62** (1940), 738–742.
- [6] P. Erdős and Z. Füredi, *The greatest angle among  $n$  points in the  $d$ -dimensional Euclidean space*, Combinatorial mathematics (Marseille-Luminy, 1981), North-Holland Math. Stud., vol. 75, North-Holland, Amsterdam, 1983, pp. 275–283.
- [7] P. Erdős, A. Rényi, and V. T. Sós, *On a problem of graph theory*, Studia Sci. Math. Hungar. **1** (1966), 215–235.
- [8] P. Erdős, *Some unsolved problems*, Michigan Math. J. **4** (1957), 291–300.
- [9] J. Friedman and N. Pippenger, *Expanding graphs contain all small trees*, Combinatorica **7** (1987), no. 1, 71–76.
- [10] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science.
- [11] P. Hall, *On representatives of subsets*, Journal of London Mathematical Society (1935), 26–30.
- [12] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number  $n$  [Quart. J. Math. **48** (1917), 76–92]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 262–275.
- [13] A. Y. Khinchin, *Three pearls of number theory*, Graylock Press, Rochester, N. Y., 1952.
- [14] A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277.
- [15] G. A. Margulis, *Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators*, Problemy Peredachi Informatsii **24** (1988), no. 1, 51–60.
- [16] M. Nair, *On Chebyshev-type inequalities for primes*, Amer. Math. Monthly **89** (1982), no. 2, 126–129.
- [17] J. Nešetřil and V. Rödl, *A short proof of the existence of highly chromatic hypergraphs without short cycles*, J. Combin. Theory Ser. B **27** (1979), no. 2, 225–227.
- [18] R. Rado, *Note on the transfinite case of Hall's theorem on representatives*, J. London Math. Soc. **42** (1967), 321–324.
- [19] P. Turán, *On a theorem of Hardy and Ramanujan*, J. London Math. Soc. **9** (1934), 274–276.