O Lema de Szemerédi e Estruturas pseudoaleatórias

Jair Donadelli

Sumário

1. Introdução

1.1. Teoria dos Grafos. Como já é usual em combinatória, denotamos por $[n]$ o subconjunto

$$[n] = \{1, 2, \ldots, n\} \subseteq \mathbb{N},$$

onde $\mathbb{N}$ é o conjunto dos números naturais. Também é usual a seguinte notação: se V é um conjunto finito qualquer e $0 \leqslant k \leqslant |V|$, então usamos $\binom{V}{k}$ para denotar a família de todos os subconjuntos de V com cardinalidade k, ou seja,

$$\binom{V}{k} = \{U \colon U \subseteq V \text{ e } |U| = k\}.$$

Usamos 2^V para denotar

$$2^V = \bigcup_{k=0}^{|V|} \binom{V}{k},$$

o conjunto de todos os subconjuntos de V.

Um *hipergrafo* G é um par ordenado $G = (V, E)$, onde $V = V(G)$, é um conjunto finito cujos elementos são chamados *vértices* e $E = E(G) \subseteq 2^V$ é o conjunto das *arestas* de G. Quando todas as arestas de G têm a mesma cardinalidade, digamos que $E \subseteq \binom{V}{k}$, então chamamos G de *hipergrafo k-uniforme*. Quando quaisquer duas arestas de G têm no máximo um elemento comum chamamos G de *hipergrafo linear*.

Um *grafo* é um hipergrafo (linear) 2-uniforme. Note que essa definição de grafo exclui os grafos com laços e com arestas múltiplas.

Usamos $e_G(A, B)$, onde $A, B \subseteq V(G)$, para o número de arestas em $E_G(A, B)$,

$$E_G(A, B) = \{e \in E(G) \colon e \cap A \neq \emptyset \text{ e } e \cap B \neq \emptyset\}$$

ou seja, as arestas de G que encontram A e B.

Dado um vértice $v \in V(G)$, chamamos de *vizinhança* de v o conjunto

$$N_G(v) = \{w \in V(G) \colon \{v, w\} \in E(G)\},$$

cuja cardinalidade denotamos por $d_G(v)$ e chamamos de *grau de* v em G.

Dizemos que H é um *subgrafo* de G, e escrevemos $H \subseteq G$, se H é um grafo tal que $V(H) \subseteq V(G)$ e $E(H) \subseteq E(G)$. Um subgrafo H é dito *subgrafo induzido* se $E(H) = E(G) \cap \binom{V(H)}{2}$. Ademais, se $U \subseteq V(G)$, então U define naturalmente um subgrafo induzido, que denotamos por $G[U]$; também, se $F \subseteq E(G)$ então $G[F] = G[U]$, onde $U = \bigcup_{e \in F} e$.

Dois grafos G e H são *isomorfos* quando existe uma bijeção $\iota \colon V(G) \to V(H)$, tal que $\{v, w\} \in E(G)$ se, e somente se, $\{\iota(v), \iota(w)\} \in E(H)$. Por *uma cópia de* H *em* G entendemos um subgrafo $\bar{H} \subseteq G$ que é isomorfo a H.

Um *caminho* em G é uma seqüência $v_1, v_2, \ldots, v_{r-1}, v_r$ de vértices $v_i \in V(G)$ dois-a-dois distintos tais que $\{v_i, v_{i+1}\} \in E(G)$, para todo $i \in [r-1]$. O grafo definido pelo caminho com r vértices e $r-1$ arestas é denotado por P^r. Um *circuito* em G é um caminho $v_1, v_2, \ldots, v_r$ com a condição adicional que $\{v_1, v_r\} \in E(G)$. O circuito com r vértices e r arestas é denotado por C^r.

O grafo com r vértices, $r \in \mathbb{N}$, e todas as $\binom{r}{2}$ arestas é denotado por K^r e chamado de *grafo completo*. Por $K^{r,s}$ denotamos o *grafo bipartido completo* com r vértices numa partição e s vértices noutra sendo as únicas arestas as rs arestas que ligam vértices de partições distintas. Quando $r = 1$, o grafo bipartido completo é chamado *estrela*.

Seja $r \geqslant 1$ um inteiro qualquer e consideremos duas funções quaisquer $\phi \colon V(G) \to [r]$ e $\varphi \colon E(G) \to [r]$. Chamamos essas funções de *r-coloração* dos vértices e das arestas, respectivamente, de G. Também, chamamos ϕ de *coloração própria* dos vértices de G, se para toda aresta $e = \{u, v\} \in E(G)$ temos $|\phi(e)| > 1$, ou seja, se sob a coloração ϕ não existem arestas *monocromáticas*. O menor $r \in \mathbb{N}$ para o qual existe uma r-coloração própria dos vértices de G é chamado o *número cromático* de G, sendo denotado por $\chi(G)$.

De um modo geral, escrevemos $G = G^n$ quando queremos ressaltar que o grafo G tem n vértices.

1.2. Teoria de Ramsey. Dados os grafos Γ, $G_1, \ldots, G_q$ $(q \geqslant 1)$, escrevemos $\Gamma \to (G_1, \ldots, G_q)$ se, para qualquer q-coloração das arestas de Γ, $\varphi \colon E(\Gamma) \to [q]$, existe $i \in [q]$ tal que

$$\Gamma[\varphi^{-1}(i)] \text{ contém uma cópia de } G_i,$$

ou seja, existe $i \in [q]$ tal que o subgrafo de Γ induzido pelas arestas da cor i contém um subgrafo H isomorfo ao grafo G_i. Neste caso, dizemos que Γ é

ramsey com relação à q-upla $(G_1, \ldots, G_q)$. Definimos o *número de ramsey*

$$\mathrm{r}(G_1, \ldots, G_q) = \min\left\{n \colon K^n \to (G_1, \ldots, G_q)\right\}.$$

O Teorema de Ramsey afirma que existe $n \in \mathbb{N}$ tal que $K^n \to (G_1, \ldots, G_q)$.

1.3. Notação assintótica. Sejam f_n e g_n seqüências de números reais, onde $f_n > 0$ para todo n suficientemente grande. Usaremos as seguintes notações para o comportamento assintótico dessas seqüências:

- $g_n = O(f_n)$, quando $n \to \infty$, se existem constantes positivas $c \in \mathbb{R}$ e $n_0 \in \mathbb{N}$ tais que $|g_n| \leqslant cf_n$, para todo $n \geqslant n_0$;
- $g_n = \Omega(f_n)$, quando $n \to \infty$, se existem constantes positivas $C \in \mathbb{R}$ e $n_0 \in \mathbb{N}$ tais que $g_n \geqslant Cf_n$, para todo $n \geqslant n_0$;
- $g_n = \Theta(f_n)$, quando $n \to \infty$, se existem constantes positivas c, $C \in \mathbb{R}$ e $n_0 \in \mathbb{N}$ tais que $Cf_n \leqslant g_n \leqslant cf_n$, para todo $n \geqslant n_0$;
- $g_n = o(f_n)$ se $g_n/f_n \to 0$, quando $n \to \infty$.

1.4. Probabilidade discreta. Estaremos sempre considerando espaços amostrais finitos, também, para nós, uma *variável aleatória* X, num espaço de probabilidade $(\Omega, \mathbb{P})$, é uma função qualquer $X \colon \Omega \to \mathbb{R}$.

Escrevemos $\mathbb{P}\{X = t\}$ para a probabilidade do conjunto de todos os pontos $\omega \in \Omega$ tais que $X(\omega) = t$, ou seja,

$$\mathbb{P}\{X = t\} = \mathbb{P}\left(\{\omega \in \Omega \colon X(\omega) = t\}\right).$$

Definimos $\mathbb{P}\{X \geqslant t\}$ analogamente.

O *valor esperado* da variável aleatória X, que denotamos por $\mathbb{E}\,X$, é dado pela média

$$\mathbb{E}\,X = \sum_{t \in X(\Omega)} t\mathbb{P}\{X = t\}.$$

Daqui por diante, será importante termos em mente que estaremos tratando com resultados assintóticos. Sendo mais preciso, estaremos diante de situações como a que segue. Seja $\{(\Omega_n, \mathbb{P}_n)\}_{n\in\mathbb{N}}$ uma seqüência de espaços de probabilidade. Suponha que temos uma seqüência de eventos $A_n \subseteq \Omega_n$. Então, estaremos interessados em saber resultados como,

$$\mathbb{P}_n(A_n) > 1/2, \text{ para todo } n \text{ suficientemente grande,}$$

ou

$$\lim_{n\to\infty} \mathbb{P}_n(A_n) = 1.$$

Também, se $\{A_n\}_{n\in\mathbb{N}}$ é uma seqüência de eventos $A_n \subseteq \Omega_n$ de modo que $\mathbb{P}_n(A_n) \to 1$ quando $n \to \infty$, dizemos que ocorre A_n *quase certamente*.

Desigualdades, desvios e momentos. Para todo inteiro positivo k, o *k-ésimo momento* de uma variável aleatória X é o valor esperado de sua k-ésima potência $\mathbb{E}\, X^k$.

O método do primeiro momento é a ferramenta mais simples no uso da esperança e segue facilmente da sua definição:

$$\mathbb{E}\, X \leqslant t \Rightarrow \mathbb{P}\left\{X \leqslant t\right\} > 0.$$

Note que se $X \geqslant 0$ e $t_0 > 0$, então

$$\mathbb{E}\, X = \sum_{t \in X(\Omega)} t\mathbb{P}\left\{X = t\right\} \quad \geqslant \quad t_0 \sum_{\substack{t \in X(\Omega) \\ t \geqslant t_0}} \mathbb{P}\left\{X = t\right\} \quad = \quad t_0 \mathbb{P}\left\{X \geqslant t_0\right\},$$

donde concluímos a seguinte desigualdade.

Desigualdade de Markov. *Se X é uma variável aleatória positiva e $t > 0$ então*

$$\mathbb{P}\left\{X \geqslant t\right\} \leqslant \frac{\mathbb{E}\, X}{t}. \tag{1}$$

Note que, se $\{X_n\}_{n \in \mathbb{N}}$ é uma seqüência de variáveis aleatórias definidas sobre a seqüência $\{(\Omega_n, \mathbb{P}_n)\}_{n \in \mathbb{N}}$ de espaços de probabilidade de modo que $\mathbb{E}\, X_n \to 0$ quando $n \to \infty$, então nós podemos deduzir de (1) que $\mathbb{P}\left\{X_n > 0\right\} \to 0$ quando $n \to \infty$ e, nesse caso, temos $X_n = 0$ quase certamente.

A *variância* de X é dada por

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

Dessa forma, se λ é um real positivo, então

$$\mathbb{P}\left\{|X - \mathbb{E}\, X| \geqslant \lambda\sqrt{\text{Var } X}\right\} = \mathbb{P}\left\{(X - \mathbb{E}\, X)^2 \geqslant \lambda^2 \text{ Var } X\right\}.$$

Usando a desigualdade de Markov e fazendo a escolha apropriada para λ, temos um método de segundo momento.

Desigualdade de Chebyshev. *Para todo real $\varepsilon > 0$ e toda variável aleatória X temos*

$$\mathbb{P}\left\{\left|X - \mathbb{E}\, X\right| \geqslant \varepsilon \mathbb{E}\, X\right\} \leqslant \frac{\text{Var } X}{\varepsilon^2 (\mathbb{E}\, X)^2}. \tag{2}$$

Da desigualdade acima, podemos facilmente concluir que se Var $X = o((\mathbb{E}\, X)^2)$, então $X > 0$ quase certamente, ou ainda, $X = (1 + o(1))\mathbb{E}\, X$ quase certamente.

Muitas vezes só conseguimos provar que o lado direito de (2) tende a zero polinomialmente. Quando queremos usar essa probabilidade um número exponencial de vezes, a Desigualdade de Chebyshev não nos dá informação suficiente e temos que recorrer às desigualdades exponenciais. Usamos $\text{Bi}(n, p)$ para denotar a distribuição *binomial*.

Desigualdade de Chernoff (**?**). *Se* $X \in \mathrm{Bi}(n,p)$, $\lambda \geqslant 0$ *e* $\varphi(x) = (1+x)\ln(1+x) - x$, *para todo* $x \geqslant -1$, *então*

$$\mathbb{P}\left\{X - \mathbb{E}\,X \geqslant \lambda\right\} \leqslant \exp\left(-\mathbb{E}\,X\varphi\left(\frac{\lambda}{\mathbb{E}\,X}\right)\right) \leqslant \exp\left(-\frac{\lambda^2}{2(\mathbb{E}\,X + \lambda/3)}\right)$$

$$e \tag{3}$$

$$\mathbb{P}\left\{X - \mathbb{E}\,X \leqslant -\lambda\right\} \leqslant \exp\left(-\mathbb{E}\,X\varphi\left(\frac{\lambda}{\mathbb{E}\,X}\right)\right) \leqslant \exp\left(-\frac{\lambda^2}{2\mathbb{E}\,X}\right)$$

Da equação acima deduzimos que para todo $\lambda > 0$

$$\mathbb{P}\left\{\left|X - \mathbb{E}\,X\right| \geqslant \lambda\mathbb{E}\,X\right\} \leqslant 2\exp\left(-\varphi(\lambda)\mathbb{E}\,X\right) \leqslant 2\exp\left(-c_\lambda\mathbb{E}\,X\right), \tag{4}$$

onde $c_\lambda = 3\lambda^2/(6+2\lambda)$.

Uma outra versão da desiguldade pode ser escrita a da seguinte forma.

Desigualdade de Chernoff (**?**). *Se* $X_1, \ldots, X_n$ *são variáveis aleatórias independentes com* $|X_i| \leqslant 1$ *e* $\mathbb{E}\,X_i = 0$, $\lambda > 0$ *e* $X = \sum_i X_i$ *então*

$$\mathbb{P}\left\{X \geqslant \lambda\right\} < \exp\left(\frac{-2\lambda^2}{n}\right) \qquad e \qquad \mathbb{P}\left\{X \leqslant -\lambda\right\} < \exp\left(\frac{-2\lambda^2}{n}\right). \tag{5}$$

Um *martingal* é uma seqüência de vetores aleatórios $X_0, X_1, \ldots X_n$ que assume valores num espaço euclidiano $\mathcal{E}$ tal que $X_0 = 0$ e $\mathbb{E}\,\|X_i\| < \infty$ para todo $i \geqslant 1$, e $\mathbb{E}\,(X_i | X_0, \ldots, X_{i-1}) = X_{i-1}$.

Desigualdade de Azuma–Hoeffding (Hayes, 2003). *Se* $X_0, X_1, \ldots, X_n$ *é um martingal tal que* $\|X_i - X_{i-1}\| \leqslant c_i$, *então para todo* $a > 0$

$$\mathbb{P}\left(\|X_n\| \geqslant a\right) < 2\exp\left(-\frac{(a - Y_0)^2}{2\sum_{i=1}^n c_i^2}\right), \tag{6}$$

onde $Y_0 = \max\{1 + \max c_i, 2\max c_i\}$.

1.5. Dois modelos de grafos aleatórios. Vamos denotar por $\mathcal{G}(n)$ o conjunto de todos os grafos sobre o conjunto de vértices $V = [n] = \{1, 2, \ldots, n\}$. Seja $N = \binom{n}{2}$.

Vejamos os dois modelos mais conhecidos para grafos aleatórios.

Grafo aleatório binomial. O primeiro modelo que apresentamos é denotado por $\mathcal{G}(n,p)$, onde $0 \leqslant p \leqslant 1$. Nesse modelo o espaço amostral é o conjunto de todos os resultados possíveis do seguinte experimento. Dado p, com $0 \leqslant p \leqslant 1$, considere uma moeda com probabilidade p de dar cara. Começamos com o grafo sem arestas, isto é, o grafo $([n], \emptyset)$ e, para cada $\{i,j\} \in \binom{[n]}{2}$, lançamos a nossa moeda independentemente para cada par de vértices. Se o resultado for cara colocamos a aresta $\{i,j\}$ no grafo, caso contrário, não colocamos a aresta. Um grafo genérico definido desta forma é denotado por

$G_{n,p}$ e o chamamos de *grafo aleatório (binomial) com n vértices e probabilidade de arestas p*. Equivalentemente, temos $\mathcal{G}(n,p)$ considerando o conjunto $\mathcal{G}(n)$ com a função de probabilidade

$$\mathbb{P}_p(J) = p^e(1-p)^{N-e},$$

para um grafo $J \in \mathcal{G}(n)$ com e arestas.

Grafo aleatório uniforme. O outro modelo para grafos aleatórios, denotado por $\mathcal{G}(n,M)$, tem como espaço amostral o conjunto de todos os $\binom{N}{M}$ grafos sobre $V = [n]$ que têm exatamente M arestas, onde $0 \leqslant M \leqslant N$. Tomamos sobre esse espaço a distribuição uniforme, ou seja, se $J \in \mathcal{G}(n)$ então

$$\mathbb{P}_M(J) = \binom{N}{M}^{-1}.$$

Escrevemos $G_{n,M}$ para um grafo genérico sorteado uniformemente dentre todos os grafos com n vértices e M arestas.

Equivalências dos modelos de grafos aleatórios. Aqui daremos alguns resultados de eqüivalência assintótica entre os modelos binomial e uniforme de grafo aleatório. Para uma referência mais completa, com as demonstrações, o leitor deve consultar **?**

Seja $\mathcal{Q}$ uma família de grafos. Pela Lei das Probabilidades Totais temos

$$\mathbb{P}\{G_{n,p} \in \mathcal{Q}\} = \sum_{M=0}^{N} \mathbb{P}\{G_{n,M} \in \mathcal{Q}\} \binom{N}{M} p^M (1-p)^{N-M}.$$

Dizemos que $\mathcal{Q}$ é uma propriedade *crescente* se todo grafo que contém algum grafo de $\mathcal{Q}$ também pertence a $\mathcal{Q}$, isto é, $H \subseteq G$ e $H \in \mathcal{Q} \Rightarrow G \in \mathcal{Q}$.

Teorema 1. *Seja $\mathcal{Q}$ crescente, $M = M(n) \to \infty$ e $\delta > 0$ fixo tal que $0 \leqslant (1-\delta)p < (1+\delta)p \leqslant 1$, onde $p = M/N$.*

(1) *Se $\mathbb{P}\{G_{n,p} \in \mathcal{Q}\} \to 1$, então $\mathbb{P}\{G_{n,M} \in \mathcal{Q}\} \to 1$.*
(2) *Se $\mathbb{P}\{G_{n,p} \in \mathcal{Q}\} \to 0$, então $\mathbb{P}\{G_{n,M} \in \mathcal{Q}\} \to 0$.*
(3) *Se $\mathbb{P}\{G_{n,M} \in \mathcal{Q}\} \to 1$, então $\mathbb{P}\left\{G_{n,(1+\delta)p} \in \mathcal{Q}\right\} \to 1$.*
(4) *Se $\mathbb{P}\{G_{n,M} \in \mathcal{Q}\} \to 0$, então $\mathbb{P}\left\{G_{n,(1-\delta)p} \in \mathcal{Q}\right\} \to 0$.*

Dizemos que $\mathcal{Q}$ é uma propriedade *convexa* se $H \subseteq G \subseteq J$ e $H, J \in \mathcal{Q}$ implicam que $G \in \mathcal{Q}$.

Teorema 2. *Sejam $\mathcal{Q}$ uma propriedade convexa e $0 \leqslant M \leqslant N$. Se $\mathbb{P}\{G_{n,M/N} \in \mathcal{Q}\} \to 1$ então $\mathbb{P}\{G_{n,M} \in \mathcal{Q}\} \to 1$.*

1.6. Tranformada de Fourier. Sejam $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ o grupo multiplicativo dos números complexos e G um grupo abeliano finito de ordem N. Um *caracter* de G é um homomorfismo $\chi\colon G \to \mathbb{C}^*$. Como $\chi(a)^N = \chi(Na) = \chi(0) = 1$ um caracter assume valores nas N raízes da unidade.

Note que o produto de caracteres $(\chi\varphi)(a) = \chi(a)\varphi(a)$ é um caracter e, então, o conjunto dos caracteres de G com o produto definido acima e o elemento unidade

$$\chi_0(a) = 1 \qquad (\forall a \in G),$$

chamado de *caracter principal* é um grupo, que é denotado por $\widehat{G}$ e chamado de *grupo dual* de G.

Algumas propriedades importantes dos caracteres seguem diretamente da definição. No seguinte resultado, temos as relações de ortogonalidade dadas em (ii) e (iv).

PROPOSIÇÃO 3. *Sejam χ, ξ, φ caracteres de G com $\chi \neq \chi_0$ e a, b, c elementos de G com $a \neq 0$. Valem as seguintes relações de ortogonalidade.*

(i) $\displaystyle\sum_{g\in G} \chi(g) = 0.$

(ii) *A soma* $\displaystyle\sum_{g\in G} \xi(g)\overline{\varphi(g)}$ *é 0 se $\xi \neq \varphi$ e N caso contrário.*

(iii) $\displaystyle\sum_{\zeta\in \widehat{G}} \zeta(a) = 0.$

(iv) *A soma* $\displaystyle\sum_{\zeta\in \widehat{G}} \zeta(b)\overline{\zeta(c)}$ *é 0 se $b \neq c$ e N caso contrário.*

DEMONSTRAÇÃO. Para o item (i), seja $b \in G$ tal que $\chi(b) \neq 1$ (que existe pois χ é não-principal). Então $\chi(b)\sum_{g\in G}\chi(g) = \sum_{g\in G}\chi(b+g) = \sum_{g\in G}\chi(g)$ donde segue o resultado.

O item (ii) para $\xi = \varphi$ é imediato, caso contrário, segue do item (i).

Note que existe um isomorfismo natural $G \cong \widehat{\widehat{G}}$, dado por $a \in G \mapsto \tilde{a} \in \widehat{\widehat{G}}$ definido por $\tilde{a}(\chi) = \chi(a)$. Assim, os itens (iii) e (iv) seguem dos itens (i) e (ii) formulados para o grupo $\widehat{G}$. □

EXERCÍCIO 4. Mostre que se G é soma direta, digamos $G = H_1 \oplus H_2$, então $\widehat{G} \cong \widehat{H_1} \oplus \widehat{H_2}$. De $\mathbb{Z}_N \cong \widehat{Z}_N$ (veja exercício 64) conclua que $G \cong \widehat{G}$, para todo G abeliano e finito.

Prova-se que $\widehat{G}$ é uma base ortonormal do espaço vetorial das funções $G \to \mathbb{C}$, denotado por $\mathbb{C}^G$, de dimensão N e com o produto interno

$$\langle f, g\rangle_G = \frac{1}{N}\sum_{a\in G} \overline{f(a)}g(a). \tag{7}$$

Logo, qualquer função $f\colon G \to \mathbb{C}$ pode ser escrita como

$$f(a) = \sum_{\chi \in \widehat{G}} c_\chi \chi(a) \qquad (\forall a \in G)$$

e os coeficientes $c_\chi = \langle f, \chi \rangle_G$ são chamados *coeficientes de Fourier*.

A função

$$\widehat{f}(\chi) = N c_{\overline{\chi}} = \sum_{a \in G} f(a)\chi(a) \qquad (\forall \chi \in \widehat{G})$$

é chamada de *transformada de Fourier* de f. A *transformada inversa* é facilmente calculada

$$f(a) = \sum_{\chi \in \widehat{G}} c_\chi \chi(a) = \sum_{\chi \in \widehat{G}} \frac{1}{N} \widehat{f}(\overline{\chi})\chi(a) = \frac{1}{N} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\chi(a)}.$$

Exercício 5. Defina $\delta \in \mathbb{C}^G$ por

$$\delta(a) = \begin{cases} 1, & \text{se } a = 0 \\ 0, & \text{caso contrário.} \end{cases}$$

Mostre que

$$\widehat{\delta}(\chi) = 1 \quad (\forall \chi \in \widehat{G}) \qquad \text{e} \qquad \delta(a) = \frac{1}{N} \sum_{\chi \in \widehat{G}} \chi(a) \quad (\forall a \in G).$$

Teorema 6 (Fórmula de Plancherel). *Para quaisquer* $f, g \in \mathbb{C}^G$

$$\langle \widehat{f}, \widehat{g} \rangle_G = N \langle f, g \rangle_{\widehat{G}}.$$

Demonstração. Para cada $a \in G$ defina a função $\chi_a\colon G \to \mathbb{C}$ por $\chi_a(b) = \delta(b - a)$. Dessa forma, temos que $\widehat{\chi_a}(\varphi) = \varphi(a)$ para todo $\varphi \in \widehat{G}$ e, por ortogonalidade

$$\langle \widehat{\chi_a}, \widehat{\chi_b} \rangle_{\widehat{G}} = \frac{1}{N} \sum_{\varphi \in \widehat{G}} \overline{\varphi(a)}\varphi(b) = \begin{cases} 1, & \text{se } a = b \\ 0, & \text{caso contrário.} \end{cases}$$

Por outro lado

$$\langle \chi_a, \chi_b \rangle_G = \frac{1}{N} \sum_{c \in G} \overline{\delta(a - c)}\delta(b - c) = \begin{cases} 1/N, & \text{se } a = b \\ 0, & \text{caso contrário.} \end{cases}$$

Portanto, $\langle \widehat{\chi_a}, \widehat{\chi_b} \rangle_{\widehat{G}} = N \langle \chi_a, \chi_b \rangle_G$.

Agora, $\{\chi_a\colon a \in G\}$ forma uma base de $\mathbb{C}^G$. Estendendo por linearidade temos a fórmula de Plancherel para quaisquer $f, g \in \mathbb{C}^G$. □

A *convolução* das funções $f, g \in \mathbb{C}^G$ é

$$f * g(a) = \sum_{b \in G} f(b)g(a-b), \tag{8}$$

e é facilmente provada a identidade

$$\widehat{f * g}(\chi) = \widehat{f}(\chi)\widehat{g}(\chi). \tag{9}$$

1.7. Matrizes reais simétricas. Assumimos que matrizes serão sempre quadradas. Se A é uma matriz sobre $\mathbb{C}$ então denotamos por A^* a sua transposta conjugada. Chamamos $\lambda \in \mathbb{C}$ de *autovetor* se existe vetor coluna não-nulo $\mathbf{v}$, chamado de *autovalor* associados de A, se

$$A\mathbf{v} = \lambda\mathbf{v}. \tag{10}$$

Equivalentemente, λ é um autovalor de A se, e somente se, for raiz do polinômio $p(x) = \det(A - xI)$, onde I é a matriz identidade. Dessa forma, pelo Teorema Fundamental da Álgebra, toda matriz tem autovalor. Agora, notemos que multiplicando ambos os lados de (10) por $\mathbf{v}^*$ temos

$$\mathbf{v}^* A\mathbf{v} = \lambda\|\mathbf{v}\|^2$$

e tomando o conjugado transposto nos dois lados da igualdade acima temos que

$$(\mathbf{v}^* A\mathbf{v})^* = \mathbf{v}^*(\mathbf{v}A)^* = \mathbf{v}^* A^*\mathbf{v} = \overline{\lambda}\|\mathbf{v}\|^2,$$

portanto, se $A = A^*$, então λ é igual ao seu conjugado complexo $\overline{\lambda}$.

PROPOSIÇÃO 7. *Uma matriz $n \times n$ real e simétrica tem autovalores λ_1, λ_2, $\ldots$, λ_n reais.* □

Dizemos que uma matriz é *ortogonal* se seus vetores coluna são ortonormais, isto é, são dois-a-dois ortogonais e de norma 1. O seguinte resultado é bastante conhecido e pode ser encontrado na maioria dos textos de Álgebra Linear como *Teorema Espectral* (Real).

TEOREMA 8. *Se A é uma matriz $n \times n$ real e simétrica então existe uma matriz ortogonal Q tal que $A = Q^{\mathrm{T}} D Q$, onde $D = \mathrm{diag}(\lambda_1, \lambda_2, \ldots, \lambda_n)$.*

Esse resultado é equivalente a: *Se A é uma matriz $n \times n$ real e simétrica então existe uma base do $\mathbb{R}^n$ formada por autovetores de A.* Não é difícil provar que essa afirmação é equivalente ao teorema acima.

Se A é real e simétrica então $\mathbf{x}^{\mathrm{T}} A\mathbf{x} = \mathbf{x}^{\mathrm{T}} Q^{\mathrm{T}} DQ\mathbf{x} = \mathbf{y}^{\mathrm{T}} D\mathbf{y}$, onde $\mathrm{y} = Q\mathbf{x}$. Observamos que se $\|\mathbf{x}\| = 1$ então $\|\mathbf{y}\| = 1$ e que $\mathbf{y}^{\mathrm{T}} D\mathbf{y} = \lambda_1 {y_1}^2 + \lambda_2 {y_2}^2 + \cdots + \lambda_n {y_n}^2$. Logo, de $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$ temos

$$\lambda_1 = \max\{\mathbf{x}^{\mathrm{T}} A\mathbf{x} \colon \mathbf{x} \in \mathbb{R}^n \text{ e } \|\mathbf{x}\| = 1\}. \tag{11}$$

Exercício 9. Mostre que se $\mathbf{x}_1$ é o autovetor associado a λ_1 então

$$\lambda_2 = \max\{\mathbf{x}^{\mathsf{T}} A\mathbf{x} \colon \mathbf{x} \in \mathbb{R}^n,\ \mathbf{x} \perp \mathbf{x}_1 \text{ e } \|\mathbf{x}\| = 1\}.$$

Finalmente enunciamos o seguinte resultado, conhecido como *Teorema de Perron-Frobenius* para matrizes reais, simétricas e não-negativas.

Teorema 10. *Se A é uma matriz real não-negativa então A tem um autovalor real $\lambda_1 > 0$ e exite um autovetor positivo associado a λ_1. Além disso $|\lambda| \leqslant \lambda_1$ para todo λ autovalor de A e $\lambda = -\lambda_1$ se e somente se A é da forma*

$$\begin{pmatrix} \mathbf{0} & B \\ B^{\mathsf{T}} & \mathbf{0} \end{pmatrix} \tag{12}$$

Para finalizar, dizemos que desses resultados podemos deduzir várias propriedades de grafos a partir do espectro da matriz de adjacências.

2. Um breve histórico

Quando Issai Schur trabalhava com distribuição de resíduos quadráticos em $\mathbb{Z}_p$ conjecturou que se os números naturais fossem particionados em um número finito de partes então pelo menos uma das partes conteria uma progressão aritmética arbitrariamente longa. Esse resultado foi demonstrado por van der Waerden (1927) e é um dos resultados pioneiros da Teoria de Ramsey.

O Teorema de van der Waerden pode ser formulado da seguinte maneira que é equivalente ao enunciado acima por um argumento de compacidade (veja Graham et al., 1980, Seção 1.5).

Teorema de van der Waerden. *Dados os naturais k e r existe um natural $W = W(k, r)$ tal que se particionamos o conjunto $\{1, 2, \ldots, W\} \subset \mathbb{N}$ em r classes, então pelo menos uma dessas classes contém uma progressão aritmética com k termos.*

Uma questão que surge naturalmente, e revelou-se muito difícil, é saber quão rápido é o crescimento de $W(k, r)$ como função de k e r. Pode-se deduzir uma cota superior para $W(k, r)$ que cresce muito rapidamente da demonstração de van der Waerden (1927). Já no caso $r = 2$ a velocidade com que $W(k, 2)$ cresce é tão rapida quanto a função de Ackermann $A_k(k)$, que é definida para todo natural k a partir de

$$A_m(k) = \begin{cases} 2 + k & \text{se } m = 1, \\ 2 & \text{se } m > 1 \text{ e } k = 1, \\ A_{m-1}(A_m(k-1)) & \text{caso contrário.} \end{cases}$$

Uma demonstração do Teorema de van der Waerden devida a Shelah (1988) fornece $W(k, 2) \leqslant A_5(k)$, que melhora muito o limitante superior mas ainda

está longe do melhor limitante inferior conhecido que é exponencial em k (Berlekamp, 1968, mostrou que $W(k+1,2) > k2^k$).

O seguinte argumento probabilístico mostra que $W(k,2) \geqslant \sqrt{2^k}$. Para cada elemento do conjunto $[n] = \{1, 2, \ldots, n\} \subset \mathbb{N}$, sorteamos com probabilidade $1/2$ uma dentre duas cores, digamos azul e vermelha, independentemente. Dessa forma um subconjunto $S \subseteq [n]$ é monocromático com probabilidade $2^{1-|S|}$. Se S é escolhido dentre as progressões aritméticas com k termos, então a probabilidade de existir S monocromático é menor que 1 dado que $(n^2/2)2^{1-k} < 1$. Ou seja, vale que $W(k,2) > \sqrt{2^k}$.

Exercício 11. Generalize o argumento acima para mostrar que $W(k,r) > \sqrt{2r^{k-1}}$.

Erdős e Turán investigaram a grandeza do maior subconjunto de $[n]$ que não contém uma progressão aritmética de k termos, a qual denotamos por $r_k(n)$, esperando melhorar a cota superior para $W(k,r)$. De fato, $r_k(n) < n/2$ implicaria que $W(k,2) < n$. Mais ainda, se $r_k(n) < \pi(n)$, onde $\pi(n) = (1+o(1))n/\log n$ é a quantidade de números primos menores ou iguais a n, então teríamos uma progressão aritmética de primos arbitrariamente longa, resolvendo assim o que na época era um velho problema da Teoria dos Números (veja seção 2.2).

Nessa investigação eles notaram que deve ser possível descobrir progressões aritméticas de k termos em qualquer subconjunto de inteiros suficientemente denso. Essa conjectura, que tinha uma recompensa de US$1000, foi resolvida por Roth para $k = 3$, (Roth, 1953) e por Szemerédi para $k = 4$ (Szemerédi, 1969) e em seguida para todo k (Szemerédi, 1975).

Essa linha de ataque ao problema revelou-se difícil e não contribuiu efetivamente para determinação de uma boa cota para o número $W(k,r)$. Mesmo determinar se $r_k(n) = o(n)$ não parecia fácil.

O Teorema de Szemerédi (1975), um *tour de fource* em combinatória, responde afirmativamente a conjectura de Erdős e Turán.

Teorema de Szemerédi. *Para todo inteiro $k > 2$ e todo real $0 < \varepsilon < 1$ existe um inteiro $n_0 = n_0(\varepsilon, k) > 0$ tal que, para todo inteiro $n \geqslant n_0$, se $A \subseteq [n]$ e $|A| > \varepsilon n$, então A deve conter uma progressão aritmética de k termos.*

Atualmente conhecemos demonstrações não combinatórias para Teorema de Szemerédi, como a que usa Teoria Ergódica e não fornece cota para n_0 devido a Furstenberg (1977), e a de Gowers (2001) que generaliza a prova de Roth usando análise harmonica e dá uma estimativa para n_0 que é

$$2^{2^{\varepsilon^{-\left(2^{2^{k+9}}\right)}}}.$$

A exata dependência de n_0 em ε e k não é conhecida.

Respondida a conjectura de Erdős e Turán, o principal problema nessa linha atualmente é descobrir a velocidade com que $r_k(n)/n$ converge para 0. Por exemplo, atualmente sabemos que $r_3(n) = o((\log\log n(\log n)^{-1})^{1/2})$ (Bourgain, 1999) e que $r_3(n) \geqslant \exp(-c\sqrt{\log n})$, (Behrend, 1946) $c > 0$.

Exercício 12 (Szekeres). Considere o conjunto dos números inteiros positivos cuja expansão ternária contém somente dígitos 0 e 1. Mostre que esse conjunto não contém progressão aritmética com 3 termos. Mostre que $r_3(3^k - 1/2) \geqslant 2^k$ e conclua que $r_3(n) \gg n^{\log_3 2}$.

2.1. O impacto em Teoria dos Grafos. A demonstração do Teorema por Szemerédi é puramente combinatória, e uma das mais difíceis da combinatória, e um passo importante dessa demonstração é conhecido como Lema de Regularidade de Szemerédi, ou simplesmente *Lema de Szemerédi*.

Ingenuamente, o Lema de Szemerédi diz que o conjunto dos vértices de todo grafo pode ser particionado em um pequeno número de subconjuntos basicamente da mesma cardinalidade, de forma que muitos dos subgrafos bipartidos induzidos por essas partes têm suas arestas distribuídas de maneira quase uniforme.

Esses subgrafos *pseudoaleatórios* satisfazem várias propriedades locais de grafos bipartidos aleatórios. Por exemplo, quase todo vértice tem grau próximo ao grau médio (veja a Afirmação 19 na página 19).

Os livros mais modernos de Teoria dos Grafos (Diestel, 1997; Bollobás, 1998) dedicam um capítulo ao lema de Szemerédi e, atualmente, é ferramenta importante para vários resultados em Teoria dos Grafos e aplicações, como é bem mostrado no *survey* Komlós and Simonovits (1996).

2.2. PA de primos. A famosa conjectura sobre a existência de progressões aritméticas de primos arbitrariamente longas foi resolvido por Green and Tao (2008). Como os próprios autores dizem, o resultado tem três ingredientes principais sendo um deles o Teorema de Szemerédi.

Teorema 13 (Green and Tao, 2008). *Os números primos contêm progressões aritméticas de k termos para todo $k \in \mathbb{N}$.*

3. O Lema de Regularidade de Szemerédi

Sejam $G = (V, E)$ um grafo e A, $B \subset V$, subconjuntos disjuntos de vértices. Lembrando que denotamos por $e_G(A, B)$ o número de arestas de G com um extremo em A e outro em B, definimos

$$d_G(A, B) = \frac{e_G(A, B)}{|A||B|},$$

chamado de *densidade do par* (A, B) no grafo G. Escrevemos $e(A, B)$ e $d(A, B)$ quando G estiver subentendido.

Na sua primeira versão, aquela usada na prova do Teorema de Szemerédi, o Lema de Regularidade foi provado para grafos bipartidos.

LEMA. *Dados reais positivos ε_1, ε_2, δ, ϱ e σ existem naturais n_0, m_0, N e M tais que para qualquer grafo bipartido $(A \cup B, E)$ com $|A| = n \geqslant N$ e $|B| = m \geqslant M$ vale o seguinte. Existem conjuntos $V_i \subseteq A$, para todo $i < n_0$, e $V_{ij} \subseteq B$, para todos $i < n_0$ e $j < m_0$ tais que*

- $\left|A \setminus \bigcup_{i<n_0} V_i\right| < \varrho n$, *e* $\left|B \setminus \bigcup_{j<m_0} V_{ij}\right| < \sigma m$ *para todo* $i < n_0$, *e*
- *para todos* $i < n_0$ *e* $j < m_0$ *e para todos* $T \subseteq V_i$ *e* $S \subseteq V_{ij}$ *vale o seguinte. Se* $|T| > \varepsilon_1|V_i|$ *e* $|S| > \varepsilon_2|V_{ij}|$, *então* $d(T, S) > d(V_i, V_{ij}) - \delta$ *e* $e(\{u\}, V_i) < (d(V_i, V_{ij}) + \delta)|V_i|$, *para cada* $u \in V_{ij}$.

Vejamos agora a versão plena do Lema de Regularidade. Para tal, primeiro introduzimos mais algumas definições. Dados um grafo $G = (V, E)$, um real $\varepsilon \leqslant 1$ positivo e A, $B \subseteq V$ disjuntos, dizemos que o par (A, B) é (ε, G)-*regular*, ou simplesmente ε-*regular* quando G está subentendido, se para quaisquer $X \subset A$ e $Y \subset B$ com $|X| \geqslant \varepsilon|A|$ e $|Y| \geqslant \varepsilon|B|$ temos

$$\left|d_G(A, B) - d_G(X, Y)\right| < \varepsilon.$$

Observe que quanto menor for ε, mais uniforme é a distribuição das arestas no grafo.

EXEMPLO 14. Seja B_M um grafo bipartido escolhido aleatória e uniformemente dentre todos os grafos bipartidos sobre o conjunto de vértices $V = [n]\times[n]$ e com $M = n^2/2$ arestas. Para todo ε, quase certamente o grafo B é ε-regular. □

EXERCÍCIO 15. Mostre o fato acima. Uma dica é mostrar que a probabilidade de ocorrer $(1/2 - \varepsilon)n^2 \leqslant e(X, Y) \leqslant (1/2 + \varepsilon)n^2$ para um par (X, Y) de subconjuntos grandes, é exponencialmente pequena. Recorra à Desigualdade de Janson e à eqüivalência entre os modelos binomial e uniforme de grafos aleatórios dados na Introdução.

EXEMPLO 16. Se $d(A, B) \leqslant \varepsilon^3$, então A e B formam um par ε-regular, ou seja, pares muito esparsos são necessariamente regulares. De fato, se $X \subseteq A$ com $|X| \geqslant \varepsilon|A|$ e $Y \subseteq B$ com $|Y| \geqslant \varepsilon|B|$, então

$$d(X, Y) = \frac{e(X, Y)}{|X||Y|} \leqslant \frac{e(A, B)}{|X||Y|} \leqslant \frac{\varepsilon^3|A||B|}{|X||Y|} \leqslant \frac{\varepsilon^3|A||B|}{\varepsilon|A|\varepsilon|B|} \leqslant \varepsilon.$$

Agora, se A e B formam um par ε-regular em G, então eles também formam um par ε-regular no complemento de G, logo, podemos concluir que pares densos, com densidade maior que $1-\varepsilon^3$, também são regulares. □

Seja $\mathcal{P} = \{V_0, V_1, \ldots, V_k\}$ uma $(k+1)$-partição do conjunto de vértices V. Dizemos que $\mathcal{P}$ é uma (ε, k)-*eqüipartição* se $|V_i| = |V_j|$ para todos $1 \leq i < j \leq k$ e $|V_0| \leqslant \varepsilon|V|$. O conjunto V_0 é chamado conjunto *excepcional* e pode ser vazio. Dizemos que a partição $\mathcal{P}$ é uma *eqüipartição* se for uma (ε, k)-eqüipartição para algum ε e algum k.

Dizemos que a (ε, k)-eqüipartição $\mathcal{P}$ é (ε, k, G)-*regular* se é uma (ε, k)-eqüipartição onde o número de pares (V_i, V_j) com $1 \leq i < j \leq k$, que não são (ε, G)-regulares é no máximo $\varepsilon\binom{k}{2}$.

Szemerédi (1978) demonstrou uma versão do Lema de Regularidade para grafos arbitrários. A versão plena do Lema de Regularidade de Szemerédi é o seguinte resultado.

Lema de Regularidade de Szemerédi. *Dados um real $0 < \varepsilon < 1$ e um inteiro $k_0 \geq 1$, existem inteiros positivos $n_0 = n_0(\varepsilon, k_0)$ e $K_0 = K_0(\varepsilon, k_0) \geqslant k_0$ tais que se $G = (V, E)$ é um grafo com pelo menos n_0 vértices, então existe uma partição (ε, k, G)-regular de V com $k_0 \leq k \leq K_0$.*

O conjunto excepcional é uma conveniência técnica para garantir que as outras classes tenham exatamente a mesma cardinalidade (veja o Corolário 30 na página 27 para uma versão sem a classe excepcional).

O Lema de Regularidade permite até $\sim \varepsilon k^2$ pares irregulares e Szemerédi (1978) perguntou se o lema vale quando não permitimos pares irregulares. Uma resposta negativa foi dada por vários pesquisadores, como mostra o seguinte exemplo descrito por Alon et al. (1994): considere o grafo bipartido $G = (A \cup B, E)$ dado por $A = \{a_1, \ldots, a_n\}$ e $B = \{b_1, \ldots, b_n\}$ e $a_i b_j \in E$ se e somente se $i \leqslant j$.

Exercício 17. Mostre que para $\varepsilon > 0$ suficientemente pequeno existe uma constatnte $c = c(\varepsilon) > 0$ tal que qualquer partição ε-regular do grafo bipartido G descrito acima necessita de pelo manos ck pares ε-irregulares.

3.1. Uma idéia da prova do Lema. Vejamos uma idéia da prova do Lema de Regularidade. Seja G um grafo de ordem n e suponha um par (A, B) de subconjuntos disjuntos de vértices que não é (ε, G)-regular. Ponha A_1 e B_1 subconjuntos de A e B, respectivamente, que atestam a ε-irregularidade, isto é, $|A_1| \geqslant \varepsilon|A|$, $|B_1| \geqslant \varepsilon|B|$ e $|d(A_1, B_1) - d(A, B)| \geqslant \varepsilon$. Sejam A_2 e B_2 os complementos de A_1 e B_1 em A e B, respectivamente. Defina uma "densidade

média" para essa partição do par (A, B) pondo

$$\mathrm{q}(\{A_1, A_2\}, \{B_1, B_2\}) = \frac{1}{n^2} \sum_{i,j} d(A_i, B_j)^2 |A_i||B_j|. \tag{13}$$

A idéia fundamental na prova do Lema de Regularidade: quando há muitos pares irregulares, refinamos a partição. Como q definido na equação (13) é limitado superiormente e a densidade cresce substancialmente, após um número finito de refinamentos teremos uma partição ε-regular de (A, B). Agora,

$$\mathrm{q}(\{A_1, A_2\}, \{B_1, B_2\}) = \sum_{i,j} \frac{e(A_i, B_j)^2}{n^2 |A_i||B_j|} = \frac{1}{n^2} \left(\frac{e(A_1, B_1)^2}{|A_1||B_1|} + \sum_{i+j>2} \frac{e(A_i, B_j)^2}{|A_i||B_j|} \right).$$

Usando a desigualdade de Cauchy-Schwarz [1]

$$\mathrm{q}(\{A_1, A_2\}, \{B_1, B_2\}) \geqslant \frac{1}{n^2} \left(\frac{e(A_1, B_1)^2}{|A_1||B_1|} + \frac{(\sum_{i+j>2} e(A_i, B_j)^2}{\sum_i |A_i| \sum_j |B_j|} \right) =$$

$$\frac{1}{n^2} \left(\frac{e(A_1, B_1)^2}{|A_1||B_1|} + \frac{(e(A, B) - e(A_1, B_1))^2}{|A||B| - |A_1||B_1|} \right).$$

Definindo $\delta = d(A_1, B_1) - d(A, B) = e(A_1, B_1)/|A_1||B_1| - e(A, B)/|A||B|$, isolamos $e(A_1, B_1)$ e substituímos na equação acima, ficando

$$n^2 \mathrm{q}(\{A_1, A_2\}, \{B_1, B_2\}) \geqslant \frac{\left(\delta |A_1||B_1| + \frac{e(A,B)}{|A_1||B_1|} \right)^2}{|A_1||B_1|} +$$

$$\frac{\left(e(A, B) - \frac{e(A,B)}{|A||B|} |A_1||B_1| - \delta |A_1||B_1| \right)^2}{|A||B| - |A_1||B_1|}$$

$$\geqslant \delta^2 |A_1||B_1| + \frac{e(A, B)^2}{|A||B|} \geqslant \frac{e(A, B)^2}{|A||B|} + \varepsilon^4 |A||B|,$$

pois $|A_1| \geqslant \varepsilon |A|$, $|B_1| \geqslant \varepsilon |B|$ e $|\delta| \geqslant \varepsilon$. Portanto $\mathrm{q}(\{A_1, A_2\}, \{B_1, B_2\}) \geqslant \mathrm{q}(A, B) + \varepsilon^4 n^{-2} |A||B|$.

Note que no caso do Lema de Regularidade estamos interessados quando as partes envolvidas têm a mesma cardinalidade, ou seja, acima $|A| = |B|$ e particionamos os pares irregulares em partes de mesma cardinalidade. Dessa forma, seguindo a bibliografia, chamaremos essa densidade média de índice da partição que é definido como segue.

Definimos o *índice da partição* $\mathcal{P} = \{V_0, V_1, \ldots, V_k\}$ por

$$\mathrm{ind}(\mathcal{P}) = \frac{1}{k^2} \sum_{1 \leqslant i < j \leqslant k} d(V_i, V_j)^2.$$

Observe que $0 \leq \mathrm{ind}(\mathcal{P}) < 1/2$.

[1] $\sum \frac{\alpha_i^2}{\mu_i} \geqslant \frac{(\sum \alpha_i)^2}{\sum \mu_i}$, que segue da usual $\sum {a_i}^2 \sum {b_i}^2 \geqslant (\sum a_i b_i)^2$.

O índice mede o quanto a partição é regular. Se a partição tem muitos pares (A, B) irregulares nós podemos tomar $X \subseteq A$ e $Y \subseteq B$ que violam a condição de regularidade em (A, B) e fazer deles elementos de uma nova partição. No refinamento o índice cresce por uma constante aditiva fixa e como o índice é limitado superiormente, após um número limitado de refinamentos teremos uma partição ε-regular. Essa idéia, que está formulada no lema abaixo, é o coração do Lema de Regularidade.

LEMA 18. *Sejam $\varepsilon \leqslant 1$ um real positivo e $\mathcal{P} = \{V_0, \ldots, V_k\}$ uma (ε, k)-eqüipartição de $V(G)$ tal que $4^k > 600\varepsilon^{-5}$. Se mais que $\varepsilon\binom{k}{2}$ pares (V_i, V_j) de elementos de $\mathcal{P}$ são ε-irregulares então existe uma $(1 + k4^k)$-eqüipartição $\mathcal{Q}$ de $V(G)$ com $< |V_0| + n/4^k$ vértices na classe excepcional e tal que*

$$\operatorname{ind}(\mathcal{Q}) \geq \operatorname{ind}(\mathcal{P}) + \frac{\varepsilon^5}{32}. \tag{14}$$

A prova do Lema de Regularidade segue por repetidas aplicações do Lema 18. Por (14), temos que no t-ésimo passo

$$\frac{1}{2} > \operatorname{ind}(\mathcal{P}_t) \geqslant \operatorname{ind}(\mathcal{P}) + \frac{t\varepsilon^5}{32},$$

portanto, com no máximo $16\varepsilon^{-5}$ passos temos uma equipartição ε-regular de $V(G)$.

Na Seção 6 veremos uma versão do Lema de Regularidade de Szemerédi, provada por Kohayakawa e Rödl independentemente, da qual podemos extrair a versão acima de Szemerédi como um caso particular. Lá daremos uma demonstração completa do Lema de Regularidade.

3.2. Limitação quantitativa. A cota superior dada pelo lema para o número de partes da eqüipartição, K_0, é extremamente grande, uma torre de 2's de altura proporcional a ε^{-5}, que indica que esse resultado é *quantitavamente* ruim. A demonstração do Lema de Regularidade envolve uma exponenciação iterada $16\varepsilon^{-5}$ vezes (veja pág. 17), portanto as estimativas em muitas das aplicações podem ser muito fracas.

Por exemplo, Chvatál et al. (1983) provaram o seguinte resultado (veja seção 5.3) usando o lema. Dado $\Delta \in \mathbb{N}$, todo grafo $G = (V, E)$ de grau máximo $\leqslant \Delta$ admite número de ramsey $\mathrm{r}(G, G)$ linear, ou seja, $\mathrm{r}(G, G) \leqslant c|V|$, onde $c = c(\Delta)$ é uma constante positiva que depende só de Δ. Por conseqüência do uso do Lema de Szemerédi, a constante c é limitada superiormente por uma torre de 2's de altura Δ. Graham et al. (2000) conseguiram uma demonstração desse resultado que evita o uso do Lema de Regularidade de Szemerédi e atinge o limitante superior $c \leqslant 2^{a\Delta(\log \Delta)^2}$, onde $a > 0$ é uma constante.

Em alguma aplicações seria útil uma cota superior exponencial, por exemplo algo da forma $\exp(\varepsilon^{\beta})$, mas Gowers (1997) mostrou que tal cota não existe, ou

seja, mostrou que existem grafos G nos quais, para qualquer partição (ε, k, G)-regular dos vértices, tem-se que k é maior ou igual a uma torre de 2's de altura proporcional a $\log(1/\varepsilon)$.

4. Como aplicar o Lema?

Suponha dados $\varepsilon \leqslant 1$ real positivo e $k_0 \geqslant 1$ inteiro. A aplicação do Lema de Regularidade sobre um grafo G com n vértices, para n suficientemente grande, nos dá uma partição $\mathcal{P} = \{V_0, V_1, \ldots, V_k\}$ tal que

$$(1-\varepsilon)\frac{n}{k} \leqslant |V_i| \leqslant \frac{n}{k}, \tag{15}$$

para todo $i \in [k]$. Ainda, dado um real positivo $\rho < 1$, considere os pares (V_i, V_j), para $1 \leqslant i < j \leqslant k$, que são (ε, G)-regulares de densidade pelo menos ρ. Então, pondo $|V_i| = m$ para todo $i \in [k]$,

(i) V_0 contém no máximo $1/2(\varepsilon n)^2$ arestas e existem no máximo $|V_0|mk \leqslant \varepsilon nmk$ arestas que ligam vértices de V_0 aos vértices das outras classes;
(ii) cada um dos no máximo $\varepsilon\binom{k}{2}$ pares irregulares contém no máximo m^2 arestas;
(iii) entre os pares ε-regulares de densidade $< \rho$ há $< \rho m^2$ arestas;
(iv) cada V_i, para $i \in [k]$, contém no máximo $\binom{m}{2}$ arestas.

Seja $G'' = G''(\mathcal{P}, \rho, \varepsilon)$ o grafo obtido de G removendo as arestas descritas nos itens (i)–(iv). Então,

$$e(G) < \frac{1}{2}(\varepsilon n)^2 + \varepsilon nmk + \frac{\varepsilon}{2}m^2k^2 + \frac{k^2}{2}\rho m^2 + \frac{1}{2}m^2k + e(G''),$$

portanto, usando o limitante superior dado em (15) para $|V_i| = m$ $(\forall i \in [k])$, temos que

$$e(G'') > e(G) - \frac{n^2}{2}\left(\rho + 4\varepsilon + \frac{1}{k_0}\right). \tag{16}$$

Esse grafo G'' obtido é muito útil nas aplicações.

4.1. O Teorema de Roth – demonstração combinatória. Vejamos uma demonstração do Teorema de Szemerédi para $k = 3$. Ponha $r_k(n)$ para a cardinalidade máxima de um subconjunto de $[n]$ que não contém uma progressão aritmética de k termos, que abreviamos k-PA. Pelo Teorema de Szemerédi temos que $r_k(n) = o(n)$. O caso $k = 3$ foi provado analiticamente por Roth em 1954. Vejamos uma demonstração combinatória deste caso.

TEOREMA. *Com a notação acima*

$$r_3(n) = o(n).$$

Demonstração. Começaremos definindo um grafo onde aplicaremos o Lema de Regularidade. Sejam X, Y e Z cópias disjuntas de $[3n]$ e seja $U \subseteq [n]$ um subconjunto qualquer. Definimos o seguinte conjunto $S = S(U)$

$$S = \left\{(x, y, z) \in X \times Y \times Z \colon y - x = z - y = \frac{z - x}{2} \in U\right\}.$$

Seja $G = (V, E)$ o grafo tripartido com $9n$ vértices obtido tomando-se $V = X \cup Y \cup Z$, e as arestas são os pares de V contidos em alguma tripla de S.

O número de arestas em G é $e(G) \geqslant 3|U|n$, pois cada elemento de $|U|$ gera pelo menos n triplas em S e cada tripla contribui com 3 arestas.

O conjunto das arestas de G pode ser decomposto em $e(G)/3$ triângulos disjuntos nas arestas, os quais chamamos de *triângulos não-espontâneos*.

A terceira observação que fazemos é que, se G contém um triângulo que é espontâneo, então U contém uma 3-PA. De fato, se x', y', z' formam um tal triângulo, então devemos ter $y' - x' \neq z' - y'$ e tomando $a = y' - x'$ e $b = z' - y'$ temos $a, b \in U$ por definição, e também $\frac{a+b}{2} = \frac{z'-x'}{2} \in U$. Logo $a, b, \frac{a+b}{2}$ é uma 3-PA em U.

Agora, vamos supor que $|U| = \alpha n$, para alguma constante $\alpha > 0$, e vamos provar que U deve conter uma progressão aritmética. Claramente, é suficiente mostrar que o grafo G deve conter um triângulo espontâneo.

Escreva $N = 9n$. Temos $e(G) \geqslant 3|U|n = 3\alpha n^2$, então podemos escrever $e(G) = \beta\binom{N}{2}$, onde β é uma constante fixa e independente de n. Aplicamos o Lema de Szemerédi em G para os parâmetros $\varepsilon = \frac{\beta}{60}$ e $k_0 = \lceil \varepsilon^{-1} \rceil$.

Agora, observamos que o número de arestas não contidas em pares com densidade pelo menos $\rho = \beta/6$ é, pela equação (16) na página 18, no máximo

$$\frac{N^2}{2}(\rho + 5\varepsilon) = \frac{N^2}{2}\frac{\beta}{4} < \frac{\beta}{3}\binom{N}{2}.$$

Removendo essas arestas, obtemos o grafo G'' que ainda contém um triângulo T, pois existiam $e(G)/3 = \beta\binom{N}{2}/3$ triângulos disjuntos nas arestas (aqueles não-espontâneos) em G. Ainda, as três arestas do triângulo T estão contidas em pares ε-regulares com densidade pelo menos $\beta/6$. Vamos supor, sem perda de generalidade, que esses pares são os dados por V_1, V_2 e V_3.

Agora, usamos o fato que muitos vértices em pares regulares têm graus próximos.

Afirmação 19. *Se (A, B) é um par ε-regular com densidade $d = d(A, B)$, então para qualquer $Y \subseteq B$ com $|Y| \geqslant \varepsilon|B|$,*

$$\left|\, \{x \in A \colon |e(\{x\}, Y)| \leqslant (d - \varepsilon)|Y|\} \,\right| < \varepsilon|A|.$$

De fato, seja X o conjunto dos vértices $x \in A$ tais que $|e(\{x\}, Y)| \leqslant (d - \varepsilon)|Y|$. Então, $e(X, Y) \leqslant |X|(d - \varepsilon)|Y|$, portanto, $d(X, Y) \leqslant d - \varepsilon$ e pela ε-regularidade do par, concluímos que $|X| < \varepsilon|U|$, provando a afirmação.

Portanto, se (V_1, V_3) e (V_2, V_3) são ε-regulares, então existem pelo menos $(1-2\varepsilon)|V_3|$ vértices em V_3, cada um ligado a pelo menos $(\beta/6-\varepsilon)|V_i|$ vértices de V_i, para $i = 1, 2$. Fixe um deles, digamos x, e ponha $N_i(x)$ para o conjunto dos vizinhos de x em V_i.

De $\beta/6 - \varepsilon = 9\beta/60 > \varepsilon$ temos, pela ε-regularidade, que existem pelo menos $(\beta/6 - \varepsilon)|N_1||N_2| > (9\beta/60)^3|V_1||V_2|$ arestas ligando vértices de $N_1(x)$ com vértices de $N_2(x)$. Cada aresta corresponde a um triângulo contendo x. Desde que, dois triângulos não-espontâneos não têm dois vértices comum, então existem no máximo $|V_1| = |V_2|$ triângulos não-espontâneos contendo o vértice x.

Portanto, para n suficientemente grande, o grafo G contém um triângulo espontâneo, ou seja, U contém uma 3-PA. □

OBSERVAÇÃO 20. Seguindo o argumento acima, se V_1, V_2 e V_3 são conjuntos disjuntos de cardinalidade m que formam, 2-a-2, pares ε-regulares de densidade ρ, então nós temos o seguinte: pela Afirmação 19, pelo menos $(1-2\varepsilon)m$ vértices v_3 de V_3 têm pelo menos $(\rho - \varepsilon)m$ vizinhos em V_1 e em V_2. Dado que $\rho > 2\varepsilon$ temos, pela ε-regularidade do par, pelo menos $(\rho - \varepsilon)^3 m^2$ arestas ligando os vizinhos de v_3 em V_1 aos vizinhos desse v_3 em V_2.

Dessa forma, o número de triângulos nessa tripla é pelo menos $t_3 = (1 - 2\varepsilon)(\rho - \varepsilon)^3 m^3$. Note que $t_3 \to \rho^3 m^3$, quando $\varepsilon \to 0$. Agora, se essa tripla é formada por grafos bipartidos aleatórios com probabilidade de arestas ρ, então o número de triângulos tende a $\rho^3 m^3$, conforme $m \to \infty$.

EXERCÍCIO 21. Sejam V_1, V_2 e V_3 conjuntos dois-a-dois disjuntos com m vértices cada e seja $T_p = (V_1 \cup V_2 \cup V_3, E)$ o grafo tripartido aleatório onde cada par uw com $u \in V_i$, $w \in V_j$ e $i \neq j$ é uma aresta com probabilidade $p \in (0, 1)$.

Mostre que o número de triângulos em T_p é $(1 + o(1))p^3 m^3$.

Na próxima seção vamos mostrar como obter uma cópia de um grafo H a partir de uma partição ε-regular dos vértices de um grafo G.

4.2. Imersão via pares regulares. Quando temos um grafo G denso, o Lema de Regularidade nos garante que se $|V(G)|$ é suficientemente grande, então conseguimos uma cópia de um grafo "pequeno" H em G.

Vamos fazer o parágrafo anterior mais preciso. Dados um grafo J, reais $\rho > \varepsilon > 0$ e um inteiro positivo m, construímos o grafo $G = G(J; m, \rho, \varepsilon)$ da seguinte forma. Para cada vértice de J tomamos um conjunto independente com m pontos. Agora, para cada aresta de J ligamos os vértices do respectivo par

de conjuntos independentes de modo a formar um par ε-regular de densidade pelo menos ρ. Dado um inteiro $t > 0$, denotamos por $J(t)$ o grafo obtido pelo procedimento acima quando os pares de conjuntos independentes cujos respectivos vértices são arestas em J induzem subgrafos bipartidos completos.

LEMA 22 (Komlós and Simonovits, 1996). *Dados o grafo J, $\Delta \geqslant 1$ e $\rho > 0$ existem α, $\varepsilon > 0$ e $m_0 \geqslant 1$ tais que para todo $m \geqslant m_0$ qualquer grafo $G = G(J; m, \rho, \varepsilon)$ contém uma cópia de qualquer subgrafo H de $J(\lfloor \alpha m \rfloor)$ com grau máximo $\leqslant \Delta$. Mais que isso, o número de cópias rotuladas de H em G é maior que $(\varepsilon m)^h$.*

DEMONSTRAÇÃO. Vamos supor, sem perda de generalidade, que $V(H) = \{v_1, \ldots, v_h\}$. Definimos

$$k = |V(J)| \quad \text{e} \quad t = \lfloor \alpha m \rfloor .$$

Além disso,

$$\alpha = \frac{(\rho - \varepsilon)^\Delta}{(2 + \Delta)}, \quad \varepsilon \leqslant \alpha \quad \text{e} \quad m_0 = \varepsilon^{-1}.$$

Consideremos $H \subseteq J(t)$ pelo homomorfismo injetor $\phi\colon V(H) \to V(J(t))$ e vamos escrever

$$\begin{aligned} V(G) &= V_1^{(G)} \cup \cdots \cup V_k^{(G)}, \text{ com } |V_i^{(G)}| = m \text{ para todo } i \in [k], \\ V(J(t)) &= V_1^{(J)} \cup \cdots \cup V_k^{(J)}, \text{ com } |V_i^{(J)}| = m \text{ para todo } i \in [k]. \end{aligned}$$

Vamos definir um homomorfismo injetor $\xi\colon V(H) \to V(G)$ indutivamente:

Passo 0: Para todo $j \in [h]$ ponha $C_j(0) = V_i^{(G)}$, onde i é tal que $\phi(v_j) \in V_i^{(J)}$.

Passo j: ($j \geqslant 1$) Escolha $\xi(v_j) \in C_j(j-1)$ tal que, para todo $\ell > j$

se $v_j \in N_H(v_\ell)$ então $\big|C_\ell(j-1) \cap N_G(\xi(v_j))\big| > (\rho - \varepsilon)\big|C_\ell(j-1)\big|$, (17)

e atualize os conjuntos

$$C_\ell(j) = \begin{cases} C_\ell(j-1) \cap N_G(\xi(v_j)) & \text{se } v_j v_\ell \in E(H), \\ C_\ell(j-1) & \text{caso contrário.} \end{cases}$$

Dessa forma, $C_j(i)$ denota o subconjunto de vértice de G candidatos a $\xi(v_j)$ no i-ésimo passo. Enquanto a imersão segue, $C_j(i)$ vai ficando menor até quando $\xi(v_j) \in C_j(j-1)$ é escolhido.

Assim, queremos escolher $\xi(v_j)$ tal que $C_\ell(j)$ não seja pequeno, isto é, não muito menor que $C_\ell(j-1)$. Porém, pela Afirmação 19, página 19, a menos de $\varepsilon|C_j(j-1)|$ escolhas para $\xi(v_j)$, temos $|C_\ell(j)| \geqslant (\rho - \varepsilon)|C_\ell(j-1)|$ para cada $\ell > j$.

Para todo $\ell > j$, defina $d_{\ell j} = |\{i \in [j] \colon v_\ell v_i \in E(H)\}|$ e, portanto,

$$|C_\ell(j)| \begin{cases} > (\rho - \varepsilon)^{d_{\ell j}} m & \text{se } d_{\ell j} > 0 \\ = m & \text{se } d_{\ell j} = 0. \end{cases}$$

Logo, temos $|C_\ell(j)| > (\rho - \varepsilon)^\Delta m \geqslant \varepsilon m$.

Então, quando escolhemos $\xi(v_j)$ todos os vértices de $C_j(j-1)$, a menos de $\Delta\varepsilon m$ deles, satisfazem (17) para todo $\ell > j$, e no máximo $t-1$ vértices já foram escolhidos. Conseqüentemente, temos pelo menos

$$|C_j(j-1)| - \Delta\varepsilon m - (t-1) > ((\rho - \varepsilon)^\Delta - \Delta\varepsilon - \alpha)m \geqslant \varepsilon m$$

escolhas para $\xi(v_j)$. □

4.2.1. *O lema "Blow-up".* Observe que o Lema 22 nos diz como descobrir uma cópia de um grafo pequeno H^h em um grafo grande G^n com $h = h(n)$ linearmente menor que n, dado que H tenha grau limitado. Tipicamente, o grafo h tem tamanho fixo com relação a n.

Um resultado de Komlós (1999) conhecido com Lema *Blow-up* mostra que com uma hipótese extra sobre G conseguimos cópias de subgrafos geradores ($\alpha = 1$) de G com grau máximo limitado. Esse resultado é um ingrediente chave nos recentes sucessos de Ajtai, Komlós e Szemerédi contra conjecturas difíceis como a de Alon e Yuster (Alon and Yuster, 1992; Komlós et al., 2001): *Para todo H existem n_0 e K tal que, se $n \geqslant n_0$ e o grau mínimo de G^n é pelo menos*

$$\left(1 - \frac{1}{\chi(H)}\right) n,$$

então G^n contém pelo menos $(n-K)/|V(H)|$ cópias vértices disjuntas de H.

Um par ε-regular (A, B) é dito (ε, δ)-super-regular se para todo $v \in A$ temos $|N(v) \cap B| \geqslant \delta|B|$ e, se para todo $w \in B$ temos $|N(w) \cap A| \geqslant \delta|A|$.

Definimos o grafo $G = G(J; m, \rho, \varepsilon, \delta)$ como acima, trocando na definição 'ε-regular' por '(ε, δ)-super-regular'. O Lema *Blow-up* é o seguinte resultado (para saber mais sobre o *Blow-up Lemma* veja Komlós, 1999).

Teorema 23. *Dados J, $\Delta \geqslant 1$ e δ, $\rho > 0$ existem α, $\varepsilon > 0$ e $m_0 \geqslant 1$ tais que para todo $m \geqslant m_0$ qualquer grafo $G = G(J; m, \rho, \varepsilon, \delta)$ contém uma cópia de qualquer subgrafo H de $J(m)$ com grau máximo $\leqslant \Delta$.*

A prova desse teorema é difícil e envolve, numa primeira fase, uma versão probabilística do algoritmo desenvolvido na prova do Lema 22 e, quando "quase todos" vértices estão imersos, os vértices restantes são todos imersos de uma só vez usando o Teorema de König-Hall (Diestel, 1997, Capítulo 2).

4.3. O Lema de Regularidade em Teoria Extremal de Grafos. Agora que estamos munidos de ferramentas e adquirimos um pouco de familiaridade com o Lema de Regularidade vamos tentar entender melhor o papel desse lema em Teoria Extremal de Grafos.

Um ponto central nas aplicações do Lema de Regularidade em Teoria Extremal de Grafos é o seguinte: dado um grafo G e fixado parâmetros $\rho > \varepsilon > 0$, construímos o grafo cujo conjunto de vértices é uma partição dos vértices de G e as arestas são dadas pelos pares (ε, G)-regulares de densidade pelo menos ρ. Assim, os subgrafos pequenos desse grafo, em geral garantidos por algum resultado extremal, também são subgrafos de G. Esse fenômeno está formalizado no Lema 22 acima. Veremos uma demonstração do famoso Teorema de Erdős–Stone baseada nesse paradigma e onde o resultado extremal usado é o conhecido Teorema de Turán.

O Teorema de Erdős–Stone, algumas vezes chamado Teorema Fundamental da Teoria Extremal (cf. Bollobás, 1995), foi provado em Erdős and Stone (1946). Esse resultado diz respeito a um problema da Teoria Extremal conhecido como o *problema do subgrafo proibido*: dados um inteiro positivo n e um grafo H determine o número máximo de arestas, denotado por $\mathrm{ex}(n, H)$, que qualquer grafo de ordem n pode ter para não conter uma cópia de H. Um grafo G que não contém H e com $\mathrm{ex}(n, H)$ arestas é dito *grafo extremal*.

Vamos analisar o caso $H = K^r$, para $r > 1$ inteiro. Um candidato natural a grafo extremal é um grafo $(r-1)$-partido completo. Suponha que A e B são partes de um grafo $(r-1)$-partido com $|A| - |B| \geqslant 2$. Note que transferindo um vértice de A para B temos um novo grafo $(r-1)$-partido com $|A| - |B|$ arestas a mais. Dessa forma, estamos interessados no grafo $(r-1)$-partido onde o tamanho das partes diferem de no máximo um vértice. Esse grafo é denotado por $T^{r-1}(n)$.

Note que, para inteiros n, $r > 1$, temos

$$e(T^{r-1}(n)) \leqslant \left(1 - \frac{1}{r-1}\right)\binom{n}{2}.$$

De fato, prova-se que se $n = (r-1)k + i$, com $0 \leqslant i < r-1$, então

$$e(T^{r-1}(n)) = \frac{1}{2}\left(\frac{r-2}{r-1}\right)(n^2 - i^2) + \binom{i}{2}. \tag{18}$$

Em 1941, Turán provou que o grafo $T^{r-1}(n)$ é extremal com relação a conter K^r. Mais que isso, esse grafo é único com essa propriedade.

Teorema 24. *Para todos n, $r > 1$ vale que $\mathrm{ex}(n, K^r) = e(T^{r-1}(n))$. Ainda, todo grafo G de ordem n que não contém K^r e com $\mathrm{ex}(n, K^r)$ arestas é o grafo $T^{r-1}(n)$ (a menos de isomorfismos).* □

Exercício 25. Mostre que o número de arestas no grafo de Turán $T^{r-1}(n)$ é dado pela equação (18) e que esse grafo é o único grafo extremal que não contém uma cópia do grafo completo K^r.

O Teorema de Erdős–Stone diz que se n for suficientemente grande, então um grafo de ordem n com uma fração $\rho > (r-2)/(r-1)$ das arestas contém não só um K^r mas um $K^r(t)$, isto é, o grafo r-partido completo com t vértices em cada classe, para todo inteiro positivo t

Teorema 26. *Dados inteiros $r \geqslant 2$ e $t \geqslant 1$ e um real $0 < \rho < 1$, existe $n_0 > 0$ tal que todo grafo com $n \geqslant n_0$ vértices e pelo menos*

$$e(T^{r-1}(n)) + \rho n^2$$

arestas, contém uma cópia do $K^r(t)$.

Em outras palavras,

$$\operatorname{ex}(n, K^r(t)) = \left(1 - \frac{1}{r-1} + o(1)\right)\binom{n}{2}.$$

O Teorema de Erdős–Stone tem o seguinte, bastante interessante, corolário.

Corolário 27. *Para todo grafo H temos*

$$\lim_{n\to\infty} \frac{\operatorname{ex}(n,H)}{\binom{n}{2}} = \left(1 - \frac{1}{\chi(H)-1}\right).$$

De fato, note que pela equação (18) temos

$$e\left(T^{r-1}\left((r-1)\left\lfloor\frac{n}{r-1}\right\rfloor\right)\right) \leqslant e(T^{r-1}(n)) \leqslant e\left(T^{r-1}\left((r-1)\left\lceil\frac{n}{r-1}\right\rceil\right)\right),$$

portanto,

$$\lim_{n\to\infty} \frac{e(T^{r-1}(n))}{\binom{n}{2}} = 1 - \frac{1}{r-1}.$$

Ponha $r = \chi(H)$. Dessa forma $H \not\subseteq T^{r-1}(n)$, portanto, $e(T^{r-1}(n)) \leqslant \operatorname{ex}(n,H)$. Por outro lado, $H \subseteq K^r(t)$ para t suficientemente grande, portanto, $\operatorname{ex}(n,H) \leqslant \operatorname{ex}(n, K^r(t))$. Fixe um t para o qual vale essa desigualdade. Para todo $\rho > 0$ temos, pelo Teorema de Erdős–Stone para $n \geqslant n_0$,

$$\operatorname{ex}(n, K^r(t)) < e(T^{r-1}(n)) + \rho n^2.$$

Então, para n suficientemente grande temos

$$\frac{e(T^{r-1}(n))}{\binom{n}{2}} \leqslant \frac{\operatorname{ex}(n,H)}{\binom{n}{2}} < \frac{e(T^{r-1}(n))}{\binom{n}{2}} + \frac{2\rho}{1-\frac{1}{n}},$$

portanto, segue o corolário.

Observamos que se $\mathcal{L} = \{H_1, \ldots, H_s\}$ é uma família de grafos, então podemos definir $\operatorname{ex}(n, \mathcal{L})$, de modo natural, como o número máximo de arestas para

um grafo de n vértices não conter algum grafo da família $\mathcal{L}$ como subgrafo. Tomando $r = \min\{\chi(H_i)\colon i \in [s]\}$, se $r \geqslant 3$ temos que

$$\mathrm{ex}(n, \mathcal{L}) = \left(1 - \frac{1}{r-1} + o(1)\right)\binom{n}{2}.$$

Essa descrição assintótica de $\mathrm{ex}(n, \mathcal{L})$ foi mostrada por Erdős and Simonovits (1966). Essa forma geral do problema do subgrafo proibido, isto é, o problema de determinar o número máximo de arestas de um grafo de ordem n que não contenha qualquer elemento de $\mathcal{L}$ é conhecido como *problema extremal do tipo Turán*.

Um esquema geral pode ser posto da seguinte forma. Seja $G = G^n$ um grafo denso, digamos que contenha βn^2 arestas. Aplicamos o Lema de Regularidade para obtermos uma (ε, k)-eqüipartição $\mathcal{P}$ de $V(G)$. Seja R o grafo definido pondo um vértice para cada classe de $\mathcal{P}$ e uma aresta ligando cada dois vértices que representam pares (ε, G)-regulares com densidade pelo menos ρ.

Pela equação (16), página 18, pelo menos $\beta n^2 - (\rho + 4\varepsilon + 1/k_0)n^2/2$ arestas de G ligam vértices em pares regulares densos. Há no máximo $(n/k)^2$ arestas em cada par, logo existem pelo menos $(2\beta - \rho - 4\varepsilon - 1/k_0)k^2/2$ pares densos em $\mathcal{P}$, ou seja, existe $\delta = \delta(\beta, \rho, \varepsilon, k_0) > 0$ tal que $e(R) > (1-\delta)\binom{k}{2}$. Se escolhemos ρ, ε e k_0 de modo que δ é suficientemente pequeno, temos que $H \subseteq R$ e pelo Lema 22, temos $H \subseteq G$.

O grafo $R = R(\mathcal{P}, d, \varepsilon)$ descrito no paragrafo acima é chamado *grafo reduzido*. Compare o grafo $G = G(R; m, \rho, \varepsilon)$ construído no começo da Seção 4.2, onde R é o grafo reduzido, com o grafo $G''(\mathcal{P}, \rho, \varepsilon)$, definido na página 18.

Vejamos uma demonstração do celebrado Teorema de Erdős–Stone. Lembremos que o Teorema de Erdős–Stone diz que se G^n tem pelo menos $e(T^{r-1}(n)) + \rho n^2$ arestas então o grafo G^n contém $K^r(t)$. Usaremos o Lema de Regularidade para mostrar que G^n tem grafo reduzido denso o suficiente para conter K^r e usaremos o Lema 22 para concluir que $K^r(t) \subseteq G^n$.

Demonstração do Teorema de Erdős–Stone. Sejam r, $t \geqslant 2$ (se $t = 1$ temos o Teorema de Turán) e seja G um grafo de ordem n e com pelo menos $e(T^{r-1}(n)) + \rho n^2$ arestas. Escolha ε suficientemente pequeno, isto é, tal que

$$\varepsilon \leqslant \frac{(\rho - \varepsilon)^{rt}}{2 + rt}, \quad \text{e} \quad k_0 > \rho^{-1}.$$

Seja $\mathcal{P} = \{V_0, V_1, \ldots, V_k\}$ a partição dada pelo Lema de Regularidade e escreva $|V_i| = m$, para todo $i \in [k]$.

Pela discussão na página anterior sabemos que o grafo reduzido $R = R(\mathcal{P}, \rho, \varepsilon)$ tem pelo menos $(2\beta - \rho - 4\varepsilon - 1/k_0)k^2/2$ arestas, onde $\beta = e(T^{r-1}(n))/n^2 + \rho$.

Portanto,

$$e(R) \geqslant \left(\frac{e(T^{r-1}(n))}{\binom{n}{2}} (1 - \frac{1}{n}) + \delta \right) \frac{k^2}{2}$$

onde $\delta = \rho - 4\varepsilon - \rho - 1/k_0 > 0$.

Agora, se n é suficientemente grande, temos que

$$e(R) > \left(1 - \frac{1}{r-1}\right) \frac{k^2}{2}, \quad \text{e} \tag{19}$$

$$\varepsilon m = \varepsilon \frac{n - |V_0|}{k} \geqslant \varepsilon \frac{n - \varepsilon n}{K_0} = \frac{(1-\varepsilon)}{K_0} n \geqslant t - 1, \tag{20}$$

portanto, por (19) temos $e(R) > e(T^{r-1}(k))$, então $K^r \subseteq R$ e conseqüentemente temos $K^r(t) \subseteq R(t)$ e, por (20) podemos aplicar o Lema 22 e teremos $K^r(t) \subseteq G$. □

Observe que provamos mais.

Teorema 28. *Sejam H um grafo de ordem h e $\rho > 0$ um real. Para todo n suficientemente grande, se*

$$e(G^n) > \left(1 - \frac{1}{\chi(H) - 1}\right) \binom{n}{2} + \rho n^2,$$

então o número de cópias rotuladas de H em G^n é maior que $(\varepsilon n / K_0)^h$, onde $\varepsilon = \varepsilon(\rho)$ e $K_0 = K_0(\varepsilon)$.

Demonstração. Seguindo a demonstração do Teorema de Erdős–Stone temos que

$$e(R) > \left(1 - \frac{1}{\chi(H) - 1} + \delta\right) \frac{k^2}{2},$$

portanto, pelo Corolário 27, na pág. 24, temos que $H \subseteq R$ e pelo Lema 22, o teorema. □

Em contrapartida, temos o seguinte resultado observado por Füredi, que diz que se um grafo tem poucas cópias de um grafo fixo, então ele pode ser coberto com poucas arestas.

Teorema 29. *Para todo grafo H de ordem h e todo real $\gamma > 0$ existe $\beta = \beta(\gamma, H) > 0$ tal que se $G = G^n$ tem no máximo βn^h cópias de H, então podemos tornar G livre de H removendo no máximo γn^2 de suas arestas.*

Demonstração. Aplicamos o Lema de Regularidade para ε suficientemente pequeno e $k_0 > \varepsilon^{-1}$. Tome $\beta = (\varepsilon/K_0)^h$ e considere o grafo $G'' = G''(\mathcal{P}, \gamma, \varepsilon)$ o grafo obtido de G removendo as arestas que não interessam.

Se $H \subseteq G''$, então $H \subseteq R = R(\mathcal{P}, \gamma, \varepsilon)$. Mas, pelo Lema 22 o número de cópias rotuladas de H em G é maior que

$$(\varepsilon m)^h > \left(\varepsilon \frac{n}{k}\right)^h \geqslant \left(\frac{\varepsilon n}{K_0}\right)^h = \beta n^h.$$

Portanto, G'' não contém H. Observarmos que de G para G'' jogamos fora no máximo γn^2 arestas. □

4.4. Variações sobre o tema. Como dissemos, a classe excepcional é um dispositivo técnico para garantir que as outras classes da partição tenham a mesma cardinalidade. De fato, podemos distribuir igualmente os vértices dessa classe entre as outras classes de modo que a ε-regularidade é preservada para um ε ligeiramente maior. Vejamos uma versão sem a classe excepcional.

Corolário 30. *Dados $0 < \varepsilon \leqslant 1$ e $k_0 \geqslant 1$, existem $n_0' = n_0'(\varepsilon, k_0)$ e $K_0' = K_0'(\varepsilon, k_0)$ tais que se $G = (V, E)$ é um grafo com pelo menos n_0' vértices, então existe uma partição $\mathcal{P} = \{V_1, \ldots, V_k\}$ de V tal que para todos $1 \leqslant i < j \leqslant k$ temos $\big||V_i| - |V_j|\big| \leqslant 1$ e o número de pares (V_i, V_j) que não são (ε, G)-regulares é no máximo $\varepsilon\binom{k}{2}$, onde $k_0 \leq k \leq K_0'$.*

Demonstração. Dado um grafo G suficientemente grande, aplicamos o Lema de Regularidade para $\varepsilon^2/8$ e k_0 e obtemos a partição $\mathcal{P}_0 = \{V_0, V_1^0, \ldots, V_k^0\}$. Ponha $n_0' = n_0$ e $K_0' = K_0$. Sabemos que $|V_0| \leqslant \varepsilon^2 n/8$ e que

$$\left(1 - \frac{\varepsilon^2}{8}\right)\frac{n}{k} \leqslant |V_i^0| \leqslant \frac{n}{k}, \text{ para todo } i \in [k].$$

Tome $\mathcal{P} = \{V_1, \ldots, V_k\}$ a partição obtida a partir de $\mathcal{P}_0$ dividindo, o mais igualmente possível, os no máximo $\varepsilon^2 n/8$ vértices de V_0 entre as classes não-excepcionais de $\mathcal{P}_0$. Dessa forma, podemos escrever $V_i = V_i^0 \cup V_i'$ com $|V_i'| \leqslant \varepsilon^2 n/(8k)$, para todo $i \in [k]$.

Vamos mostrar que se (V_ℓ^0, V_j^0) é $(\varepsilon^2/8, G)$-regular, então (V_ℓ, V_j) é (ε, G)-regular.

Para $i = j$, $\ell \in [k]$ distintos, seja $X_i \subseteq V_i$ tal que $|X_i| \geqslant \varepsilon|V_i|$. Então, podemos naturalmente escrever X_i como a união disjunta $X_i^0 \cup X_i'$. Portanto,

$$|X_i^0| = |X_i| - |X_i'| \geqslant \varepsilon|V_i| - |V_i'| = \varepsilon|V_i^0| - (1-\varepsilon)|V_i'| \geqslant \left(\varepsilon - \frac{\varepsilon^2}{8}\right)\frac{n}{k}.$$

Por outro lado, $|X_i'| \leqslant |V_i'| \leqslant \varepsilon^2 n/(8k)$. Também, $|V_i^0| \geqslant (1 - (\varepsilon^2/8))n/k$.

Vamos considerar a seguinte condição de continuidade da densidade entre pares

Exercício 31. Suponha $A = A^0 \cup A'$ e $B = B^0 \cup B'$. Se $|A^0|, |B^0| \geqslant C$ e $|A'|, |B'| \leqslant c \leqslant C$, então $\big|d(A,B) - d(A^0, B^0)\big| < \frac{3c}{C}$.

Para $i = j$, ℓ temos que

$$|X_i^0| \geqslant \left(\varepsilon - \frac{\varepsilon^2}{8}\right)\frac{n}{k} > \frac{\varepsilon^2}{8}\frac{n}{k} \geqslant \frac{\varepsilon^2}{8}|V_i^0|.$$

Ainda,

$$\begin{aligned}\big|d(V_\ell, V_j) - d(X_\ell, X_j)\big| \leqslant &\big|d(V_\ell, V_j) - d(V_\ell^0, V_j^0)\big| + \\ &\big|d(X_\ell^0, X_j^0) - d(X_\ell, X_j)\big| + \big|d(V_\ell^0, V_j^0) - d(X_\ell^0, X_j^0)\big|.\end{aligned}$$

Do parágrafo anterior e do Exercício 31 tiramos que

$$\big|d(V_\ell, V_j) - d(X_\ell, X_j)\big| \leqslant \frac{6\frac{\varepsilon^2}{8}\frac{n}{k}}{\left(\varepsilon - \frac{\varepsilon^2}{8}\right)\frac{n}{k}} + \frac{\varepsilon^2}{8} < \varepsilon.$$

□

Uma versão do Lema de Regularidade afirma que se colorirmos as arestas de um grafo, então podemos particioná-lo em um número limitado de classes de forma que quase todos os pares são regulares em cada cor, simultaneamente. Para tanto, defina $d_c(A, B)$ como a densidade das arestas de cor c entre o par (A, B).

Teorema 32. *Dados um real positivo $\varepsilon \leqslant 1$ e inteiros positivos r, $k_0 \geqslant 1$, existem $K_0 = K_0(\varepsilon, k_0, r)$ e $n_0 = n_0(\varepsilon, k_0, r)$ tais que para grafos $G_1, G_2, \ldots, G_r$ sobre o mesmo conjunto V de pelo menso $n_)$ vértices o seguinte vale. Existe uma (ε, k)-eqüipartição de V com $k_0 \leqslant k \leqslant K_0$ tal que pelo menos $(1-\varepsilon)\binom{k}{2}$ pares (V_i, V_j) são (ε, k, G_c)- regular para todo $c \in [r]$.*

Para demonstrar esse resultado, usamos a prova original substituindo a definição de índice por

$$\mathrm{ind}(\mathcal{P}) = \frac{1}{k^2}\sum_c \sum_{i,j} d_c(V_i, V_j)^2.$$

Uma variante útil em aplicações é o seguinte enunciado.

Teorema 33. *Dado um real $0 < \varepsilon < 1$ existe um inteiro $K_0 = K_0(\varepsilon, k_0)$ tais que se $G = (V, E)$ é um grafo e $d \in [0, 1]$ é um número real qualquer, então existe uma partição $V_0, V_1, \ldots, V_k$ de $V(G)$ e um subgrafo $G' = (V, E')$ de G com as seguinte propriedades*

(i) $k \leq K_0$;
(ii) $|V_0| \leqslant \varepsilon|V|$;
(iii) $|V_1| = |V_2| = \cdots = |V_k|$;
(iv) $d_{G'}(v) > d_G(v) - (d + \varepsilon)|V|$ *para todo* $v \in V(G)$;
(v) $G'[V_i] = \emptyset$; *e*

(vi) $G'[V_i \times V_j]$, *para* $1 \leqslant i < j \leqslant k$, *são* ε*-regulares com densidade* 0 *ou maior que* d.

5. Algumas aplicações clássicas

5.1. O Teorema de Ruzsa-Szemerédi. O próximo resultado, o Teorema de Ruzsa–Szemerédi, também foi uma das primeiras aplicações do Lema de Regularidade. Na sua demonstração Ruzsa and Szemerédi (1978) usaram a primeira versão do Lema de Regularidade, aquela que se referia a grafos bipartidos.

TEOREMA 34. *Se* H *é um hipergrafo* 3*-uniforme sobre* n *vértices contendo* cn^2 *hiperarestas, então existem* 6 *vértices que geram* 3 *ou mais hiperarestas, para todo* $n \geqslant n_0(c)$.

DEMONSTRAÇÃO. Suponha que H um hipergrafo tal que quaisquer 6 vértices geram menos que 3 hiperarestas. Vamos mostrar que $e(H) = o(n^2)$.

Construa um grafo $G = G^n(H)$ da seguinte forma: para cada $\{x, y, z\} \in E(H)$ ponha $\{x, y\}$, $\{y, z\}$ e $\{x, z\}$ em $E(G)$. Então $e(G) = 3e(H)$ e como seis vértices geram no máximo duas triplas de H temos que o número de triângulos em G é o máximo $\binom{n}{2} = o(n^3)$, ou seja, para todo $\delta > 0$ o número de triângulos em G é menor que δn^3.

Observe que o Teorema 29, página 26, no caso de triângulos diz que dado um real positivo γ existe um real positivo β tal que para todo $G = G^n$ com no máximo βn^3 triângulos, existe $E' \subseteq E(G)$ com $|E'| \leqslant \gamma n^2$ tal que a remoção de E' das arestas de G torna-o livre de triângulos. Portanto, existe E' tal que $G \setminus E'$ é livre de triângulos. Como os únicos triângulos de G são aqueles gerados por alguma aresta de H temos que $e(H) < \gamma n^2$, para todo real positivo γ. □

Vejamos agora uma versão equivalente do teorema acima. Um *emparelhamento* é um subconjunto de arestas duas-a-duas disjuntas. Dizemos que um emparelhamento M em G é *induzido* se as únicas arestas de G ligando vértices de M são aquelas de M.

TEOREMA 35. *Se* G^n *é a união de* n *emparelhamentos induzidos, então* $e(G^n) = o(n^2)$.

DEMONSTRAÇÃO. Vamos provar a seguinte afirmação: Seja $0 < \varepsilon < 1$ arbitrário e $n \geqslant 2K_0/\varepsilon^2$, onde $K_0 = K_0(\varepsilon, k_0)$, é dado pelo Lema de Regularidade para $k_0 = 4\varepsilon^{-1}$). Se para algum inteiro positivo k o grafo G^n é a união de k emparelhamentos induzidos, então $e(G^n) < 5\varepsilon n^2 + k\varepsilon n$.

Tome $\rho = 2\varepsilon$ e considere o grafo $G'' = G''(\mathcal{P}, \rho, \varepsilon)$, onde $\mathcal{P} = \{V_0, \ldots, V_k\}$ é uma partição (ε, k, G^n)-regular dada pelo Lema de Regularidade. Vejamos que todo emparelhamento induzido em G'' contém no máximo εn arestas.

Tome $I \subseteq G''$ um emparelhamento induzido em G'', ponha $U = V(I)$, $U_i = U \cap V_i$ e $\Lambda = \{i \in [k] \colon |U_i| > \varepsilon |V_i|\}$. Também, ponha $L = \bigcup_{i \in \Lambda} U_i$ e $S = U \setminus L$. Então

$$|S| \leqslant \sum_{i \notin \Lambda} |U_i| \leqslant \sum_{i \notin \Lambda} \varepsilon \frac{n}{k} \leqslant \varepsilon n.$$

Se $|U| > 2\varepsilon n$, então $|L| > |U|/2$ e, portanto, existem u, $v \in L$ adjacentes. Suponha, sem perda de generalidade, que $u \in V_1$ e $v \in V_2$. Então $d(V_1, V_2) > 2\varepsilon$ e como $|U_i| \geqslant \varepsilon |V_i|$ $(i = 1, 2)$ temos que $d(U_1, U_2) > \varepsilon$, ou seja, existem mais que $\varepsilon |U_1||U_2| \geqslant \min\{|U_1|, |U_2|\}$ arestas ligando vértices de U_1 a U_2, contradizendo o fato de I ser induzido.

Logo, $|U| \leqslant 2\varepsilon n$ donde segue que I contém no máximo εn arestas. Portanto, como $e(G'') > e(G^n) - 5\varepsilon n^2$ e G^n é a união de k emparelhamentos induzidos, segue que $e(G^n) < 5\varepsilon n^2 + k\varepsilon n$. □

Exercício 36. Demonstre a equivalência entre os teoremas 34 e 35.

Essa versão do Teorema de Ruzsa–Szemerédi tem a seguinte conexão com o Teorema de Roth sobre 3-pa. Seja $f(k, n)$ o número máximo de arestas que pode conter um grafo de ordem n que é uma união de k emparelhamentos induzidos, ou seja,

$$f(k, n) = \max\left\{ e(G^n) \colon G^n = \bigcup_{i \in [k]} M_i, \text{ onde } M_i \text{ é emparelhamento induzido} \right\}.$$

Então,

$$r_3(n) \leqslant \frac{f(n, 5n)}{n}.$$

De fato, tome $a_1, \ldots, a_{r_3(n)}$ uma seqüência de inteiros positivos que não contém uma 3-pa. Defina o grafo bipartido $G = ([2n] \cup [3n], E)$, onde

$$E = \{(x + a_i, x + 2a_i) \colon x \in [n] \text{ e } i \in [r_3(n)]\}.$$

Então $|E| = r_3(n)n$ e $G = \bigcup_x \{(x + a_i, x + 2a_i) \colon i \in [r_3(n)]\}$. Resta observar que cada fator da união é um emparelhamento induzido em G. Portanto, $f(n, 5n) \geqslant r_3(n)n$. A desigualdade $f(k, n) < 5\varepsilon n^2 + k\varepsilon n$, para todo n suficientemente grande, prova que $r_3(n) = o(n)$.

O Lema de Regularidade, o Teorema de Ruzsa-Szemerédi e suas conseqüências foram generalizados para hipergrafos por Gowers **??**Nagle et al. (2005); Rödl and Skokan (2004) e independentemente por Rödl e eus colaboradores. Denotamos por K^t o hipergrafo k-uniforme completo de ordem t.

Teorema 37. *Se um hipergrafo H k-uniforme de ordem n contém $o(n^t)$ cópias do hipergrafo k-uniforme completo K^t, então podemos tornar G livre de K^t removendo $o(n^k)$ hiperarestas.*

EXERCÍCIO 38. Deduza o seguinte resultado do teorema acima.

TEOREMA 39. *Se H é um hipergrafo k-uniforme tal que toda aresta pertence a exatamente um subgrafo k-uniforme completo K^{k+1}, então $|E(H)| = o(|V(H)|^k)$.*

Observamos que o caso $k = 2$ da Teorema 39 é o Teorema de Ruzsa-Szemerédi. O caso $k = 3$ foi provado em Frankl and Rödl (2002).

Ajtai and Szemerédi (1974) generalizaram o teorema de Roth provaram o seguinte resultado. A prova que apresentamos é de Solymosi (2003).

TEOREMA 40. *Para todo $\delta > 0$ existe um natural n_0 tal que para todo $n \geqslant n_0$ todo subconjunto de $[n]^2$ com pelo menos δn^2 pontos contém um tripla da forma $\{(a, b), (a + d, b), (a, b + d)\}$ para algum inteiro $d \neq 0$.*

DEMONSTRAÇÃO. Seja $S \subset [n]^2$ com pelo menos δn^2 pontos. Definimos o grafo biprtido $G_S = (A \cup B, E)$ tomando A e B como duas cópias disjuntas de $\{1, 2, \ldots, n\}$ e um par $(i, j) \in A \times B$ é uma aresta se forem um ponto de S.

Particionamos as arestas da seguinte forma, (i, j) e (k, ℓ) estão na mesma classe se, e só se, $i + j = k + \ell$. É fácil de ver que cada classe é um emparelhamento.

Como $|E(G_S)| \geqslant \delta n^2 \neq o(|V(G_S)|)$ temos que, para n suficientemente grande, pelo menos um emparelhemanto não é induzido. Logo, existem $i, k \in A$ e $j, \ell \in B$ com (i, j) e (k, ℓ) na mesma classe e arestas (i, ℓ), (k, ℓ) e (i, j) que definem uma tripla como a que procuramos. □

EXERCÍCIO 41. Deduza o teorema de Ajtai-Szemerédi diretamente do Teorema 29, página 26 para triângulos. Deduza o Teorema de Roth do Teorema de Ajtai-Szemerédi.

Solymosi (2004) mostrou, usando o caso $k = 3$ do Teorema 39 demonstrado por Frankl e Rödl, que um subconjunto de $[n]^2$ de densidade $\delta > 0$ deve conter um quadrado, ou seja, quatros pontos com coordenadas (a, b), $(a+d, b)$, $(a, b+d)$ e $(a+b, b+d)$, do qual o Teorema de Szemerédi par 4-PA é facilmente deduzido.

EXERCÍCIO 42. Mostre que o Teorema 39 implica o Teorema de Szemerédi.

EXERCÍCIO 43 (Sárközy and Selkow, 2004). Dados $c_1 > 0$ e $c_2 \geqslant 1$ existem n_0 e η tais que o seguinte vale. Se G é um grafo de ordem pelo menos n_0 e tamanho pelo menos $c_1 n^2$ dado pela união de emparelhamentos $M_1, M_2, \ldots, M_m$ com $m \leqslant c_2 n$, então existem $i \in [m]$ e $A, B \subset V(M_i)$ tais que

(1) $(A \times B) \cap M_i = \emptyset$,
(2) $|A| = |B| \geqslant \eta n$,

(3) $|E(G[A \times B])| \geqslant (c_1/4)|A||B|$.

Mostre a afirmação (a dica é usar o lema de regularidade, versão Teorema 33) acima.

5.2. Um resultado do tipo Ramsey-Turán. Relembrando o Teorema de Turán, no caso específico do K^4, nos diz que um grafo com n vértices $G = G^n$ pode ter no máximo $(2/3)\binom{n}{2} \asymp n^2/3$ arestas para não conter um grafo completo com 4 vértices. Além disso, o grafo extremal é tripartido completo com $\approx n/3$ vértices em cada um dos conjuntos independentes.

Exercício 44. Denotamos por $\alpha(G)$ o tamanho do maior conjunto independente, ou seja, a cardinalidade do maior subconjunto de $V(G)$ que não induz aresta. Mostre que todo grafo J de grau médio $> \alpha(J)$ contém triângulo.

Uma das primeiras aplicações do Lema de Regularidade é o seguinte resultado do tipo Ramsey-Turán demonstrado por Szemerédi (1972).

Teorema 45. *Se G^n não contém K^4 e $\alpha(G^n) = o(n)$, então $e(G^n) < n^2/8 + o(n^2)$.*

Demonstração. Vamos supor que n é suficientemente grande. Suponhamos também que $e(G^n) > (1/8 + \xi)\, n^2$, para alguma constante positiva ξ, e que $\alpha(G^n) < \delta n$ para toda constante positiva δ. Vamos mostrar que tal grafo deve conter um K^4.

Aplicamos o Lema de Regularidade para $\varepsilon = \xi/7$ e $k_0 = \lceil \varepsilon^{-1} \rceil$ e podemos supor, para $K_0 = K_0(\varepsilon, k_0)$ dado pelo Lema de Regularidade, que

$$e(G^n) > \left(\frac{1}{8} + 6\varepsilon\right) n^2, \quad \alpha(G^n) \leqslant \frac{\varepsilon^2}{K_0}\,(n-1) \quad \text{e} \quad n \geqslant \frac{K_0}{\varepsilon}.$$

Seja $\mathcal{P}$ uma partição (ε, k, G)-regular dos vértices de G dada pelo Lema de Regularidade. Seja $|V_i| = m$, para todo $i \in [k]$. Note que $\alpha(G) < \varepsilon^2 m$. Tomamos $\rho = 2\varepsilon$ e consideramos o grafo reduzido $R = R(\mathcal{P}, \rho, \varepsilon)$. A demonstração segue em dois casos.

Primeiro, suponha que $e(R) > k^2/4$. Pelo Teorema de Turán o grafo R contém um triângulo, digamos V_1V_2, V_2V_3 e V_1V_3. Sabemos que pelo menos uma fração $1 - 2\varepsilon$ dos vértices de V_1 têm pelo menos $(\rho - \varepsilon)m$ vizinhos em V_2 e em V_3. Fixe um tal $v \in V_1$ e ponha X seus vizinhos em V_2 e Y seus vizinhos em V_3. Agora, $|X|, |Y| \geqslant \varepsilon m$, portanto, $|d(X,Y) - \rho| < \varepsilon$, donde tiramos que $e(X,Y) \geqslant \varepsilon^3 m^2$. Usamos esse fato e o exercício acima, lembrando que $\alpha(G) < \varepsilon^2 m$, para concluir que $G[X \cup Y]$ contém triângulo e, portanto, $G[V_1 \cup V_2 \cup V_3]$ contém K^4. Com isso terminamos o primeiro caso.

Agora, podemos supor que $e(R) \leqslant k^2/4$. Tome $G'' = G''(\mathcal{P}, \rho, \varepsilon)$, o grafo obtido a partir de G não considerando as arestas descritas em (i)–(iv) na página 18.

Por (16), página 18, temos que $e(G'') > (1/8 + \varepsilon)n^2$. Então,

$$\sum_{1 \leqslant i < j \leqslant k} d(V_i, V_j) = \frac{e(G'')}{m^2} \geqslant e(G'')(n/k)^{-2} > (1/8 + \varepsilon)k^2,$$

e no máximo $k^2/4$ dessas densidades são não-nulas, portanto, a média dessas densidades não-nulas é maior que $\mu = 1/2 + 4\varepsilon$. Logo, existe um par com densidade maior que μ. Sem perda de generalidade, assumimos que $d(V_1, V_2) > \mu$.

Vamos mostrar que $H = G[V_1 \cup V_2]$ contém K^4.

Pelo menos $(1 - \varepsilon)m$ vértices de V_1 têm, cada um, mais que $(\rho - \varepsilon)|V_2| = (1/2 + 3\varepsilon)m$ vizinhos em V_2. Escolha dois deles, digamos x, $y \in V_1$, adjacentes. Isso pode ser feito pois podemos tomar ε pequeno o suficiente para que $(1 - \varepsilon)m > 6\varepsilon m$. Então $|N(x) \cap N(y) \cap V_2| > 6\varepsilon m > \varepsilon^2 m$, portanto, existem z, $w \in N(x) \cap N(y)$ adjacentes. Dessa forma, $K^4 \subseteq H \subseteq G$. □

Bollobás and Erdős (1976) contruiram uma seqüência de grafos $(H^n)_{n \in \mathbb{N}}$ com $K^4 \not\subseteq H^n$, $\alpha(H^n) = o(n)$ e $e(H^n) > n^2/8 - o(n^2)$, ou seja, a constante $1/8$ é a melhor possível.

O problema de determinar

$$\max \{e(G^n) \colon K^p \not\subseteq G^n \text{ e } \alpha(G^n) = o(n)\},$$

foi resolvido por Erdős and Sós (1969) para p ímpar e foi completamente resolvido, usando o Lema de Regularidade, por Erdős et al. (1983).

De uma maneira geral, um *Problema extremal do tipo Ramsey-Turán* tem a seguinte formulação: sejam $\mathcal{L} = \{L_1, \ldots, L_r\}$ uma família de grafos, $c \colon E(G^n) \to [r]$ uma r-coloração das arestas de G^n tal que para todo $i \in [r]$ não temos um L_i monocromático da cor i e $\alpha(G^n) \leqslant m$, para $m = m(n)$. Nestas condições, qual é o número máximo de arestas que G^n pode ter? Note que, pelo Teorema de Ramsey, se m é fixo então não existe um grafo com as propriedades acima, logo o caso que interessa é $m \to \infty$, com $m = o(n)$. Para uma coletânea de resultados e aplicações da Teoria de Ramsey-Turán veja o trabalho de Simonovits and Sós (2001).

5.3. Grafos com número de Ramsey linear. Vejamos uma aplicação em Teoria de Ramsey. Denote por $\mathrm{r}(H)$ o menor número natural tal que para todo grafo de ordem $\mathrm{r}(H)$, ou o grafo contém uma cópia de H ou o seu complemento contém uma cópia de H. Naturalmente, $\mathrm{r}(H)$ é o número de Ramsey $\mathrm{r}(H, H)$ como foi definido na seção 1.2.

O seguinte resultado é devido a Chvatál et al. (1983). Ele diz que o número de Ramsey, $\mathrm{r}(H)$, de um grafo com grau limitado é linear no tamanho do grafo.

TEOREMA 46. *Para todo inteiro positivo Δ existe uma constante $c = c(\Delta)$ tal que para todo grafo H^n com grau máximo $\leqslant \Delta$ vale que*

$$\mathrm{r}(H^n) \leqslant cn.$$

DEMONSTRAÇÃO. Fixamos $k_0 = \mathrm{r}(K^{\Delta+1})$ e escolhemos ε tal que

$$\varepsilon \leqslant \frac{(1/2-\varepsilon)^\Delta}{\Delta+2} \quad \text{e} \quad \varepsilon < \frac{1}{k_0-1} - \frac{1}{r},$$

para todo $r \geqslant k_0$. Tomamos

$$c = \frac{K_0}{\varepsilon(1-\varepsilon)},$$

onde $K_0 = K_0(\varepsilon, k_0)$ é dado pelo Lema de Regularidade.

Seja G um grafo G de ordem $N = cn \geqslant n_0(\varepsilon, k_0)$, seja $\mathcal{P} = \{V_0, \ldots, V_k\}$ uma partição (ε, k, G)-regular dada pelo Lema de Regularidade, seja $m = |V_i|$ para todo $i \in [k]$. Observamos que,

$$\varepsilon m = \varepsilon \frac{N - |V_0|}{k} \geqslant \varepsilon \frac{N - \varepsilon N}{K_0} \geqslant cn \frac{\varepsilon(1-\varepsilon)}{K_0} = n. \tag{21}$$

Tomando o grafo reduzido $R = R(\mathcal{P}, 0, \varepsilon)$ temos que

$$e(R) > (1-\varepsilon)\binom{k}{2} = \left(1 - \frac{1}{k} - \varepsilon + \frac{\varepsilon}{k}\right)\frac{k^2}{2} > \left(1 - \frac{1}{k} - \varepsilon\right)\frac{k^2}{2} = \left(1 - \frac{1}{k_0 - 1}\right)\frac{k^2}{2},$$

portanto, pelo Teorema de Turán, temos $K^{k_0} \subseteq R$.

Defina uma 2-coloração das arestas de R por

$$c(V_iV_j) = \begin{cases} \text{AZUL} & \text{se } d(V_i, V_j) \geqslant 1/2, \\ \text{VERMELHO} & \text{caso contrário,} \end{cases}$$

para todos i, $j \in [k]$ distintos.

Denote por R^{A} e R^{V} os subgrafos induzidos em R pelas arestas de cor AZUL e cor VERMELHO, respectivamente. Então, esses são os grafos reduzidos para os paramêtros $(\mathcal{P}, 1/2, \varepsilon)$ em G e em $\overline{G}$, respectivamente.

Pela definição $k_0 = \mathrm{r}(K^{\Delta+1})$ temos $K^{\chi(H)} \subseteq K^{k_0}$ monocromático, portanto, ou $H^n \subseteq R^{\text{A}}(n)$ ou $H^n \subseteq R^{\text{V}}(n)$. Logo, por (21) e pela escolha de ε podemos usar o Lema 22, página 21, para concluir que $H^n \subseteq G$ ou $H^n \subseteq \overline{G}$. □

5.4. Grafos universais. Por toda esta seção γ, δ, σ, ε e β denotam reais positivos menores que 1.

Diferente do que vimos até agora, os resultados desta seção dizem respeito a subgrafos induzidos. Neste caso, existe uma versão para o grafo reduzido, o *grafo reduzido induzido* $I(\mathcal{P}, \beta, \varepsilon)$ e uma versão "induzida" do Lema 22 que diz que todo subgrafo $H \subseteq I$ induzido do grafo reduzido induzido I é subgrafo induzido do grafo G original.

O grafo reduzido induzido $I(\mathcal{P}, \beta, \varepsilon)$ é definido como na Seção 4.2, página 20, com a condição extra que

$$0 < \beta < 1/2 \text{ } \textit{e para todos } V_i, V_j \in \mathcal{P} \textit{ temos que } \beta < d(V_i, V_j) < 1 - \beta.$$

Vejamos, sem nos aprofundarmos nos detalhes, que um subgrafo induzido de I é um subgrafo induzido do grafo original G.

Sejam $G = G^n$ um grafo, $\mathcal{P} = \{V_0, V_1, \ldots, V_k\}$ uma partição do seu conjunto de vértices. Seja H um subgrafo induzido de $I = I(\mathcal{P}, \beta, \varepsilon)$ com conjunto de vértices $V(H) = \{V_{\ell_1}, \ldots, V_{\ell_h}\}$. Agora fazemos como no Lema 22, vamos escolher $v_1, \ldots, v_h \in V(G)$ tal que $G[\{v_i\}_{i=1}^h]$ é uma cópia induzida de H em G.

Ponha $C_j(0) = V_{\ell_j}$ o conjunto de vértices candidatos a v_j. No i-ésimo passo escolhemos $v_i \in C_i(i-1)$ tal que para todo $j > i$ temos

$$\begin{aligned} |N_G(v_i) \cap C_j(i-1)| &> (\beta - \varepsilon)|C_j(i-1)| \text{ se } V_{\ell_i}V_{\ell_j} \in E(H) \text{ e} \\ |N_G(v_i) \cap C_j(i-1)| &< (\beta + \varepsilon)|C_j(i-1)| \text{ se } V_{\ell_i}V_{\ell_j} \notin E(H), \end{aligned}$$

e fazemos a atualização $C_j(i) = C_j(i-1) \cap N_G(v_i)$.

Dessa forma, v_i é adjacente a mais que $(\beta-\varepsilon)|C_j(i-1)|$ ou não é adjacente a mais que $(1-(\beta+\varepsilon))|C_j(i-1)| \geqslant (\beta-\varepsilon)|C_j(i-1)|$ vértices de $C_j(i-1)$ dependendo se $V_{\ell_i}V_{\ell_j}$ é ou não uma aresta de H.

Dizemos que um grafo G tem a propriedade $P(k, m, \beta, \varepsilon)$, para $0 < \beta < 1/2$, k e m inteiros, se seu conjunto de vértices $V(G)$ pode ser particionado em k subconjuntos $V_1, \ldots, V_k$ de mesma cardinalidade m tal que todo par (V_i, V_j) são ε-regulares com densidade maior que β e menor que $1 - \beta$, para todo $1 \leqslant i < j \leqslant k$. Um grafo que contém todos os subgrafos de ordem k como subgrafo induzido é chamado de *k-universal*.

Lema 47 (Rödl, 1986). *Dados $0 < \beta < 1/2$ real e $k > 0$ inteiro existem $\varepsilon_k = \varepsilon(k, \beta)$ e $m_k = m(k, \beta)$ tal que todo grafo G com a propriedade $P(k, m, \beta, \varepsilon_k)$, com $m \geqslant m_k$, é k-universal.*

Demonstração. A prova é por indução em k, para todo β. Para $k = 2$ tome $m_k = \lfloor 1/\beta \rfloor \geqslant 2$ e $\varepsilon_k = \beta$.

Suponha que o resultado vale para todo inteiro positivo $\leqslant k$ e para todo $0 < \beta < 1/2$. Dados $k+1$ e β tome $\varepsilon_k = \varepsilon(k, \beta/2)$ e $m_k = m(k, \beta/2)$, para os quais vale o lema, e defina

$$\varepsilon_{k+1} = \varepsilon(k+1, \beta) = \min\left\{\frac{1}{2(k+1)}, \frac{\beta}{2}\varepsilon_k\right\} \quad \text{e}$$

$$m_{k+1} = m(k+1, \beta) = \max\left\{2\left\lceil\frac{m_k}{\beta}\right\rceil, k+1\right\}.$$

Seja G um grafo com a propriedade $P(k+1, m, \beta, \varepsilon_{k+1})$, onde $m \geqslant m_{k+1}$. Escolha um vértice $u_{k+1} \in V_{k+1}$ com mais que $(d(V_{k+1}, V_j) - \varepsilon_{k+1})|V_j|$ e menos que $(d(V_{k+1}, V_j) + \varepsilon_{k+1})|V_j|$ vizinhos em V_j, para todo $j \in [k]$.

Agora, para todo $j \in [k]$ escolha $B_j \subseteq V_j$ tal que

(i) $|B_j| = \lceil \beta m/2 \rceil \geqslant m_k$,

(ii) se $v_j v_{k+1} \in E(H)$ então $uu_{k+1} \in E(V_j, V_{k+1})$, para todo $u \in B_j$ e, se $v_j v_{k+1} \notin E(H)$ então $u, u_{k+1} \notin E(V_j, V_{k+1})$, para todo $u \in B_j$.

Queremos aplicar a hipótese de indução em $B_1, \ldots, B_k$. Vamos mostrar que os pares (B_i, B_j) são (ε_k, G)-regulares.

Sejam $X_i \subseteq B_i$ e $X_j \subseteq B_j$ subconjuntos com pelo menos uma fração ε_k dos vértices. Temos, assim, $|X_i| \geqslant \varepsilon_k |B_i| \geqslant (2\varepsilon_{k+1}/\beta) \lceil \beta m/2 \rceil \geqslant \varepsilon_{k+1} m$, e também, analogamente, $|X_j| \geqslant \varepsilon_{k+1} m$. Como o par (V_i, V_j) é ε_{k+1}-regular temos

$$|d(X_i, X_j) - d(B_i, B_j) \leqslant |d(X_i, X_j) - d(V_i, V_j)| + |d(V_i, V_j) - d(B_i, B_j)| < \\ < 2\varepsilon_{k+1} < \varepsilon_k.$$

Logo, por indução, existem $u_1, \ldots, u_k$, com $u_i \in B_i$ para todo $i \in [k]$, tal que $u_i u_j \in E(G)$ se, e somente se, $v_i v_j \in E(H)$, portanto, $G[u_1, \ldots, u_{k+1}]$ é isomorfo a H. □

Erdős (1979) perguntou se, dado um inteiro positivo k, existe δ tal que todo grafo G de ordem n suficientemente grande e tal que para todo $S \subseteq V(G)$ com $|S| \geqslant n/2$ vale que

$$\left(\frac{1}{2} - \delta\right) \binom{|S|}{2} < e(G[S]) < \left(\frac{1}{2} + \delta\right) \binom{|S|}{2},$$

então G contém K^k.

Dizemos que um grafo G tem a propriedade (γ, δ, σ) se para todo $S \subseteq V(G)$ com $|S| \geqslant \gamma |V(G)|$ temos

$$(\sigma - \delta) \binom{|S|}{2} < e(G[S]) < (\sigma + \delta) \binom{|S|}{2}.$$

Rödl (1986) provou o seguinte resultado que responde na afirmativa a pergunta de Erdős. De fato, ele provou um resultado mais forte que aquele conjecturado.

Teorema 48. *Para todo inteiro positivo k e para todos σ e γ, existe δ e existe um inteiro positivo n_0 tal que todo grafo de ordem $n \geqslant n_0$ com a propriedade (γ, δ, σ) contém todo grafo de ordem k como subgrafo induzido.*

Esboço da demonstração. Observe que se o grafo G_n tem a propriedade (γ, δ, σ) então o seu complemento satisfaz $(\gamma, \delta, 1-\sigma)$. Também, como podemos considerar os complementos dos grafos em questão, vamos supor $\sigma \leqslant 1/2$.

Suponha

$$k > \max\left\{\frac{4}{\sigma}, \frac{4}{4-7\sigma}, \frac{3}{1-\gamma}\right\}. \tag{22}$$

Ponha $m_0 = k$ e

$$\varepsilon = \min\left\{\frac{1}{m_0}, \varepsilon(k, \sigma/2), 1 - \frac{m_0\gamma}{m_0 - 3}\right\}$$
$$\delta = \min\left\{\frac{\sigma}{4} - \frac{1}{m_0}, 1 - \frac{7\sigma}{4} - \frac{1}{m_0}, \frac{\sigma}{24}(1-\varepsilon)^2\frac{1}{M^2}\right\}$$
$$N_1 = \max\left\{\left\lceil\frac{M}{1-\varepsilon}\right\rceil m(k, \sigma/2), n_0(\varepsilon, m_0)\right\},$$

onde $M = M(\varepsilon, m_0)$ e $n_0(\varepsilon, m_0)$ são dados pelo Lema de Regularidade. Por (22) temos que ε e δ são positivos.

Seja G_n, para $n \geqslant N_1$, com a propriedade (γ, δ, σ) e uma partição (ε, t, G_n)-regular $\mathcal{P} = \{V_0, \ldots, V_t\}$ dada pelo Lema de Regularidade. Prova-se que

$$\frac{\sigma}{2} \leqslant d(V_i, V_j) \leqslant 1 - \frac{\sigma}{2} \text{ para todos } i,\, j \in [t], \tag{23}$$

donde deduzimos o teorema da seguinte forma: o número de arestas do grafo reduzido $R(\mathcal{P}, d, \varepsilon)$ para $d = 0$ é maior que $(1-\varepsilon)\binom{t}{2}$ e, pelo Teorema de Turán, podemos conluir que $K^{m_0} \subseteq R$.

Sejam $V_{s_1}, \ldots, V_{s_{m_0}}$ pares 2-a-2 (ε, G_n)-regulares. Temos $|V_{s_i}| \geqslant N_1(1-\varepsilon)/M \geqslant m(k, \sigma/2)$ e $\varepsilon \leqslant \varepsilon(k, \sigma/2)$. Logo, G_n satisfaz a $(k, m(k, \beta), \beta, \varepsilon(k, \beta))$ para $\beta = \sigma/2$. □

Rödl também provou o seguinte resultado.

Teorema 49. *Para todo inteiro positivo k e para todos σ e δ com $\delta < \sigma < 1 - \delta$, existe γ e um inteiro positivo n_0 tal que todo grafo de ordem $n \geqslant n_0$ com a propriedade (γ, δ, σ) contém todos os grafos de ordem k como subgrafo induzido.*

Demonstração. Antes de demonstrarmos esse teorema, observe que se

$$\delta_1 = \max\left\{\sigma + \delta - \frac{1}{2}, \frac{1}{2} - \sigma + \delta\right\}$$

então, se G_n satisfaz (γ, δ, σ) também satisfaz $(\gamma, \delta_1, 1/2)$ e podemos assumir que $0 < \delta < 1/2$. Portanto, é suficiente provarmos o teorema para $\sigma = 1/2$ e para todo k e todo $\delta < 1/2$.

Defina $\beta = 1/2 - \delta$ e assuma que $k \geqslant 3/\beta$. Seja m_0 o menor inteiro tal que qualquer três coloração das arestas do K^{m_0} induz algum K^k monocromático. Ponha

$$\varepsilon = \min\left\{{m_0}^{-1}, \varepsilon_k\left(k, \frac{1}{2}\beta m\right)\right\}$$

e sejam M_0, n_0 e a partição $V_0, \ldots, V_t$ de $V(G)$ dados pelo Lema de Regularidade, onde G é um grafo com

$$N_0 = \max\left\{n_0, \frac{M_0 m_k}{1-\varepsilon}\right\}$$

vértices e com a propriedade (γ, δ, σ) para

$$\gamma = \frac{k(1-\varepsilon)}{M_0}.$$

Se R é o grafo reduzido para $d = 0$ temos $e(R) > (1-\varepsilon)\binom{t}{2} > (1-\frac{1}{m_0-1})\binom{t}{2}$, portanto, pelo Teorema de Turán temos que $K^{m_0} \subseteq R$, ou seja, existem classes $V_{s_0}, \ldots, V_{s_{m_0}}$ tal que todo par (V_{s_i}, V_{s_j}) é (ε, G)-regular.

Para tal K^{m_0}, considere $\varphi\colon E(K^{m_0}) \to [3]$ uma 3-coloração de suas arestas dada por

(i) $\varphi(\{i,j\}) = 1$ se $d(V_{s_i}, V_{s_j}) \leq \beta/2$;
(ii) $\varphi(\{i,j\}) = 2$ se $\beta/2 < d(V_{s_i}, V_{s_j}) < 1 - \beta/2$; e
(iii) $\varphi(\{i,j\}) = 3$ se $d(V_{s_i}, V_{s_j}) \geq 1 - \beta/2$.

Vejamos que não pode ocorrer K^k monocromático da cor 1 ou 3. Primeiro, para cor 1. Se $G' = G[\bigcup_i V_{s'_i}]$ temos, onde $V_{s'_i}$ são os vértices do K^k monocromático e pondo $m = |V_i|$,

$$\mathrm{d}(G') = \frac{e(G')}{\binom{|V(G')|}{2}} \leqslant \frac{\binom{t}{2}m^2\frac{\beta}{2} + \binom{m}{2}t}{\binom{tm}{2}} < \frac{1}{2}\beta + \frac{1}{k} < \frac{1}{2} - \delta.$$

Para a cor 3 temos

$$\mathrm{d}(G') \geqslant \frac{\binom{t}{2}m^2(1-\frac{\beta}{2})}{\binom{tm}{2}} > 1 - \frac{\beta}{2} - \frac{1}{k} < \frac{1}{2} + \delta.$$

Como $|V(G')| \geqslant \frac{k}{M}|V(G)|(1-\varepsilon) = \gamma|V(G)|$ contradizendo o fato de G ter a propriedade $(\gamma, \delta, 1/2)$.

Para a cor 2 temos que G satisfaz a propriedade $(k, m, \beta/2, \varepsilon_k)$, para $m \geqslant m_k$. De fato, para todos i e j temos

$$|V_{s'_i}| = |V_{s'_j}| \geqslant (1-\varepsilon)\frac{N_0}{t} \geqslant (1-\varepsilon)\frac{N_0}{M_0} \geqslant \frac{1-\varepsilon}{M_0}\frac{M_0 m_k}{1-\varepsilon} = m_k$$

e $d(V_{s'_i}, V_{s'_j}) \in (\beta/2, 1-\beta/2)$ com esses pares ε_k-regulares por definição. □

6. Um Lema de Regularidade para grafos esparsos

Para uma seqüência de grafos com $e(G_n) = o(n^2)$ o Lema de Regularidade não fornece informação alguma. Ele aproxima G_n pelo grafo vazio pois o número de arestas que desprezamos é quadrático no número de vértices. Nesta seção veremos uma variante do Lema de Regularidade para grafos esparsos.

Fixe um grafo $G = (V, E)$. Para uma partição $\mathcal{Q}$ de V dizemos que G é $(\mathcal{Q}, \eta)$-*uniforme*, para $0 < \eta \leqslant 1$ fixo, se para algum $p \in [0, 1]$ e para todo A, $B \subseteq V$ disjuntos quando $\mathcal{Q}$ é trivial ou pertencentes a partes diferentes da partição se $\mathcal{Q}$ não é trivial, e tais que $|A|$, $|B| \geqslant \eta|V|$, temos a seguinte condição de pseudoaleatoriedade

$$\big|e_G(A, B) - p|A||B|\big| \leqslant \eta p|A||B|.$$

Se $\mathcal{Q}$ é trivial e $\eta > 0$ está fixo, o grafo aleatório $G_{n,p}$ é um exemplo de grafo $(\mathcal{Q}, \eta)$-uniforme; neste caso de partição trivial dizemos simplesmente η-uniforme. Um grafo aleatório $G_{n,p}$ com $p = p(n) = C/n$ é η-uniforme quase-sempre, para C dependendo somente de η.

Para um subgrafo gerador H de G definimos a *densidade relativa de H em G* no par (A, B) de subconjuntos disjuntos de V por

$$d_{H,G}(A, B) = \begin{cases} e_H(A, B)/e_G(A, B) & \text{se } e_G(A, B) > 0, \\ 0 & \text{caso contrário.} \end{cases} \tag{24}$$

Dizemos que o par (A, B) de subconjuntos disjuntos de V é (ε, H, G)-*regular* se para todo $X \subseteq A$ e $Y \subseteq B$ com $|X| \geqslant \varepsilon|A|$ e $|Y| \geqslant \varepsilon|B|$ temos

$$|d_{H,G}(A, B) - d_{H,G}(X, Y)| < \varepsilon.$$

Dizemos que uma partição (ε, k)-equipotente $V_0, V_1, \ldots, V_k$ dos vértices de G é (ε, H, G)-regular se o número de pares (V_i, V_j), para $1 \leqslant i < j \leqslant k$, que não são (ε, H, G)-regulares é no máximo $\varepsilon\binom{k}{2}$. O seguinte resultado foi provado por Kohayakawa em 1991 (veja Kohayakawa, 1997, por exemplo), e independentemente, por Rödl.

Teorema 50. *Dados um real positivo $\varepsilon \leqslant 1$ e inteiros m_0, $l \geqslant 1$, existem constantes positivas $\eta = \eta(\varepsilon, m_0, l)$ e $M = M(\varepsilon, m_0, l) \geqslant m_0$ tais que para todo grafo $(\mathcal{Q}, \eta)$-uniforme G, onde $\mathcal{Q}$ é uma l-partição de $V(G)$, se $H \subseteq G$ é um subgrafo gerador de G, então existe uma $(k + 1)$-partição (ε, H, G)-regular de $V(G)$ que refina $\mathcal{Q}$, com $m_0 \leqslant k \leqslant M$.*

O papel da partição $\mathcal{Q}$ é unicamente de controlar a partição dada pelo teorema no caso de grafos l-partidos. Note que essa versão implica o caso denso se tomamos $G = K^n$; por esse motivo dedicamos a Seção 6.3 a uma demonstração desse caso esparso, incluindo sua versão para o Lema 18.

Vejamos uma variante do caso esparso. Sejam $G = (V, E)$ fixo e $0 < \eta \leqslant 1$ e $0 < p \leqslant 1$. Dizemos que G é η-*superiormente-uniforme com densidade p* se para todos A, $B \subseteq V$ disjuntos com $|A|$, $|B| \geqslant \eta|V|$ temos

$$e_G(A, B) \leqslant (1 + \eta)p|A||B|.$$

Definimos a *p-densidade* entre A e B em G por

$$d_{G,p}(A,B) = \frac{e_G(A,B)}{p|A||B|}$$

e escrevemos $d_p(A,B)$ se G é subentendido. Note a relação entre a definição de p-densidade com a de densidade de G relativa à $G_{n,p}$ (eq. (24)).

Para $0 < \varepsilon \leqslant 1$ e $A, B \subseteq V$ disjuntos não-vazios dizemos que (A,B) é (ε,p)-*regular* se para todos $X \subseteq A$ e $Y \subseteq B$ com $|X| \geqslant \varepsilon|A|$ e $|Y| \geqslant \varepsilon|B|$ temos

$$\left|d_p(A,B) - d_p(X,Y)\right| < \varepsilon.$$

Uma partição (ε,k)-equipotente $\mathcal{P} = \{V_0, V_1, \ldots, V_k\}$ do conjunto de vértices V é (ε,p)-regular se $|V_0| \leqslant \varepsilon|V|$ e no máximo $\varepsilon\binom{k}{2}$ pares (V_i,V_j), para $1 \leqslant i < j \leqslant k$, não são (ε,p)-regulares.

Temos então a seguinte versão esparsa que é útil nos casos em que o grafo esparso não é subgrafo de algum grafo η-uniforme fixo.

Teorema 51. *Dados $0 < \varepsilon \leqslant 1$ e $m_0 \geqslant 1$ existem constantes positivas $\eta = \eta(\varepsilon, m_0)$ e $M = M(\varepsilon, m_0) \geqslant m_0$ tais que qualquer grafo η-superiormente-uniforme G com densidade $0 < p \leqslant 1$ admite uma $(k+1)$-partição (ε,p)-regular de $V(G)$, com $m_0 \leqslant k \leqslant M$.* □

6.1. O caso esparso em Teoria Extremal de Grafos. Considere a seguinte generalização do problema do subgrafo proibido. Sejam G e H grafos e defina $\mathrm{ex}(G,H)$ como o número máximo de arestas que um subgrafo de G pode ter para que H não ocorra como subgrafo. Formalmente,

$$\mathrm{ex}(G,H) = \max\left\{e(J)\colon H \not\subseteq J \subseteq G\right\}.$$

Dessa forma, $\mathrm{ex}(n,H) = \mathrm{ex}(K^n,H)$.

No caso de subgrafos extremais de grafos aleatórios, isto é, quando $G = G_{n,p}$, o resultado mais simples conhecido é o seguinte, de Babai et al. (1990).

Teorema 52. *Se F_n é um subgrafo de $G_{n,1/2}$ com o máximo possível de arestas sem conter K^3 e B_n é um subgrafo bipartido de $G_{n,1/2}$ com o máximo possível de arestas, então $e(F_n) = e(B_n)$. Ainda, F_n é bipartido quase-sempre.* □

Também é sabido (de Babai et al., 1990) que se H é 3-cromático, fixado $0 < p < 1$, e $F_n \subseteq G_{n,p}$ é livre de H com o número máximo de arestas, então

$$e(B_n) \leqslant e(F_n) \leqslant e(B_n) + o(n^2)$$

quase-sempre. Ainda, removendo $o(n^2)$ arestas de F_n podemos torná-lo bipartido. Esse resultado generaliza-se para grafos r-cromáticos.

Kohayakawa et al. (1997) conjecturaram

Conjectura 53. *Para todo grafo não-vazio H de ordem pelo menos 3 e para todo $0 < p = p(n) \leqslant 1$ tal que $pn^{1/d_2(H)} \to \infty$ quando $n \to \infty$, onde*

$$d_2(H) = \max\left\{\frac{e(J)-1}{|J|-2} \colon J \subseteq H,\, |J| \geqslant 3\right\},$$

temos que

$$\mathrm{ex}(G_{n,p}, H) = \left(1 - \frac{1}{\chi(H)-1} + o(1)\right) e(G_{n,p}) \tag{25}$$

vale quase-sempre.

Os casos $H = K^3$ e $H = C^4$ foram, essencialmente, provados por Frankl and Rödl (1986) e Füredi Füredi (1994), respectivamente.

Em Kohayakawa et al. (1997), Kohayakawa, Łuczak e Rödl provaram o caso $H = K^4$ e observaram que uma aplicação simples do Teorema 51 prova a conjectura quando H é uma floresta. O caso $H = C^l$ foi provado por Haxell, Kohayakawa e Łuczak Haxell et al. (1995, 1996). De fato, nesses casos foram verificados a Conjectura 54 abaixo

Vejamos como a versão esparsa do Lema de Regularidade, o Teorema 50, se aplica no caso dessa conjectura. Seja J um subgrafo do grafo η-uniforme $G_{n,p}$. Pelo Teorema 50, temos uma partição $(\varepsilon, J, G_{n,p})$-regular $\mathcal{P}$ de $V(G_{n,p})$.

Se sabemos que para algum $\gamma > 0$ temos

$$e(J) \geqslant \left(1 - \frac{1}{\chi(H)-1} + \gamma\right) e(G_{n,p}).$$

então é fácil encontrarmos $|H|$ partes de $\mathcal{P}$ que "formam uma cópia" de H e no caso p constante, podemos mostrar que essas partes geram uma cópia de fato de H (cf. Lema 22). Infelizmente, esse não é o caso quando $p \to 0$ conforme $n \to \infty$; aqui muito "trabalho extra" precisou ser feito nos resultados parciais conhecidos (Haxell et al., 1995, 1996; Kohayakawa and Kreuter, 1997; Kohayakawa et al., 1997).

Vejamos uma conjectura (Kohayakawa et al., 1997) que implica (25). Sejam m um inteiro positivo e H um grafo com $V(H) = \{v_1, \ldots, v_h\}$, para $h \geqslant 3$, $0 < p = p(m) \leqslant 1$ e seja $\mathbf{V}_m = (V_i)_{i=1}^h$ uma família de conjuntos 2-a-2 disjuntos, cada um de cardinalidade m. Dados reais $0 < \varepsilon \leqslant 1$ e $0 < \gamma \leqslant 1$ e um inteiro positivo T dizemos que um grafo h-partido F com partição $V(F) = V_1 \cup \cdots \cup V_h$ e com T arestas é um

$$(\varepsilon, \gamma, H; \mathbf{V}_m, T)\text{-grafo}$$

se, para todo $1 \leqslant i < j \leqslant h$, todo par (V_i, V_j) é (ε, p)-regular e se $\gamma \leqslant d_{F,p}(V_i, V_j) \leqslant 1$ sempre que $v_i v_j \in E(H)$.

Conjectura 54. *Dados* $0 < \alpha \leqslant 1$ *e* $0 < \gamma \leqslant 1$ *existem constantes* $\varepsilon = \varepsilon(\alpha, \gamma) > 0$ *e* $C = C(\alpha, \gamma)$ *tais que se* $p = p(m) \geqslant Cm^{-1/d_2(H)}$, *então o número de* $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$*-grafos livres de* H *é no máximo*

$$\alpha^T \binom{\binom{h}{2} m^2}{T}$$

para todo T *e todo* m *suficientemente grande.*

Vamos assumir a Conjectura 54 e vamos provar a Conjectura 53.

Seja $\delta > 0$ dado. Vamos mostrar que existe um K positivo tal que se $p = Kn^{-1/d_2(H)}$ então

$$\mathrm{ex}(G_{n,p}, H) = \left(1 - \frac{1}{\chi(H) - 1} + \delta\right) \frac{n^2 p}{2},$$

vale quase-sempre.

Tome

$$\alpha = \frac{\gamma}{2\mathrm{e}\binom{h}{2}}$$

e $0 < \gamma < \delta/5$. Então, pela Conjectura 53 existem $\varepsilon > 0$ e $C > 0$ tais que, quaisquer que sejam m e T, o número de $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-grafos H-livres é no máximo

$$\alpha^T \binom{\binom{h}{2} m^2}{T}$$

se $p \geqslant Cm^{-1/d_2(H)}$. Podemos assumir que $\varepsilon < \delta/5$.

Agora, sejam η e M_0 dados pelo Lema 51. Assuma que $\eta < \delta < 5$ e tome $K = (M_0)^{1/d_2(H)} C$.

Seja G um grafo η-superiormente-uniforme com densidade $p = Kn^{-1/d_2(H)}$ de ordem n suficientemente grande. Então, todo subgrafo de G com pelo menos

$$\left(1 - \frac{1}{\chi(H) - 1} + \delta\right) \frac{n^2 p}{2}$$

arestas contém um subgrafo isomorfo àlgum $(\varepsilon, \gamma, H; \mathrm{V}_m, T)$-grafo, onde $n/M_0 \leqslant m \leqslant n/m_0$, para todo T e para $m_0 = \max\{5/\delta, k_1\}$, onde k_1 é tal que

$$mathrmex(G_{n,p}, H) \leqslant \left(1 - \frac{1}{\chi(H) - 1} + \varrho\right) \binom{k}{2}$$

para $\varrho < \delta/5$ e todo $k \geqslant k_1$.

De fato, seja $F \subseteq G$ com pelo menos $(1 - 1/(\chi(H) - 1) + \delta)n^2 p/2$ arestas. Claramente, F é η-superiormente-uniforme com densidade p.

Seja $\mathcal{P} = (V_i)_{i=0}^k$ a partição (ε, p)-regular (ε, k)-equipotente dada pelo Lema 51. Ponha $m = |V_i|$, para todo $i \in [k]$. Seja $R = R(\mathcal{P}, \gamma, \varepsilon)$ o grafo reduzido de F.

Se

$$e(R) > \left(1 - \frac{1}{\chi(H) - 1} + \varrho\right) \binom{k}{2}$$

então F contêm um $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-subgrafo para algum T. Agora, suponha que $e(R) < (1 - 1/(\chi(H) - 1) + \varrho)\binom{k}{2}$. Dessa forma,

$$\begin{aligned} e(F) &\leqslant \left(\tfrac{\varepsilon^2 n^2}{2} + \varepsilon n^2 + k\tbinom{k}{2} + \varepsilon\tbinom{k}{2}\left(\tfrac{n}{k}\right)^2 + \gamma\tbinom{k}{2}\left(\tfrac{n}{k}\right)^2 + \right. \\ &\qquad \left. \left(1 - \tfrac{1}{\chi(H)-1} + \varrho\right)\tbinom{k}{2} \right)(1+\eta)p \\ &< \left(5\varepsilon + \tfrac{1}{k} + \gamma + \left(1 - \tfrac{1}{\chi(H)-1} + \varrho\right) + \eta\right)\tfrac{n^2 p}{2} \\ &= \left(1 - \tfrac{1}{\chi(H)-1} + \varrho + \eta + \gamma + 5\varepsilon + \tfrac{1}{k}\right)\tfrac{n^2 p}{2} \\ &< \left(1 - \tfrac{1}{\chi(H)-1} + \delta\right)\tfrac{n^2 p}{2}. \end{aligned}$$

uma contradição.

Portanto, todo subgrafo de G com pelo menos $(1 - 1/(\chi(H) - 1) + \delta)n^2 p/2$ arestas contém algum $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-subgrafo.

Observe que não é difícil provar que o grafo aleatório $G_{n,p}$ é η-superiormente-uniforme quase-sempre. Dessa forma, resta provar que para quaisquer inteiros positivos m e T, com $n/M_0 \leqslant m \leqslant n/m_0$, um $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-subgrafo de $G_{n,p}$ contêm H quase-certamente.

Como $p(m) = Km^{-1/d_2(H)} \geqslant Cm^{-1/d_2(H)}$, podemos usar a Conjectura 53. Qualquer $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-grafo tem pelo menos $e(H)\gamma p m^2$ arestas. Fixe $T \geqslant e(H)\gamma p m^2$ e fixe m, com $n/M_0 \leqslant m \leqslant n/m_0$.

Então, o número esperado de $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-subgrafos de $G_{n,p}$ livres de H é no máximo

$$n^{hm} p^T \alpha^T \binom{\binom{h}{2} m^2}{T} \leqslant n^{hm} \left(\frac{p\alpha \mathrm{e}\binom{h}{2} m^2}{T} \right)^T < n^{hm} \left(\frac{\alpha \mathrm{e}\binom{h}{2}}{e(H)\gamma} \right)^T = o(1),$$

que, somando sobre todo m e todo T, ainda temos que o número esperado de $(\varepsilon, \gamma, H; \mathbf{V}_m, T)$-subgrafos de $G_{n,p}$ livres de H é $o(1)$. O resultado segue da desigualdade de Markov. Portanto temos que a Conjectura 53 implica a Conjectura 54.

6.2. Progressões aritméticas em subconjuntos esparsos dos inteiros.

6.3. Uma demonstração do caso esparso do Lema de Regularidade. Se $\mathcal{P}_0$ e $\mathcal{P}_1$ são partições equipotentes de V, então dizemos que $\mathcal{P}_1$ *refina* $\mathcal{P}_0$ se toda classe não-excepcional de $\mathcal{P}_1$ está contida em alguma classe não-excepcional de $\mathcal{P}_0$. Se $\mathcal{P}_0$ é uma partição arbitrária, então $\mathcal{P}_1$ *refina* $\mathcal{P}_0$ se toda classe não-excepcional de $\mathcal{P}_1$ está contida em alguma classe de $\mathcal{P}_0$.

Começamos pelo lema abaixo que é uma forma defectiva da desigualdade de Cauchy-Schwarz e que é importante na demonstração do Lema de Regularidade.

LEMA 55. *Sejam $d_1, \ldots, d_n$ reais. Então para todo inteiro não-negativo $m < n$*

$$\sum_{i=1}^{n} {d_i}^2 \geqslant \frac{1}{n}\left(\sum_{i=1}^{n} d_i\right)^2 + \frac{mn}{n-m}\left(\frac{1}{m}\sum_{i=1}^{m} d_i - \frac{1}{n}\sum_{i=1}^{n} d_i\right)^2. \tag{26}$$

Em particular, se

$$\frac{1}{m}\sum_{i=1}^{m} d_i = \alpha\frac{1}{n}\sum_{i=1}^{n} d_i,$$

então

$$\sum_{i=1}^{n} {d_i}^2 \geqslant \frac{1}{n}\left(1 + (\alpha-1)^2\frac{m}{n-m}\right)\left(\sum_{i=1}^{n} d_i\right)^2. \tag{27}$$

DEMONSTRAÇÃO. Ponha $S_n = \sum_{i=1}^{n} d_i$ e $Q_n = \sum_{i=1}^{n} {d_i}^2$. Então

$$0 \leqslant \sum_{i=1}^{n}\left(d_i - \frac{S_n}{n}\right)^2 = \sum_{i=1}^{n}\left({d_i}^2 - 2d_i\frac{S_n}{n} + \frac{{S_n}^2}{n^2}\right) = Q_n - \frac{{S_n}^2}{n}, \tag{28}$$

portanto,

$$Q_n - Q_m = \sum_{i=m+1}^{n} {d_i}^2 \geqslant \frac{1}{n-m}\left(\sum_{i=m+1}^{n} d_i\right)^2 = \frac{(S_n - S_m)^2}{n-m}.$$

Então

$$\begin{aligned} Q_n = Q_m + (Q_n - Q_m) &\geqslant \frac{{S_m}^2}{m} + \frac{(S_n - S_m)^2}{n-m} \\ &= \frac{1}{n}{S_n}^2 + \frac{nm}{n-m}\left(\frac{S_n}{n} - \frac{S_m}{m}\right)^2. \end{aligned}$$

e demonstramos (26). Agora, provar (27) é fácil. Observe que (28) é a desigualdade usual de Cauchy-Schwarz. □

Fixe $G = (V, E)$ e $\mathcal{Q} = \{U_1, \ldots, U_l\}$ uma l-partição de V. Assuma que G é $(\mathcal{Q}, \eta)$-uniforme para algum $0 < \eta \leqslant 1$. Seja $p = p(G)$ tal que, para todos A, $B \subset V$ tais que A e B são subconjuntos de partes distintas de $\mathcal{Q}$, ou disjuntos se $\mathcal{Q}$ é trivial, e $|A|$, $|B| \geqslant \eta|V|$ vale que

$$\left|e_G(A,B) - p|A||B|\right| \leq \eta p|A||B|.$$

Vejamos um resultado de continuidade sobre $d_{H,G}$ e $d^2_{H,G}$.

LEMA 56. *Fixe $0 < \delta \leq 10^{-2}$. Sejam $A, B \subset V$ tais que A e B são subconjuntos de partes distintas de $\mathcal{Q}$, ou disjuntos se $\mathcal{Q}$ é trivial, com $\delta|A|$, $\delta|B| \geq \eta|V|$. Se $X \subset A$ e $Y \subset B$, $|X| \geq (1-\delta)|A|$ e $|Y| \geq (1-\delta)|B|$, então*

(i) $|d_{H,G}(X,Y) - d_{H,G}(A,B)| \leq 5\delta$,
(ii) $|d_{H,G}(X,Y)^2 - d_{H,G}(A,B)^2| \leq 9\delta$.

DEMONSTRAÇÃO. Vamos provar (i). Observe que $\eta \leqslant \delta$, então

$$\begin{aligned} d_{H,G}(X,Y) \geqslant \frac{e_H(X,Y)}{e_G(X,Y)} &\geqslant \frac{e_H(A,B) - 2(1+\eta)p\delta|A||B|}{e_G(A,B)} \\ &\geqslant d_{H,G}(A,B) - 2\delta\frac{1+\eta}{1-\eta} \geqslant d_{H,G}(A,B) - 3\delta. \end{aligned}$$

Por outro lado,

$$\begin{aligned} d_{H,G}(X,Y) \leqslant \frac{e_H(A,B)}{e_G(X,Y)} &\leqslant \frac{e_H(A,B)}{(1-\eta)p|X||Y|} \\ &\leqslant \frac{e_H(A,B)}{(1-\eta)p(1-\delta)^2|A||B|} \leqslant \frac{1+\eta}{(1-\eta)(1-\delta)^2} d_{H,G}(A,B) \\ &\leqslant d_{H,G}(A,B) + 5\delta, \end{aligned}$$

portanto temos (i). A prova de (ii) é similar. □

Fixe uma constante $0 < \varepsilon \leq 1/2$ e um subgrafo gerador $H \subset G$. Seja $\mathcal{P}_0$ uma $(m+1)$-partição equipotente de V que refina $\mathcal{Q}$, com $4^m \geq \varepsilon^{-5}$. Assumimos que $\eta \leq \eta_0 = \eta_0(m) = 1/m4^{m+1}$ e que $n = |V| \geq n_0 = n_0(m) = m4^{1+2m}$.

Definimos uma partição equipotente $\mathcal{P}_1$ de V a partir de $\mathcal{P}_0$ da seguinte forma. Para cada par (ε, H, G)-irregular $(V_s^{(0)}, V_t^{(0)})$ de classes de $\mathcal{P}_0$, com $1 \leq s < t \leq m$, escolhemos $X = X(s,t) \subset V_s^{(0)}$, $Y = Y(s,t) \subset V_t^{(0)}$ que atestam a irregularidade do par, isto é, tais que $|X|, |Y| \geq \varepsilon|V_s^{(0)}| = \varepsilon|V_t^{(0)}|$, e $|d_{H,G}(X,Y) - d_{H,G}(V_s^{(0)}, V_t^{(0)})| \geq \varepsilon$.

Fixado $1 \leq s \leq m$, os conjuntos $X(s,t)$ em

$$\{X = X(s,t) \subset V_s^{(0)} \colon 1 \leq t \leq m \text{ e } (V_s^{(0)}, V_t^{(0)}) \text{ não é } (\varepsilon, H, G)\text{-regular}\}$$

definem um partição natural de $V_s^{(0)}$ em no máximo 2^{m-1} partes. Vamos chamar essas partes de *átomos* de $V_s^{(0)}$. Tome $q = 4^m$ e ponha $c = \lfloor |V_s^{(0)}|/q \rfloor$, para qualquer $1 \leq s \leq m$. Note que $c \geq \eta n$. Trivialmente, podemos escolher uma partição $\mathcal{P}_1$ de V que refina $\mathcal{P}_0$ tal que

(i) $V_0^{(0)}$ é uma classe de $\mathcal{P}_1$,
(ii) para todo $1 \leq s \leq m$, todo átomo $A \subset V_s^{(0)}$ contém exatamente $\lfloor |A|/c \rfloor$ classes de $\mathcal{P}_1$,
(iii) para todo $1 \leq s \leq m$, o conjunto $V_s^{(0)}$ contém exatamente $q = \lfloor |V_s^{(0)}|/c \rfloor$ classes de $\mathcal{P}_1$.

Observe que $q^2 = 4^{2m} \leqslant |V_s^{(0)}| = cq + r$, com $r < c$, portanto, $\left\lfloor |V_s^{(0)}|/c \right\rfloor = q = 4^m$. Então, podemos assumir que $\mathcal{P}_1$ tem exatamente $m4^m$ classes não-excepcionais e, é fácil provar o seguinte lema.

LEMA 57. *A partição* $\mathcal{P}_1 = \{V_0^{(1)}, \ldots, V_{m_1}^{(1)}\}$ *definida a partir de* $\mathcal{P}_0$ *como acima é equipotente e refina* $\mathcal{P}_0$*, com* $m_1 = mq = m4^m$ *e* $|V_0^{(1)}| \leq |V_0^{(0)}| + n4^{-m}$. □

No que segue, para $1 \leq s \leq m$, sejam $V_s(i)$, para $1 \leq i \leq q$, as classes de $\mathcal{P}_1$ que estão contidas na classe $V_s^{(0)}$ de $\mathcal{P}_0$. Também, para todo $1 \leq s \leq m$, pomos $C_s = \bigcup_{1 \leq i \leq q} V_s(i)$.

Fixe $1 \leq s \leq m$. Note que $|C_s| \geq |V_s^{(0)}| - (c-1) \geq |V_s^{(0)}| - q^{-1}|V_s^{(0)}| \geq |V_s^{(0)}|(1-q^{-1})$. Como $q^{-1} \leq 10^{-2}$ e $q^{-1}|V_s^{(0)}| \geq c \geq \eta n$, pelo Lema 56 temos,

$$|d_{H,G}(C_s, C_t) - d_{H,G}(V_s^{(0)}, V_t^{(0)})| \leq 5q^{-1} \tag{29}$$

e

$$|d_{H,G}(C_s, C_t)^2 - d_{H,G}(V_s^{(0)}, V_t^{(0)})^2| \leq 9q^{-1}, \tag{30}$$

para todo $1 \leq s < t \leq m$.

Seguindo a idéia da prova no caso denso, definimos o *índice* $\mathrm{ind}(\mathcal{R})$ de uma partição equipotente $\mathcal{R} = \{V_0, \ldots, V_r\}$ de V por

$$\mathrm{ind}(\mathcal{R}) = \frac{2}{r^2} \sum_{1 \leq i < j \leq r} d_{H,G}(V_i, V_j)^2,$$

e observe que $0 \leq \mathrm{ind}(\mathcal{R}) < 1$. Os próximos lemas mostram que para $\mathcal{P}_1$ definido como acima temos que $\mathrm{ind}(\mathcal{P}_1) \geq \mathrm{ind}(\mathcal{P}_0) + \varepsilon^5/100$. A prova do primeiro lema é baseada na desigualdade de Cauchy-Schwarz.

LEMA 58. *Suponha* $1 \leq s < t \leq m$. *Então*

$$\frac{1}{q^2} \sum_{i,\,j=1}^{q} d_{H,G}(V_s(i), V_t(j))^2 \geq d_{H,G}(V_s^{(0)}, V_t^{(0)})^2 - \frac{\varepsilon^5}{100}.$$

DEMONSTRAÇÃO. Seja $(V_s^{(0)}, V_t^{(0)})$ um par de conjuntos de $\mathcal{P}_0$. Então,

$$\begin{aligned}
&\frac{1}{q^2} \sum_{i=1}^{q} \sum_{j=1}^{q} d_{H,G}(V_s(i), V_t(j)) = \frac{1}{q^2} \sum_{i,j} \frac{e_H(V_s(i), V_t(j))}{e_G(V_s(i), V_t(j))} \\
&\geqslant \sum_{i,j} \frac{e_G(V_s(i), V_t(j))}{(1+\eta)q^2 p |V_s(i)||V_t(j)|} = \frac{e_H(C_s, C_t)}{(1+\eta)p|C_s||C_t|} \\
&\geqslant \frac{1-\eta}{1+\eta} d_{H,G}(C_s, C_t) \geqslant d_{H,G}(C_s, C_t) - 2\eta.
\end{aligned}$$

Usando a desigualdade de Cauchy-Schwarz,

$$\frac{1}{q^2} \sum_{i,j} d_{H,G}(V_s(i), V_t(j))^2 \geqslant d_{H,G}(C_s, C_t)^2 - 4\eta,$$

e, por (30), temos

$$d_{H,G}(C_s, C_t)^2 \geqslant d_{H,G}(V_s^{(0)}, V_t^{(0)})^2 - \frac{9}{q},$$

e o lema segue de $9q^{-1} + 4\eta \leqslant \varepsilon^5/100$. □

A desigualdade no Lema 58 pode ser melhorada se $(V_s^{(0)}, V_t^{(0)})$ é um par (ε, H, G)-irregular. Formalizamos isso no seguinte lema, que é provado usando a forma defectiva de Cauchy-Schwarz (Lema 55).

LEMA 59. *Seja $1 \leq s < t \leq m$ tais que $(V_s^{(0)}, V_t^{(0)})$ não é (ε, H, G)-regular. Então*

$$\frac{1}{q^2} \sum_{i,\, j=1}^{q} d_{H,G}(V_s(i), V_t(j))^2 \geq d_{H,G}(V_s^{(0)}, V_t^{(0)})^2 + \frac{\varepsilon^4}{40} - \frac{\varepsilon^5}{100}.$$

DEMONSTRAÇÃO. Sejam $X = X(s,t) \subseteq V_s^{(0)}$ e $Y = Y(s,t) \subseteq V_t^{(0)}$ como definido acima e sejam $X^* \subseteq X$ e $Y^* \subseteq Y$ tais que cada um é uma união de classes de $\mathcal{P}_1$ e maximal com esssa propriedade.

Podemos supor, sem perda de generalidade, que

$$X^* = \bigcup_{i=1}^{q_s} V_s(i) \quad \text{e} \quad Y^* = \bigcup_{j=1}^{q_t} V_t(j).$$

Da maximalidade que assumimos temos que $|X^*| \geqslant |X| - 2^{m-1}(c-1) \geqslant |X|(1 - 2^{m-1}c/|X|) \geqslant |X|(1 - 2^{m-1}/q\varepsilon) = |X|(1 - 1/\varepsilon 2^{m+1})$. Da mesma forma, $|Y^*| \geqslant |Y|(1 - 1/\varepsilon 2^{m+1})$. Também, note que $1/\varepsilon 2^{m+1} \leqslant 10^{-2}$ e que $|X|/\varepsilon 2^{m+1}$, $|Y|/\varepsilon 2^{m+1} \geqslant \eta n$.

Pelo Lema 56, temos

$$|d_{H,G}(X^*, Y^*) - d_{H,G}(X, Y)| \leqslant \frac{5}{\varepsilon 2^{m+1}},$$

e sabemos, de (29), que

$$|d_{H,G}(C_s, C_t) - d_{H,G}(V_s^{(0)}, V_t^{(0)})| \leqslant 5q^{-1}.$$

Desde que $|d_{H,G}(X,Y) - d_{H,G}(V_s^{(0)}, V_t^{(0)})| \geqslant \varepsilon$ e $5q^{-1} + 5/\varepsilon 2^{m+1} \leqslant \varepsilon/2$, temos

$$|d_{H,G}(X^*, Y^*) - d_{H,G}(C_s, C_t)| \geqslant \varepsilon/2. \tag{31}$$

Ponha $d_{ij} = d_{H,G}(V_s(i), V_t(j))$, para todo $i \in [q]$. Na prova do lema anterior verificamos que

$$\sum_{i=1}^{q} \sum_{j=1}^{q} d_{ij} = \frac{1-\eta}{1+\eta} q^2 d_{H,G}(C_s, C_t) \geqslant (1-2\eta) q^2 d_{H,G}(C_s, C_t).$$

Da mesma forma,

$$\sum_{i=1}^{q}\sum_{j=1}^{q} d_{ij} \leqslant (1+3\eta)q^2 d_{H,G}(C_s, C_t);$$

$$\sum_{i=1}^{q_s}\sum_{j=1}^{q_t} d_{ij} \geqslant (1-2\eta)q_s q_t d_{H,G}(X^*, Y^*) \text{ e}$$

$$\sum_{i=1}^{q_s}\sum_{j=1}^{q_t} d_{ij} \leqslant (1+3\eta)q_s q_t d_{H,G}(X^*, Y^*).$$

Note que $q_s m = |X^*| \geqslant |X| - 2^{m-1}c \geqslant \varepsilon|V_s^{(0)}| - 2^{m-1}c \geqslant eqc - 2^{m-1}c$, então $q_s \geqslant eq - 2^{m-1} \geqslant eq/2$. Da mesma forma, $q_t \geqslant eq/2$.

Ponha $\rho = q_s q_t q^{-2} \geqslant \varepsilon^4/2$ e $d_{s,t}^C = d_{H,G}(C_s, C_t)$. Por (31), temos

$$\begin{aligned}\sum_{i=1}^{q_s}\sum_{j=1}^{q_t} d_{ij} &\geqslant \frac{1-2\eta}{1+3\eta}\frac{q_s q_t}{q^2}\left(1+\frac{\varepsilon}{2{d_{s,t}^C}^2}\right)\sum_{i=1}^{q}\sum_{j=1}^{q} d_{ij} \\ &\geqslant \rho\left(1+\frac{\varepsilon}{3{d_{s,t}^C}^2}\right)\sum_{j=1}^{q} d_{ij},\end{aligned}$$

ou senão, temos

$$\begin{aligned}\sum_{i=1}^{q_s}\sum_{j=1}^{q_t} d_{ij} &\leqslant \frac{1-2\eta}{1+3\eta}\frac{q_s q_t}{q^2}\left(1-\frac{\varepsilon}{2{d_{s,t}^C}^2}\right)\sum_{i=1}^{q}\sum_{j=1}^{q} d_{ij} \\ &\leqslant \rho\left(1-\frac{\varepsilon}{3{d_{s,t}^C}^2}\right)\sum_{j=1}^{q} d_{ij}.\end{aligned}$$

Neste ponto, usamos a forma defectiva da desigualdade de Cauchy-Schwarz para concluir que

$$\sum_{i=1}^{q}\sum_{j=1}^{q} d_{ij}^2 \geqslant q^2\left({d_{s,t}^C}^2 + \frac{\varepsilon^2\rho}{10} - 4\eta\right),$$

portanto,

$$\begin{aligned}&\frac{1}{q^2}\sum_{i=1}^{q}\sum_{j=1}^{q} d_{H,G}(V_s(i), V_t(j))^2 \\ &\qquad \geqslant d_{H,G}(C_s, C_t)^2 + \frac{\varepsilon^2\rho}{10} - 4\eta \\ &\qquad \geqslant d_{H,G}(V_s^{(0)}, V_t^{(0)})^2 + \frac{\varepsilon^4}{40} - (9\eta^{-1} + 4\eta) \\ &\qquad \geqslant d_{H,G}(V_s^{(0)}, V_t^{(0)}) + \frac{\varepsilon^4}{40} - \frac{\varepsilon^5}{100},\end{aligned}$$

e está provado o lema. □

O seguinte resultado, que segue dos Lemas 58 e 59, é o correspondente do Lema 18 para o caso esparso.

LEMA 60. *Suponha $m \geq 1$ e $0 < \varepsilon \leq 1/2$ são tais que $4^m \geq 1800\varepsilon^{-5}$. Seja $G = G_n$ um grafo $(\mathcal{Q}, \eta)$-uniforme de ordem $n \geq n_0 = n_0(m) = m4^{2m+1}$, onde $\mathcal{Q}$ é uma partição de $V(G)$ em l classes, e assuma que $\eta \leq \eta_0 = \eta_0(m) = 1/m4^{m+1}$. Seja $H \subset G$ um subgrafo gerador de G. If $\mathcal{P} = \{V_0, \ldots, V_m\}$ é uma partição equipotente (ε, H, G)-irregular de $V(G)$ que refina $\mathcal{Q}$, então existe uma partição $\mathcal{P}_1 = \{V_0', \ldots, V_{m_1}'\}$ equipotente de $V(G)$ tal que*

(i) *$\mathcal{P}_1$ refina $\mathcal{P}$,*
(ii) *$m_1 = m4^m$,*
(iii) *$|V_0'| \leq |V_0| + n4^{-m}$, e*
(iv) *$\operatorname{ind}(\mathcal{P}_1) \geq \operatorname{ind}(\mathcal{P}) + \varepsilon^5/100$.*

DEMONSTRAÇÃO. Sejam $\mathcal{P}$ como descrito no lema e $\mathcal{P}_1 = \{V_0', \ldots, V_{m_1}'\}$ o refinamento construído a partir de $\mathcal{P}$ como descrito nesta seção ($V_i' = V_i^{(1)}$). Vamos mostrar que $\mathcal{P}_1$ satisfaz (i)–(iv).

Pelo Lema 57, só precisamos verificar (iv). Pelos Lemas 58 e 59, temos

$$\begin{aligned}
\operatorname{ind}(\mathcal{P}_1) &= \frac{2}{m^2q^2}\sum_{i=1}^{q}\sum_{i=1}^{q} d_{H,G}(V_i', V_j')^2 \\
&\geqslant \frac{2}{m^2}\sum_{1\leqslant s<t\leqslant m}\frac{1}{q^2}\sum_{i,j} d_{H,G}(V_s(i), V_t(j))^2 \\
&\geqslant \frac{2}{m^2}\left(\sum_{1\leqslant s<t\leqslant m}\left(d_{H,G}(V_s, V_t)^2 - \frac{\varepsilon^5}{100}\right) + \varepsilon\binom{m}{2}\frac{\varepsilon^4}{40}\right) \\
&\geqslant \operatorname{ind}(\mathcal{P}) - \frac{\varepsilon^5}{100} + \frac{\varepsilon^5}{50} \\
&\geqslant \operatorname{ind}(\mathcal{P}) + \frac{\varepsilon^5}{100},
\end{aligned}$$

e está provado o "coração" do Lema de Regularidade. □

DEMONSTRAÇÃO DO TEOREMA 50. Seja $G = G_n$ um grafo $(\mathcal{Q}, \eta)$-uniforme, $\mathcal{Q} = \{U_1, \ldots, U_l\}$, e $H \subseteq G$ um subgrafo gerador. Assuma $n \geqslant M$, e $\varepsilon \leqslant 1/2$. Sejam $m_0 \geqslant 1$ e $l \geqslant 1$ inteiros dados.

Tome $s \geqslant 1$ tal que $4^{s/4l} \geqslant 1800\varepsilon^{-5}$, $s \geqslant \max\{2m_0, 3l/\varepsilon\}$ e $\varepsilon 4^{s-1} \geqslant 1$. Defina $f(0) = s$ e, indutivamente, $f(t) = f(t-1)4^{f(t-1)}$.

Agora, tome $t_0 = \lfloor 100\varepsilon^{-5} \rfloor$ e $N = \max\{n_0 f(t) \colon 0 \leqslant t \leqslant t_0\} = f(t_0)^{2f(t_0)+1}$, $M_0 = \max\{6l/\varepsilon, N\}$ e $\eta = \eta(\varepsilon, k_0, l) = \min\{\eta_0 f(t) \colon 0 \leqslant t \leqslant t_0\} = (1/4)f(t_0 + 1) > 0$.

Também, seja T o conjunto dos inteiros $t \geqslant 0$ tais que existe uma $(k+1)$-partição $\mathcal{P}_t = \{V_0, V_1, \ldots, V_k\}$ de $V(G)$ tal que

(i) $\mathcal{P}_t$ refina $\mathcal{Q}$,
(ii) $s/4l \leqslant k \leqslant f(t)$,
(iii) $\mathrm{ind}(\mathcal{P}_t) \geqslant t\varepsilon^5/100$, e
(iv) $|V_0| \leqslant \varepsilon n(1 - 2^{-t+1})$.

Tal partição existe para $t = 0$: tome $c = \lceil n/s \rceil$ e $\mathcal{R}$ a partição de $V(G)$ em blocos de cardinalidade c, exceto possivelmente um que terá cardinalidade no máximo $c-1$ e tal que cada U_i contém $\lfloor |U_i|/c \rfloor$ blocos de $\mathcal{R}$. Agrupando os no máximo l blocos de $\mathcal{R}$ de cardinalidade no máximo $c-1$ em V_0 temos (iv) $|V_0| \leqslant l(c-1) < lc < l\lceil n\varepsilon/(3l) \rceil \leqslant n\varepsilon/2$, pois $n \geqslant M \geqslant 6l/\varepsilon$. Claramente, (i) e (iii) valem. Vamos verificar (ii).

Temos $m \leqslant n/c \leqslant s = f(0)$ e sabemos que existe $i \in [l]$ tal que $|U_i| \geqslant n/l$, portanto,

$$m \geqslant \left\lfloor \frac{|V_i|}{c} \right\rfloor \geqslant \left\lfloor \frac{n/l}{\lceil n/s \rceil} \right\rfloor \geqslant \frac{1}{2}\frac{n/l}{n/s} = \frac{s}{4l}.$$

Se uma partição $\mathcal{P}_t$ existe, então $t \leqslant t_0 = \lfloor 100\varepsilon^{-5} \rfloor$, pois $\mathrm{ind}(\mathcal{P}_t) \geqslant 1$. Considere t o maior inteiro para o qual $\mathcal{P}_t$ existe. Afirmamos que $\mathcal{P}_t$ é (ε, H, G)-regular: caso contrário, o lema anterior implica a existência de $\mathcal{P}_{t+1}$, contra a maximalidade de t. □

6.4. Uma variante. Na demonstração da versão para grafos esparsos do Lema de Szemerédi o fato do grafo ser (η, D, p)-esparso, sendo, portanto, a p-densidade de um par limitada, isto é, $d_p(U, W) \leqslant D$, foi usado para garantir que o índice de uma partição é limitado superiormente, ou seja, $\mathrm{ind}(\Pi) < D^2$. Então poderíamos chamar de esparso um grafo no qual toda partição fosse limitada.

Essa alternativa foi tomada por Łuczak (2000) que provou a seguinte variante do Lema de Szemerédi para grafos esparsos. Seja G um grafo, $f\colon [0,\infty) \to [0,\infty)$ uma função e $\Pi = (V_1, \ldots, V_k)$ uma eqüipartição de $V(G)$. Defina o índice da partição Π por

$$\mathrm{ind}_f(\Pi) = \sum_{1 \leqslant i < j \leqslant k} \frac{|V_i||V_j|}{|V|^2} f\left(d_p(V_i, V_j)\right),$$

e chame o grafo G de (f, L, b)-esparso, para reais L e $b > 1$, se para toda k-eqüipartição Π de V com $2 \leqslant k \leqslant L$, temos $\mathrm{ind}_f(\Pi) \leqslant b$. Aqui, a p-densidade de um par de subconjuntos disjuntos é tomada para o fator de escala $p = e(G)/|V(G)|^2$.

Lema 61. *Dados uma função positiva e estritamente convexa f e reais $\varepsilon > 0$ e $b > 1$, existe um L tal que todo grafo G de ordem pelo menos L*

e (f, L, b)*-esparso admite uma partição balanceada* (ε, k)*-regular para algum* $1/\varepsilon \leqslant k \leqslant L$. □

7. Conjuntos pseudoaleatórios

Começamos este capítulo fazendo algumas considerações gerais sobre caracteres e transformada de Fourier em grupos abelianos finitos. Seja G um grupo abeliano de ordem N e $A \subset G$ um subconjunto. Denotamos por A, também, a função característica do conjunto A, isto é, $A(x) = 1$ se $x \in A$ e, caso contrário $A(x) = 0$. Com essa notação $\widehat{A}(\chi)$ é a transformada de Fourier da função A no caracter χ.

Lembramos que que $\widehat{G}$ é o grupo dual dos caracteres de G e que é uma base ortonormal das funções de G em $\mathbb{C}$. Também, se $f\colon G \to \mathbb{C}$, então a norma definida pelo produto interno definido em (7), pág. 8,

$$\|f\|_G = \sqrt{\langle f, f\rangle_G} = \left(\frac{1}{N}\sum_{a\in G} \overline{f(a)} f(a)\right)^{1/2}.$$

Note que, para $A, B \subset G$, temos

$$|A \cap B| = N\langle A, B\rangle_G = \langle \widehat{A}, \widehat{B}\rangle_{\widehat{G}} \tag{32}$$

e em particular $|A| = N\|A\|_G^2 = \|\widehat{A}\|_{\widehat{G}}^2$ e $\|\widehat{f}\|_{\widehat{G}} = \sqrt{N}\|f\|_G$ como conseqüências de fórmula de Plancherel. Observamos também que $\widehat{A}(\chi_0) = |A|$. Daqui por diante, sempre que for possível omitiremos os subscritos em $\langle\cdot,\cdot\rangle$ e $\|\cdot\|$.

Por outro lado,

$$N\|\widehat{A}\|^2 = \sum_{\chi\in\widehat{G}} \overline{\widehat{A}(\chi)}\widehat{A}(\chi) = \sum_{\chi\in\widehat{G}} |\widehat{A}(\chi)|^2 \leqslant |A|^2 + (N-1)\left(\max_{\chi_0\neq\chi\in\hat{G}} |\widehat{A}(\chi)|\right)^2,$$

ou seja,

$$\max_{\chi\neq\chi_0} |\widehat{A}(\chi)| \geqslant \left(\frac{(N-|A|)|A|}{N-1}\right)^{1/2}.$$

Definindo

$$\Phi(A) = \max\{|\widehat{A}(\chi)|\colon \chi \neq \chi_0,\ \chi \in \widehat{G}\} \tag{33}$$

e $t = \min\{N-|A|, |A|\}$, temos para todo $A \subseteq G$ que $\sqrt{t/2} \leqslant \Phi(A) \leqslant |A|$.

Exercício 62. Mostre que $\Phi(A) = \Phi(G \setminus A)$ para todo $A \subseteq G$.

Logo, para todo $A \subseteq G$

$$\sqrt{\frac{|A|}{2}} \leqslant \Phi(A) \leqslant |A|. \tag{34}$$

Exemplo 63. Vamos supor que $|A| = m < \log_k N$ e consideremos a partição do $\mathbb{Z}_N$

$$\mathbb{Z}_N = \bigcup_{j=0}^{k-1} \left[j\frac{N}{k}, (j+1)\frac{N}{k}\right). \tag{35}$$

Para cada $t \in \mathbb{Z}_N$ associamos a m-tupla $(P_a(t))_{a\in A}$, onde P_a é a parte que contém $at \pmod N$.

Como $k^m < N$ temos que existem t_1 e t_2 em $\mathbb{Z}_N$ tais que $P_a(t_1) = P_a(t_2)$ para todo $a \in A$. Dessa forma $a(t_1 - t_2) \pmod N \in (-N/k, N/k)$ para todo $a \in A$ e

$$\Phi(A) \geqslant \sum_{a\in A} \exp\left(\frac{2\pi i a(t_1 - t_2)}{N}\right) \geqslant |A| \cos\left(\frac{2\pi}{k}\right).$$

Em particular, se $\Phi(A) \leqslant |A|/2$ então $|A| \geqslant \log_6 N$. □

O nosso objetivo agora é estudar a relação entre $\Phi(A)$ e a uniformidade da distribuição de A. Vamos investigar a relação entre $\Phi(A)$ e a discrepância da distribuição de A no $\mathbb{Z}_N$.

Tome $\omega = \exp(2\pi i/N)$ a N-ésima raiz primitiva da unidade. É fácil provar que a função $\omega_j \colon \mathbb{Z}_N \to \mathbb{C}^*$ dada por

$$\omega_j(a) = \omega^{ja} \qquad (\forall a \in \mathbb{Z}_N)$$

é um caracter de $\mathbb{Z}_N$ para todo $j \in \mathbb{Z}$. Daqui em diante, para simplificar, escreveremos sempre $\widehat{A}(t)$ para $\widehat{A}(\omega_t)$, a transformada de Fourier no caracter $\omega_t \in \widehat{\mathbb{Z}_N}$. Essa notação é justificada pelo seguinte exercício.

Exercício 64. Mostre que

(1) $\omega_i = \omega_j$ se, e somente se, $i = j \pmod N$;
(2) $\widehat{\mathbb{Z}_N} = \{\omega_0, \omega_1, \ldots \omega_{N-1}\} \cong \mathbb{Z}_N$.

Vejamos mais alguns exemplos onde calculamos $\hat{A}$ para $A \subset \mathbb{Z}_N$.

Exemplo 65. Para um intervalo $I = [a + 1, a + m] \subset \mathbb{Z}_N$ temos que

$$|\widehat{I}(r)| = \left|\sum_{s=1}^{m} \omega^{(a+s)r}\right| = \left|\frac{1 - \omega^{mr}}{1 - \omega^r}\right| \leqslant \frac{2}{|1 - \omega^r|} \leqslant \frac{N}{2r},$$

pois $|1 - \exp(i\theta)| \geqslant 2\theta/\pi$, para todo $\theta \in [0, \pi]$. Tomamos $\theta = 2\pi r/N$. □

Exemplo 66. Sejam $a_1, a_2, \ldots, a_m$ elementos do conjunto A em ordem crescente e tal que $|a_j/N - j/m| \leqslant \varepsilon$, para algum $\varepsilon \in (0, 1)$. Usando a desigualdade $|\exp(ix) - \exp(iy)| \leqslant |x - y|$ temos $|\exp(2\pi i a_j/n) - \exp(2\pi ij/m)| \leqslant 2\pi\varepsilon$. Somando para todo j

$$|\widehat{A}(1)| = \left|\sum_{j=1}^{m} \mathrm{e}^{\frac{2\pi i a_j}{N}}\right| = \left|\sum_{j=1}^{m} \mathrm{e}^{\frac{2\pi i a_j}{N}} - \sum_{j=1}^{m} \mathrm{e}^{\frac{2\pi ij}{m}}\right| \leqslant 2\pi\varepsilon|A|.$$

Do mesmo modo podemos obter que $|\widehat{A}(t)| \leqslant 2\pi\varepsilon t|A|$, que não é muito informativo para t grande. Agora, supondo por um instante que N é primo,

temos para todo $t \neq 0$

$$|\widehat{A}(t)| = \left|\sum_{a=0}^{N-1} A(a)\omega_t(a)\right| = \left|\sum_{b=0}^{N-1} A(t^{-1}b)\omega(b)\right| = \left|\sum_{b=0}^{N-1} tA(b)\omega(b)\right| = |\widehat{tA}(1)|,$$

e repetindo os cálculos do começo desse exemplo temos $|\widehat{tA}(1)| \leqslant 2\pi\varepsilon|A|$. □

Exercício 67. Mostre que $\Phi(kA) = \Phi(A)$ para todo k com $\mathrm{mdc}(k, N) = 1$.

Para "medir" a distribuição de A definimos a *discrepância* de A em I por

$$D_A(I) = \left|\frac{|A \cap I|}{|A|} - \frac{|I|}{N}\right|. \tag{36}$$

Note que estamos falando de $|\mathbb{P}\{x \in I | x \in A\} - \mathbb{P}\{x \in I\}|$ com relação à distribuição uniforme de probabilidades. Tomando $\mathcal{I} \subseteq 2^{\mathbb{Z}_N}$ definimos

$$D_A(\mathcal{I}) = \max\{D_A(I) \colon I \in \mathcal{I}\}.$$

Além dessas definições, ainda temos

$$xA = \{xa \colon a \in A\} \pmod N$$

e $\mathcal{I}_N$ denota a família dos intervalos do $\mathbb{Z}_N$.

Finalmente, definimos que A é *ε-uniforme* (mod N) se para todo $x \in \mathbb{Z}_N$ com $\mathrm{mdc}(x, N) = 1$ vale que

$$D_{xA}(\mathcal{I}_N) \leqslant \varepsilon.$$

Proposição 68. *Se $A \subseteq \mathbb{Z}_N$ é ε-uniforme* (mod n) *para todo n tal que $n|N$ então $\Phi(A) \leqslant \varepsilon 2\pi|A|$.*

Demonstração. Se $\mathrm{mdc}(t, N) = 1$ então t tem um inverso multiplicativo em $\mathbb{Z}_N$ e $|\widehat{A}(t)| = |\widehat{tA}(1)| \leqslant 2\pi\varepsilon|A|$, como no exemplo 66.

Vamos supor que $\mathrm{mdc}(t, N) = d > 1$. Dessa forma, existem m e n tais que $t = md$ e $N = nd$, logo

$$|\widehat{A}(t)| = \left|\sum_{a\in A} \mathrm{e}^{\frac{2\pi i t a}{N}}\right| = \left|\sum_{a\in A} \mathrm{e}^{\frac{2\pi i m a}{n}}\right| = \left|\sum_{a'\in A'} \mathrm{e}^{\frac{2\pi i a'}{n}}\right| \leqslant 2\pi\varepsilon|A|,$$

onde $A' = mA \pmod n$ e a desigualdade é como no exemplo 66. □

Por outro lado, se $\Phi(A) \leqslant \varepsilon N$ então $\sum_r |\widehat{A}(r)|^4 \leqslant \varepsilon^2 N^4$, e $|A| \geqslant \delta N$ implicam $D_A(I) \leqslant \varepsilon^{1/2}\delta^{-1}$. De fato,

$$(\varepsilon N)^2 N^2 \geqslant \Phi(A)^2 N^2 \geqslant \Phi(A)^2 \sum_r |\widehat{A}(r)|^2 \geqslant \sum_r |\widehat{A}(r)|^4, \tag{37}$$

donde tiramos o seguinte

$$\left||A \cap I| - \frac{|A||I|}{N}\right| = \frac{1}{N}\left|\sum_{r\neq 0} \overline{\widehat{A}(r)}\widehat{I}(r)\right| \leqslant \frac{1}{N}\left(\sum_{r\neq 0}\left|\overline{\widehat{A}(r)}\right|^4\right)^{1/4}\left(\sum_{r\neq 0}|\widehat{I}(r)|^{4/3}\right)^{3/4},$$

a igualdade vem de (32) e a desigualdade é a conhecida desigualdade de Hölder. Pela estimativa do exemplo 65

$$|A|D_A(I) = \left||A \cap I| - \frac{|A||I|}{N}\right| \leqslant \frac{1}{N}\left(\varepsilon^2 N^4\right)^{1/4}\left(N^{4/3}\right)^{3/4} \tag{38}$$

ou seja, $D_A(I) \leqslant \varepsilon^{1/2}\delta^{-1}$.

Na próxima seção mostramos que conjuntos típicos têm $\Phi(A)/|A|$ pequeno.

7.1. Coeficientes de conjuntos aleatórios. Vamos mostrar que um subconjunto A escolhido aleatoriamente de maneira uniforme em 2^G tem $\Phi(A)$ pequeno.

Teorema 69. *Escolha $\epsilon > 0$. Com probabilidade $1 - O(N^{-\epsilon})$ o subconjunto $A \subseteq G$ satisfaz*

$$\Phi(A) < 3\sqrt{(1+\epsilon)t \ln N},$$

onde $t = \min\{|A|, N - |A|\}$.

Demonstração. Podemos assumir $|A| = t \leqslant N/2$. Se $\pi \in S_N$ é uma permutação escolhida aleatória, independente e uniformemente então consideramos o conjunto $A = \{g_{\pi(1)}, g_{\pi(2)}, \ldots, g_{\pi(t)}\}$

Dessa maneira $X_0 = \widehat{A}(\chi)$ é uma variável aleatória com valor esperado $\mathbb{E}\, X_0 = 0$ para χ não-principal.

Para todo $1 \leqslant i \leqslant t$ definimos

$$X_i = \mathbb{E}\left(\widehat{A}(\chi)|g_{\pi(1)}, \ldots, g_{\pi(i-1)}\right),$$

e como $|\chi(g) - \chi(h)| \leqslant 2$, para quaisquer $g, h \in G$ temos que $|X_i - X_{i-1}| \leqslant 2$ e da equação (6), pág. 6

$$\mathbb{P}\left(\|X_t\| \geqslant a\right) < 2\exp\left(-\frac{(a-4)^2}{8t}\right) \leqslant 2\exp\left(-\frac{a^2}{9t}\right). \tag{39}$$

Tomando $a = 3\sqrt{(1+\varepsilon)t \ln N}$ temos

$$\begin{aligned}\mathbb{P}\left(\Phi(A) \geqslant 3\sqrt{(1+\varepsilon)t \ln N}\right) \leqslant & N\mathbb{P}\left(\|X_t\| \geqslant 3\sqrt{(1+\varepsilon)t \ln}\right) \\ < & 2N\exp\left(-(1+\varepsilon)\ln N\right) \\ = & 2NN^{-(1+\varepsilon)} = O(N^{-\varepsilon}).\end{aligned} \tag{40}$$

□

O seguinte exercício mostra que o resultado também vale no modelo binomial de subconjunto aleatório.

EXERCÍCIO 70. Seja $A \subseteq G$ um subconjunto aleatório obtido escolhendo-se cada elemento de $G = \{g_0, \ldots, g_{N-1}\}$ com probabilidade 1/2. Tome ι_i, $1 \leqslant i \leqslant N$, a variável aleatória com valores em $\{-1, 1\}$ onde 1 significa que g_i foi escolhido. Defina

$$\xi(\chi) = \sum_{i=0}^{N-1} \frac{\iota_i + 1}{2} \chi(g_i) = \frac{1}{2} \sum_{i=0}^{N-1} \iota_i \chi(g_i).$$

Use a Desigualdade de Chernoff (5), pág. 6, na parte real e na parte imaginaria de ξ para mostrar que $\Phi(A) < \sqrt{(1+\varepsilon)N \log N}$ com probabilidade $1 - O(N^{-\varepsilon})$, para todo $\varepsilon > 0$.

7.2. Pseudoaleatoriedade no $\mathbb{Z}_N$. Em Chung and Graham (1992) foi provado que para todo $A \subseteq \mathbb{Z}_N$ as seguintes propriedades, que são satisfeitas quase certamente para subconjuntos aleatórios do $\mathbb{Z}_N$, são equivalentes.

Soma exponencial: Para todo $j \neq 0$, $j \in \mathbb{Z}_N$, vale que

$$\left|\widehat{A}(j)\right| = \left| \sum_{t \in \mathbb{Z}_N} A(t) \omega_j(t) \right| = o(N). \tag{41}$$

Translação fraca: Para quase todo $x \in \mathbb{Z}_N$

$$\left|A \cap (A + x)\right| = \frac{|A|^2}{N} + o(N). \tag{42}$$

Translação forte: Para todo $B \subseteq \mathbb{Z}_N$ e quase todo $x \in \mathbb{Z}_N$

$$\left|A \cap (B + x)\right| = \frac{|A||B|}{N} + o(N). \tag{43}$$

2-padrão: Para quase todos $x, y \in \mathbb{Z}_N$

$$\left|(A - x) \cap (A - y)\right| = \sum_{t \in \mathbb{Z}_N} A(t + x) A(t + y) = \frac{|A|^2}{N} + o(N). \tag{44}$$

k-padrão: Para quase todos $x_1, x_2, \ldots, x_k \in \mathbb{Z}_N$

$$\left| \bigcap_{i=1}^{k} (A - x_i) \right| = \sum_{t \in \mathbb{Z}_N} \prod_{i=1}^{k} A(t + x_i) = \frac{|A|^k}{N^{k-1}} + o(N). \tag{45}$$

2-representação: Para quase todo $x \in \mathbb{Z}_N$

$$\sum_{t_1 + t_2 = x} A(t_1) A(t_2) = \frac{|A|^2}{N} + o(N). \tag{46}$$

k-representação: Para quase todo $x \in \mathbb{Z}_N$

$$\sum_{t_1 + t_2 + \cdots + t_k = x} \prod_{i=1}^{k} A(t_i) = \frac{|A|^k}{N^{k-1}} + o(N). \tag{47}$$

$2t$-ciclo:

$$\sum_{x_1,x_2,\ldots,x_{2t}} A(x_1+x_2)A(x_2+x_3)\cdots A(x_{2t-1}+x_{2t})A(x_{2t}+x_1) = |A|^{2t} + o(N^{2t}). \tag{48}$$

Densidade relativa: Para todo $B \subseteq \mathbb{Z}_N$

$$\sum_{t\in\mathbb{Z}_N} B(t)\big|B\cap(A-t)\big| = \sum_{t,u\in\mathbb{Z}_N} B(t)B(u)A(t+u) = \frac{|A||B|^2}{N} + o(N^2). \tag{49}$$

Essas propriedades são satisfeitas para subconjuntos aleatórios do $\mathbb{Z}_N$ de cardinalidade δN com probabilidade $1-o(1)$. Um subconjunto que satisfaz alguma dessas propriedades é chamado de *pseudoaleatório*.

Exemplo 71 (k-representação $\Rightarrow$ soma exponencial $\Rightarrow$ translação forte). Definimos a matriz $M = (m_{i,j})$ por $m_{i,j} = A(j-i)$ para todo $i,j \in \mathbb{Z}_N$. Claramente temos $m_{i+1,j+1} = m_{i,j}$, onde a soma dos índices é mod N. Uma matriz com essa propriedade é chamada de *circulante* e cumpre o seguinte resultado.

Exercício 72. Uma matriz circulante tem autovalores e autovetores

$$\lambda_j = \sum_i m_{0,i}\omega_j(i) = \sum_i A(i)\omega_j(i) \tag{50}$$

$$v_j = \big(\omega_j(0),\omega_j(1),\ldots,\omega_j(N-1)\big), \tag{51}$$

para $j \in \mathbb{Z}_N$, respectivamente. Além disso, $MM^{\mathtt{T}} = M^{\mathtt{T}}M$.

Agora, continuando no nosso exemplo, M^k na posição (i,j) é

$$\begin{aligned} m_{i,j}^k &= \sum_{v_1,v_2,\ldots,v_{k-1}\in\mathbb{Z}_N} m_{i,v_1}m_{v_1,v_2}\cdots m_{v_{k-2},v_{k-1}}m_{v_{k-1},j} \\ &= \big|\big\{v_1,v_2,\ldots,v_{k-1}\colon A(v_1-i) = A(v_2-v_1) = \cdots = A(j-v_{k-1})\big\}\big| \\ &= \sum_{u_1+u_2+\cdots+u_k=j-i} A(u_1)A(u_2)\cdots A(u_k) \\ &= \frac{|A|^k}{N} + o(N^{k-1}) \quad \text{para quase todo } j-i\in\mathbb{Z}_N. \end{aligned} \tag{52}$$

A matriz $(MM^{\mathtt{T}})^k$ dada por $b_{i,j} = \sum_\ell m_{i,\ell}^k m_{\ell,j}^k$ satisfaz

$$b_{i,j} = \frac{|A|^{2k}}{N} + o(N^{2k-1}).$$

Assim, traço$\big((MM^{\mathtt{T}})^k\big) = \sum_j \lambda_j^{2k} = |A|^{2k} + o(N^{2k})$. Como $\lambda_0 = |A|$ temos

$$\sum_{j\neq 0} \lambda_j^{2k} = o(N^{2k}),$$

donde $\widehat{A}(j) = \lambda_j = o(N)$, para todo $j \neq 0$.

Vejamos a segunda implicação. Podemos supor que $|A|, |B| > \delta N$, para algum $\delta > 0$, pois de outro modo a implicação é trivialmente valida.

Seja B um subconjunto de $\mathbb{Z}_N$ e denotemos por $\mathbf{B}$ o vetor coluna característico de B.

Definimos o vetor

$$\mathbf{v}(B) = \frac{N}{|B|(N-|B|)}\mathbf{B} - \frac{1}{N-|B|}\mathbb{Z}_{\mathbf{N}}. \tag{53}$$

Portanto $\mathbf{v}(B)$ e $\mathbb{Z}_{\mathbf{N}}$ são ortogonais e

$$\mathbf{B} = \frac{|B|(N-|B|)}{N}\left(\frac{1}{N-|B|}\mathbb{Z}_{\mathbf{N}} + \mathbf{v}(B)\right). \tag{54}$$

A matriz $M = (m_{i,j})$ é como acima. Logo, por definição, a i-ésima linha de $M\mathbf{B}$ é $\sum_j A(j-1)B(j) = |(A+i) \cap B|$. Também,

$$M\mathbf{B} = \frac{|A||B|}{N}\mathbb{Z}_{\mathbf{N}} + \frac{|B|(N-|B|)}{N}M\mathbf{v}(B).$$

Suponha que existe $\varepsilon > 0$ tal que

$$\sum_x \big||A \cap (B+x)| - (|A||B|/N)\big| > 3\varepsilon|A||B|. \tag{55}$$

Definimos

$$W = \left\{y\colon \left||A \cap (B+y)| - \frac{|A||B|}{N}\right| > \varepsilon\frac{|A||B|}{N}\right\} \tag{56}$$

$$W' = \left\{y \in W\colon |A \cap (B+y)| > (1+\varepsilon)\frac{|A||B|}{N}\right\} \tag{57}$$

$$W'' = -W'. \tag{58}$$

Por (55), podemos assumir que $|W| > 2\varepsilon|A|$ e assim, sem perda de generalidade, que $|W'| > \varepsilon|A|$.

De modo análogo a (53) e (54) temos

$$\mathbf{v}(W'') = \frac{N}{|W''|(N-|W''|)}\mathbf{W}'' - \frac{1}{N-|W''|}\mathbb{Z}_{\mathbf{N}} \tag{59}$$

$$\mathbf{W}'' = \frac{|W''|(N-|W''|)}{N}\left(\frac{1}{N-|W''|}\mathbb{Z}_{\mathbf{N}} + \mathbf{v}(W'')\right). \tag{60}$$

Agora, usando $(\cdot,\cdot)$ para o produto interno usual no $\mathbb{R}^N$, temos

$$\begin{aligned}(\mathbf{W}'', M\mathbf{B}) &= \sum_{i,j} W''(i)m_{i,j}B(j) = \sum_{i\in W''} A(j-i)B(j)\\ &= \sum_{y\in W'} |A \cap (B+y)| \geqslant (1+\varepsilon)\frac{|A||B|}{N}|W'|.\end{aligned} \tag{61}$$

Por outro lado,

$$
\begin{aligned}
&(\mathbf{W}'', M\mathbf{B}) = \\
&\quad \left(\frac{|W'|}{N}\mathbb{Z}_{\mathbf{N}} + \frac{|W'|(N-|W'|)}{N}\mathbf{v}(W''), \frac{|A||B|}{N}\mathbb{Z}_{\mathbf{N}} + \frac{|B|(N-|B|)}{N}M\mathbf{v}(B) \right) \\
&\leqslant \frac{|W'||A||B|}{N} + \frac{|W'|(N-|W'|)|B|(N-|B|)}{N^2}\Phi(A)\|\mathbf{v}(W'')\|\|\mathbf{v}(B)\|.
\end{aligned} \tag{62}
$$

Calculando as normas temos

$$
\begin{aligned}
\|\mathbf{v}(B)\| &= \left(\frac{1}{|B|} + \frac{1}{N-|B|} \right)^{1/2} \\
\|\mathbf{v}(W'')\| &= \left(\frac{1}{|W'|} + \frac{1}{N-|W'|} \right)^{1/2},
\end{aligned} \tag{63}
$$

e a última linha da equação (62) fica

$$
\begin{aligned}
&(\mathbf{W}'', M\mathbf{B}) = \frac{|W'||A||B|}{N} + \\
&\frac{|W'|(N-|W'|)|B|(N-|B|)}{N^2}\Phi(A)\left(\frac{1}{|B|} + \frac{1}{N-|B|} \right)^{1/2}\left(\frac{1}{|W'|} + \frac{1}{N-|W'|} \right)^{1/2} \\
&\qquad = \frac{|W'||A||B|}{N} + \frac{(|W'|(N-|W'|)|B|(N-|B|))^{1/2}}{N^2}\Phi(A) \\
&\qquad \leqslant \frac{|W'||A||B|}{N} + \frac{N}{4}\Phi(A).
\end{aligned} \tag{64}
$$

Finalizando, de (61) e (64)

$$
\Phi(A) \geqslant \frac{4\varepsilon|W'||B||A|}{N^2} \geqslant 4\varepsilon^2\delta^3 N. \tag{65}
$$

Dessa forma, provamos uma versão quantitativa do que queríamos:

Afirmação 73. *Dados $\alpha, \beta, \varepsilon > 0$ existe ε' tal que $\varepsilon' \to 0$ com $\varepsilon \to 0$ de modo que o seguinte vale. Para todo $A \subset \mathbb{Z}_N$ de cardinalidade αN, se $\Phi(A) \leqslant \varepsilon N$ então $\sum_x D_{B+x}(A) \leqslant \varepsilon' N$, para todo $B \subset \mathbb{Z}_N$ de cardinalidade βN.*

Chamamos a atenção para o fato de "translação forte" $\Rightarrow$ "2-representação" segue imediatamente da definição e que "2-representação" $\Rightarrow$ "k-representação" pode ser provado sem muita dificuldade usando indução em $k \geqslant 2$ e a desigualdade de Cauchy-Schwarz. Com isso, temos a equivalência dessas quatro propriedades:

$$\begin{array}{ccc} \text{translação forte} & \Longrightarrow & \text{2-representação} \\ \Uparrow & & \Downarrow \\ \text{soma exponencial} & \Longleftarrow & k\text{-representação} \end{array}$$

Na seção 7.6 mostraremos indiretamente que "densidade relativa", "2-padrão" e "$2t$-ciclo" são equivalentes. O restante das equivalências são deixadas como exercício. □

Se $A \subseteq \mathbb{Z}_N$ é pseudoaleatório então também é pseudoaleatório o conjunto $A \cap I$, onde I é qualquer intervalo no $\mathbb{Z}_N$ de comprimento βN, para $\beta > 0$.

De fato, como em (38), $\Phi(A) \leqslant \varepsilon N$ implica em

$$\left| \frac{|A \cap I|}{|I|} - \frac{|A|}{N} \right| < \varepsilon^{1/2} \beta^{-1}.$$

Vamos usar que se $A \subset \mathbb{Z}_N$ é pseudoaleatório e $A' = A \cap [0, n)$ com $n = \beta N$ então

$$\left| |A \cap (B + x)| - \frac{|A||B|}{N} \right| = o(N) \quad \text{e} \quad \left| \frac{|A|}{N} - \frac{|A'|}{n} \right| = o(1), \tag{66}$$

e indicar uma prova de que A' satisfaz "translação fraca". Em Chung and Graham (1992) foi provado uma versão quantitativa usando o resultado acima, deixaremos os detalhes para o leitor.

Sejam $I_1, I_2, \ldots, I_\ell$ intervalos de mesmo comprimento $\Omega(N)$ que particionam o $\mathbb{Z}_N$. Escrevemos $A'_i = A \cap I_i$ para todo $i \in [\ell]$. Da definição de A'_i e da hipótese sobre as densidades temos que

$$\left|A' \cap (A' + x)\right| = \sum_{i=i}^{\ell} \left|A' \cap (A'_i + x)\right| \quad \text{e} \quad \frac{|A'||A|}{N} = \frac{|A'|^2}{n} + o(n). \tag{67}$$

Note que $A \cap (A'_i + x) \subseteq \mathbb{Z}_N$ é igual a $A' \cap (A'_i + x) \subseteq \mathbb{Z}_n$ exceto para um índice $j \in [\ell]$, supondo que o comprimento dos intervalos é suficientemente grande. Assim, para quase todo x e todo i, $i \neq j$

$$\left| |A' \cap (A'_i + x)| - \frac{|A||A'_i|}{N} \right| = \left| |A \cap (A'_i + x)| - \frac{|A||A'_i|}{N} \right| = o(N). \tag{68}$$

Queremos estimar $\left||A' \cap (A' + x)| - |A'|^2 n^{-1}\right|$ como $o(N)$ para quase todo x. As duas últimas equações acima nos dão

$$\begin{aligned} \sum_x \left| |A' \cap (A' + x)| - \frac{|A'|^2}{n} \right| \leqslant \sum_x \sum_{i \neq j} \left| |A' \cap (A'_i + x)| - \frac{|A'|^2}{n} \right| \leqslant \\ \sum_x \sum_{i \neq j} \left| |A \cap (A'_i + x)| - \frac{|A'||A|}{N} \right| = o(N^2). \end{aligned} \tag{69}$$

Do fato de A ser pseudoaleatório sabemos que $A + a$ é pseudoaleatório para todo $a \in \mathbb{Z}_N$, portanto, podemos concluir que $A \cap [a, a + n)$ é pseudoaleatório

em $\mathbb{Z}_N$. Também é pseudoaleatório o conjunto A' definido por $A'(i) = A(c+di)$ para $0 \leqslant i < n$ e $\mathrm{mdc}(d, N) = o(N)$.

7.3. 3-pa's em conjuntos pseudoaleatórios. Vamos considerar o problema (seguindo Ajtai et al. (1986)): Dados $A, B, C \subseteq G$ quantos soluções tem a equação

$$x + y + z = 0, \tag{70}$$

onde $(x, y, z) \in A \times B \times C$.

O número de soluções da equação (70) é (veja Exercício 5, pág. 9)

$$\begin{aligned} S &= \sum_{(x,y,z)\in A\times B\times C} \delta(x+y+z) \\ &= \frac{1}{N}\sum_{\chi\in\widehat{G}} \left(\sum_{(x,y,z)\in A\times B\times C} \chi(x+y+z) \right) \\ &= \frac{1}{N}\sum_{\chi\in\widehat{G}} \left(\sum_{(x,y,z)\in A\times B\times C} \chi(x)\chi(y)\chi(z) \right) \\ &= \frac{1}{N}\sum_{\chi\in\widehat{G}} \left(\sum_{x\in G} A(x)\chi(x) \right) \left(\sum_{y\in G} B(y)\chi(y) \right) \left(\sum_{z\in G} C(z)\chi(z) \right) \\ &= \frac{1}{N}\sum_{\chi\in\widehat{G}} \widehat{A}(\chi)\widehat{B}(\chi)\widehat{C}(\chi). \end{aligned} \tag{71}$$

Portanto, o número de soluções é

$$S = \frac{|A||B||C|}{N} + \frac{1}{N} \sum_{\chi\in\widehat{G},\, \chi\neq\chi_0} \widehat{A}(\chi)\widehat{B}(\chi)\widehat{C}(\chi). \tag{72}$$

O próximo passo é estimar o desvio $\left|S - N^{-1}|A||B||C|\right|$

$$\begin{aligned} \left| \frac{1}{N} \sum_{\chi\in\widehat{G},\, \chi\neq\chi_0} \widehat{A}(\chi)\widehat{B}(\chi)\widehat{C}(\chi) \right| &\leqslant \frac{1}{N} \sum_{\chi\in\widehat{G},\, \chi\neq\chi_0} |\widehat{A}(\chi)||\widehat{B}(\chi)||\widehat{C}(\chi)| \\ &\leqslant \frac{\Phi(C)}{N} \sum_{\chi\in\widehat{G},\, \chi\neq\chi_0} |\widehat{A}(\chi)||\widehat{B}(\chi)|, \end{aligned}$$

e usando a desigualdade de Cauchy-Schwarz temos

$$\sum_{\chi\in\widehat{G}} |\widehat{A}(\chi)||\widehat{B}(\chi)| \leqslant \left(\sum_{\chi\in\widehat{G}} |\widehat{A}(\chi)|^2 \right)^{1/2} \left(\sum_{\chi\in\widehat{G}} |\widehat{B}(\chi)|^2 \right)^{1/2}, \tag{73}$$

o lado direito da desigualdade acima é igual a $(N\|\widehat{A}\|^2 N\|\widehat{B}\|^2)^{1/2}$ que, pela observação que segue a equação (32), pág. 52, é igual a $N\sqrt{|A||B|}$.

Concluindo

$$\left|S - \frac{|A||B||C|}{N}\right| \leqslant \Phi(C)\sqrt{|A||B|}. \tag{74}$$

EXERCÍCIO 74. Mostre que $\Phi(A) = \Phi(A+b)$ para todos $b \in G$ e $A \subseteq G$. Conclua que a equação acima vale para o número de soluções de $x+y+z=a$, onde $(x,y,z) \in A \times B \times C$ e $a \in G$.

EXERCÍCIO 75. Mostre que o número de soluções de $x_1 + \cdots + x_k = 0$, com $x_i \in A_i \subseteq G$, é

$$\frac{|A_1||A_2|\cdots|A_k|}{N} + \frac{1}{N} \sum_{\chi_0 \neq \chi \in \widehat{G}} \prod_{i=1}^{k} \widehat{A_i}(\chi).$$

EXERCÍCIO 76. Denote por $Q(A)$ o número de quádruplas $(a,b,c,d) \in A^4$ tais que $a+b=c+d$. Mostre que $Q(A) = N^{-1}\sum_r |\hat{A}(r)|^4$. Mostre que para A de cardinalidade δN

(i) se $\Phi(A) \leqslant \varepsilon N$ então $Q(A) \leqslant (\delta^4 + \varepsilon^2\delta)N^3$;
(ii) se $Q(A) \leqslant (\delta^4 + \varepsilon)N^3$ então $\Phi(A) \leqslant \varepsilon^{1/4}N$;
(iii) se $Q(A) \leqslant \delta^4 N^3 + o(N^3)$ então para qualquer progressão aritmética P módulo N vale $|A \cap P| = \delta|P| + o(N)$.

Não é difícil provar que se $A \subseteq \{1,2,\ldots,N\}$ é um subconjunto aleatório com $|A| = \delta N$, então o número esperado de progressões aritméticas de três termos em A é $\delta^3 N^2$. Agora, o número de progressões aritméticas mod N em A é igual ao número de soluções da equação $x + z = 2y \pmod N$ e se A tem a propriedade da "soma exponencial" então

$$\left|\#\big(3\text{-PA } \pmod N \subset A\big) - \delta^3 N^2\right| = o(N^2). \tag{75}$$

EXERCÍCIO 77. Mostre que se $\Phi(A) \leqslant \varepsilon N$ então

$$\left|\#(3\text{-PA } \pmod N \subset A) - \delta^3 N^2\right| \leqslant \varepsilon\delta N^2.$$

Notemos que $(x,y,z) \in A$ pode ser uma 3-PA trivial com $x=y=z$ ou sobreposta, com $x=z$. Por exemplo, no último caso encaixa-se a 3-PA $(1,4,1)$ no $\mathbb{Z}_6$.

Um truque para termos uma estimativa para o número de progressões sem sobreposição é considerar $B = A \cap (N/3, 2N/3]$. Tomamos como S o número de triplas $(x,y,z) \in A \times B \times B$ tal que $x+z = 2y \pmod N$. No máximo N soluções são triviais, i.e., a razão é zero. Assim, número de progressões aritméticas em A satisfaz,

$$\left|\#\big(3\text{-PA} \subset A\big) - \frac{\delta^3}{9}N^2\right| = o(N^2), \tag{76}$$

pois "soma exponencial" implica discrepância de A no intervalo pequena e, portanto, $\big||B| - \delta N/3\big| = o(N)$. Em particular, A contém uma progressão não degenerada de três termos tão logo $N > 9\delta^{-3}$.

Exercício 78. Mostre que se $\Phi(A) \leqslant \varepsilon N$ então

$$\big|\#(3\text{-pa} \subset A) - \delta|B|^2\big| \leqslant \varepsilon N|B|.$$

Lema 79. *Se $A \subseteq \{1, \ldots, N-1\}$, $N > 26\delta^{-3}$, $|A| = \delta N$ e $\Phi(A) \leqslant (\delta^2/16)N$ então A contém uma* 3-pa.

Demonstração. Para $\Phi(A) \leqslant \varepsilon N$ sabemos que $\big||B| - \delta N/3\big| \leqslant \sqrt{\varepsilon}N/9$ (veja(38)). Se $\varepsilon \leqslant (1/16)\delta^2$ então $|B| \geqslant \delta N/4$ e portanto

$$\#(3\text{-pa} \subset A) \geqslant \delta|B|^2 - \varepsilon N|B| \geqslant \frac{\delta^3}{16}N^2 - \frac{13\delta^3}{16\cdot 36}N^2 \geqslant \frac{13\delta^3}{16\cdot 36}N^2 > N,$$

como há $\leqslant N$ pa's triviais, segue o resultado. □

7.4. A demonstração de Roth. Vamos supor que existe $r \in [N-1]$ tal que $\widehat{A}(r) \geqslant \varepsilon N$ e mostrar que A tem densidade alta numa progressão aritmética genuína de $\sim \sqrt{N}$ termos. Definimos

$$P = P(q) = \{hq\colon |h| \leqslant m\} \subset \mathbb{Z}_N, \tag{77}$$

tal que $q|P| < N$ e temos

$$\begin{aligned}\left|\sum_{u=0}^{N-1}\left(\frac{|A\cap(P+u)|}{|P|} - \frac{|A|}{N}\right)\omega_t(u)\right| &= \left|\sum_{u=0}^{N-1}\frac{|A\cap(P+u)|}{|P|}\omega_t(u)\right| \\ &= \frac{1}{|P|}\left|\sum_{u=0}^{N-1}|A\cap(P+u)|\,\omega_t(u)\right| \\ &= \frac{1}{|P|}|\widehat{A*P}(t)| = \frac{1}{|P|}|\widehat{A}(t)\widehat{P}(t)|,\end{aligned}$$

portanto,

$$|\widehat{d_{P+u}(A)}(r)| \geqslant \varepsilon N\frac{|\widehat{P}(r)|}{|P|}, \quad \text{onde} \quad d_{P+u}(A) = \frac{|A\cap(P+u)|}{|P|} - \frac{|A|}{N} \tag{78}$$

Vamos supor que

$$\textit{existe } P = P(q) \textit{ com } q|P| < N \textit{ tal que } |\widehat{P}(r)| \geqslant |P|/2. \tag{79}$$

Como cada $a \in A$ pertence a $P+u$ para exatos $|P|$ valores de $u \in \mathbb{Z}_N$ concluímos que $\sum_u |A\cap(P+u)| = |A||P|$

$$\sum_{u=0}^{N-1} d_{P+u}(A) = 0$$

e, portanto[2] de (78) e (79),

$$\sum_{u=0}^{N-1} |d_{P+u}(A)| + d_{P+u}(A) = \sum_{u=0}^{N-1} |d_{P+u}(A)| \geqslant |\widehat{d_{P+u}(A)}(r)| \geqslant \frac{\varepsilon}{2}N.$$

Assim, para algum u temos

$$|d_{P+u}(A)| + d_{P+u}(A) \geqslant \frac{\varepsilon}{2},$$

que, por sua vez, implica em $d_{P+u}(A) \geqslant \varepsilon/4$. Concluindo esta etapa, reescrevemos a implicação como

$$\big|A \cap (P+u)\big| \geqslant \left(\delta + \frac{\varepsilon}{4}\right)|P|. \tag{80}$$

Prova da equação (79). Considerando as coleções de pares

$$\big\{(i, ir)\colon i \in \{0, \ldots, N-1\}\big\} \text{ ou } \big\{((n-1)-i, ir)\colon i \in \{0, \ldots, N-1\}\big\}$$

numa partição de $\{0, 1, \ldots, N-1\}^2$ em $\left\lfloor\sqrt{N-1}\right\rfloor^2$, $< N$, quadrados, segue do princípio da casa dos pombos que existem ℓ e k, $0 \leqslant \ell < k \leqslant N-1$, tais que $k - \ell \leqslant \sqrt{N}$ e $r(k-\ell) \leqslant \sqrt{N} \pmod N$. Tomamos $q = k - \ell$ e definimos

$$P = \left\{hq\colon |h| < \left\lfloor (2\pi)^{-1}\sqrt{N}\right\rfloor\right\}.$$

Temos

$$\big|\widehat{P}(r) - |P|\big| \leqslant \left|\sum_{u=0}^{N-1} P(u)(\omega_r(u) - 1)\right| \leqslant \sum_{|h|\leqslant |P|/2} \big|\omega_r(hq) - 1\big| \leqslant \frac{|P|}{2}.$$

□

Proposição 80. *Se $|\widehat{A}(r)| \geqslant \varepsilon N$ para algum $r \neq 0$ então existe uma progressão aritmética em $\mathbb{Z}$ com pelo menos $(1/32)\varepsilon\sqrt{N}$ termos e tal que*

$$\big|A \cap (P+u)\big| \geqslant \left(\delta + \frac{\varepsilon}{8}\right)|P|.$$

Demonstração. Tomamos P como a progressão acima e a escrevemos como união de duas progressões aritméticas genuínas $P = P_1 \cup P_2$, onde $|P_1| \leqslant |P_2|$.

Se $|P_1| \leqslant (\varepsilon/8)|P_2|$ então $|A \cap P_2| \geqslant (\delta + \varepsilon/8)|P| \geqslant (\delta + \varepsilon/8)|P_2|$. Senão $|P_1|, |P_2| \geqslant (\varepsilon/8)|P|$ e, portanto, A deve ter densidade $\geqslant \delta + \varepsilon/8$ em uma delas. □

Lema 81. *Se $A \subseteq \{1, \ldots, N-1\}$, $N > 26\delta^{-3}$, $|A| = \delta N$. Ou A contém uma* 3-pa *genuína, ou existe uma* pa *$P \subseteq \mathbb{Z}$ com pelo menos $(\delta^2/512)\sqrt{N}$ termos e tal que*

$$\big|A \cap P\big| \geqslant \left(\delta + \frac{\delta^2}{128}\right)|P|.$$

[2] diretamente da definição de $\hat{f}$ vale que $\sum_x |f(x)| \geqslant |\hat{f}(k)|$, para todo $k \neq 0$.

Demonstração. Se A não contém uma 3-PA então, pelo Lema 79, temos existe $r \in [N-1]$ tal que $\widehat{A}(r) > (\delta^2/16)N$. Pela proposição anterior, existe uma PA P com pelo menos $(1/32)(\delta^2/16)\sqrt{N}$ termos e com

$$\left|A \cap (P+u)\right| \geqslant \left(\delta + \frac{\delta^2/16}{8}\right)|P|.$$

□

Demonstração do Teorema de Roth. Vamos mostrar um subconjunto $A \subseteq \{1, 2, \ldots, N-1\}$ com pelo menos δN elementos e $N > \exp\exp(C\delta^{-1})$ então A contém uma 3-PA, para alguma constante positiva C.

Se A não contém uma 3-PA então tomamos uma PA $P_1 \subset \mathbb{Z}$ dada pelo Lema 81. Identificamos P_1 com $\{1, 2, \ldots, N_1 - 1\}$ simplesmente enumerando os elementos de P_1, e $A_1 \simeq A \cap P_1$. Sabemos que A_1 não contém 3-PA não-trivial, $|A_1| = \delta_1 N_1$ com $N_1 \geqslant (\delta^2/512)\sqrt{N}$ e $\delta_1 \geqslant \delta + \delta^2/128$.

Iterando $k = 128/\delta$ vezes teremos $A_k \subset \{1, 2, \ldots, N_k\}$ com densidade $\delta_k \geqslant \delta + \delta$. Iterando mais $k/2$ vezes a densidade salta de 2δ para 4δ. Dessa forma, após $(128/\delta)(1 + 1/2 + \cdots + 1/2^{\ell-1})$ passo atingiremos densidade pelo menos $2^\ell\delta$. Conseqüentemente, teremos densidade maior que um em $256/\delta$ passos, uma contradição desde que N seja suficientemente grande de modo a não termos jogado fora todos os elementos.

Depois de k passos teremos uma progressão com pelo menos $(\delta^2/512)^2 N^{1/2^k}$ termos, então precisamos de $N^{1/2^k} \geqslant \delta^{-4}512^2$. Tomando logaritmos

$$\lg N \geqslant 2^k \lg(\delta^{-4}512^2) = 2^{256\delta^{-1}}(4\lg\delta^{-1} + 18), \tag{81}$$

como $4\lg\delta^{-1} + 18 \leqslant 2^{2\delta^{-1}}$ é suficiente escolhermos $N \geqslant 2^{2^{258\delta^{-1}}}$; ou, ainda, $N \geqslant \exp\exp(180\delta^{-1})$. □

Exercício 82 (Gowers, 2005). O seguinte exemplo mostra que uma simples generalização do argumento de Roth não funciona para progressões aritméticas com 4 termos.

Para o conjunto $A = \{x \colon |x^2| \leqslant 10000\} \subseteq \mathbb{Z}_N$ temos que $\Phi(A) = O(\sqrt{N}\log N)$ enquanto que o número de progressões aritméticas (em $\mathbb{Z}_N$) de 4 termos é maior que $10^{-16}N^2$.

(i) Prove que se $f(x) = \omega_a(x^2)$ então $|\widehat{f}(t)| = \sqrt{N}$ para todo t.

(ii) Tome $I = [-\lfloor N/10000\rfloor, \lfloor N/10000\rfloor]$. Mostre que $A(x) = I(x^2)$. Escreva $A(x)$ em termos dos coeficientes de Fourier de I.

(iii) Use (i) e uma estimativa para os coeficientes de I.

Agora, mostre que o número de 4-PA's em A é $\gg 10^{-16}N^2$.

Gowers (2001) redefiniu a noção de pseudoaleatoriedade para generalizar o argumento de Roth. No caso de 4-PA, A é chamado de ε-uniforme se $\Phi(A) \leqslant \varepsilon N$

e de ε^2-*quadraticamente-uniforme* se $A \cap A + k$ é ε-uniforme para pelo menos $(1-\varepsilon)N$ valores de k. O resultado de Gowers para conjuntos pseudoaleatórios é: *Se A de cardinalidade δN é $(\leqslant 2^{-208}\delta^{112})$-quadraticamente-uniforme então A contém uma* 4-PA *para todo N suficientemente grande.*

EXEMPLO 83 (Gowers, 2001). O conjunto $A = \{s \in \mathbb{Z}_N : |s^2| \leqslant N/10\}$ é uniforme mas não é quadraticamente-uniforme. Se $s \in A \cap A + k$ então $s \in \frac{1}{2k}\{s \in \mathbb{Z}_N : |s - k/2| \leqslant N/5\}$, portanto $A \cap A + k$ não é uniforme para qualquer que seja k. Não daremos as demonstrações.

EXERCÍCIO 84. O objetivo desse exercício é dar uma cota inferior para $r_3(N)$. O resultado é de Behrend (1946).

(1) Seja $S(0,r) \subseteq \mathbb{R}^n$ a esfera de raio r e centro na origem do sistema cartesiano. Tome $M = \lfloor N^{1/n}/2 \rfloor$, $n = \sqrt{\log N}$, e considere a intersecção $A = [M]^n \cap S(0,r)$.

Mostre que existe r no intervalo $[\sqrt{n}, \sqrt{n}M]$ tal que

$$|A| \geqslant \frac{M^n}{n(M^2-1)} > \frac{M^{n-2}}{n}.$$

(Dica: princípio da casa dos pombos.)

(2) Prove os seguintes fatos a respeito da projeção $\rho : A \to [N]$ dada por $\rho(x) = (2M)^{-1}\sum_{i=1}^{n} x_k(2M)^k$: (i) ρ é injetora; (ii) se $\rho(x) + \rho(y) = \rho(2z)$ então $x + y = 2z$, e (iii) $\max\{\rho(x) : x \in A\} \leqslant (2M)^n$.

(3) Mostre que $|\rho(A)| \geqslant N\exp(-\log n - n\log 2 - (2/n)\log N)$.

(4) Use o fato de uma reta encontrar $S(0,r)$ em no máximo dois pontos para concluir que $\rho(A)$ não contém 3-PA.

□

7.5. Um Lema de Regularidade para grupos abelianos. Green (2005) provou um resultado do tipo do Lema de Regularidade para grupos abelianos. Nessa seção vamos mostrar esse resultado restrito ao grupo $G = \mathbb{Z}_2^n$ de ordem $N = 2^n$.

Começamos com algumas observações elementares sobre análise de Fourier nesse grupo. Primeiro, $\widehat{\mathbb{Z}_2} = \{-1, 1\}$. Para $x, g \in G$ definimos $\chi_g(x) = (-1)^{(g,x)} = (-1)^{g^{\mathrm{T}}\cdot x}$ e não é difícil mostrar que $\widehat{G} = \{\chi_g : g \in G\}$. Disso temos que a transformada de Fourier de f é dada por $\widehat{f}(g) = \sum_x f(x)(-1)^{g^{\mathrm{T}}\cdot x}$.

Para o subgrupo $H \subseteq G$ usamos a notação usual para as classes laterais, ou seja $H + g = \{x + g : x \in H\}$. Ainda, denotamos por A_{H+g} a função característica do conjunto $A \cap H + g$. Com essa notação $\widehat{A_{H+g}}(t) = \sum_{x\in H}(A \cap (H+g))(x)\chi_t(x) = \sum_{x\in H}(A_{H+g})(x)(-1)^{x^{\mathrm{T}}\cdot t}$.

Com essa notação, dizemos que g é (ε, A, H)-*regular* se $\Phi(A_{H+g}) \leqslant \varepsilon|H|$, e dizemos que H é ε-*regular* para A se mais que $(1-\varepsilon)N$ elementos g de G são (ε, A, H)-*regular*.

Teorema 85. *Dados $0 < \varepsilon < 1/2$ e $A \subseteq G$. Existem um inteiro $K_0 = K_0(\varepsilon^{-3})$ e subgrupo $H \subseteq G$ de índice $\leqslant K_0$ que é ε-regular para A.*

Demonstração. Definimos

$$\operatorname{ind}(A, H) = \frac{1}{N}\sum_g \left(\frac{|A_{H+g}|}{|H|}\right)^2 \tag{82}$$

e observamos que $0 \leqslant \operatorname{ind}(A, H) \leqslant 1$.

Vamos mostrar que existe uma seqüência $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_k$ de subgrupos tal que $|G/H_i| \leqslant 2^{|G/H_{i-1}|}$ e $\operatorname{ind}(A, H_i) \geqslant \operatorname{ind}(A, H_{i-1}) + \varepsilon^3$, sempre que H_{i-1} não é ε-regular.

Se $H \subseteq G$ não é regular para A existem pelo menos εN elementos $g \in G$ tais que $\Phi(A_{H+g}) \geqslant \varepsilon|H|$.

Se $g_1, g_2 \in H+g$ então A_{H+g_1} é uma translação de A_{H+g_2} e isso implica em $\widehat{A_{H+g_1}}(t) = \widehat{A_{H+g_2}}(t)(-1)^{(g_2-g_1,t)}$ o que implica que os coeficientes de Fourier são grandes nos mesmos pontos $t \in \widehat{G}$. Isso implica que existem K, $\varepsilon \leqslant K/|G/H| \leqslant 1/2$, $t_i \in \widehat{H}$, $i \in [K]$, e classes laterais $H + g_i$ tais que $\widehat{A_{H+g}}(t_i) \geqslant \varepsilon|H|$ para todo $g \in H + g_i$.

Seja $H' = \{x \in H \colon (x, t_i) = 0 \text{ para todo } i \in [K]\}$ subgrupo de H. É imediato que $|G/H'| \leqslant 2^{|G/H|}$. Vamos mostra que ind cresce como afirmado. Primeiro, observamos que $\widehat{H'}(t_i) = |H'|$. Agora

$$\begin{aligned}
N|H'|^2|H|\operatorname{ind}(A, H') &= \sum_g |A_{H'+g}|^2 = \sum_g \sum_{h\in H} |A_{H'+(g+h)}|^2 \\
&= \sum_g \sum_h \left|\sum_x A(x-g-h)H'(x)\right|^2 \\
&= \sum_g \sum_h (A_{H+g} * H'(h))^2 \\
&= \sum_g \sum_{t\in\widehat{H}} |\widehat{A_{H+g}}(t)|^2 ||\widehat{H'}(t)|^2 \\
&= N|H|^2|H'|^2\operatorname{ind}(A, H) + \sum_g \sum_{t\neq 0} |\widehat{A_{H+g}}(t)|^2|\widehat{H'}(t)|^2.
\end{aligned}$$

Para finalizar

$$\begin{aligned}
\sum_g \sum_{t\neq 0} |\widehat{A_{H+g}}(t)|^2|\widehat{H'}(t)|^2 &\geqslant \sum_{i=1}^{K} \sum_{g\in H+g_i} |\widehat{A}(t_i)|^2|\widehat{H'}(t_i)|^2 \\
&\geqslant \varepsilon^2 K|H|^2|H'|^2 \geqslant \varepsilon^3 N|H|^2|H'|^2
\end{aligned}$$

Portanto, $\mathrm{ind}(A,H') \geqslant \mathrm{ind}(A,H) + \varepsilon^3$.

Como no caso do Lema de Regularidade, a prova do teorema segue de iteradas aplicações desse resultado. Os detalhes ficam a cargo do leitor. □

Sejam $A \subset G$ um subconjunto e $H \subset G$ um subgrupo ε-regular para A. Remova de A cada $g \in A$ tal que

(i) A_{H+g} não é ε-regular, ou
(ii) $|A_{H+g}| \leqslant (2\varepsilon)^{1/3}|H|$.

O *conjunto reduzido* resultante, é denotado por A' é a construção equivalente, nesse caso, à de grafo reduzido.

Exercício 86. Mostre que $|A'| \geqslant |A| - 3\varepsilon^{1/3}N$.

Chamamos de triângulo uma tripla $(a,b,c) \in A^3$ tal que $a+b+c=0$. Analogamente ao teorema 29 para triângulos

Teorema 87 (Green, 2005). *Se $A \subset G$ é um subconjunto com pelo menos $o(N^2)$ triângulos então podemos tornar A livre de triângulos removendo $o(N)$ elementos*

Exercício 88. Demonstre o teorema.

Green (2005) mostrou a seguinte conexão com o Lema de Regularidade de Szemerédi. Seja $G = (X \cup Y, E)$ com X e Y cópias disjuntas de $\mathbb{Z}_2^n$ e $ab \in E$ se e somente se $a+b \in A$ onde $A \subseteq \mathbb{Z}_2^n$.

Seja H um subgrupo de $\mathbb{Z}_2^n$ e ε^2-regular para A e vamos mostrar que se $x_1 - x_2$ é (ε, A, H)-regular então o par $(H+x_1, H+x_2)$ é (ε, G) regular.

Tomemos subconjuntos $U + x_i \subset H + x_i$ de cardinalidade $|U + x_i| \geqslant \varepsilon|H|$, $i = 1,2$. O número de arestas em $(U+x_1, U+x_2)$ é o número de soluções de $u + v - a = 0$, $(u,v,a) \in U + x_1 \times U + x_2 \times A$, ou seja

$$\begin{aligned} e(U+x_1, U+x_2) &= \frac{1}{|H|}\sum_t \widehat{A}(t)\widehat{U+x_1}(t)\widehat{U+x_2}(t) \\ &= \frac{1}{|H|}\sum_t \widehat{A_{H+x_1-x_2}}(t)\widehat{U}(t)\widehat{U}(t), \end{aligned}$$

e, portanto temos

$$\begin{aligned} \big|d_G(U+x_1, U+x_2) - & d_G(H+x_1, H+x_2)\big| = \\ & \left|\frac{1}{|H||U|^2}\sum_{t\neq 0} \widehat{A_{H+x_1-x_2}}(t)\widehat{U}(t)\widehat{U}(t)\right| \\ & \leqslant \frac{1}{|H||U|^2}\Phi(A_{H+x_1-x_2})\|\widehat{U}\|_2^2 \\ & \leqslant \frac{\varepsilon^2|H|}{|U|} \leqslant \varepsilon. \end{aligned}$$

Como para cada i há no máximo εk^2 j's para os quais $x_i - x_j$ não é (ε, A, H)-regular, temos que $V(G)$ é particionado pelas classes laterais $H + x_i$, $i \in [k]$.

7.6. Conexões com grafos. Chung and Graham (1992) provaram ainda que as propriedades mostradas na seção 7.2 são equivalentes com certas propriedades de grafos. Estudaremos essas propriedades na próxima seção. Por enquanto, veremos algumas conexões.

Definimos o grafo G_A cujos vértices são os inteiros de $\mathbb{Z}_N$ e ij é uma aresta se e somente se $i + j \in A$. Supomos que A é pseudoaleatório e fixamos $\delta = |A|/N$.

A primeira propriedade é que, por "densidade relativa", para qualquer subconjunto de vértices $U \subset \mathbb{Z}_N$

$$e(U) = \frac{1}{2} \sum_{i \in \mathbb{Z}_N} \sum_{j \in \mathbb{Z}_N} U(i)U(j)A(i+j) = \frac{\delta}{2}|U|^2 + o(N^2). \tag{83}$$

Não é difícil mostrar a recíproca, ou seja, se $e_{G_A}(U)$ é como na equação acima para todo U, então A tem a propriedade "densidade relativa".

Pela "2-padrão", para quase todos $i, j \in \mathbb{Z}_N$ vale que $|N(i) \cap N(j)| = \delta|A| + o(N)$, logo

$$\sum_{i \in \mathbb{Z}_N} \sum_{j \in \mathbb{Z}_N} \big||N(i) \cap N(j)| - \delta^2 N\big| = o(N^3). \tag{84}$$

Aqui também vale a recíproca.

Mais uma conexão é dada pela "$2t$-ciclo" que é equivalente a dizer que o número de circuitos de comprimento $2t$ em G_A é

$$\#(C^{2t} \subseteq G_A) = |A|^{2t} + o(N^{2t}) = (1 + o(1))(\delta N)^{2t}. \tag{85}$$

Se G_δ é o grafo aleatório no modelo binomial com probabilidade de aresta δ, então as equações (83), (84) e (83) valem com probabilidade tendendo a 1, quando $N \to \infty$, para qualquer $0 < \delta < 1$ constante.

Como as propriedades de subconjunto do $\mathbb{Z}_N$ são equivalentes, provamos que en G_A

$$\begin{aligned} e(U) = \frac{\delta}{2}|U|^2 + o(N^2) &\Leftrightarrow \sum_{i,j \in \mathbb{Z}_N} \big||N(i) \cap N(j)| - \delta^2 N\big| = o(N^3) \\ &\Leftrightarrow \#(C^{2t}) = (1 + o(1))(\delta N)^{2t}. \end{aligned}$$

8. Grafos pseudoaleatórios

Na seção anterior vimos três propriedades em grafos que são equivalentes. Nessa seção, Teorema 89 abaixo, veremos uma coleção de propriedades, que incluem essas três, e que são equivalentes para grafos de densidade p, $0 < p < 1$. Um grafo que satisfaz alguma (portanto, todas) dessas propriedades é dito *grafo pseudoaleatório*.

No que segue adotamos as seguintes notações, $N^*_G(H)$ e $N_G(H)$ denotam o número de cópias induzidas e não necessariamente induzidas de H em G^n, respectivamente. Denotamos por $N_G(x)$ o conjunto dos vértices adjacentes ao vértice x em G. Usamos $A = A(G)$ para a matriz $(a_{x,y})_{x,y\in V(G)}$ de adjacências de G e $\lambda_1, \ldots, \lambda_{|V|}$ são seus autovalores reais. Denotamos por $A\triangle B$ a diferença simétrica dos conjuntos A e B, ou seja, $A\triangle B = (A \cup B) \setminus (A \cap B)$.

Teorema 89. *Para todo $p \in (0,1)$ fixo são equivalentes:*
$\mathbf{P_1}(s)$: *Para todo grafo H de ordem s, para $s \geqslant 4$ inteiro fixo,*

$$N^*_{G^n}(H) = (1 + o(1))n^s p^{e(H)}(1-p)^{\binom{s}{2}-e(H)}.$$

$\mathbf{P_2}(t)$: *Para $t \geqslant 4$ inteiro par,*

$$e(G^n) = \frac{n^2 p}{2} + o(n^2) \quad e \quad N_{G^n}(C^t) \leqslant (np)^t + o(n^t).$$

$\mathbf{P_3}$: *Se $\lambda_1 \geqslant |\lambda_2| \geqslant \cdots \geqslant |\lambda_n|$ são os autovalores de $A(G^n)$, então*

$$e(G^n) \geqslant \frac{n^2 p}{2} + o(n^2), \qquad \lambda_1 = (1 + o(1))np \qquad e \qquad \lambda_2 = o(n).$$

$\mathbf{P_4}$: *Para cada $U \subseteq V(G^n)$, temos*

$$e(U) = \frac{p}{2}|U|^2 + o(n^2).$$

$\mathbf{P_5}$: *Para cada $U \subseteq V(G^n)$, com $|U| = \lfloor n/2 \rfloor$, temos*

$$e(U) = \left(\frac{p}{8} + o(1)\right) n^2.$$

$\mathbf{P_6}$: *Para todo x, $y \in V(G^n)$, se $S(x,y) = V(G^n) \setminus (N(x)\triangle N(y))$, então*

$$\sum_{x,y\in V} \big||S(x,y)| - (p^2 - (1-p)^2)n\big| = o(n^3).$$

$\mathbf{P_7}$: *Para todos x, $y \in V(G^n)$*

$$\sum_{x,y\in V} \big||N(x) \cap N(y)| - p^2 n\big| = o(n^3).$$

□

Note que $\mathbf{P_2}$ vale somente para circuitos pares. O seguinte exemplo mostra a diferença, neste contexto, entre circuitos pares e circuitos ímpares. Sejam G um grafo com $4n$ vértices e V_1, V_2, V_3, V_4 subconjuntos disjuntos de $V(G)$, cada um de tamanho n. Em V_1 e em V_2 colocamos todas arestas, entre V_3 e V_4 colocamos todas as aresta e entre $V_1 \cup V_2$ e $V_3 \cup V_4$ colocamos as arestas com probabilidade $1/2$. Esse grafo não é pseudoaleatório, entretanto, valem $\mathbf{P_1}(3)$ e $\mathbf{P_2}(2t+1)$ para todo t fixo.

Todas essas propriedades são facilmente verificadas valerem para o grafo aleatório $G_{n,p}$ quase-sempre. Como foi observado em Chung et al. (1989), um

fato bastante interessante é que $\mathbf{P_2}(\mathbf{4})$ é forte suficiente para termos pseudoaleatoriedade.

EXEMPLO 90. Nesse exemplo, mostraremos algumas das implicações entre as propriedades enunciadas no teorema acima, notadamente, que envolve os autovalores da matriz de adjacências.

Primeiro, assumimos $\mathbf{P_3}$. Denotamos por $d_1, d_2, \ldots, d_n$ os graus do vértices de $V(G^n) = [n]$. Pondo $\mathbf{v} = (1, 1, \ldots, 1)^{\mathtt{T}}$ temos de (11), página 10, que

$$np + o(n) = \lambda_1 \geqslant \frac{\mathbf{v}^{\mathtt{T}} A \mathbf{v}}{\|\mathbf{v}\|^2} = \frac{\sum d_i}{n} = \frac{2e(G^n)}{n} \geqslant np + o(n), \tag{86}$$

e assim podemos concluir que

$$\sum_{i=1}^{n} |d_i - np| = o(n^2). \tag{87}$$

EXERCÍCIO 91. Conclua de (87) que G^n é quase-regular, ou seja, quase todos[3] os vértices têm grau $(1 + o(1))np$.

Agora, vamos mostrar que as arestas estão bem distribuídas. Seja $S \subset V$ um subconjuto de vétices e $\mathbf{s}$ seu vetor (coluna) característico. Observamos que

$$\mathbf{s}^{\mathtt{T}} A \mathbf{s} = \sum_{i=1}^{n} \sum_{j=1}^{n} s_j s_i a_{j,i} = \sum_{i=1}^{n} d_S(i) = 2e(S), \tag{88}$$

onde $d_S(i)$ é o grau de i em $G[S]$. Pelo Teorema Espectral temos que se $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ é uma base ortonormal de autovetores, com λ_i o autovalor associado a $\mathbf{x}_i$, então

$$A = \sum_{i=1}^{n} \lambda_i \mathbf{x}_i \mathbf{x}_i^{\mathtt{T}} = \lambda_1 \mathbf{x}_1 \mathbf{x}_1^{\mathtt{T}} + \sum_{i=2}^{n} \lambda_i \mathbf{x}_i \mathbf{x}_i^{\mathtt{T}} = A_1 + B,$$

onde a última igualdade é uma definição.

Se α_i é a coordenada de $\mathbf{s}$ na base ortonormal de autovetores, ou seja, $\alpha_i = \langle \mathbf{s}, \mathbf{x}_i \rangle = \mathbf{s}^{\mathtt{T}} \mathbf{x}_i$, então $\sum_i \alpha_i^2 = \|\mathbf{s}\| = |S|$. Como $\mathbf{s} = \sum_i \alpha_i \mathbf{x}_i$ temos

$$\mathbf{s}^{\mathtt{T}} A_1 \mathbf{s} = \alpha_1^2 \lambda_1 \quad \text{e} \quad \mathbf{s}^{\mathtt{T}} B \mathbf{s} = \sum_{j=2}^{n} \alpha_j^2 \lambda_j, \tag{89}$$

e resta estimar os α_i's.

Denotamos por $\mathbf{u}$ o vetor $\frac{1}{\sqrt{n}}\mathbf{1}$ de modo que

$$\alpha_1 = \langle \mathbf{s}, \mathbf{u} \rangle - \langle \mathbf{s}, \mathbf{x}_1 - \mathbf{u} \rangle = \frac{|S|}{\sqrt{n}} + \langle \mathbf{s}, \mathbf{x}_1 - \mathbf{u} \rangle$$

[3]Relembrando que quase todos nese caso significa todos menos $o(n)$ deles.

e portanto, por Cauchy-Schwarz e por $\|\mathbf{x}_1 - \mathbf{u}\| = o(1)$, cuja demostração adiaremos, temos

$$\left|\alpha_1 - \frac{|S|}{\sqrt{n}}\right| \leqslant \|\mathbf{s}\|\|\mathbf{x}_1 - \mathbf{u}\| = o(\sqrt{|S|}).$$

Também temos $|\mathbf{s}^{\mathtt{T}} B\mathbf{s}| \leqslant |\lambda_2||\sum_{i\neq 1}\alpha_i^2| \leqslant |\lambda_2||S|$. Juntando essas estimativas com as equações (88) e (89) fechamos com

$$e(S) = \frac{|S|^2}{2}p + o(n^2).$$

Restou ainda $\|\mathbf{x}_1 - \mathbf{u}\| = o(1)$ para provarmos.

$$\|\mathbf{x}_1 - \mathbf{u}\|^2 = \langle \mathbf{x}_1 - \mathbf{u}, \mathbf{x}_1 - \mathbf{u}\rangle = \langle \mathbf{u}, \mathbf{u}\rangle + \langle \mathbf{x}_1, \mathbf{x}_1\rangle - 2\langle \mathbf{u}, \mathbf{x}_1\rangle = 2 - 2\langle \mathbf{u}, \mathbf{x}_1\rangle.$$

Portanto, se $\mathbf{u} = \sum_i \beta_i \mathbf{x}_i$ então devemos estimar β_1.

Consideremos os vetores

(i) $A\mathbf{u} = \frac{1}{\sqrt{n}}(d_1, d_2, \ldots, d_n)^{\mathtt{T}}$,

(ii) $\mathbf{d} = \frac{1}{\sqrt{n}}(d_1 - np, d_2 - np, \ldots, d_n - np)^{\mathtt{T}} = A\mathbf{u} - np\mathbf{u} = \sum_i \beta_i(\lambda_i - np)\mathbf{x}_i$.

Pelo exercício 91 temos que $\|\mathbf{d}\| = o(n)$ e por (ii)

$$\|d\|^2 = \sum_{i=1}^{n} \beta_i^2(\lambda_i - np)^2 \geqslant \sum_{i=2}^{n} \beta_i^2(\lambda_i - np)^2 \geqslant (np - o(n))^2 \sum_{i=2}^{n} \beta_i^2 = (np - o(n))^2(1 - \beta_1^2)$$

logo

$$\beta_1 \geqslant \beta_1^2 \geqslant 1 - \frac{\|\mathbf{d}\|^2}{(np - o(n))^2}$$

e

$$\|\mathbf{x}_1 - \mathbf{u}\|^2 = 2 - 2\beta_1 \leqslant 2 - 2 + 2\frac{\|\mathbf{d}\|^2}{(np - o(n))^2} = o(1).$$

Nosso próximo passo é deduzir $\mathbf{P_3}$ a partir de $\mathbf{P_2}(4)$. No i-ésimo elemento da diagonal de A^4 temos o número de passeios fechados com quatro arestas que começam em i, logo, $\mathrm{tr}(A^4) = N(C^4) + o(n^4)$. Também, $\mathrm{tr}(A^4) = \sum_{i=1}^{n} {\lambda_i}^4$. Assumindo que o número de cópias de C^4 é o esperado, ou seja, assumindo $\mathbf{P_2}(4)$, temos

$$\sum_{i=1}^{n} {\lambda_i}^4 \leqslant n^4p^4 + o(n^4). \tag{90}$$

Como acima,

$$\lambda_1 \geqslant \frac{\mathbf{v}^{\mathtt{T}} A\mathbf{v}}{\|\mathbf{v}\|^2} = \frac{\sum d_i}{n} = \frac{2e(G^n)}{n} = np + o(n), \tag{91}$$

ou seja,

$$n^4p^4 + o(n^4) \leqslant {\lambda_1}^4 \leqslant \sum_{i=1}^{n} {\lambda_i}^4 \leqslant n^4p^4 + o(n^4) \tag{92}$$

portanto, $|\lambda_1| = np + o(n)$ e $|\lambda_2| = o(n)$. □

Simonovits and Sós (1991) acrescentaram mais uma propriedade a lista de Chung, Graham e Wilson. Eles provaram que $\mathbf{P_s}$ abaixo é uma propriedade pseudoaleatória de grafos.

$\mathbf{P_s}$: Para todo real positivo $\varepsilon \leqslant 1$ e todo inteiro positivo k_0 existem inteiros positivos $n_0 = n_0(\varepsilon, m_0)$ e $K_0 = K_0(\varepsilon, m_0)$ tal que G^n, para $n \geqslant n_0$, admite uma partição (ε, k, G^n)-regular $V_0, V_1, \ldots, V_k$, com $k_0 \leqslant k \leqslant K_0$, tal que

$$(V_i, V_j) \text{ é } (\varepsilon, G^n)\text{-regular e } |d(V_i, V_j) - p| < \varepsilon$$

não vale para no máximo $\varepsilon\binom{k}{2}$ pares (V_i, V_j), com $1 \leqslant i < j \leqslant k$.

Vamos mostrar que $\mathbf{P_4} \Rightarrow \mathbf{P_s}$. Seja G^n uma seqüência de grafos e assma que para todo todo $X \subseteq V$ temos $e(X) = |X|^2 p/2 + o(n^2)$.

Sejam ε e k_0 dados. Ponha $K_0 = k = k_0$. Considere $V_0, \ldots, V_k$ arbitrários com $|V_0| < k$ e $|V_i| = \lfloor n/k \rfloor$. Seja $N_1 = N_1(\varepsilon, k)$ tal que $\varepsilon N_1 \geqslant k$.

Para quaisquer $U, W \subseteq V(G^n)$ disjuntos

$$\begin{aligned} e(U,W) &= e(U \cup W) - e(U) - e(W) = (|U| + |W|)^2 \frac{p}{2} - |U|^2 \frac{p}{2} - |W|^2 \frac{p}{2} + o(n^2) \\ &= |U||W|p + o(n^2), \end{aligned}$$

logo, existe $N_2 = N_2(\varepsilon, k)$ tal que para todo $n \geqslant N_2$

$$\big|e(U,W) - p|U||W|\big| < \frac{(1-\varepsilon)^2\varepsilon^3}{k^2} n^2.$$

Definimos $n_0(\varepsilon, k) = \max\{N_1, N_2\}$, assim para $n \geqslant n_0$ nós temos $|V_0| < k \leqslant \varepsilon N_1 \leqslant \varepsilon n$ e $(1-\varepsilon)n/k < |V_i|$ para todo $i \in [k]$.

Exercício 92 ($\mathbf{P_s} \Rightarrow \mathbf{P_2}$). Mostre que para $t \in \mathbb{N}$ a propriedade $\mathbf{P_s}$ implica $\mathbf{P_2}(2t)$ (veja observação 20, pág. 20).

Outra propriedade equivalente as acima foi posta por Kohayakawa (2003) e foi usada para projetar um algoritmo ótimo para verificar regularidade no sentido de Szemerédi. Dizemos que um grafo J é (ϱ, A)-*uniforme*, para $0 \leqslant \varrho \leqslant 1$ e $A \in \mathbb{R}$, se para todos $U, W \subset V(J)$ disjuntos vale

$$\big|e(U,W) - \varrho|U||W|\big| \leqslant A\sqrt{\varrho|V||U||W|}. \tag{93}$$

Um grafo G satisfaz a propriedade $P_{J,\Delta}(\varepsilon)$, para $\varepsilon \in (0,1)$, se G e J têm o mesmo conjuntode vértices e

$$\sum_{ij \in E(J)} \big||N_G(i) \Delta N_G(j)| - p^2 n\big| \leqslant p^2 n \varepsilon e(J). \tag{94}$$

Dessa forma,

Proposição 93. *$P_{J,\Delta}(o(1))$ é uma propriedade pseudoaleatória.*

A existência de grafos uniformes pode ser estabelecida por meios construtivos (grafos de Ramanujan, por exemplo).

Outros parâmetros foram introduzidos por Chung and Graham (1991) como a *discrepância* e o *desvio* definidos por

$$\begin{aligned} \operatorname{disc}(G^n) &= \frac{2}{n^2} \max_{W \subseteq V(G^n)} \left| e(G^n[W]) - e(\overline{G^n[W]}) \right| \text{ e} \\ \operatorname{dev}(G^n) &= \frac{1}{n^4} \left(EC_4 - OC_4 \right), \end{aligned}$$

onde EC_4 é o número de tuplas $(a,b,c,d) \in V^4$ tais que uma quantidade par dos 2-subconjuntos $\{a,b,\}$, $\{b,c\}$, $\{c,d\}$ e $\{d,a\}$ são arestas de G^n, e OC_4 é o equivalente para quantidade ímpar de arestas.

Proposição 94. $\operatorname{dev}(G^n) = o(1)$ *é uma propriedade pseudoaleatoria.*

Terminamos essa seção deixando como exercício algumas propriedades dadas em Chung and Graham (1991) envolvendo esses conceitos.

Exercício 95. Demonstre as seguintes afirmações

(i) $\operatorname{disc}(G^n) \leqslant \operatorname{dev}(G^n)^{1/4}$ e $\operatorname{dev}(G^n) \leqslant 16 \operatorname{disc}(G^n)^{1/4}$;
(ii) $e(G^n) \geqslant \frac{n^2}{2} p \left(1 - \operatorname{dev}(G^n)^{1/4}\right)$;
(iii) $N(C^4) \leqslant (np)^4 (1 + \operatorname{dev}(G^n)^{1/4})^4$;
(iv) $|\lambda_1 - np| \leqslant np \operatorname{dev}(G^n)^{1/4}$;
(v) $|\lambda_2| \leqslant n \operatorname{dev}(G^n)^{1/6}$.

9. Construções explícitas

Um grande número de construções são baseadas em propriedades de resíduos de inteiros, por exemplo, se q é uma potência de primo então $(a^{(q-1)/2}, (a-1)^{(q-1)/2})$ vale $(\pm 1, \pm 1)$ aproximadamente $q/4$ vezes e mais ou menos de forma independente para a escolhido aleatoriamente.

Dizemos que um inteiro a é um *resíduo quadrático* módulo um primo $p \geqslant 3$ se p não divide a e

$$a \equiv x^2 \pmod{p}$$

para algum inteiro x. O *símbolo de Legendre*, $(\cdot/p)$, é definido da seguinte forma: se p divide a, então $(a/p) = 0$, senão

$$(a/p) = \begin{cases} +1 & \text{se } a \text{ é resíduo quadrático de } p, \\ -1 & \text{se } a \text{ não é resíduo quadrático de } p. \end{cases}$$

Os seguintes resultados são teoremas básicos de álgebra facilmente encontrados em livros texto (por exemplo Ireland and Rosen, 1990, cap. 5).

(a) *Metade dos inteiros a tais que $1 \leqslant a \leqslant p-1$ são resíduos quadráticos de p.*
(b) *Se d divide $p-1$, então $x^d \equiv 1 \pmod{p}$ tem exatamente d soluções.*
(c) *Para todo primo p vale $a^p \equiv a \pmod{p}$.*

Desses três resultados, temos que o conjunto dos resíduos quadráticos de p é igual ao conjunto das soluções de

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Portanto, se p não divide a, vale que

$$(a/p) \equiv a^{\frac{p-1}{2}} \pmod{p}, \tag{95}$$

e, se p também não divide b, temos que

$$(a/p)(b/p) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv (ab/p). \tag{96}$$

Dizendo de outra forma, a é um resíduo quadrático se $x^2 = a$ tem solução no corpo $\mathbb{Z}_p$, p ímpar.

Denotamos por $\mathbb{F}_q$ o corpo finito de ordem q potência de primo. Um caracter do grupo $(\mathbb{F}_q, +)$ como definido na seção 1.6 é chamado de *caracter aditivo*.

Exercício 96. Mostre que se $G = (\mathbb{F}_p, +)$ então $\Phi(aA + b) = \Phi(A)$, $a \neq 0$.

Um *caracter multiplicativo* de $\mathbb{F}_q^* = (\mathbb{F}_q \setminus \{0\}, \cdot)$ é uma função $\gamma\colon \mathbb{F}_q^* \to \mathbb{C}^*$ tal que

$$\gamma(a \cdot b) = \gamma(a)\gamma(b),$$

para todos $a, b \in \mathbb{F}_q$. Como conseqüência da definição temos $\gamma(1) = 1$ e $\gamma(a^{-1}) = \overline{\gamma(a)}$. Usualmente, a função é estendida para o 0 pondo $\gamma(0) = 0$.

Exemplo 97 (Caracter resíduo quadrático). Um exemplo de caracter multiplicativo é $\gamma(x) = x^{(q-1)/2}$ que vale 1 nos quadrados de $\mathbb{F}_q$, vale 0 no 0 e vale -1 nos outros elementos do corpo. Em particular, quando q é primo nós temos que $\gamma(x) = (x/q)$. □

Exemplo 98. O caracter $\gamma_0(a) = 1$ para todo $a \neq 0$ é chamado de *trivial*. □

Exercício 99. Mostre que $\sum_a \gamma(a) = 0$ para todo γ não-trivial, onde a soma é sobre todos os elementos de $\mathbb{F}_p$.

Como o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico, se g é um gerador do grupo então γ fica completamente definida por $\gamma(g)$. A *ordem* de um caracter multiplicativo γ é o menor inteiro positivo n tal que $\gamma(a)^n = 1$, para todo $a \in \mathbb{F}_q^*$.

Exercício 100. O conjunto $\widehat{\mathbb{F}_p^*}$ dos caracteres com a multiplicação $\gamma\delta(a) = \gamma(a)\delta(a)$ é um grupo cíclico de ordem $p-1$. Mais que isso,

$$\widehat{\mathbb{F}_p^*} = \{\lambda^1, \ldots, \lambda^{p-2}, \lambda^{p-1}\} \tag{97}$$

onde $\lambda(g) = \exp(2\pi i/(p-1))$. Observe que λ^{p-1} é trivial.

Exercício 101. Se $a \neq 1$ então existe um caracter $\gamma \in \widehat{\mathbb{F}_p^*}$ tal que $\gamma(a) \neq 1$.

O seguinte exercício nos dará um citério para o número de soluções de $x^n = a$, $a \in \mathbb{F}_p^*$ para $p-1$ divisível por n.

Exercício 102. Se $p = rn+1$ e a não é uma n-ésima potência então existe um caracter γ tal que γ^n é trivial e $\gamma(a) \neq 1$.

Agora, consideremos p da forma $rn+1$ e seja $\gamma = \lambda^{(p-1)/n}$, λ como (97) acima. De $\gamma(g) = \exp(2\pi i/n)$ caracter, temos que *existem n caracteres cuja ordem divide n* pois os caracteres $\gamma^1, \ldots, \gamma^{n-1}, \gamma^n = \gamma_0$ são distintos. Ainda, se $a \in \mathbb{F}_p^*$ e $a = x^n$ para algum $x \in \mathbb{F}_p^*$, então $\gamma(a) = \gamma(x)^n = 1$. Logo

$$\sum_{\gamma} \gamma(a) = n$$

pnde a soma é sobre todo γ cuja ordem divide n.

Agora, se $a \neq x^n$, para todo $x \in \mathbb{F}_p^*$, então $a = g^\ell$ com $n \not| \ell$ e, para γ dado no exercício 101 temos que $\gamma(a) = \gamma(g)^\ell \neq 1$. Logo, a soma $S = \sum \gamma^i(a)$ sobre todo $i \in \{1, \ldots, n-1, n\}$ é zero pois $\gamma(a)S = S$. Logo,

$$\sum_{\substack{\gamma \in \widehat{\mathbb{F}_p^*} \\ \gamma^n = 1}} \gamma(a) = \begin{cases} n, & \text{se } a \in \{x^n : x \in \mathbb{F}_p^*\} \\ 0, & \text{caso contrário.} \end{cases} \tag{98}$$

Proposição 103. *Se $n|p-1$ então o número de soluções de $x^n = a$, $a \in \mathbb{F}_p$ é $\sum \gamma(a)$, onde a soma é sobre todo caracter cuja ordem divide n.*

Demonstração. Dos dois parágrafos acima, sabemos que resta provar o caso $a = 0$. Nesse caso, a equação só tem uma solução e a soma do enunciado resulta em 1 pela contribuição do caracter trivial. □

Exercício 104. Seja p um primo ímpar. Mostre que o número de soluções de $x^2 = a$ no $\mathbb{Z}_p$ é $1 + (a/p)$.

Exercício 105. Sejam p primo e $d = \text{mdc}(n, p-1)$. Mostre que o número de soluções de $x^n = a$, $a \in \mathbb{F}_p$, é $\sum \gamma(a)$, onde a soma é sobre todo γ tal que γ^d é trivial. (*Dica*: Em $\mathbb{F}_p^*$ a equação $x^n = a$ tem solução se, e somente se, $a^{(p-1)/d} = 1$.)

Exercício 106. Mostre um isomorfismo entre os subgrupos

(i) $\left\{\gamma \in \widehat{\mathbb{F}_p^*} \colon \gamma^n = 1\right\}$,

(ii) $U^\perp = \left\{\gamma \in \widehat{\mathbb{F}_p^*} \colon \gamma|_U = 1\right\}$ onde $U = \{x \in \mathbb{F}_p \colon x^n = 1\}$, e

(iii) $\widehat{\mathbb{F}_p^*/U}$.

Para demonstrar a pseudoaleatoriedade de alguns exemplos de conjuntos, usaremos o seguinte resultado.

Teorema 107. *Se χ e γ são caracteres de $\mathbb{F}_q$, aditivo e multiplicativo respectivamente, então a* soma de Gauss *sobre $\mathbb{F}_q$*

$$G(\chi, \gamma) = \sum_{a \in \mathbb{F}_q} \chi(a)\gamma(a)$$

satisfaz

(i) $G(\chi_0, \gamma_0) = q - 1$, *onde χ_0 é principal e γ_0 trivial;*

(ii) $G(\chi_0, \gamma) = 0$ *se $\gamma \neq \gamma_0$;*

(iii) $G(\chi, \gamma_0) = -1$ *se $\chi \neq \chi_0$;*

(iv) *e nos outros casos $|G(\chi, \gamma)| = \sqrt{q}$.*

Demonstração. Vamos provar somente o último item.

$$\begin{aligned}
|G(\chi,\gamma)|^2 &= \overline{G(\chi,\gamma)}G(\chi,\gamma) \\
&= \sum_{a,b \in \mathbb{F}_q^*} \chi(b-a)\gamma(ba^{-1}) \\
&= \sum_{c,a \in \mathbb{F}_q^*} \chi(ac-a)\gamma(c) \\
&= \sum_{c \in \mathbb{F}_q^*} \gamma(c) \sum_{a \in \mathbb{F}_q^*} \chi(a(c-1)) \\
&= \gamma(1)(q-1) - \sum_{1 \neq c \in \mathbb{F}_q^*} \gamma(c) \\
&= \gamma(1)q - \sum_{c \in \mathbb{F}_q^*} \gamma(c) \\
&= \gamma(1)q = q.
\end{aligned}$$

□

Corolário 108. *Se χ é um caracter aditivo não-principal e $p = nr + 1$ primo então*

$$\left| \sum_{\gamma \in \widehat{\mathbb{F}_p^*}} G(\chi, \gamma) \right| < (n-1)\sqrt{p}.$$

Demonstração.

$$\left|\sum_{\gamma\in\widehat{\mathbb{F}_p^*}} G(\chi,\gamma)\right| \leqslant \sum_{\substack{\gamma\in\widehat{\mathbb{F}_p^*}\\ \gamma^n=1}} |G(\chi,\gamma)| < -1+(n-1)\sqrt{p}.$$

□

Usaremos, também, o próximo resultado famoso devido Weil e usado para deduzir a hipótese de Riemann para curvas sobre corpos finitos.

Teorema 109 (Teorema de Weil). *Seja $f(X)\in\mathbb{F}_q[X]$ um polinômio com m zeros distintos e que não seja da forma $c(g(X))^d$, onde $g(X)\in\mathbb{F}_q[X]$, $c\in\mathbb{F}_q$ e d é a ordem do caracter multiplicativo χ. Então*

$$\left|\sum_{x\in\mathbb{F}_q} \chi(f(x))\right| \leqslant (m-1)\sqrt{q}. \tag{99}$$

□

Exemplo 110 (Chung and Graham, 1992). Defina para p primo

$$Q_2 = \left\{x^2 \colon x\in\mathbb{Z}_p\right\} \subset \mathbb{Z}_p.$$

Vamos mostrar que Q_2 satisfaz a propriedade "soma exponencial".

Primeiro, notemos que $\chi(a)=(a/p)$ é um caracter multiplicativo do corpo $\mathbb{Z}_p$ dos resíduos módulo p. Para $j\neq 0$,

$$\widehat{Q_2}(j) = \frac{1}{2}\sum_{t\in\mathbb{Z}_p}(1+(t/p))\omega_j(t) = \frac{1}{2}\sum_{t\in\mathbb{Z}_p}(t/p)\omega_j(t) = \frac{1}{2}\sum_{t\in\mathbb{Z}_p}\chi(t)\omega_j(t).$$

Usando o teorema 107 temos $|\widehat{Q_2}(j)| = |G(\omega_j,\chi)| = \sqrt{p}/2$. □

Exemplo 111. Generalizando o exemplo anterior, defina para p primo da forma $rn+1$

$$Q_n = \left\{x^n \colon x\in\mathbb{Z}_p^*\right\} \subset \mathbb{Z}_p.$$

Para ω_j, temos

$$\sum_{\substack{\gamma\in\widehat{\mathbb{Z}_p^*}\\ \gamma^n=1}} G(\omega_j,\gamma) = \sum_{a\in\mathbb{Z}_p}\omega_j(a)\sum_{\substack{\gamma\in\widehat{\mathbb{Z}_p^*}\\ \gamma^n=1}}\gamma(a) = n\sum_{a\in\mathbb{Z}_p}\omega_j(a)Q_n(a) = n\widehat{Q_n}(\omega_j)$$

onde a primeira igualdade segue da definição da soma de Gauss e a segunda da equação (98), lembrando que usamos $Q_n(a)$ para a função característica do conjunto Q_n.

Usando o corolário 108 temos

$$|\widehat{Q_n}(\omega_j)| \leqslant \frac{1}{n}\sum_{\gamma}|G(\omega_j,\gamma)| \leqslant \frac{1}{n}(n-1)\sqrt{p} < \sqrt{p}.$$

Usando exercício 96 podemos concluir que $aQ_n + b$ é pseudoaleatório para todo $a \neq 0$. □

Exercício 112. Mostre que se p é um primo qualquer, então $Q_n = Q_d$, onde $d = \mathrm{mdc}(n, p-1)$.

Exemplo 113. Outro exemplo de Chung and Graham (1992) é $AQ_n \subset \mathbb{Z}_p$ para A formado por $t \leqslant n$ elementos de $\mathbb{Z}_p^*$ tais que se $a, b \in A$ então $ab^{-1} \notin Q_n$. Nesse caso,

$$|\widehat{AQ_n}(j)| = \left|\sum_a AQ_n(a)\omega_j(a)\right| = \frac{1}{n}\sum_{a\in A}\left|\sum_x \omega_j(ax^n)\right| \leqslant \frac{1}{n}\sum_{a\in A}\Phi(aQ_n),$$

de onde segue que $|\widehat{AQ_n}(j)| \leqslant (t/n)\Phi(Q_n) = O(\sqrt{p})$. □

Exemplo 114 (Grafos de Paley). O *grafo de Paley*, Q_2^p, é um dos exemplos de grafos pseudoaleatórios mais conhecidos. Ele é definido para todo primo $p \equiv 1 \pmod 4$ pondo $V(Q_2^p) = \mathbb{Z}_p$, o corpo finito de ordem p identificado com $\{0, 1, \ldots, p-1\}$, e as arestas são dadas por $E(Q_2^p) = \{\{i, j\} \colon i - j \in Q_2\}$. Note que da escolha de p temos que $(-1/p) = (-1)^{(p-1)/2} = 1$ e isso quer dizer que $\{i, j\} \in E(Q_p)$ está bem definido pois

$$(i - j/p) = 1 \Leftrightarrow (i - j/p)(-1/p) = 1 \Leftrightarrow (j - i/p) = 1.$$

Agora, observe que $k \in V(Q_p)$ é adjacente a i, $j \in V(Q_p)$ distintos, ou não-adjacente a ambos se, e somente se, $\frac{k-i}{k-j}$ é um resíduo quadrático de p. Mas, para quaisquer um dos $(1/2)(p-1) - 1$ resíduos quadráticos a, de p, diferente de 1, existe um único k tal que

$$\frac{k-i}{k-j} = 1 + \frac{j-i}{k-j} = a.$$

Assim, $S(i, j) = 1/2(p-3)$, portanto, $\mathbf{P_6}$ vale.

Um resultado simples e útil sobre propriedades de quase todos os grafos é o seguinte: dados $i, j \in \mathbb{N}$, *para todos subconjuntos de vértices disjuntos U e W, $|U| \leqslant i$, $|W| < j$, existe $v \notin U \cup W$ tal que $vu \in E$, para todo $u \in U$, e $vw \notin E$, para todo $w \in W$*. Essa propriedade vale para G_p, para todo $p \in (0, 1)$ fixo e todo $i, j \in \mathbb{N}$, com probabilidade $1 - o(1)$.

Vamos ver o que acontece nos grafos de Paley. Denotamos por $\chi(x) = (x/p)$ o caracter resíduo quadrático. Sejam $U, W \subset \mathbb{Z}_p$ disjuntos com $|U| + |W| = m$. Para todo $v \in \mathbb{Z}_p$ seja

$$h(v, U, W) = \prod_{u\in U}(1 + \chi(v - u)) \times \prod_{w\in W}(1 - \chi(v - w)), \tag{100}$$

portanto, facilmente verificamos que

$$h(v,U,W)=\begin{cases}2^m, & \text{se } vu\in E\ (\forall u\in U),\ vw\notin E\ (\forall w\in W) \text{ e } v\notin U\cup W\\ 2^{m-1}, & \text{se } vu\in E\ (\forall u\in U),\ vw\notin E\ (\forall w\in W) \text{ e } v\in U\cup W\\ 0, & \text{caso contrário.}\end{cases}$$

Desenvolvendo o produto em (100) verificamos

$$\begin{aligned}h(v,U,W)&=\left(1+\sum_{\substack{U'\subseteq U\\ U'\neq\emptyset}}\prod_{u\in U'}\chi(v-u)\right)\left(1+\sum_{\substack{W'\subseteq W\\ W'\neq\emptyset}}(-1)^{|W'|}\prod_{w\in W'}\chi(v-w)\right)\\ &=1+\sum_{\substack{W'\subseteq W\\ W'\neq\emptyset}}\sum_{\substack{U'\subseteq U\\ U'\neq\emptyset}}(-1)^{|W'|}\chi\left(\prod_{z\in U'\cup W'}\chi(v-z)\right)\end{aligned}$$

e somando cada lado sobre todo $v\in\mathbb{Z}_p$

$$\sum_v h(v,U,W)-p=\sum_{\substack{W'\subseteq W\\ W'\neq\emptyset}}\sum_{\substack{U'\subseteq U\\ U'\neq\emptyset}}(-1)^{|W'|}\sum_v\chi\left(\prod_{z\in U'\cup W'}\chi(v-z)\right)$$

e usando o Teorema de Weil, concluímos que

$$\begin{aligned}\left|\sum_v h(v,U,W)-p\right|&=\sum_{\substack{W'\subseteq W\\ W'\neq\emptyset}}\sum_{\substack{U'\subseteq U\\ U'\neq\emptyset}}\left|\sum_v\chi\left(\prod_{z\in U'\cup W'}\chi(v-z)\right)\right|\\ &\leqslant\sum_{\substack{W'\subseteq W\\ W'\neq\emptyset}}\sum_{\substack{U'\subseteq U\\ U'\neq\emptyset}}(|U'|+|W'|-1)\sqrt{p}\\ &=(m2^{m-1}-2^m-1)\sqrt{p}.\end{aligned}$$

Seja S o número de vértices $v\notin U\cup W$ tais que $vu\in E\ (\forall u\in U)$ e $vw\notin E\ (\forall w\in W)$. Por definição,

$$2^mS=\left|\sum_{v\notin U\cup W}h(v,U,W)\right|\leqslant m2^{m-1}.$$

Como $\left|\sum_{v\in U\cup W}h(v,U,W)\right|\leqslant m2^{m-1}$,

$$\left|S-\frac{p}{2^m}\right|=\frac{1}{2^m}\left|\sum_{v\notin U\cup W}h(v,U,W)-p\right|\leqslant\frac{m}{2}+\frac{m-2}{2}\sqrt{p}.\qquad(101)$$

Exercício 115. Mostre os seguintes propriedades dos grafos de Paley

(i) Q_2^p é $(p-1)/2$-regular, vértices adjacentes têm $(q-5)/4$ vizinhos em comum e vértices não-adjacentes $(q-1)/4$. Também, existem $(q-1)/4$ vértices adjacentes a i e não adjacentes a j, para todos $i \neq j$ não-adjacentes.

(ii) Se $|U| + |W| = m < (1/4)\log p$ e S e como (101) acima, então Q_2^p contém uma cópia de todos os grafos de ordem m como subgrafo induzido.

Para $U, W \subseteq \mathbb{Z}_p$ disjuntos, vamos mostrar a discrepância na distribuição das arestas em $Q_2^p[U]$ e $Q_2^p[(U,W)]$. Para isso, começamos com um exercício cujas asserções serão usadas no próximo lema.

Exercício 116. Sejam χ e γ caracteres aditivo não-principal e multiplicativo, respectivamente, do $\mathbb{Z}_p$ e sejam $c \in \mathbb{Z}_p$ e $T \subseteq \mathbb{Z}_p$. Mostre que

(i) $\gamma(c)G(\chi,\overline{\gamma}) = \sum_x \overline{\gamma}(x)\chi(cx)$;

(ii) $\sum_x \left|\sum_{t\in T}\chi(tx)\right|^2 = p|T|$.

Lema 117. *Se γ é um caracter multiplicativo não-trivial de $\mathbb{Z}_p$ e $U, W \subset \mathbb{Z}_p$ então*

$$\left|\sum_{u\in U}\sum_{w\in W}\gamma(u-w)\right| \leqslant \sqrt{p|U||W|}. \tag{102}$$

Demonstração. Usando definições, o exercício anterior e a desigualdade de Cauchy-Schwarz

$$\begin{aligned}
\sqrt{p}\left|\sum_{u\in U}\sum_{w\in W}\gamma(u-w)\right| &= \left|G(\chi,\overline{\gamma})\sum_{u\in U}\sum_{w\in W}\gamma(u-w)\right| \\
&= \left|\sum_{u\in U}\sum_{w\in W}\sum_x \overline{\gamma}(x)\chi((u-w)x)\right| \\
&= \left|\sum_x \overline{\gamma}(x)\sum_{u\in U}\chi(ux)\sum_{w\in W}\overline{\chi}(wx)\right| \\
&\leqslant \sum_x \left|\sum_{u\in U}\chi(ux)\right|\left|\sum_{w\in W}\chi(wx)\right| \\
&\leqslant \left(\sum_x \left|\sum_{u\in U}\chi(ux)\right|^2\right)^{1/2}\left(\sum_x \left|\sum_{w\in W}\chi(wx)\right|^2\right)^{1/2} \\
&= q|U|^{1/2}|W|^{1/2},
\end{aligned}$$

a última linha é conseqüência do item (ii) do exercício. □

Corolário 118. *Se $U, W \subset \mathbb{Z}_p$ são disjuntos então*

$$\left| e_{Q_2^p}(U) - \frac{1}{2}\binom{|U|}{2} \right| \leqslant \frac{1}{4}|U|\sqrt{p}$$

e

$$\left| e_{Q_2^p}(U,W) - \frac{1}{2}|U||W| \right| \leqslant \frac{1}{2}\sqrt{p|U||W|}.$$

Terminamos este exemplo com duas observações. Primeiro, que Q_2^p difere do grafo aleatório de ordem p e probabilidade de aresta $1/2$, $G_{p,1/2}$, no seguinte: Graham and Ringrose (1990) provaram que o tamanho do clique máximo de Q_2^p é tão grande quanto $\log p \log\log\log p$ para infinitos valores de p, enquanto que o valor esperado de é $(1+o(1))\log p$ (Bollobás, 1985). □

Exemplo 119 (Grafos de Ramanujan). Seja G um grupo e $S \subseteq G$ um subconjunto finito de G tal que $S = S^{-1}$. O *grafo de Cayley* é o grafo $C(G,S)$ com $V(C) = G$ e

$$E(C) = \{\{g,h\} \subset G \colon gh^{-1} \in S\}.$$

Por exemplo, $C(\mathbb{Z}_d, \{-1,1\})$ é um circuito com d vértices e $C(\mathbb{Z}_2^n, \{e_i\}_{i=1}^n)$, para $e_i = (0,0,\ldots,1,\ldots,0)$, é o n-cubo.

Exercício 120. Determine os grafos $C(\mathbb{Z}_6, \{2,-2\})$ e $C(S^3, \{(123),(132),(12)\})$. O gupo S^3 é o das pemutações de três letras. Mostre que os grupos não são isomorfos e que os grafos de Cayley são isomorfos.

Exercício 121. Determine o grafo $C(\mathbb{Z}^2, \{(1,0),(-1,0),(0,1),(0,-1)\})$.

Não é difícil provar que o grafo $C(G,S)$

- é $|S|$-regular;
- não tem laço se, e somente se, a identidade e_G não pertence a S; e
- é conexo se, e somente se S gera G, ou seja, $g = s_1 \cdots s_2 \cdots s_k$, $s_i \in S$ para todo $i \in [k]$, para todo $g \in G$.

No caso de G ser abeliano, podemos determinar os autovlaores e autovetores do grafo de Cayley da seguinte forma. Se $A = A(C(G,S))$ é a matriz de adjacências indexada por G, χ um caracter de G e $\mathbf{v}_\chi = (\chi(g))_{g\in G}$ então

$$(A\mathbf{v}_\chi)_g = \sum_{h\in G}(A)_{g,h}\chi(h) = \sum_{h\in S-g}\chi(h) = \sum_{h\in S}\chi(h-g) = \left(\sum_{h\in S}\chi(h)\right)\chi(g).$$

Da ortogonalidade dos caracteres podemos concluir que

$$\lambda_\chi = \sum_{h\in S}\chi(h)$$

são os autovalores que corresponde aos autovetores $\mathbf{v}_\chi$ de A.

Por exemplo, para $p = 2nr + 1$ primo, e $S = Q_n$ as n-ésimas potências do $\mathbb{Z}_p$, temos $|\sum_x \chi(x^n)| \leqslant (n-1)\sqrt{p}$ e, portanto, os autovalores não triviais $|\lambda| = O(\sqrt{p})$. Por outro lado, um conhecido teorema de Alon e Boppana diz que esse resultado é ótimo. O seguinte exercício mostra uma versão mais fraca desse teorema.

Exercício 122. Seja G^n um grafo d-regular com autovalores $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$. Na posição i da diagonal de A^2 temos o grau do vértice i, logo $\mathrm{tr}(A^2) = nd$.

Mostre que $\mathrm{tr}(A^2) \leqslant d^2 + (n-1)\lambda^2$, onde $\lambda = \max\{|\lambda_2|, |\lambda_n|\}$. Conclua que $\lambda \geqslant (1 - o(1))\sqrt{d}$.

Com a notação acima, dizemos que um grafo d-regular é um *Grafo de Ramanujan* se

$$\lambda \leqslant 2\sqrt{d-1}.$$

Lubotzky et al. (1988) construíram grafos de Ramanujan como grafos de Paley definidos da seguinte maneira. Sejam p e q primos ímpares distintos. Seja $\mathrm{GL}(2,p)$ o grupo das matrizes 2×2 invertíveis com entradas do $\mathbb{Z}_p$ e $\mathrm{SL}(2,p)$ o grupo das matrizes 2×2 de determinante 1 com entradas do $\mathbb{Z}_p$. Como é usual, denotamos por $\mathrm{PGL}(2,p)$ o grupo quociente $\mathrm{GL}(2,p)$ módulo os múltiplos escalares da matriz identidade $\alpha\mathbf{I}$, e $\mathrm{PSL}(2,p)$ o grupo quociente $\mathrm{SL}(2,p)$ módulo

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Um teorema de Jacobi diz que um inteiro positivo n pode ser representado como soma de 4 quadrados de $8\sum_{d|n, 4\nmid d} d$ maneiras. Assim, existem $p+1$ seqüências (a_1, a_2, a_3, a_4) com $a_1 > 0$ ímpar e a_2, a_3, a_4 inteiros pares tais que $a_1^2 + a_2^2 + a_3^2 + a_4^2 = p$. A cada seqüência $\mathbf{a}$ associamos a matriz

$$\begin{pmatrix} a_1 + ia_2 & a_3 + ia_4 \\ -a_3 + ia_4 & a_1 - ia_2 \end{pmatrix}$$

de $\mathrm{PGL}(2,p)$, onde i é um inteiro tal que $i^2 \equiv -1 \pmod{p}$. Seja S o conjunto dessas $p+1$ matrizes.

Caso $(p/q) = 1$. O grafo $X^{p,q} = C(\mathrm{PGL}(2,p), S)$ é $(p+1)$-regular sobre $q(q^2-1)/2$ vértices com cada autovalor, além de $p+1$, é no máximo $2\sqrt{p}$.

Caso $(p/q) \neq 1$. O grafo $X^{p,q} = C(\mathrm{PSL}(2,p), S)$ é bipartido, $(p+1)$-regular sobre $q(q^2-1)$ vértices. Cada autovalor, além de $p+1$ e $-(p+1)$ é no máximo $2\sqrt{p}$.

A determinação do espectro desses grafos depende de uma boa estimativa para o número de soluções de sobre $a_1^2 + 4q^2a_2^2 + 4q^2a_3^2 + 4q^2a_4^2 = p^k$ dada

por Eichler e Igusa uma expressão para o número de soluções dessa equação quadrática em função dos autovalores de $X^{p,q}$. Os detalhes são bastante técnicos e podem ser vistos em (Lubotzky et al., 1988). □

Referências

Ajtai, M., Babai, L., Hajnal, P., Komlós, J., Pudlák, P., Rödl, V., Szemerédi, E., and Turán, G. (1986). Two lower bounds for branching programs. In *Proc. 18th STOC*, pages 30–38.

Ajtai, M. and Szemerédi, E. (1974). Sets of lattice points that form no squares. *Studia Sci. Math. Hungar.*, 9:9–11.

Alon, N., Duke, R. A., Lefmann, H., Rödl, V., and Yuster, R. (1994). The algorithmic aspects of the regularity lemma. *J. Algorithms*, 16(1):80–109.

Alon, N. and Yuster, R. (1992). Almost h-factors in dense graphs. *Graphs and Combinatorics*, 8:95–102.

Babai, L., Simonovits, M., and Spencer, J. (1990). Extremal subgraphs of random graphs. *J. Graph Theory*, 14(5):599–622.

Behrend, F. (1946). On sets of integers which contain no three terms in arihmetical progression. *Proc. Nat. Acad. Sci.*, 32:331–332.

Berlekamp, E. R. (1968). A construction for partitions which avoid long arithmetic progressions. *Canadian Mathematics Bulletin*, 11:409–414.

Bollobás, B. (1985). *Random graphs*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], London.

Bollobás, B. (1995). Extremal graph theory. In *Handbook of combinatorics, Vol. 1, 2*, pages 1231–1292. Elsevier, Amsterdam.

Bollobás, B. (1998). *Modern Graph Theory*. Springer-Verlag, New York.

Bollobás, B. and Erdős, P. (1976). On a Ramsey-Turán type problem. *J. Combin. Theory Ser. B*, 21:166–168.

Bourgain, J. (1999). On triples in arithmetic progression. *Geom. Funct. Anal.*, 9(5):968–984.

Chung, F. R. K. and Graham, R. L. (1991). Quasi-random set systems. *Journal of the American Mathematical Society*, 4(1):151–196.

Chung, F. R. K. and Graham, R. L. (1992). Quasi-random subsets of Z_n. *J. Combin. Theory Ser. A*, 61(1):64–86.

Chung, F. R. K., Graham, R. L., and Wilson, R. M. (1989). Quasi-random graphs. *Combinatorica*, 9(4):345–362.

Chvatál, C., Rödl, V., Szemerédi, E., and Trotter, Jr., W. T. (1983). The Ramsey number of a graph with bounded maximum degree. *J. Combin. Theory Ser. B*, 34(3):239–243.

Diestel, R. (1997). *Graph theory*. Springer-Verlag, New York. Translated from the 1996 German original.

Erdős, P., Hajnal, A., Sós, V., and Szemerédi, E. (1983). More results on Ramsey-Turán type problem. *Combinatorica*, 3(1):69–82.

Erdős, P. and Sós, V. (1969). Some remarks on Ramsey's and Turán's theorems. In et al., P. E., editor, *Combinatorics, Theory and Applications*, volume 4, pages 395–404, Ballatonfüred. Proceedings of the Colloquium on Mathematical Society János Bolyai.

Erdős, P. (1979). Some old and new problems in various branches of combinatorics. In *Proceedings of the Tenth Southeastern Conference on Combinatorics, Graph Theory and Computing*, pages 19–37, Florida Atlantic Univ., Boca Raton, Fla., 1979.

Erdős, P. and Simonovits, M. (1966). A limit theorem in graph theory. *Studia Sci. Math. Hungar*, 1:51–57.

Erdős, P. and Stone, A. H. (1946). On the structure of linear graphs. *Bull. Amer. Math. Soc.*, 52:1087–1091.

Frankl, P. and Rödl, V. (1986). Large triangle-free subgraphs in graphs without K_4. *Graphs Combin.*, 2(2):135–144.

Frankl, P. and Rödl, V. (2002). Extremal problems on set systems. *Random Structures Algorithms*, 20(2):131–164.

Füredi, Z. (1994). Random Ramsey graphs for the four-cycle. *Discrete Math.*, 126(1-3):407–410.

Furstenberg, H. (1977). Ergodic behaviour of diogonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse MAth.*, 31:204–256.

Gowers, W. T. (1997). Lower bounds of tower type for Szemerédi's uniformity lemma. *Geom. Funct. Anal.*, 7(2):322–337.

Gowers, W. T. (2001). A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588.

Gowers, W. T. (2005). Additive number theory examples sheet 3. www.dpmms.cam.ac.uk/˜wtg10/addnothex033.pdf.

Graham, R. L., Rödl, V., and Ruciński, A. (2000). On graphs with linear Ramsey numbers. *J. Graph Theory*, 35(3):176–192.

Graham, R. L., Rothschild, B. L., and Spencer, J. H. (1980). *Ramsey theory*. John Wiley & Sons Inc., New York. Wiley-Interscience Series in Discrete Mathematics, A Wiley-Interscience Publication.

Graham, S. W. and Ringrose, C. J. (1990). Lower bounds for least quadratic nonresidues. In *Analytic number theory (Allerton Park, IL, 1989)*, pages 269–309. Birkhäuser Boston, Boston, MA.

Green, B. (2005). A Szemerédi-type regularity lemma in abelian groups, with applications. *Geom. Funct. Anal.*, 15(2):340–376.

Green, B. and Tao, T. (2008). The primes contain arbitrarily long arithmetic progressions. *Annals of Math.*, 167(2):481–547.

Haxell, P. E., Kohayakawa, Y., and Łuczak, T. (1995). Turán's extremal problem in random graphs: forbidding even cycles. *J. Combin. Theory Ser. B*, 64(2):273–287.

Haxell, P. E., Kohayakawa, Y., and Łuczak, T. (1996). Turán's extremal problem in random graphs: forbidding odd cycles. *Combinatorica*, 16(1):107–122.

Hayes, T. (2003). A large deviation inequality for vector valued martingales. *Combinatorics, Probability and Computing*.

Ireland, K. and Rosen, M. (1990). *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition.

Kohayakawa, Y.; Rödl, V. (2003). Szemerédi's regularity lemma and quasi-randomness. In *Recent advances in algorithms and combinatorics*, volume 11 of *CMS Books Math./Ouvrages Math. SMC*, pages 289–351. Springer, New York.

Kohayakawa, Y. (1997). Szemerédi's regularity lemma for sparse graphs. In *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 216–230. Springer, Berlin.

Kohayakawa, Y. and Kreuter, B. (1997). Threshold functions for asymmetric Ramsey properties involving cycles. *Random Structures Algorithms*, 11(3):245–276.

Kohayakawa, Y., Łuczak, T., and Rödl, V. (1997). On K^4-free subgraphs of random graphs. *Combinatorica*, 17(2):173–213.

Komlós, J. (1999). The blow-up lemma. *Combin. Probab. Comput.*, 8(1-2):161–176. Recent trends in combinatorics (Mátraháza, 1995).

Komlós, J. (1999). The Blow-up Lemma. *Combinatorics, Probability and Computing*, 8:161–176.

Komlós, J., Sarkozy, G., and Szemerédi, E. (2001). Proof of the alon-yuster conjecture. *Discrete Mathematics*, 235:255–269.

Komlós, J. and Simonovits, M. (1996). Szemerédi's regularity lemma and its applications in graph theory. In *Combinatorics, Paul Erdős is eighty, Vol. 2 (Keszthely, 1993)*, pages 295–352. János Bolyai Math. Soc., Budapest.

Lubotzky, A., Phillips, R., and Sarnak, P. (1988). Ramanujan graphs. *Combinatorica*, 8(3):261–277.

Łuczak, T. (2000). On triangle-free random graphs. *Random Structures Algorithms*, 16(3):260–276.

Nagle, B., Rodl, V., and Schacht, M. (2005). The counting lemmafor k-regular uniform hypergraphs. *Randon Structures and Algorithms*. to appear.

Rödl, V. (1986). On universality of graphs with uniformly distributed edges. *Discrete Math.*, 59(1-2):125–134.

Rödl, V. and Skokan, J. (2004). Regularity lemma for k-uniform hypergraphs. *Random Struct. Algorithms*, 25(1):1–42.

Roth, K. F. (1953). On certain sets of integers. *J. London Math. Soc.*, 28:104–109.

Ruzsa, I. and Szemerédi, E. (1978). Triple systems with no six points carrying three triangles. In *Combinatorics (Proc. Fifth Hungarian Colloq., Keszthely, 1976)*, volume 18 of *Colloq. Math. Soc. János Bolyai*, pages 939–945, Amsterdam. North-Holland.

Sárközy, G. and Selkow, S. (2004). An extension of the Ruzsa-szemerédi theorem. *Combinatorica*, 25(1):77–84.

Shelah, S. (1988). Primitive recursive bounds for van der Waerden numbers. *J. Amer. Math. Soc.*, 1(3):683–697.

Simonovits, M. and Sós, V. T. (1991). Szemerédi's partition and quasirandomness. *Random Structures Algorithms*, 2(1):1–10.

Simonovits, M. and Sós, V. T. (2001). Ramsey-Turán theory. *Discrete Mathematics*, 229:293–340.

Solymosi, J. (2003). Note on a generalization of Roth's theorem. In *Discrete and Computational Geometry*, volume 25 of *Algorithms Comb.*, pages 825–837. Springer.

Solymosi, J. (2004). A note on a question of Erdős os and Graham. *Combinatorics, Probability and Computing*, 13:263–267.

Szemerédi, E. (1969). On sets of integers containing no four elements in arithmetic progression. *Acta Math. Acad. Sci. Hungar.*, 20:89–104.

Szemerédi, E. (1972). On graphs containing no complete subgraph with 4 vertices. *Mat. Lapok*, 23:113–116 (1973).

Szemerédi, E. (1975). On sets of integers containing no k elements in arithmetic progression. *Acta Arith.*, 27:199–245. Collection of articles in memory of Juriĭ Vladimirovič Linnik.

Szemerédi, E. (1978). Regular partitions of graphs. In *Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976)*, pages 399–401. CNRS, Paris.

van der Waerden, B. L. (1927). Beweis einer Baudetschen Vermutung. *Nieuw Archief voor Wiskunde*, 15:212–216.

Índice Remissivo