Versões Probabilísticas de Resultados da Teoria Combinatória dos Números

Bruno Fernandes Cerqueira Leite

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do grau
de
Mestre em Matemática

Área de Concentração: **Matemática**
Orientador: **Prof. Dr. Yoshiharu Kokayakawa**

Durante a elaboração deste trabalho, o autor recebeu
apoio financeiro da FAPESP (processo 02/10983-7).

São Paulo, dezembro de 2004

Versões Probabilísticas de Resultados da Teoria Combinatória dos Números

Este exemplar corresponde à redação final da dissertação de mestrado devidamente corrigida e defendida por Bruno F. C. Leite e aprovada pela comissão julgadora.

São Paulo, dezembro de 2004.

Banca examinadora:

- Prof. Dr. Yoshiharu Kohayakawa — IME-USP
- Prof. Dr. Carlos Gustavo Tamm de Araújo Moreira — IMPA
- Prof. Dr. Jozef Skokan — IME-USP

Para a Luciana

(seu apoio foi tão grande que eu
poderia citá-la como co-autora...)

Agradecimentos

Agradeço aos meus familiares, pela ajuda que me deram.

Agradeço aos professores Edson de Faria e Yoshiharu Kohayakawa, pela fantástica orientação que tive nestes últimos cinco anos.

Agradeço a todos os meus amigos (em particular, Mac e Roberta), pelo companheirismo e pelas alegrias que me proporcionaram.

Agradeço em especial à Luciana, pela imensa compreensão e paciência, e por ter estado sempre ao meu lado, mesmo nos momentos mais difíceis (que não foram poucos). Sem ela, a conclusão deste trabalho teria sido praticamente impossível.

Agradeço, por fim, à FAPESP, pelo apoio financeiro dado durante o mestrado e ao longo de dois projetos de Iniciação Científica.

$$\sum_{j=1}^{\infty} \frac{1}{j^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6} \qquad (!)$$

(Euler, 1736)

Resumo

Neste trabalho, provamos versões probabilísticas de dois teoremas clássicos da Teoria Combinatória dos Números: os Teoremas de Schur e de Sárközy.

Em 1916, Schur provou que se $\mathbb{N}$ é finitamente colorido, uma das cores contém uma solução da equação $x + y = z$. Nossa versão probabilística do Teorema de Schur é, na verdade, uma versão probabilística "de densidade" do Teorema de Schur. Ela afirma, grosso modo, que fixando-se $0 < \eta \leq 1/2$, um subconjunto "típico" X de $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ tem a seguinte propriedade: para todo subconjunto $D \subset X$ com $|D| \geq (1/2 + \eta)|X|$, existem $x, y, z \in D$ satisfazendo $x + y = z$.

Em 1978, Sárközy mostrou que se $A \subset \mathbb{N}$ é um subconjunto com densidade superior positiva, então $A-A$ contém um quadrado diferente de zero. Em nossa versão probabilística do Teorema de Sárközy, provamos que, fixado $0 < \eta \leq 1$, um subconjunto "típico" X de $\mathbb{Z}_n$ tem a seguinte propriedade: para todo subconjunto $D \subset X$ com $|D| \geq \eta|X|$, existem $x, y \in D$ tais que $x - y$ é um quadrado diferente de zero.

Observamos que os dois teoremas acima são especialmente interessantes quando consideramos subconjuntos esparsos de $\mathbb{Z}_n$, isto é, quando temos $|X| = o(n)$.

Os enunciados precisos destas versões são os teoremas 13 e 14 do presente trabalho. A noção formal do que é um subconjunto "típico" pode ser vista na definição 11. Generalizações dos resultados acima são discutidas nos capítulos 4 e 5.

Abstract

In this work, we prove probabilistic versions of two classical theorems from Combinatorial Number Theory: Schur's theorem and Sárközy's theorem.

In 1916, Schur proved that if $\mathbb{N}$ is finitely colored, then one of its colors contains a solution to the equation $x + y = z$. Our probabilistic version of Schur's theorem is actually a "density" probabilistic version of Schur's theorem. It states, roughly, that for a fixed $0 < \eta \leq 1/2$, a "typical" subset X of $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ has the following property: for every subset $D \subset X$ with $|D| \geq (1/2 + \eta)|X|$, there are $x, y, z \in D$ such that $x + y = z$.

In 1978, Sárközy showed that if $A \subset \mathbb{N}$ is a subset with positive upper density, then $A - A$ contains a square different from zero. In our probabilistic version of Sárközy's theorem, we prove that, given $0 < \eta \leq 1$, a "typical" subset $X \subset \mathbb{Z}_n$ has the following property: for every subset $D \subset X$ with $|D| \geq \eta|X|$, there are $x, y \in D$ such that $x - y$ is a square different from zero.

We observe that both theorems above are particularly interesting when we consider sparse subsets of $\mathbb{Z}_n$, that is, when we have $|X| = o(n)$.

The precise statements of these results are the theorems 13 and 14 of this work. The formal notion of what is a "typical" subset can be found in definition 11. Generalizations of the results above are discussed in chapters 4 and 5.

Conteúdo

Capítulo 1

Introdução

Neste trabalho, estamos interessados em investigar versões probabilísticas de teoremas clássicos da Teoria Combinatória dos Números. Dedicaremos especial atenção a dois problemas que resolvemos: provamos versões probabilísticas de densidade do Teorema de Schur e do Teorema de Sárközy.

1.1 Exemplos de versões probabilísticas

Como veremos a seguir, versões probabilísticas de muitos teoremas clássicos já foram estudadas. Como exemplo, examinaremos inicialmente os Teoremas de van der Waerden e Szemerédi.

Em 1927, van der Waerden provou o famoso teorema abaixo ([37]).

Teorema 1 (van der Waerden, 1927). *Qualquer partição de $\mathbb{N}$ em um número finito de partes é tal que alguma parte contém progressões aritméticas arbitrariamente longas.*

Erdős e Turán [9] conjecturaram uma versão mais forte que o Teorema de van der Waerden, a saber, eles conjecturam a "versão de densidade" do teorema 1: se uma parte dos inteiros é "grande", então ela contém progressões aritméticas arbitrariamente longas. Esta conjectura foi confirmada nesta generalidade apenas em 1975, por Szemerédi, através de seu célebre resultado:

Teorema 2 (Szemerédi, 1975). *Todo conjunto $A \subset \mathbb{N}$ com densidade superior positiva, isto é, com*

$$\bar{d}(A) = \limsup_{n\to\infty} n^{-1}|A \cap \{1, \ldots, n\}| > 0, \tag{1.1}$$

contém progressões aritméticas arbitrariamente longas.

No que se segue, será mais conveniente considerar as seguintes versões "finitas" dos teoremas 1 e 2.

Teorema 3 (van der Waerden, versão finita). *Para quaisquer inteiros positivos r e k, existe um inteiro $n_0 = n_0(r,k)$ com a seguinte propriedade: para todo $n \geq n_0$, toda partição de $[n] = \{1, \ldots, n\}$ em r partes é tal que alguma parte contém uma progressão aritmética com k elementos.*

Teorema 4 (Szemerédi, versão finita). *Para todo real $\eta > 0$ e inteiro positivo k, existe um inteiro $n_0 = n_0(\eta, k)$ com a seguinte propriedade: para todo $n \geq n_0$, todo conjunto $A \subset [n]$ com densidade pelo menos η, isto é,*

$$n^{-1}|A \cap [n]| \geq \eta, \tag{1.2}$$

contém uma progressão aritmética com k elementos.

Usando um resultado conhecido em combinatória como "princípio da compacidade" (veja o capítulo 1 de [15]), não é difícil estabelecer a equivalência entre as diferentes versões dos teoremas.

Será conveniente escrever

$$\Gamma \to (\mathrm{PA}_k)_r \tag{1.3}$$

se $\Gamma \subset \mathbb{N}$ satisfaz a propriedade descrita no teorema 3, isto é, se toda partição $\Gamma = U_1 \cup \cdots \cup U_r$ é tal que algum U_i contém uma progressão aritmética com k elementos. Em outras palavras: escrevemos (1.3) se para toda coloração de Γ com r cores (ou 'toda r-coloração de Γ'), existe uma progressão aritmética de tamanho k monocromática. Definimos de forma análoga a notação

$$\Gamma \to_\eta \mathrm{PA}_k \tag{1.4}$$

para todo conjunto $\Gamma \subset \mathbb{N}$ finito. Escrevemos (1.4) se todo $U \subset \Gamma$ com $|U| \geq \eta|\Gamma|$ contém uma progressão aritmética com k elementos.

Os teoremas 3 e 4 dizem que segmentos iniciais $\Gamma = [n]$ de $\mathbb{N}$ suficientemente grandes satisfazem as relações (1.3) e (1.4). Ao passarmos tais teoremas para o contexto de resultados probabilísticos, a pergunta essencial é a seguinte:

(*) *O que podemos dizer sobre conjuntos típicos $\Gamma \subset [n]$?*

Para podermos falar sobre "conjuntos típicos", definimos inicialmente uma distribuição de probabilidade sobre os subconjuntos de $[n]$. A distribuição mais simples que podemos considerar é a distribuição uniforme; na realidade, fixamos um inteiro $N \leq n$ e consideramos o conjunto $\binom{[n]}{N}$ de todos

os subconjuntos $\Gamma \subset [n]$ de cardinalidade N e o munimos com a medida de probabilidade uniforme. Escreveremos $[n]_N$ para um conjunto aleatório sorteado uniformemente ao acaso dentre todos os membros de $\binom{[n]}{N}$. Assim, para todo conjunto fixo $X \subset [n]$ com $|X| = N$, temos

$$\mathbb{P}([n]_N = X) = \binom{n}{N}^{-1}. \tag{1.5}$$

Os dois próximos resultados que enunciamos fornecem uma resposta a nossa pergunta acima (*). Observamos que o primeiro resultado, devido a Rödl e Ruciński [31], é um resultado que pode se considerar completo, pois trata da propriedade (1.3) para todo k e r.

Teorema 5 (Rödl e Ruciński, 1995). *Para todos inteiros $k \geq 3$ e $r \geq 2$, existem constantes positivas c e C tais que*

$$\lim_{n\to\infty} \mathbb{P}([n]_N \to (\mathrm{PA}_k)_r) = \begin{cases} 0 & \text{se } N \leq cn^{1-1/(k-1)}, \\ 1 & \text{se } N \geq Cn^{1-1/(k-1)}. \end{cases} \tag{1.6}$$

O teorema 5 afirma que ocorre uma transição quando a ordem de grandeza de N passa por $n^{1-1/(k-1)}$. Este fenômeno se repetirá em muitos outros teoremas deste tipo.

O segundo resultado probabilístico que enunciamos, provado em [24], é ainda parcial, pois trata da relação (1.4) apenas para $k = 3$.

Teorema 6 (Kohayakawa, Łuczak e Rödl, 1996). *Para todo real $\eta > 0$, existem constantes positivas c e C tais que*

$$\lim_{n\to\infty} \mathbb{P}([n]_N \to_\eta \mathrm{PA}_3) = \begin{cases} 0 & \text{se } N \leq cn^{1/2}, \\ 1 & \text{se } N \geq Cn^{1/2}. \end{cases} \tag{1.7}$$

A demonstração do teorema 6 é, infelizmente, bastante sutil e não parece admitir uma generalização simples para $k > 3$. O fato de se conhecer uma versão probabilística 'completa' do teorema 3, mas ter-se apenas uma tal versão para $k = 3$ do teorema 4 é razoável, pois, ao que tudo indica, o teorema 4 é substancialmente mais profundo que o teorema 3.

1.2 Os Teoremas de Schur e Sárközy

Em 1916, I. Schur provou o teorema a seguir:

Teorema 7 (Schur, 1916). *Para todo inteiro positivo r, vale o seguinte. Se $\mathbb{N}$ é colorido com r cores, então uma das cores contém uma solução da equação $x + y = z$.*

Diremos que $x + y = z$ é a equação de Schur, e uma tripla que satisfaz a equação de Schur será dita uma tripla de Schur. Usando o princípio da compacidade, pode-se obter a versão equivalente e "finita" do teorema acima:

Teorema 8 (Schur, versão finita). *Para todo inteiro positivo r, existe um inteiro n_0 tal que se $n \geq n_0$ e $[n] = \{1, 2, \ldots, n\}$ é colorido com r cores, então uma das cores contém uma tripla de Schur.*

De modo análogo às definições dadas em (1.3) e (1.4), definimos as notações

$$\Gamma \to (\text{Schur})_r \tag{1.8}$$

e

$$\Gamma \to_\eta (\text{Schur}) \tag{1.9}$$

para todo conjunto $\Gamma \subset \mathbb{N}$ finito (ou ainda $\Gamma \subset G$, com G grupo abeliano e Γ finito). Escrevemos (1.8) se toda partição $\Gamma = U_1 \cup \cdots \cup U_r$ é tal que algum U_i contém uma tripla de Schur, e escrevemos (1.9) se todo $D \subset \Gamma$ com $|D| \geq \eta|\Gamma|$ contém uma tripla de Schur. O Teorema de Schur diz que para todo r, existe $n_0 = n_0(r)$ tal que, se $n \geq n_0$, $[n] \to (\text{Schur})_r$.

Assim como o Teorema de van der Waerden tem sua versão de densidade (o Teorema de Szemerédi), podemos também provar uma versão de densidade para o Teorema de Schur:

Teorema 9 (Schur, versão densidade). *Para todo $0 < \eta \leq 1/2$, existe $n_0 \in \mathbb{N}$ tal que, se $n \geq n_0$, então $[n] \to_{1/2+\eta} (\text{Schur})$.*

Prova. A densidade não pode ser qualquer; de fato, se trocarmos '$1/2+\eta$' por alguma constante entre 0 e $1/2$, o teorema é falso. Para ver isso, considere o conjunto dos ímpares em $[2n]$, que tem densidade $1/2$ mas não tem triplas de Schur.

Tome $n_0 = n_0(\eta) = 1/\eta$ e fixe $n \geq n_0$. Suponha que $D \subset [n]$, $|D| \geq (1/2 + \eta)n$ e D não contém triplas de Schur. Seja $(D - D)^+ = \{d_1 - d_2 \colon d_1, d_2 \in D \text{ e } d_1 > d_2\}$. Note que $(D - D)^+ \subset [n]$ e

$$|(D - D)^+| \geq |D| - 1 \geq (1/2 + \eta - 1/n)n \geq n/2.$$

Como $|D| \geq (1/2 + \eta)n$, segue que existe $x \in D \cap (D - D)^+$, e portanto x escreve-se como $x = z - y$ onde $x, y, z \in D$. Mas então $x + y = z$, contradizendo o fato de D não ter triplas de Schur. □

No capítulo 4, iremos provar uma versão probabilística do teorema de Schur. Antes de chegarmos lá, temos um pequeno capítulo sobre quasi-aleatoriedade e um capítulo com resultados sobre regularidade.

Na seção inicial do capítulo 4, falaremos brevemente sobre o teorema principal do artigo [19]. Usaremos o mais importante resultado auxiliar da prova deste teorema (o lema dos pares proibidos) na seção 4.2, para provar a versão probabilística do Teorema de Schur de que já falamos. Antes de enunciarmos esta versão, veremos duas definições simples.

Definição 10. *Seja η real com $0 < \eta \leq 1/2$. Dizemos que $D \subset \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ tem a propriedade* Schur(η) *se $D \to_{1/2+\eta}$ (Schur).*

Ou seja, D tem a propriedade Schur(η) se qualquer subconjunto de D com densidade $1/2 + \eta$ tem uma solução da equação de Schur. Note que a soma é considerada módulo n.

Definimos abaixo o conceito de conjunto aleatório que usaremos ao longo de todo nosso trabalho.

Definição 11. *Dados $n \in \mathbb{N}$ e $0 \leq p \leq 1$, obtemos o subconjunto aleatório $\mathbb{Z}_{n,p} \subset \mathbb{Z}_n$ da seguinte forma: para cada $j \in \mathbb{Z}_n$, colocamos j em $\mathbb{Z}_{n,p}$ com probabilidade p e de modo independente. Ou seja, realizamos n sorteios independentes.*

Podemos agora enunciar o problema abaixo, que é bastante natural, tendo em vista as versões probabilísticas dos Teoremas de van der Waerden e Szemerédi:

Problema 12 (Problema Schur(η)**).** *Para todo $0 < \eta \leq 1/2$, existe uma constante $C = C(\eta)$ tal que, se $p = p(n) \geq Cn^{-1/2}$, então, com probabilidade tendendo a 1 quando $n \to \infty$, $\mathbb{Z}_{n,p}$ tem a propriedade* Schur(η).

No capítulo 4, iremos discutir os parâmetros do enunciado, esclarecendo perguntas razoáveis como "Por que, ao tratarmos da propriedade PA_3, a densidade pode ser qualquer $0 < \eta < 1$, enquanto que, neste problema, exige-se que a densidade seja maior que $1/2$?" ou "O que acontece se p for muito menor que $n^{-1/2}$?", etc.

Infelizmente, só conseguimos resolver uma versão um pouco mais fraca do problema 12, que enunciamos abaixo.

Teorema 13 (Teorema Schur(η)**).** *Para todo $0 < \eta \leq 1/2$, existe uma constante $C = C(\eta)$ tal que, se $p = p(n) \geq C \log n/\sqrt{n}$, então, com probabilidade tendendo a 1 quando $n \to \infty$, $\mathbb{Z}_{n,p}$ tem a propriedade* Schur(η).

Na seção 4.2, é dada uma prova do teorema 13. Se conseguíssemos provar a conjectura 55 (enunciada na seção 4.3), teríamos então uma prova para o

enunciado original (problema 12).

Na prova do teorema 13, mostramos que se S é um subconjunto de um conjunto aleatório de $\mathbb{Z}_n$, então $S - S = \{s_1 - s_2 \colon s_1, s_2 \in S\}$ tem uma certa propriedade interessante. Note que a estrutura de $S - S$ está claramente relacionada ao problema de Schur, pois se $(S-S) \cap S \neq \emptyset$, segue imediatamente que há uma solução da equação de Schur ($x+y = z$ ou $z-y = x$) em S. Conhecendo tal propriedade interessante, era natural investigarmos o mesmo tipo de problema mudando apenas a equação envolvida.

Seria interessante, por exemplo, provar algum teorema envolvendo a equação $x+y = 3z$, ou a equação $x-y = 3z$. Infelizmente, aqui nossas tentativas foram infrutíferas. No entanto, ao pensar na equação $x-y = z^2 \bmod n$ (n primo), obtivemos algum sucesso. Antes de detalhar isto, iremos definir as notações

$$\Gamma \to_\eta \text{Diferença}(S) \tag{1.10}$$

e

$$\Gamma \to_\eta \text{Soma}(S) \tag{1.11}$$

para todo conjunto $\Gamma \subset \mathbb{N}$ finito e todo $S \subset \mathbb{N}$ (ou ainda $\Gamma \subset G$, onde Γ é finito, G é um grupo abeliano ou um corpo e $S \subset G$). Escrevemos (1.10) se todo $D \subset \Gamma$ com $|D| \geq \eta|\Gamma|$ contém x, y com $x - y \in S$, e escrevemos (1.11) se todo $D \subset \Gamma$ com $|D| \geq \eta|\Gamma|$ contém x, y com $x + y \in S$.

No teorema abaixo, n percorrerá somente os primos de $\mathbb{N}$. Definimos $\text{Quad}(n) \subset \mathbb{Z}_n$ como o conjunto dos quadrados não-nulos módulo n, ou seja, $\text{Quad}(n) = \{1^2 \bmod n, 2^2 \bmod n, \ldots, (n-1)^2 \bmod n\}$. Usaremos no capítulo 5 o fato (simples) que $|\text{Quad}(n)| = (n-1)/2$, quando n é primo ímpar.

Teorema 14 (Sárközy probabilístico). *Para todos $0 < \eta, \gamma < 1$, existem constantes $C = C(\eta, \gamma)$ e $n_0 = n_0(\eta, \gamma)$ tais que, se $p = p(n) \geq C/n$ e se n é um primo com $n \geq n_0$, então, com probabilidade pelo menos $1 - \gamma$, temos que*

$$\mathbb{Z}_{n,p} \to_\eta \textit{Diferença}(\text{Quad}(n))$$

(as operações são feitas módulo n).

Conseguimos provar o teorema 14 usando um resultado muito recente e ainda não publicado de Gerke, Kohayakawa, Rödl e Steger ([12]) que trata de herança de regularidade (tudo isto será esclarecido mais adiante). No capítulo 5, enunciaremos este resultado sobre herança de regularidade, e veremos como empregá-lo para demonstrar o teorema 14.

Uma outra versão do teorema acima, aparentemente bem mais difícil, seria exigir que o z ou o z^2 (da equação $x - y = z^2 \bmod n$) esteja também

contido na η-fração de $\mathbb{Z}_{n,p}$, assim como x e y. Chamaremos esta versão de "versão difícil do problema de Sárközy".

O nome "Sárközy" está sendo citado em menção ao seguinte teorema ([33], veja também [11]):

Teorema 15 (Sárközy, 1978). *Se $A \subset \mathbb{N}$ é um conjunto com densidade superior positiva, então $A - A$ contém um quadrado diferente de* 0.

Lembramos que a densidade superior de um conjunto $A \subset \mathbb{N}$ foi definida pela equação 1.1.

Ainda com relação ao teorema 14, veremos que ele seguirá imediatamente de um teorema mais geral, e veremos que este teorema mais geral nos renderá outros resultados interessantes. Detalharemos tudo isso no capítulo 5. Por fim, no capítulo 6 fazemos algumas últimas considerações e enunciamos alguns problemas correlatos que não soubemos resolver.

Para fechar a introdução, desejamos justificar o motivo do interesse nas equações que estudamos.

1.3 Por que o interesse nas equações $x + y = z$ e $x - y = z^2$?

Nesta seção, damos um breve panorama do que já foi feito na área de versões probabilísticas de resultados da Teoria Combinatória dos Números, e aproveitamos para dar uma breve justificativa sobre o interesse nas equações $x + y = z$ e $x - y = z^2$. Como o leitor poderá conferir nesta seção, muita coisa já foi feita na área de sistemas lineares, e, por isso, ao estudarmos a equação $x - y = z^2$, tentamos estudar algo aparentemente novo, e não excessivamente difícil. Já o estudo da equação de Schur justifica-se pelo fato de ela ser a mais simples equação que é P-regular mas não D-regular (estas definições encontram-se logo adiante), e pelo fato de já existirem teoremas probabilísticos que versam sobre equações (ou sistemas lineares de equações) D-regulares, ao passo que o problema análogo para equações (ou sistemas) P-regulares está em aberto.

Vamos começar a esclarecer isto citando dois resultados determinísticos: o Teorema de Rado e o Teorema de Frankl, Rödl e Graham.

1.3.1 Resultados determinísticos: os Teoremas de Rado e de Frankl–Graham–Rödl

O teorema 5 não é a versão mais geral do que se conhece nesta direção. De fato, pelo menos em certos casos, é conhecida uma versão probabilística do

célebre Teorema de Rado [30], que generaliza o Teorema de van der Waerden.

Seja $A = (a_{ij})$ uma matriz $k \times l$ com entradas inteiras, e seja $\mathcal{L}(A)$ o sistema de equações

$$A\mathbf{x} = \mathbf{0}. \tag{1.12}$$

Dizemos que A é *regular em relação a partições de* $\mathbb{N}$, ou *P-regular para* $\mathbb{N}$, se para todo natural r e toda partição $\mathbb{N} = U_1 \cup \cdots \cup U_r$, existe $\mathbf{x} \in \mathbb{N}^l$ com todas as suas entradas em algum U_i tal que $A\mathbf{x} = \mathbf{0}$. Isto é, A é P-regular para $\mathbb{N}$ se qualquer partição finita de $\mathbb{N}$ é tal que o sistema $\mathcal{L}(A)$ admite uma solução inteiramente contida em uma das partes.

Rado [30] caracterizou as matrizes P-regulares, generalizando amplamente o resultado de van der Waerden. Para formularmos o resultado de Rado, precisamos introduzir uma nova definição.

Sejam $\mathbf{a}_j$ $(1 \leq j \leq l)$ as colunas de A. Dizemos que A satisfaz a *propriedade das colunas* se podemos reordenar as colunas de A de forma que, para algum s, existam $0 = l_0 < \cdots < l_s = l$ tais que se

$$\mathbf{b}_j = \sum\{\mathbf{a}_{j'} : l_{j-1} < j' \leq l_j\} \qquad (1 \leq j \leq s),$$

então

(i) $\mathbf{b}_1 = \mathbf{0}$

e

(ii) para todo $1 < j \leq s$, o vetor $\mathbf{b}_j$ é uma combinação linear sobre $\mathbb{Q}$ dos vetores $\mathbf{a}_{j'}$ $(j' \leq l_{j-1})$.

O célebre resultado de Rado é o seguinte.

Teorema 16 (Rado, 1937). *A matriz A é P-regular para $\mathbb{N}$ se e só se A satisfaz a propriedade das colunas.*

É fácil verificar que o teorema 16 generaliza o Teorema de van der Waerden. De fato, para se obter o Teorema de van der Waerden a partir do Teorema de Rado, basta considerar a matriz correspondente ao sistema

$$x_1 - 2x_2 + x_3 = \cdots = x_{k-2} - 2x_{k-1} + x_k = 0. \tag{1.13}$$

Uma generalização análoga para o Teorema de Szemerédi, que examinaremos a seguir, foi obtida por Frankl, Graham, e Rödl [10].

Uma matriz A é dita *regular em relação a densidade para* $\mathbb{N}$, ou *D-regular para* $\mathbb{N}$, se todo conjunto $S \subset \mathbb{N}$ com densidade superior positiva, isto é, com

$$\bar{d}(S) = \limsup_{n\to\infty} n^{-1}|S \cap [n]| > 0, \tag{1.14}$$

é tal que (1.12) admite uma solução $\mathbf{x}$ com todas as suas entradas em S. Segue que uma matriz D-regular é P-regular.

Diremos que uma matriz A é *irredundante* se (1.12) não implicar que $\mathbf{x}$ tem duas entradas x_i e x_j (com $i \neq j$) tais que $x_i = x_j$. Diremos que uma solução $\mathbf{x} = (x_1, \ldots, x_l)$ é *própria* se todos os x_i forem distintos.

No que segue, o caso das matrizes redundantes não nos interessará. Frankl, Graham, e Rödl [10] provaram o seguinte resultado.

Teorema 17 (Frankl, Graham e Rödl, 1988). *Uma matriz irredundante tem uma solução própria em cada conjunto $S \subset \mathbb{N}$ com densidade superior positiva se e só se a soma de suas colunas é nula.*

O teorema 17 generaliza o Teorema de Szemerédi (veja (1.13)); entretanto, observamos que a prova do teorema 17 usa o Teorema de Szemerédi.

1.3.2 Versões probabilísticas: resultados de Graham, Rödl e Ruciński

Uma generalização impressionante do teorema 5 é o teorema 18, devido a Rödl e Ruciński [32]. Se $\Gamma \subset \mathbb{N}$ e A é uma matriz inteira, generalizando (1.3), escrevemos

$$\Gamma \to (A)_r \tag{1.15}$$

se toda partição $\Gamma = U_1 \cup \cdots \cup U_r$ de Γ em r partes é tal que (1.12) admite uma solução $\mathbf{x}$ com todas as suas entradas em algum U_i.

Precisamos ainda definir um parâmetro $m(A)$ para matrizes A; este parâmetro mede, de certa forma, o grau de liberdade que temos para obter soluções de (1.12). Observamos que a definição exata deste parâmetro não é muito importante, pelo menos em uma primeira leitura; é suficiente observar que $m(A)$ é um real satisfazendo $0 < m(A) \leq 1$, que depende apenas de A.

Se Q é um subconjunto de colunas de A, escrevemos $h(Q)$ para o posto da matriz que obtemos ao eliminar as colunas em Q de A. Pomos

$$m(A) = \max_q \max_Q \frac{q-1}{q-1+h(Q)-k}, \tag{1.16}$$

onde o primeiro máximo é tomado sobre todos os inteiros $1 \leq q \leq l$ e o segundo máximo é tomado sobre todos os conjuntos de colunas Q com $|Q| = q$. No caso da matriz A do sistema (1.13), um argumento simples, mas que omitimos, mostra que $m(A) = k - 1$.

Teorema 18 (Rödl e Ruciński, 1997). *Sejam A uma matriz D-regular para $\mathbb{N}$ e r um inteiro positivo. Existem constantes positivas c e C tais que*

$$\lim_{n\to\infty} \mathbb{P}([n]_N \to (A)_r) = \begin{cases} 0 & \text{se } N \leq cn^{1-1/m(A)}, \\ 1 & \text{se } N \geq Cn^{1-1/m(A)}. \end{cases} \tag{1.17}$$

No teorema 18, o caso em que a matriz A é apenas regular em relação a partições de $\mathbb{N}$ encontra-se em aberto.

Conjectura 19 (Rödl e Ruciński, 1997). *O Teorema 18 é também válido para matrizes A regulares em relação a partições de $\mathbb{N}$.*

A matriz mais simples que é P-regular mas não é D-regular é a matriz correspondente à equação $x + y - z = 0$. O fato dessa matriz ser P-regular é exatamente o conteúdo do Teorema de Schur (teorema 7).

Um passo na direção da conjectura 19 é o seguinte resultado, devido a Graham, Rödl, e Ruciński [14]. Abaixo, escrevemos

$$\Gamma \to (\text{Schur})_r \tag{1.18}$$

se toda partição de Γ em r partes é tal que a equação $x + y = z$ é solúvel em alguma das partes.

Teorema 20 (Graham, Rödl e Ruciński, 1996). *Temos*

$$\lim_{n\to\infty} \mathbb{P}([n]_N \to (\text{Schur})_2) = \begin{cases} 0 & \text{se } N/n^{1/2} \to 0, \\ 1 & \text{se } N/n^{1/2} \to \infty. \end{cases} \tag{1.19}$$

Finalmente, observamos que no caso de matrizes D-regulares, um resultado mais forte que aquele do Teorema 18 pode ser verdade. De fato, podemos levantar o seguinte problema. Generalizando (1.4), dados uma matriz A, um real $\eta > 0$, e $\Gamma \subset \mathbb{N}$, escrevemos

$$\Gamma \to_\eta A \tag{1.20}$$

se todo conjunto $U \subset \Gamma$ com $|U| \geq \eta|\Gamma|$ contém uma solução de (1.12).

Problema 21. *Sejam A uma matriz D-regular para $\mathbb{N}$ e η um real positivo. Prove que existem constantes positivas c e C tais que*

$$\lim_{n\to\infty} \mathbb{P}([n]_N \to_\eta A) = \begin{cases} 0 & \text{se } N \leq cn^{1-1/m(A)}, \\ 1 & \text{se } N \geq Cn^{1-1/m(A)}. \end{cases} \tag{1.21}$$

Dado o grau de dificuldade das conjecturas acima enunciadas, resolvemos atacar problemas mais simples. Mesmo com essa opção, o material novo que obtivemos (o conteúdo das seções 4.2, 4.3, 5.1, 5.2 e 5.3) já é um pouco complicado tecnicamente.

Capítulo 2

Quasi-aleatoriedade em $\mathbb{Z}_n$ e em grafos

O objetivo deste capítulo é definir quasi-aleatoriedade e enunciar o teorema principal de [5]. Vamos começar com uma discussão bastante simplificada e informal.

Digamos que em algum concurso da loto (onde os números vão de 1 a 50 e cada apostador escolhe 6 números) o resultado do sorteio seja $\{1, 2, 3, 4, 5, 6\}$. Qualquer pessoa diria que tal evento "nunca ocorre" ou "é impossível". De fato, apesar de sabermos que $\{1, 2, 3, 4, 5, 6\}$ tem a mesma probabilidade que $\{4, 9, 17, 26, 32, 49\}$, temos alguma "sensação" de que o último evento é "mais razoável" que o primeiro.

Intuitivamente, um conjunto "com cara de aleatório" deve "ser aprovado" em alguns testes de aleatoriedade. Por exemplo, um conjunto S "com cara de aleatório" em $\{1, 2 \ldots, 50\}$ deve ter a propriedade que $\sum_{s\in S} e^{2\pi is/50}$ é "pequeno", ou seja, os vetores $(e^{2\pi is/50})_{s\in S}$ devem estar bem distribuídos em $S^1 = \{x \in \mathbb{C} \colon |x| = 1\}$, e não todos concentrados em alguma direção. Note que (sempre intuitivamente!) esse critério já exclui a possibilidade de que $\{1, 2, 3, 4, 5, 6\}$ tenha "cara de aleatório", uma vez que os vetores $(e^{2\pi is/50})_{s\in\{1,2,3,4,5,6\}}$ estão todos apontando em direções próximas.

Vamos olhar agora para subconjuntos de $\mathbb{Z}_n$. Dado $S \subset \mathbb{Z}_n$, gostaríamos de poder dizer objetivamente se S "se parece" com um subconjunto aleatório $\mathbb{Z}_{n,p} \subset \mathbb{Z}_n$. Isto é, seria interessante conhecer algumas propriedades de conjuntos aleatórios que, de certa forma, os caracterizam. Dito de outra maneira, queremos propriedades que "captem" a aleatoriedade de um conjunto aleatório.

Vamos dar um exemplo. É fácil ver que o tamanho esperado de $\mathbb{Z}_{n,p}$ é

np, e que o tamanho esperado da interseção de dois conjuntos $\mathbb{Z}_{n,p}$ sorteados independentemente é np^2. Dados $S \subset \mathbb{Z}_n$ e $x \in \mathbb{Z}_n$, defina $S+x = \{s+x\colon s \in S\}$. Para p fixo, uma propriedade que "quase todos" os conjuntos $\mathbb{Z}_{n,p}$ possuem é a seguinte: para "quase todo" $x \in \mathbb{Z}_n$, $\big||\mathbb{Z}_{n,p} \cap (\mathbb{Z}_{n,p} + x)| - np^2\big|$ é "pequeno".

Podemos assim enunciar um outro critério de quasi-aleatoriedade: para que um conjunto $S \subset \mathbb{Z}_n$ com $|S| = pn$ seja considerado "com cara de aleatório", $\big||S \cap (S + x)| - np^2\big|$ deve ser "pequeno" para "quase todo" x.

Naturalmente, os exemplos acima são bastante simplificados e servem apenas para introduzir o conceito de quasi-aleatoriedade. Veremos logo abaixo que um conjunto será dito quasi-aleatório quando ele satisfaz uma série de critérios (como os acima) para ter "cara de aleatório". Naturalmente, os critérios devem ser satisfeitos por quase todo conjunto aleatório. Assim, apesar de não ser aleatório, um conjunto quasi-aleatório "comporta-se" como se o fosse, já que tem muitas propriedades de conjuntos aleatórios.

O que Chung e Graham fizeram em [5] foi, basicamente, listar alguns critérios de quasi-aleatoriedade e provar o seguinte teorema: se um conjunto satisfaz um desses critérios, então ele satisfaz todos os outros. Ou seja, são todos critérios equivalentes. O teorema é extremamente surpreendente, pois a primeira impressão que se tem é que não há relação clara entre os critérios propostos.

Dizendo deste modo, pode parecer que o artigo de Chung e Graham é extremamente simples, o que é falso. A prova da equivalência dos critérios não é trivial, e, mais ainda, a grande dificuldade está em achar critérios que não sejam nem fracos nem fortes demais. Por exemplo, considere o critério C definido da seguinte forma: $S \subset \mathbb{Z}_n$ satisfaz C se e só se $|S \cap \{1, 2, \ldots, \lfloor n/2 \rfloor\}| = |S|/2 + o(n)$ (onde pensamos em $\{1, 2, \ldots, \lfloor n/2 \rfloor\}$ como subconjunto de $\mathbb{Z}_n$ e não de $\mathbb{Z}$). É fácil provar que quase todo conjunto aleatório $\mathbb{Z}_{n,1/2}$ satisfaz C, mas é claro (intuitivamente) que C é uma propriedade fraca demais para "captar" o "grau de aleatoriedade" de um conjunto.

Enunciaremos o teorema principal de [5] formalmente. Para $S \subset \mathbb{Z}_n$, seja χ_S a função indicadora de S (χ_S vale 1 em S e 0 fora de S). Definimos o grafo de Chung-Graham de S, $\mathrm{CG}(S) = \mathrm{CG}_n^+(S)$, como o grafo que tem $\mathbb{Z}_n$ como conjunto de vértices e $\{\{i, j\}\colon i+j \in S\}$ como conjunto de arestas. Lembramos que as somas são sempre consideradas módulo n. Dados $S, T \subset \mathbb{Z}_n$, denotamos $s = |S|$ e $t = |T|$.

Listamos abaixo propriedades que um certo conjunto $S \subset \mathbb{Z}_n$ poderia possuir. Para este S, escreveremos simplesmente χ em vez de χ_S. Por "quase todo $x \in X$", deve-se entender "para todos os elementos de X,

exceto no máximo $o(|X|)$". Como dissemos, Chung e Graham provaram que estas propriedades são todas equivalentes. Dado que todas as propriedades envolvem a notação assintótica "o pequeno", $o(.)$, é conveniente explicarmos melhor o que queremos dizer com "a propriedade P implica a propriedade P'". Cada uma das ocorrências de $o(1)$ (digamos) pode ser substituída por alguma função $f(n)$ apropriada, e que vai a 0 quando $n \to \infty$. Nesse sentido, escrever $P \Rightarrow P'$ significa que se $S \subset \mathbb{Z}_n$ satisfaz $P = P(f(n))$, então também deve satisfazer $P' = P'(f'(n))$.

Para compreender melhor as três últimas propriedades é necessário saber o que é um grafo quasi-aleatório. Veremos isto logo a seguir.

Vamos às propriedades.

1. (WT) — Weak translation. Para quase todo $x \in \mathbb{Z}_n$,
$$|S \cap (S + x)| = s^2/n + o(n).$$

2. (ST) — Strong translation. Para todo $T \subset \mathbb{Z}_n$ e quase todo $x \in \mathbb{Z}_n$,
$$|S \cap (T + x)| = st/n + o(n).$$

3. $(P(k))$ — k-pattern. Para todo k fixo e para quase todos $u_1, \ldots, u_k \in \mathbb{Z}_n$,
$$\sum_x \prod_{j=1}^{k} \chi(x + u_j) = s^k/n^{k-1} + o(n).$$

4. $(R(k))$ — k-representation. Para todo k fixo e para quase todo $x \in \mathbb{Z}_n$,
$$\sum_{u_1+\cdots+u_k=x} \prod_{j=1}^{k} \chi(u_j) = s^k/n + o(n^{k-1}).$$

5. (EXP) — Exponential sum. Para todo $j \neq 0$ em $\mathbb{Z}_n$,
$$\sum_{x \in \mathbb{Z}_n} \chi(x) \exp\left(\frac{2\pi i j x}{n}\right) = o(n).$$

6. (GRAPH) — Quasi-random graph. O grafo $\mathrm{CG}(S)$ é quasi-aleatório.

7. $(C(2t))$ — $2t$-cycle.
$$\sum_{x_1,\ldots,x_{2t}} \chi(x_1+x_2)\chi(x_2+x_3)\ldots\chi(x_{2t-1}+x_{2t})\chi(x_{2t}+x_1) = s^{2t}+o(n^{2t}).$$

8. (DENSITY) — Relative Density. Para todo $T \subset \mathbb{Z}_n$,

$$\sum_{x,y} \chi_T(x)\chi_T(y)\chi_S(x+y) = st^2/n + o(n^2).$$

Não daremos aqui a prova da equivalência entre todas estas propriedades. A demonstração pode ser encontrada em [5].

Vamos agora definir informalmente quasi-aleatoriedade em grafos. Estaremos interessados em critérios satisfeitos por grafos aleatórios. O modelo de grafo aleatório que usaremos neste trabalho será sempre o modelo binomial, que definimos a seguir. Um grafo aleatório $G_{n,p}$ é um grafo com n vértices em que cada uma das $\binom{n}{2}$ arestas entra no grafo com probabilidade p, de modo independente das demais. Denotamos por $\mathcal{G}(n,p)$ o espaço de probabilidade resultante. Para mais informações sobre grafos aleatórios, damos duas referências: [4] e [22].

A idéia geral para se definir quasi-aleatoriedade em grafos é a mesma do caso em $\mathbb{Z}_n$: lista-se um série de propriedades que se espera de um grafo aleatório, prova-se que são todas equivalentes (no sentido explicado acima), e define-se um grafo como sendo quasi-aleatório se e só se ele satisfaz uma das propriedades (e portanto, satisfaz todas). Em 1989, este roteiro foi seguido por Chung, Graham e Wilson [6] e sete critérios foram propostos para dizer se um grafo G com n vértices tem "cara" de $G_{n,1/2}$ (só foi tratado o caso $p = 1/2$). Enunciamos dois dos critérios de [6], apenas a título de exemplo.

As propriedades abaixo se referem a um grafo $G = (V, E)$ com n vértices. Para $U \subset V(G)$, $G[U]$ é o grafo induzido por U, isto é, o grafo com $V(G[U]) = U$ e $E(G[U]) = E(G) \cap \binom{U}{2}$ ($\binom{U}{2}$ é o conjunto de todos os subconjuntos de U com 2 elementos).

1. Para todo $S \subset V(G)$, o grafo induzido por S tem $|S|^2/4 + o(n^2)$ arestas.

2. Para $v \in V(G)$, seja $\Gamma(v)$ o conjunto dos vizinhos de v em G. Então

$$\sum_{v_1,v_2 \in V(G)} \Big| |\Gamma(v_1) \cap \Gamma(v_2)| - n/4 \Big| = o(n^3).$$

Para encerrar, desejamos dizer que de especial interesse para nós é a equivalência entre os critérios (EXP) e (GRAPH) para quasi-aleatoriedade em $\mathbb{Z}_n$. Grosso modo, temos que se S tem seus coeficientes de Fourier pequenos (isto é, satisfaz (EXP)), então $\mathrm{CG}(S)$ tem certas propriedades especiais, que não detalharemos agora. A relação entre estes dois critérios será vista com mais atenção na seção 3.2.

Capítulo 3

Regularidade em grafos

A noção de regularidade é central em nosso trabalho. Abstratamente falando, um grafo G tem propriedades de regularidade quando para todos $U, W \subset V(G)$ com $|U|$ e $|W|$ "grandes", temos algum tipo de informação sobre o número de arestas em G entre U e W.

Vamos fixar a notação para o capítulo. Seja $G = G^n$ um grafo com n vértices. Para $U, W \subset V(G)$ com $U \cap W = \emptyset$, escrevemos $E(U, W) = E_G(U, W)$ para denotar o conjunto das arestas de G que ligam U a W. Colocamos $e(U, W) = e_G(U, W) = |E_G(U, W)|$.

Começamos definindo o conceito de η-regularidade.

3.1 η-Regularidade

Definição 22. *Suponha que $0 < \eta \leq 1$ e $0 < p \leq 1$. Dizemos que um grafo G com n vértices é η-regular com densidade p se para todos $U, W \subset V(G)$ com $U \cap W = \emptyset$ e $|U|, |W| \geq \eta n$ temos*

$$\big|e_G(U, W) - p|U||W|\big| \leq \eta p|U||W|.$$

O lema 24 mostra que grafos aleatórios $G_{n,p}$ são muito provavelmente η-regulares, desde que $d = np$ seja suficientemente grande. Lembramos que $G_{n,p}$ é o grafo aleatório em n vértices em que cada uma das $\binom{n}{2}$ arestas entra no grafo com probabilidade p e de modo independente das demais arestas.

Antes de enunciar e provar o lema 24, vamos deixar registrado um resultado que usaremos frequentemente neste trabalho. Trata-se de uma forma da desigualdade de Hoeffding (veja as desigualdades 5.5 e 5.6 de [28]), que estima a probabilidade de uma certa soma de variáveis aleatórias desviar-se muito de sua média:

Lema 23 (Desigualdade de Hoeffding). *Sejam $X_1, X_2, \ldots, X_n$ variáveis aleatórias independentes com $0 \leq X_j \leq 1$ para todo j, e sejam $Y = \sum_{j=1}^{n} X_j$ e $y = E[Y]$. Então, para todo $0 < t < 1$ temos*

$$\mathbb{P}\Big(Y - y \geq ty\Big) \leq \exp\Big(\frac{-t^2 y}{3}\Big),$$

$$\mathbb{P}\Big(Y - y \leq -ty\Big) \leq \exp\Big(\frac{-t^2 y}{2}\Big)$$

e, finalmente,

$$\mathbb{P}\Big(|Y - y| \geq ty\Big) \leq 2\exp\Big(\frac{-t^2 y}{3}\Big).$$

Aplicaremos a desigualdade de Hoeffding na demonstração do lema a seguir.

Lema 24. *Fixe $0 < \eta \leq 1$ e considere o grafo aleatório $G_p = G_{n,p} \in \mathcal{G}(n,p)$ com $0 < p = p(n) < 1$. Seja $d = d(n) = np(n)$. Então, existe uma constante $d_0 = d_0(\eta)$ tal que, se $d > d_0$, quase todo G_p é η-regular com densidade p.*

Prova. Veremos que podemos escolher $d_0(\eta) = 6/\eta^4$. Fixe um grafo G e fixe também $U, W \subset V(G)$ com $U \cap W = \emptyset$ e $|U|, |W| \geq \eta n$. Por Hoeffding, a probabilidade de que tenhamos $\big|e_G(U,W) - p|U||W|\big| \geq \eta p|U||W|$ é no máximo $2\exp(-\eta^2 p|U||W|/3) \leq 2\exp(-\eta^4 pn^2/3) = 2\exp(-\eta^4 dn/3)$. Com isso, a probabilidade de haver um par (U,W) que viole a condição de η-regularidade é no máximo

$$2^n 2^n \, 2\exp(-\eta^4 dn/3) \leq 2\exp(2n - \eta^4 dn/3).$$

Esta última exponencial vai a zero quando $n \to \infty$, se $d > d_0(\eta) = 6/\eta^4$. □

Agora, definiremos uma outra condição de regularidade para grafos, mais forte que a η-regularidade. Novamente, seja $d = np$.

Definição 25. *Seja $G = G^n$ um grafo com n vértices, e suponha $A > 0$, $p > 0$. Seja $d = pn$. Dizemos que G é (p, A)-uniforme se, para todos os conjuntos $U, W \subset V(G)$ com $U \cap W = \emptyset$, temos*

$$\big|e_G(U,W) - p|U||W|\big| \leq A\sqrt{d|U||W|}.$$

Dentro do espírito desta seção, observamos que um nome mais adequado para a propriedade acima seria (p, A)-regularidade, mas nos decidimos por "uniformidade" simplesmente para manter o termo que já está em uso na literatura. O próximo lema é uma observação trivial, mas que desejamos deixar registrada.

Lema 26. *Se $p \geq A^2/(\eta^4 n)$ e $G = G^n$ é um grafo (p, A)-uniforme com n vértices, então G é η-regular com densidade p.*

Prova. Sejam $U, W \subset V(G)$ com $|U|, |W| \geq \eta n = \eta |V(G)|$. Temos que

$$A\sqrt{pn|U||W|} \leq \eta p|U||W| \Leftrightarrow A^2 n \leq \eta^2 p|U||W|.$$

Mas, de fato, temos $\eta^2 p|U||W| \geq \eta^2(\eta n)^2 A^2/(\eta^4 n) = A^2 n$, como queríamos. □

Nos próximos lemas, estimaremos $e(G[U])$ (número de arestas do grafo induzido por U) quando U é um subconjunto de vértices de um grafo com propriedades de regularidade. Escrevemos $O_1(x)$ para denotar um termo y que satisfaz $|y| \leq x$.

Lema 27. *Seja G um grafo. Para todo $U \subset V(G)$, temos*

$$e(G[U]) = \frac{\binom{u}{2}}{\lfloor u/2 \rfloor \lceil u/2 \rceil} \operatorname{Med}_S e_G(S, U \setminus S), \tag{3.1}$$

onde $u = |U|$ e $\operatorname{Med}_S e_G(S, U \setminus S)$ é a média de $e_G(S, U \setminus S)$ quando S percorre todos os subconjuntos $S \subset U$ de tamanho $|S| = \lfloor u/2 \rfloor$.

Prova. Fixe $U \subset V(G)$ e note que

$$\sum_S{}^* e_G(S, U \setminus S) = m e(G[U]), \tag{3.2}$$

onde a soma com estrela é sobre todos os subconjuntos $S \subset U$ de tamanho $|S| = \lfloor u/2 \rfloor$, e m é o número de vezes que uma certa aresta pré-fixada ab de $G[U]$ é contada na soma (é claro que cada aresta é contada o mesmo número de vezes). Ou seja, m é o número de subconjuntos $S \subset U$ de tamanho $|S| = \lfloor u/2 \rfloor$ que "separam" a aresta ab, isto é, o número de subconjuntos $S \subset U$ de tamanho $|S| = \lfloor u/2 \rfloor$ tais que exatamente uma das extremidades de ab está em S.

Dada uma aresta ab, existem $\binom{u-2}{\lfloor u/2 \rfloor - 1}$ subconjuntos S que separam ab com $a \in S$ ($|S| = \lfloor u/2 \rfloor$), e $\binom{u-2}{\lfloor u/2 \rfloor - 1}$ que separam ab com $b \in S$. Logo $m = 2\binom{u-2}{\lfloor u/2 \rfloor - 1}$. Agora, usaremos duas identidades de fácil verificação: para $u \geq 2$ e $k \geq 1$, temos que

$$\binom{u-2}{k} = \frac{u-k-1}{u-1}\binom{u-1}{k} \quad \text{e} \quad \binom{u-1}{k-1} = \frac{k}{u}\binom{u}{k}.$$

Com o auxílio delas, vemos que

$$\begin{aligned} m &= 2\binom{u-2}{\lfloor u/2\rfloor - 1} = \frac{2\lceil u/2\rceil}{u-1}\binom{u-1}{\lfloor u/2\rfloor - 1} \\ &= \frac{2\lceil u/2\rceil\lfloor u/2\rfloor}{u(u-1)}\binom{u}{\lfloor u/2\rfloor} = \frac{\binom{u}{\lfloor u/2\rfloor}}{\binom{u}{2}}\lceil u/2\rceil\lfloor u/2\rfloor, \end{aligned}$$

e pela equação 3.2, temos que

$$\begin{aligned} e(G[U]) &= \frac{1}{m}\sum_S{}^* e_G(S, U\setminus S) = \frac{1}{m}\binom{u}{\lfloor u/2\rfloor}\operatorname{Med}_S e_G(S, U\setminus S) \\ &= \frac{\operatorname{Med}_S e_G(S, U\setminus S)\binom{u}{2}}{\lceil u/2\rceil\lfloor u/2\rfloor}, \end{aligned}$$

como queríamos. □

Lema 28. *Fixe $A > 0$, $C \geq 1$ e $0 \leq p \leq 1$. Sejam $G = G^n$ um grafo com n vértices e $U \subset V(G)$.*

- *Se G é (p, A)-uniforme, temos*

$$e(G[U]) = p\binom{|U|}{2} + O_1(Ad^{1/2}|U|),$$

  onde $d = np$.

- *Se G é η-regular com densidade p e $\lfloor |U|/2\rfloor \geq \eta n$, temos*

$$e(G[U]) = p\binom{|U|}{2} + O_1\left(\eta p\binom{|U|}{2}\right).$$

- *Se G é um grafo tal que, para todo $U \subset V(G)$ com $|U| = \lfloor n/2\rfloor$, temos $e_G(U, V\setminus U) \geq p\lfloor n/2\rfloor\lceil n/2\rceil$, então*

$$e(G) \geq p\binom{n}{2}.$$

Prova. Todas as asserções seguem imediatamente do lema 27. Mostraremos apenas a terceira, para exemplificar. Fixe $U \subset V(G)$ com $|U| = \lfloor n/2\rfloor$. Pelo lema 27, temos que

$$\begin{aligned} e(G) = e(G[V(G)]) &= \frac{\binom{n}{2}}{\lfloor n/2\rfloor\lceil n/2\rceil}\operatorname{Med}_S e_G(U, V\setminus U) \\ &\geq \frac{\binom{n}{2}}{\lfloor n/2\rfloor\lceil n/2\rceil}p\lfloor n/2\rfloor\lceil n/2\rceil = p\binom{n}{2}. \end{aligned}$$

□

3.2 Transformada de Fourier e regularidade

O objetivo desta seção é usar a transformada de Fourier discreta para mostrar que certos grafos são bastante regulares. Começamos relembrando as propriedades da transformada que nos serão úteis.

Dada uma função $f\colon \mathbb{Z}_n \to \mathbb{C}$, definimos $\mathcal{T}(f)\colon \mathbb{Z}_n \to \mathbb{C}$, a transformada de Fourier de f, por

$$\mathcal{T}(f)(x) = \sum_{y\in\mathbb{Z}_n} f(y)e^{-2\pi iyx/n}.$$

Note que há uma associação óbvia entre o conjunto das funções de $\mathbb{Z}_n$ em $\mathbb{C}$ e o espaço vetorial $\mathbb{C}^n$: a cada função $f\colon \mathbb{Z}_n \to \mathbb{C}$, associamos o vetor $(f(0), f(1), \ldots, f(n-1)) \in \mathbb{C}^n$. Assim, podemos ver a transformada de Fourier como uma aplicação de $\mathbb{C}^n$ em si mesmo, e é fácil ver que tal aplicação é linear. Além disso, sabe-se que a transformada de Fourier é uma transformação linear que leva bases ortogonais em bases ortogonais e que "estica" cada vetor por um fator $\sqrt{n}$: para todo $x \in \mathbb{C}^n$, temos $||\mathcal{T}(x)|| = \sqrt{n}||x||$, onde a norma considerada é a usual em $\mathbb{C}^n$.

Dadas funções f e g, ambas de $\mathbb{Z}_n$ em $\mathbb{C}$, definimos a convolução $f * g : \mathbb{Z}_n \to \mathbb{C}$ por

$$(f * g)(x) = \sum_{y\in\mathbb{Z}_n} f(y)g(x-y).$$

Uma propriedade importante da convolução é que a transformada de Fourier da convolução é o produto das transformadas, isto é, $\mathcal{T}(f * g)(x) = \mathcal{T}(f)(x)\mathcal{T}(g)(x)$. A prova é simples, mas não a daremos aqui.

No que segue, usaremos os grafos definidos abaixo. O grafo de Chung-Graham com adição já foi definido anteriormente, mas julgamos conveniente repetir sua definição aqui.

Definição 29. *Dado $S \subset \mathbb{Z}_n$, definimos o "grafo de Chung-Graham com adição", ou simplesmente "grafo de Chung-Graham", $\mathrm{CG}_n(S) = \mathrm{CG}_n^+(S)$, por $V(\mathrm{CG}_n^+(S)) = \mathbb{Z}_n$, e $ab \in E(\mathrm{CG}_n^+(S))$ se e só se $a + b \in S$. Definimos também o "grafo de Chung-Graham com subtração", $\mathrm{CG}_n^-(S)$ por $V(\mathrm{CG}_n^-(S)) = \mathbb{Z}_n$, e $ab \in E(\mathrm{CG}_n^-(S))$ se e só se $a - b \in S \cup (-S)$. Todas as operações são feitas módulo n.*

A razão de exigirmos que $a - b \in S \cup (-S)$, em vez de simplesmente $a - b \in S$, é que desejamos obter um grafo comum, e não um grafo dirigido.

Nos lemas a seguir, provaremos algo sobre o número de arestas entre U e W no grafo $\mathrm{CG}_n(R) = \mathrm{CG}_n^+(R)$, e isto será útil para estabelecer uma

conexão entre os coeficientes de Fourier de R e a η-regularidade do grafo $\mathrm{CG}_n^+(R)$.

O produto interno nos lemas a seguir é o usual em $\mathbb{C}^n$: se $W = (w_i)_{i=1}^n$ e $Z = (z_i)_{i=1}^n$ são vetores de $\mathbb{C}^n$, $\langle W, Z\rangle = \sum_{i=1}^n w_i \bar{z_i}$. Não faremos distinção entre um subconjunto de $\mathbb{Z}_n$ e sua função indicadora.

Lema 30. *Sejam $R, U, W \subset \mathbb{Z}_n$ com $U \cap W = \emptyset$. Então*

$$e_{\mathrm{CG}_n^+(R)}[U, W] = \langle R, U * W\rangle.$$

Prova. Basta notar que

$$\begin{aligned}\langle R, U * W\rangle &= \sum_r R(r) \sum_u U(u)W(r-u) \\ &= \sum_r R(r) \sum_{u,\ w\colon u+w=r} U(u)W(w) \\ &= \Big|\{u \in U, w \in W\colon u + w \in R\}\Big| = e_{\mathrm{CG}_n^+(R)}[U, W]. \quad (3.3)\end{aligned}$$

□

Lema 31. *Sejam $R, U, W \subset \mathbb{Z}_n$ com $U \cap W = \emptyset$. Então*

$$\Big|e_{\mathrm{CG}_n^+(R)}[U, W] - \frac{1}{n}|R||U||W|\Big| \leq \Big(\max_{j\neq 0} |\mathcal{T}(R)(j)|\Big)\sqrt{|U||W|}. \quad (3.4)$$

Prova. Temos

$$\begin{aligned}e_{\mathrm{CG}_n^+(R)}[U, W] &= \langle R, U * W\rangle = \frac{1}{n}\langle \mathcal{T}(R), \mathcal{T}(U * W)\rangle \\ &= \frac{1}{n}\sum_j \mathcal{T}(R)(j)\mathcal{T}(U * W)(j) = \frac{1}{n}\sum_j \mathcal{T}(R)(j)\mathcal{T}(U)(j)\mathcal{T}(W)(j) \\ &= \frac{1}{n}|R||U||W| + \frac{1}{n}\sum_{j\neq 0} \mathcal{T}(R)(j)\mathcal{T}(U)(j)\mathcal{T}(W)(j), \quad (3.5)\end{aligned}$$

e, por Cauchy-Schwarz,

$$\Big|\frac{1}{n}\sum_{j\neq 0} \mathcal{T}(R)(j)\mathcal{T}(U)(j)\mathcal{T}(W)(j)\Big| \leq \frac{1}{n}\Big(\max_{j\neq 0} |\mathcal{T}(R)(j)|\Big)||\mathcal{T}(U)||_2||\mathcal{T}(W)||_2,$$

de onde segue o resultado, pois o lado direito da expressão acima é igual a $\max_{j\neq 0} |\mathcal{T}(R)(j)|\sqrt{|U||W|}$. □

Agora iremos tratar do grafo de Chung-Graham com subtração.

Lema 32. *Sejam $R, U, W \subset \mathbb{Z}_n$ com $U \cap W = \emptyset$. Então*

$$\left|e_{\mathrm{CG}_n^-(R)}[U,W] - \frac{1}{n}|R \cup (-R)||U||W|\right| \leq \left(\max_{j\neq 0}|\mathcal{T}(R\cup(-R))(j)|\right)\sqrt{|U||W|}. \tag{3.6}$$

Prova. Da equação 3.3 segue que

$$\langle R \cup (-R), U * (-W)\rangle = \left|\{u \in U, w \in W \colon u - w \in R \cup (-R)\}\right|.$$

Portanto, $e_{\mathrm{CG}_n^-(R)}[U,W] = \langle R\cup(-R), U*(-W)\rangle$. Daqui em diante, a prova é análoga à do lema 31. □

O próximo lema é o resultado principal desta seção. Ele mostra que a η-regularidade dos grafos de Chung-Graham está ligada aos coeficientes de Fourier de um conjunto apropriado.

Lema 33. *Seja $R \subset \mathbb{Z}_n$. Se $\max_{j\neq 0}|\mathcal{T}(R)(j)| \leq \eta^2|R|$, o grafo $\mathrm{CG}_n^+(R)$ é η-regular com densidade $|R|/n$. Se $\max_{j\neq 0}|\mathcal{T}(R\cup(-R))(j)| \leq \eta^2|R\cup(-R)|$, o grafo $\mathrm{CG}_n^-(R)$ é η-regular com densidade $|R\cup(-R)|/n$.*

Prova. Provaremos apenas a primeira asserção. Sejam $U, W \subset \mathbb{Z}_n$ com $|U|, |W| \geq \eta n$. Observe primeiramente que

$$\max_{j\neq 0}|\mathcal{T}(R)(j)| \leq \eta^2|R| \leq \eta\frac{|R|}{n}\sqrt{|U||W|}.$$

Logo,

$$\max_{j\neq 0}|\mathcal{T}(R)(j)|\sqrt{|U||W|} \leq \eta\frac{|R|}{n}|U||W|,$$

e o resultado segue, pelo lema 31. □

Para terminar, observe que, se $d = pn$ e $\left(\max_{j\neq 0}|\mathcal{T}(R)(j)|\right)\sqrt{|U||W|} \leq A\sqrt{d|U||W|}$, então o grafo $\mathrm{CG}_n^+(R)$ é (p, A)-uniforme para $p = |R|/n$ (veja a definição 25). Veja também que a condição acima equivale a termos

$$\left(\max_{j\neq 0}|\mathcal{T}(R)(j)|\right) \leq A\sqrt{pn}.$$

3.3 O Lema de Regularidade de Szemerédi

Nesta seção, falaremos um pouco sobre o Lema de Regularidade de Szemerédi [35], comentaremos brevemente sua demonstração e daremos um exemplo de como o lema pode ser aplicado. Também enunciaremos uma extensão do lema, observada independentemente por Kohayakawa e Rödl (veja [23] ou [26]), apropriada para se lidar com grafos esparsos (isto é, grafos com quantidade subquadrática de arestas). É interessante notar que a primeira aparição do Lema de Regularidade na literatura foi em [34] (ainda em uma forma um pouco diferente de sua "forma final" de [35]), como ferramenta para a prova do Teorema de Szemerédi sobre inteiros em progressões aritméticas, que é o teorema 2 do capítulo 1.

Vamos relembrar a notação que usaremos. Ao longo da seção, $G = G^n$ será um grafo com n vértices. Para $U, W \subset V(G)$ com $U \cap W = \emptyset$, escrevemos $E(U,W) = E_G(U,W)$ para denotar o conjunto das arestas de G que ligam U a W. Colocamos $e(U,W) = e_G(U,W) = |E_G(U,W)|$ e definimos a densidade do par (U,W), $d(U,W)$, por $d(U,W) = e_G(U,W)/(|U||W|)$. Note que $0 \leq d(U,W) \leq 1$.

Na definição a seguir, vemos que um par (U,W) é Szemerédi-regular quando todo subgrafo "grande" (X,Y) de (U,W) tem quase a mesma densidade do par (U,W). Precisamente, temos:

Definição 34 (ε-Szemerédi-regularidade). *Dados $\varepsilon > 0$, um grafo G e $U, W \subset V(G)$ disjuntos, dizemos que o par (U,W) é ε-Szemerédi-regular se para todos $X \subset U$ e $Y \subset W$ com $|X| \geq \varepsilon|U|$ e $|Y| \geq \varepsilon|W|$, temos*

$$|d(X,Y) - d(U,W)| \leq \varepsilon.$$

No que vem a seguir, trabalharemos sempre com um certo tipo especial de partições do conjunto de vértices de um grafo G.

Definição 35 (Partições equitáveis). *Dizemos que uma partição $P = (V_i)_{i=0}^k$ de $V = V(G)$ é (ε, k)-equitável se $|V_0| \leq \varepsilon n$ e $|V_1| = \ldots = |V_k|$. Dizemos que V_0 é a classe excepcional de P.*

Quando o valor de ε não for relevante, diremos simplesmente que P é k-equitável. Diremos também que P é equitável quando for k-equitável para algum k.

O Lema de Regularidade nos diz que para todo grafo G com $n = |V(G)|$ grande, existe uma partição equitável de $V(G)$ em um número "apropriado" de partes, $V(G) = \cup_{j=0}^k V_j$, tal que quase todos os pares (V_i, V_j) com $1 \leq i < j \leq k$ são Szemerédi-regulares.

Teorema 36 (Lema de Regularidade de Szemerédi). *Para todos $\varepsilon > 0$ e $m > 0$, existem inteiros $M = M(\varepsilon, m)$ e $N = N(\varepsilon, m)$ tais que para todo grafo G com $n \geq N(\varepsilon, m)$ vértices, existe uma partição (ε, k)-equitável de $V(G)$, $V(G) = \cup_{j=0}^{k} V_j$, com $m \leq k \leq M(\varepsilon, m)$, e tal que no máximo εk^2 dos pares (V_i, V_j) $(1 \leq i < j \leq k)$ não são ε-Szemerédi-regulares.*

Vamos explicar o papel de m e M no lema. Note que o resultado afirma algo sobre a distribuição das arestas entre os pares (V_i, V_j) com $1 \leq i < j \leq k$, e não diz nada sobre as arestas que estão contidas em cada classe V_i. Assim, seria interessante se o número de arestas "internas" (ou seja, contidas em alguma classe) fosse (em proporção) muito pequeno. Isto é conseguido escolhendo-se um m suficientemente grande, pois o número de arestas "internas" é limitado por $k\binom{n/k}{2} \sim \binom{n}{2}/k \leq \binom{n}{2}/m$. Por outro lado, é essencial que o número de classes da partição seja limitado ($k \leq M$) pois, por exemplo, a partição de $V(G)$ em n classes com um único vértice em cada é trivialmente 0-Szemerédi-regular. De fato, a característica fundamental do Lema de Szemerédi é que o número de classes da partição é limitado e o limitante M não depende do grafo G.

Iremos agora rascunhar a demonstração do Lema de Regularidade. Embora a demonstração em [35] tenha apenas duas páginas, a prova do lema não pode ser considerada fácil; de fato, os argumentos em [35] estão extremamente condensados. Recomendamos fortemente a leitura das seções IV.5 e IV.6 de [3], onde são dadas uma prova menos concisa e mais "didática" do Lema de Regularidade, bem como algumas aplicações simples. A referência já clássica para quem deseja estudar com mais detalhes o Lema de Regularidade e suas consequências em teoria dos grafos é o survey de Komlós e Simonovits [27].

Vamos à "prova". Para cada partição P de $V(G)$, $P = (V_j)_{j=0}^{k}$, definimos o índice de P, $\mathrm{ind}(P)$, por

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

Como a soma contém $\binom{k}{2}$ parcelas e cada uma delas está entre 0 e 1, é claro que sempre temos $0 \leq \mathrm{ind}(P) \leq 1/2$.

Se P e $\tilde{P}$ são partições equitáveis de $V(G)$, diremos que $\tilde{P}$ refina P se toda classe não-excepcional de $\tilde{P}$ está inteiramente contida em uma classe não-excepcional de P. Dito isto, a idéia fundamental para provar o teorema 36 está contida no lema abaixo.

Lema 37. *Seja G um grafo com n vértices, e seja $P = (V_j)_{j=0}^{k}$ uma partição (ε, k)-equitável de $V(G)$. Se ε é tal que $4^k > 600\varepsilon^{-5}$ e mais de εk^2 pares*

(V_i, V_j) $(1 \leq i < j \leq k)$ não são ε-Szemerédi-regulares, então existe um refinamento $\tilde{P} = (\tilde{V}_j)_{j=0}^{1+k4^k}$ de P tal que $\mathrm{ind}(\tilde{P}) \geq \mathrm{ind}(P) + \varepsilon^5/20$, $V_0 \subset \tilde{V}_0$ e $|\tilde{V}_0 \setminus V_0| \leq n/4^k$.

Com este resultado, é fácil provar o teorema 36. Seja m_0 o menor inteiro que satisfaz $m_0 \geq m$ e $4^{m_0} > 600\varepsilon^{-5}$. Começamos com uma partição $(\varepsilon/2, m_0)$-equitável qualquer de $V(G)$. Se esta partição tem no máximo εm_0^2 pares Szemerédi-regulares, fim de prova; caso contrário, usando o lema acima, refinamos a partição inicial. Iteramos este processo até chegarmos à partição desejada. Isto ocorrerá em no máximo $10\varepsilon^{-5}$ iterações, pois cada iteração aumenta o índice em pelo menos $\varepsilon^5/20$, e por outro lado sabemos que o índice de uma partição é sempre menor ou igual a $1/2$. Defina $f : \mathbb{N} \to \mathbb{N}$ por $f(0) = m_0$ e $f(t+1) = 1 + f(t)4^{f(t)}$. Então a partição final terá no máximo $f(10\varepsilon^{-5})$ classes (e portanto colocamos $M = f(10\varepsilon^{-5})$). É importante notar que o fato de a classe excepcional aumentar muito pouco a cada iteração também é crucial, pois a classe excepcional da partição final deve ter no máximo εn elementos (por definição de equitabilidade). Do lema acima segue que, se a classe excepcional inicial tem no máximo $\varepsilon n/2$ elementos, então a classe excepcional da partição final tem no máximo

$$\frac{\varepsilon n}{2} + \frac{n}{4^{m_0}} + \frac{n}{4^{f(m_0)}} + \frac{n}{4^{f(f(m_0))}} + \cdots \leq \frac{\varepsilon n}{2} + \frac{2n}{4^{m_0}},$$

e pela escolha de m_0, isto é no máximo $\frac{\varepsilon}{2}n + \frac{\varepsilon^5}{300}n \leq \varepsilon n$.

Na seção 3.4, veremos o Lema de Regularidade em ação, e com isso o leitor poderá sentir a grande força do resultado. No entanto, apesar de sua força, o Lema de Regularidade tem uma limitação importante: para grafos com quantidade subquadrática de arestas ($e(G) = o(n^2)$) todo par (U, W) é Szemerédi-regular, e portanto o Lema de Szemerédi não nos dá nenhuma informação.

De fato, para todo $X \subset U$ e $Y \subset W$ com $|X| \geq \varepsilon|U|$ e $|Y| \geq \varepsilon|W|$, temos

$$|d(X,Y) - d(U,W)| = \Big|\frac{e(X,Y)}{|X||Y|} - \frac{e(U,W)}{|U||W|}\Big| = |o(1) - o(1)| = o(1),$$

já que $e(X,Y)$ e $e(U,W)$ são $o(n^2)$ enquanto que tanto $|X||Y|$ como $|U||W|$ são $\Omega(n^2)$. Lembramos que escrevemos $f(n) = \Omega(g(n))$ se existir uma constante $C > 0$ tal que para todo n suficientemente grande, $|f(n)| \geq C|g(n)|$. Em outras palavras, $f(n) = \Omega(g(n))$ se e só se $g(n) = O(f(n))$.

Na seção 3.5, veremos uma variante "esparsa" do Lema de Szemerédi, que contorna parcialmente esta dificuldade.

3.4 Aplicando o Lema de Regularidade

Nesta seção, daremos uma aplicação do Lema de Regularidade de Szemerédi, para ilustrar seu mecanismo básico de uso.

Em muitas aplicações do Lema de Regularidade, começamos com um grafo qualquer G e a partir dele, construímos dois grafos especiais: o grafo reduzido de G e o grafo limpo de G. Vamos defini-los a seguir. Dados um grafo G, uma partição k-equitável P de $V(G)$ e dois parâmetros $\varepsilon > 0$ e $0 \leq d < 1$, definimos o grafo reduzido de G (que denotaremos por $R = R(G, P, \varepsilon, d)$) por $V(R) = [k] = \{1, 2, \ldots, k\}$ e ij é aresta de R se e só se o par (V_i, V_j) é ε-Szemerédi-regular com densidade $d(V_i, V_j) \geq d$. Definimos também o grafo limpo de G (que denotaremos por $L(G, P, \varepsilon, d)$) por $V(L) = V(G)$ e $e \in E(L)$ se e só se $e \in E(G)$ e existem $1 \leq i \neq j \leq k$ tais que e liga V_i a V_j e ij é aresta do grafo reduzido. Isto é, obtemos L a partir de G apagando arestas até restarem apenas as arestas que ligam pares ε-Szemerédi-regulares com densidade pelo menos d.

O grafo limpo de G é mais fácil de se lidar do que o grafo original G, e ele ainda contém a maior parte das arestas de G, se ε e d forem pequenos, e se k for grande. De fato, suponha que temos uma partição k-equitável $P = (V_j)_{j=0}^{k}$ dada pelo Lema de Regularidade aplicado com parâmetros ε e $m = \lceil 1/\varepsilon \rceil$, por exemplo. Seja n' o tamanho de cada classe não-excepcional. Se $e \in E(G) \setminus E(L)$, há quatro casos: e está contida em algum V_j ($j \neq 0$), e é incidente a V_0, e liga duas classes que formam um par ε-Szemerédi-irregular ou e liga duas classes que formam um par com densidade inferior a d. Assim, $|E(G) \setminus E(L)| \leq k\binom{n'}{2} + \varepsilon n^2 + \varepsilon\binom{k}{2}n'^2 + dn'^2\binom{k}{2}$, e como temos $n' \leq n/k$ segue que $|E(G) \setminus E(L)| \leq \frac{1}{k}\binom{n}{2} + \varepsilon n^2 + \varepsilon n^2/2 + dn^2/2 \leq \frac{1}{k}\binom{n}{2} + (2\varepsilon + \varepsilon + d)n^2/2 \leq (\frac{1}{k} + 4\varepsilon + d)\binom{n}{2}$. Como escolhemos $m = \lceil 1/\varepsilon \rceil$, temos $1/k \leq 1/m = 1/\lceil 1/\varepsilon \rceil \leq \varepsilon$. Assim, $|E(G) \setminus E(L)|$ é uma fração pequena de $\binom{n}{2}$ (e, portanto, de $e(G)$, já que assumimos implicitamente que $e(G) = \Omega(n^2)$), se ε e d forem pequenos e se m for grande.

A importância do grafo reduzido de G segue do fato que todo subgrafo de R com grau máximo "pequeno" é também subgrafo de G. Para formular isto mais precisamente, definiremos o grafo $R(t)$ obtido a partir de R trocando-se cada vértice de R por t vértices independentes, e trocando cada aresta de R pelo grafo bipartido completo $K_{t,t}$. Com isso, enunciamos uma consequência muito interessante do Lema de Regularidade (para uma demonstração, veja [27]).

Teorema 38 ("Key Lemma"). *Dados $d > \varepsilon > 0$, um grafo R e um inteiro positivo n', construa um grafo G trocando cada vértice de R por n' vértices,*

e trocando as arestas de R por pares ε-Szemerédi-regulares com densidade maior ou igual a d. Seja H um subgrafo de $R(t)$ com h vértices e grau máximo $\Delta > 0$, e seja $\varepsilon_0 = (d-\varepsilon)^{\Delta}/(2+\Delta)$. Se $\varepsilon \leq \varepsilon_0$ e se $t-1 \leq \varepsilon_0 n'$, então $H \subset G$.

Agora, usaremos o Lema de Szemerédi para dar uma prova bem curta (mas não muito detalhada) do famoso Teorema de Erdős, Stone e Simonovits.

Começaremos contextualizando o problema. Lembramos que o tamanho de um grafo G é seu número de arestas, e a ordem de G é o número de vértices de G. Dados grafos G e H, definimos $\mathrm{ex}(G,H)$ como o máximo tamanho de um subgrafo de G que não contém cópias de H. O problema é determinar ou estimar $\mathrm{ex}(G,H)$. Em 1941, Turán inaugurou a Teoria Extremal dos Grafos com seu histórico artigo [36] em que é determinado com exatidão o valor de $\mathrm{ex}(K_n, K_p)$, onde K_t é o grafo completo com t vértices. Abaixo, enunciamos uma versão levemente mais fraca do Teorema de Turán, mas que será mais adequada aos nossos propósitos.

Teorema 39 (Turán, 1941). *Se G é um grafo com n vértices e mais de $(1-\frac{1}{p-1})n^2/2$ arestas, então G contém uma cópia de K_p. Ou seja, $\mathrm{ex}(K_n, K_p) \leq (1-\frac{1}{p-1})n^2/2$.*

Mencionamos que no capítulo 29 de [1] são dadas 5 provas extremamente elegantes do Teorema de Turán.

Um passo natural então é trocar os grafos completos K_p por grafos gerais H e investigar $\mathrm{ex}(K_n, H)$, onde H é um certo grafo fixo. Em 1946, Erdős e Stone [8] realizaram um importante avanço nesta questão, ao provar o teorema abaixo. Definamos $K_p(t,\ldots,t)$ como o grafo p-partido completo em que cada classe tem t vértices.

Teorema 40 (Erdős e Stone, 1946). *Se $p \geq 2$ e $t \geq 1$,*

$$\mathrm{ex}(K_n, K_p(t,\ldots,t)) = \left(1 - \frac{1}{p-1} + o(1)\right)\binom{n}{2}.$$

Em [7], Erdős e Simonovits observaram que o resultado acima implicava o teorema a seguir. Este resultado, que hoje é conhecido como o Teorema de Erdős, Stone e Simonovits, determina o comportamento assintótico de $\mathrm{ex}(K_n, H)$ para todo H.

Teorema 41 (Erdős, Stone e Simonovits, 1966). *Seja $\chi(H)$ o número cromático de H. Então*

$$\mathrm{ex}(K_n, H) = \left(1 - \frac{1}{\chi(H)-1} + o(1)\right)\binom{n}{2}.$$

Vamos mostrar que o teorema 40 implica o teorema 41. Seja $K(p,n)$ o grafo p-partido com n vértices, em que as classes $C_1, C_2, \ldots, C_p$ da p-partição satisfazem $|C_1| \leq |C_2| \leq \ldots \leq |C_p| \leq |C_1| + 1$, e tal que $e \in E(K(p,n))$ se e só se e liga C_i a C_j para algum par (i,j) com $i \neq j$. Uma conta simples mostra que $e(K(p,n)) = (1 - \frac{1}{p} + o(1))\binom{n}{2}$, e como para todo H e todo n temos $H \not\subset K(\chi(H)-1, n)$, segue que

$$\mathrm{ex}(K_n, H) \geq e\Big(K\big(\chi(H)-1, n\big)\Big) = \left(1 - \frac{1}{\chi(H)-1} + o(1)\right)\binom{n}{2}. \quad (3.7)$$

Por outro lado, pelo teorema 40, temos

$$\mathrm{ex}(K_n, H) \leq \mathrm{ex}(K_n, K_{\chi(H)}(|V(H)|, \ldots, |V(H)|)) = \left(1 - \frac{1}{\chi(H)-1} + o(1)\right)\binom{n}{2}.$$

Iremos agora dar uma prova curta do teorema 40, via Lema de Regularidade.

Prova do teorema 40. Pela equação 3.7, vemos que é suficiente provarmos apenas a cota superior para $\mathrm{ex}(K_n, K_p(t\ldots,t))$. Fixe $\beta > 0$ e suponha que G é um grafo com n vértices (n suficientemente grande) e mais de $(1 - \frac{1}{p-1} + \beta)\binom{n}{2}$ arestas. Tome $d = \beta/2$ e $\varepsilon = (\beta/10)^{pt}$ e considere o grafo reduzido de G, $R(G, P, \varepsilon, d)$, onde $P = (V_j)_{j=1}^k$ é uma partição k-equitável dada pelo Lema de Regularidade de Szemerédi aplicado a G com parâmetros ε e $m = \lceil 1/\varepsilon \rceil$. Considere também o grafo limpo de G, $L(G, P, \varepsilon, d)$. É fácil ver que

$$\frac{e(R)}{k^2/2} \geq \frac{e(L)}{n^2/2} > 1 - \frac{1}{p-1}.$$

Logo, pelo Teorema de Turán, R contém uma cópia de K_p, e, pelo teorema 38, temos que G contém uma cópia de $K_p(t, \ldots, t)$, que é o que queríamos mostrar. □

Um problema muito interessante que está em aberto é o de provar uma versão probabilística do teorema 41. Por exemplo, o teorema 41 nos diz que, para n grande, se fixarmos $l \geq 1$ e pegarmos um pouco mais da metade das arestas de K_n, teremos necessariamente uma cópia de um circuito de comprimento $2l+1$, $\mathcal{C}^{2l+1}$. Uma pergunta natural é: "É verdade que, com probabilidade tendendo a 1 quando $n \to \infty$, se pegarmos um pouco mais da

metade das arestas do grafo aleatório $G_{n,p}$, teremos obrigatoriamente uma cópia de $\mathcal{C}^{2l+1}$?" Veremos no próximo capítulo que isso vale, se $p = p(n) \geq Cn^{-1+1/2l}$, onde C é uma constante grande.

De modo geral, a questão é investigar $\mathrm{ex}(G_{n,p}, H)$. Seria interessante se tivéssemos um teorema do tipo "se $p = p(n)$ é suficientemente grande, então quase todo $G_{n,p}$ satisfaz $\mathrm{ex}(G_{n,p}, H) \leq \left(1 - \frac{1}{\chi(H)-1} + o(1)\right) e(G_{n,p})$", mas até o momento, resultados deste tipo só foram provados para alguns grafos H. Este problema, intitulado "Problema de Turán para grafos aleatórios", tem atraído considerável atenção nos últimos anos. Segundo Janson, Łuczak e Ruciński, "trata-se de um dos mais importantes problemas em aberto na área de grafos aleatórios" ([22], capítulo 8). O enunciado preciso do problema foi formulado por Kohayakawa, Łuczak e Rödl em [25].

Haxell, Kohayakawa e Łuczak resolveram o problema quando H é um circuito [18, 19] (No próximo capítulo, veremos detalhadamente alguns dos métodos usados em [19], pois eles serão empregados para provar uma versão probabilística do Teorema de Schur). Em [25], Kohayakawa, Łuczak e Rödl resolveram o caso $H = K_4$. Recentemente, Gerke, Schickinger e Steger [13] resolveram o caso $H = K_5$. Todos os artigos acima citados usaram alguma variante esparsa do Lema de Regularidade. Estas variantes são o assunto da próxima seção.

3.5 A versão esparsa do Lema de Regularidade

Em meados da década de 90, Y. Kohayakawa e V. Rödl descobriram independentemente versões esparsas do Lema de Regularidade [23, 26]. Enunciaremos aqui apenas uma dessas versões, e a empregaremos na seção 4.1.

Nas definições abaixo, G será um grafo e U e W serão sempre subconjuntos disjuntos de $V(G)$ com $u = |U|$ e $w = |W|$.

Definição 42 (Densidade relativa $d_{H,G}(U,W)$). *Seja H um subgrafo de G com $V(H) = V(G)$. Definimos $d_{H,G}(U,W)$ por*

$$d_{H,G}(U,W) = \begin{cases} e_H(U,W)/e_G(U,W) & \text{se } e_G(U,W) > 0, \\ 0 & \text{se } e_G(U,W) = 0. \end{cases}$$

Definição 43 (Pares (ε, H, G)-regulares). *Fixe $\varepsilon > 0$. Dizemos que o par (U,W) é (ε, H, G)-regular se para todos $U' \subset U$ e $W' \subset W$ com $|U'| \geq \varepsilon|U|$ e $|W'| \geq \varepsilon|W|$ temos*

$$|d_{H,G}(U',W') - d_{H,G}(U,W)| \leq \varepsilon.$$

Definição 44 (Partições (ε, H, G)-regulares). *Seja $P = (V_i)_{i=0}^{k}$ uma partição (ε, k)-equitável de $V = V(G)$. Dizemos que P é (ε, H, G)-regular se no máximo $\varepsilon\binom{k}{2}$ pares (V_i, V_j) (com $1 \leq i < j \leq n$) não são (ε, H, G)-regulares.*

Agora podemos enunciar o resultado de Kohayakawa e Rödl, que é uma extensão do Lema de Regularidade de Szemerédi.

Teorema 45 (Kohayakawa, Rödl). *Dados $\varepsilon > 0$ e $k_0 \geq 1$, existem constantes $\eta = \eta(\varepsilon, k_0)$ e $K_0 = K_0(\varepsilon, k_0) \geq k_0$ que dependem somente de ε e k_0 tais que, se G é um grafo η-regular e H é um subgrafo de G com $V(H) = V(G)$, então existe uma partição de $V = V(G)$ que é (ε, k)-equitável e (ε, H, G)-regular, com $k_0 \leq k \leq K_0$.*

A prova deste resultado segue bem de perto a prova do Lema de Regularidade original, e por isso não faremos maiores comentários sobre ela. Note também que se tomarmos $G = K_n$, o grafo completo com n vértices, recuperamos o Lema de Szemerédi original.

Recomendamos a leitura de [23] para os interessados em conhecer algumas aplicações da versão esparsa do Lema de Regularidade. Além de estar se mostrando uma ferramenta útil no ataque ao Problema de Turán para grafos esparsos (veja a seção anterior), mencionamos que a versão esparsa do Lema de Szemerédi foi empregada na prova do teorema 6, e também foi útil para se encontrar um novo critério de quasi-aleatoriedade para grafos [26]. Por sua vez, deste novo critério segue imediatamente o seguinte fato: existe um algoritmo que verifica se um grafo com n vértices é quasi-aleatório (no sentido de Chung, Graham e Wilson [6]) em tempo $O(n^2)$. Isto é surpreendente, pois o tempo de leitura de grafo já é quadrático na entrada. O melhor algoritmo conhecido até então levava tempo $O(n^{2,376})$.

Capítulo 4

Uma versão probabilística do Teorema de Schur

Nosso principal objetivo neste capítulo é provar o teorema 13. Isto será feito na seção 4.2. Na seção 4.1, provaremos o lema dos pares proibidos, um resultado auxiliar muito importante na prova. A seção final, 4.3, é dedicada ao enunciado de uma conjectura que, se verdadeira, nos permitiria resolver o problema 12. Discutimos também uma variante do problema.

Ao longo de todo o capítulo, usaremos a seguinte definição. Uma função $A : \mathbb{N} \to \mathbb{R}^+$ é uma A-função se existe uma constante $c > 0$ tal que, para todo n, $1 \leq A(n) \leq c\sqrt{\log n}$.

4.1 O lema dos pares proibidos

Nesta seção, falaremos um pouco sobre o que é feito em [19], com forte ênfase no resultado que chamaremos de lema dos pares proibidos. Começamos com algumas definições. Escrevemos $G = G^n$ para dizer que G é um grafo com n vértices, e denotaremos o circuito de comprimento l por $\mathcal{C}^l$. Mais precisamente, um circuito de comprimento l em G é um conjunto de l vértices de G distintos, $\{v_1, \ldots, v_l\}$, tais que para todo $i \in \mathbb{Z}_l$, $v_i v_{i+1} \in E(G)$.

Para $0 < \gamma < 1$ e grafos G, H, escrevemos $G \to_\gamma H$ se em qualquer subconjunto de arestas de G com cardinalidade maior que $\gamma e(G)$ há uma cópia de H. O principal resultado de [19] é o seguinte.

Teorema 46 (Haxell, Kohayakawa e Łuczak, 1996). *Para todo $0 < \eta < 1/2$ e todo inteiro positivo l, existe uma constante $C = C(\eta, l) > 0$ tal que quase todo grafo $G_{n,p}$ com $p = p(n) \geq Cn^{-1+1/2l}$ satisfaz $G_{n,p} \to_{1/2+\eta} \mathcal{C}^{2l+1}$.*

Ou seja, os autores resolveram o Problema de Turán para grafos aleatórios no caso em que H é um circuito ímpar. O teorema acima prova que, desde que $p = p(n)$ seja suficientemente grande (ou "vá a zero suficientemente devagar"), então quase certamente $\mathrm{ex}(G_{n,p}, \mathcal{C}^{2l+1}) \leq (1/2+\eta)e(G_{n,p})$. Como sempre, ao dizer que quase todo grafo $G_{n,p}$ tem a propriedade Q, queremos dizer que $\lim_{n\to\infty} \mathbb{P}((G_{n,p} \text{ tem a propriedade } Q) = 1$.

Na demonstração do nosso teorema 13, usaremos não apenas o principal lema de [19] (o lema dos pares proibidos) como também as idéias da prova do teorema 46.

O lema dos pares proibidos é a principal ferramenta na demonstração do teorema 46. Nesta seção, nosso principal objetivo é provar este lema.

Começaremos definindo o grafo dos pares proibidos. Dado um grafo H e um inteiro $l \geq 1$, vamos definir o grafo $J = J(H) = J_l(H)$ em $V(H)$ ligando dois vértices $x, y \in V(H)$ em J se e só se existir um caminho entre x e y de comprimento $2l$, em H. Mais precisamente, ligamos x a y em $J_l(H)$ se e só se existirem vértices $v_1, v_2, \ldots, v_{2l-1}$ distintos tais que as arestas $xv_1, v_1v_2, \ldots, v_{2l-1}y$ estão todas em H. Esse grafo será extremamente importante, e será chamado de grafo dos pares proibidos. Suponha que estamos interessados em grafos H que não possuem circuitos $\mathcal{C}^{2l+1}$, e suponha que xy é um par proibido por H. Então, não pode haver aresta em H ligando x a y, ou então fecharíamos um circuito de comprimento $2l+1$ em H. Daí vem o nome "pares proibidos".

Podemos agora enunciar o lema dos pares proibidos. Fixe constantes reais $C > 0$ e $0 < \gamma_0 \leq 1$. Fixe uma A-função $A = A(n)$ e suponha que $G = G^n$ é um grafo (p, A)-uniforme, onde $p = p(n) \geq CA^2n^{-1+1/2l}$, e seja H um subgrafo de G com pelo menos $\gamma_0 e(G)$ arestas. O lema abaixo diz que $e(J_l(H))$ é quase tão grande quanto $(e(H)/e(G))\binom{n}{2}$, se C e n forem suficientemente grandes.

Lema 47 (Lema dos pares proibidos). *São dados um inteiro $l \geq 1$, reais $0 < \delta \leq 1$, $0 < \gamma_0 \leq 1$, e uma A-função $A = A(n)$. Existe uma constante $C_0 = C_0(l, \delta, \gamma_0) > 0$ tal que vale o seguinte. Seja $G = G^n$ um grafo (p, A)-uniforme com $p = p(n) \geq C_0A^2n^{-1+1/2l}$, e seja $H \subset G$ um subgrafo de G com $e(H) \geq \gamma_0 e(G)$. Então, se n for suficientemente grande, temos $e(J_l(H)) \geq (1-\delta)(e(H)/e(G))\binom{n}{2}$.*

Há dois ingredientes importantes na prova do lema 47: a versão esparsa para o lema de regularidade de Szemerédi (teorema 45) e o lema 48 que veremos a seguir. Seja $H = H^k$ um grafo com k vértices, e suponha que $\bar{\gamma} = (\gamma_e)_{e\in H}$ é uma família de pesos $0 \leq \gamma_e \leq 1$ nas arestas $e \in E(H)$ de H. Para $x \in V(H)$, seja $\Gamma(x)$ o conjunto dos vértices vizinhos de x

em H. Dados vértices $x, y \in V(H)$, não necessariamente distintos, seja $Z_{x,y} = \Gamma_H(x) \cap \Gamma_H(y)$ o conjunto dos vizinhos comuns de x e y, e defina

$$w(x,y) = w_{H,\bar{\gamma}}(x,y) = \begin{cases} 0 & \text{se } Z_{x,y} = \emptyset, \\ \max\{\gamma_{zy} \colon z \in Z_{x,y}\} & \text{se } Z_{x,y} \neq \emptyset. \end{cases}$$

Para $x \in V(H)$, defina o $\bar{\gamma}$-grau de x, $d^{\bar{\gamma}}(x)$, por $d^{\bar{\gamma}}(x) = d^{H,\bar{\gamma}}(x) = \sum_{y \in \Gamma_H(x)} \gamma_{xy}$. Seja $\bar{\gamma}(H) = \sum_{e \in E(H)} \gamma_e$. Fixada uma ordenação $\chi = (x_1, \ldots, x_k)$ dos vértices de H, definimos $w(H, \bar{\gamma}, \chi) = \sum_{1 \leq i \leq j \leq k} w(x_i, x_j)$. Dizemos que uma ordenação $\chi = (x_1, \ldots, x_k)$ dos vértices de H respeita $\bar{\gamma}$ se, para todo $1 \leq i \leq k$, o vértice x_i é um vértice de $\bar{\gamma}_i$-grau mínimo em $H_i = H[x_i, \ldots, x_k]$, o subgrafo de H induzido por $x_i, \ldots, x_k$, onde $\bar{\gamma}_i = (\gamma_e)_{e \in E(H_i)}$. Note que uma tal ordenação sempre existe: ache primeiro x_1, depois x_2, etc. Agora podemos enunciar um dos ingredientes para a prova do lema dos pares proibidos.

Lema 48. *Seja $H = H^k$ um grafo com k vértices e sem laços, e suponha que é dada uma família de pesos $\bar{\gamma} = (\gamma_e)_{e \in H}$ com $0 \leq \gamma_e \leq 1$. Se $\chi = (x_1, \ldots, x_k)$ é uma ordenação dos vértices de H que respeita $\bar{\gamma}$, então $w(H, \bar{\gamma}, \chi) \geq \bar{\gamma}(H)$.*

Prova. Provaremos o resultado por indução em k. Se $k = 1$, não há nada para provar. Suponha agora $k \geq 2$, e assuma que o lema já foi provado para valores menores de k. Considere $H_2 = H[x_2, \ldots, x_k]$ e $\bar{\gamma}_2 = (\gamma_e)_{e \in E(H_2)}$. Obviamente, $\chi_2 = (x_2, \ldots, x_k)$ é uma ordenação dos vértices de H_2 que respeita $\bar{\gamma}_2$, e por indução segue que $w(H_2, \bar{\gamma}_2, \chi_2) \geq \bar{\gamma}_2(H_2)$. Se $\Gamma_H(x_1) = \emptyset$, temos $w(H, \bar{\gamma}, \chi) = w(H_2, \bar{\gamma}_2, \chi_2) \geq \bar{\gamma}_2(H_2) = \bar{\gamma}(H)$. Por outro lado, se $\Gamma_H(x_1) \neq \emptyset$, tomamos um elemento qualquer $z \in \Gamma_H(x_1)$. Pela hipótese sobre a ordenação χ, temos $d^{H,\bar{\gamma}}(z) \geq d^{H,\bar{\gamma}}(x_1)$, e portanto

$$\begin{aligned} w(H, \bar{\gamma}, \chi) &\geq w(H_2, \bar{\gamma}_2, \chi_2) + \sum_{y \in \Gamma_H(z)} w(x_1, y) \\ &\geq \bar{\gamma}_2(H_2) + \sum_{y \in \Gamma_H(z)} \gamma_{zy} = \bar{\gamma}_2(H_2) + d^{H,\bar{\gamma}}(z) \geq \bar{\gamma}_2(H_2) + d^{H,\bar{\gamma}}(x_1) \\ &= \bar{\gamma}(H), \end{aligned}$$

como queríamos. □

O lema 50 é o ponto chave para provar o lema dos pares proibidos. Para descrevê-lo, sejam $l \geq 1$ um inteiro e $C, \varepsilon, \mu > 0$ reais positivos. Fixe uma A-função $A = A(n)$, e fixe também reais $0 < \rho \leq \gamma \leq 1$. Seja $G = G^n$ um

grafo (p, A)-uniforme com $p = p(n) \geq CA^2 n^{-1+1/2l}$, e seja H um subgrafo de G com $V(H) = V(G)$. São dados três conjuntos dois a dois disjuntos $V_1, V_2, V_3 \subset V = V(G)$, com $|V_i| = m \geq \mu n$ $(i = 1, 2, 3)$ e tais que os pares (V_1, V_2) e (V_2, V_3) são (ε, H, G)-regulares com $d_{1,2} = d_{H,G}(V_1, V_2) \geq \rho$ e $d_{2,3} = d_{H,G}(V_2, V_3) \geq \gamma$. Basicamente, o lema 50 afirma que o grafo dos pares proibidos, $J_l(H)$, é tal que $e_{J_l}(V_1, V_3)$ é quase tão grande como γm^2, desde que C e n sejam grandes, e ε seja suficientemente pequeno.

Na prova do lema 50, usaremos as seguintes definições. Seja J um grafo bipartido com bipartição $V(J) = X \dot{\cup} Y$. Dizemos que J é (b, f)-expansor se para todo $U \subset V(J)$ com $|U| \leq b$ e tal que $U \subset X$ ou $U \subset Y$, temos que $|\Gamma_J(U)| \geq f|U|$, onde $\Gamma_J(U) = \cup_{u \in U} \Gamma_J(u)$ e $\Gamma_J(u)$ é o conjunto dos vizinhos de u no grafo J. Se G é um grafo e $U, W \subset V(G)$, $U \cap W = \emptyset$, então $G[U, W]$ será o grafo bipartido com vértices $U \dot{\cup} W$ e arestas $E_G(U, W)$.

O seguinte lema será necessário para provar o lema 50. A versão esparsa do Lema de Regularidade é usada em sua demonstração.

Lema 49. *Sejam $0 < \varepsilon \leq 1/5$ e $0 < \rho \leq 1$ reais dados, e suponha que $0 < \eta \leq \varepsilon/8$. Seja $G = G^n$ um grafo com n vértices, η-uniforme com densidade $0 < p \leq 1$, e seja H um subgrafo de G com $V(H) = V(G)$. Suponha que, para $(i, j) = (1, 2)$ e $(i, j) = (2, 3)$, temos que (V_i, V_j) é um par (ε, H, G)-regular com $d_{i,j} = d_{H,G}(V_i, V_j) \geq \rho$. Suponha também que $|V_i| \geq (\eta/\varepsilon)n$ para $i \in \{1, 2, 3\}$. Então, existem conjuntos $V_i' \subset V_i$ $(i \in \{1, 2, 3\})$ tais que*

$$|\Gamma_H(x) \cap V_j'| \geq (1 - 5\varepsilon/\rho) d_{i,j} e_G(V_i, V_j)/|V_i|$$

para todos $(i, j) \in \{(1, 2), (2, 1), (2, 3), (3, 2)\}$ e todo $x \in V_i'$. Além disso, temos que $|V_i'| \geq (1 - 2\varepsilon)|V_i|$ para $i \in \{1, 2, 3\}$.

Prova. A prova é muito similar à prova do lema 3.2 de [17], e por isso não a daremos aqui. □

Lema 50. *São dados um inteiro $l \geq 1$, reais $C > 0$, $0 < \delta \leq 1$, $0 < \mu \leq 1$ e $0 < \rho \leq \gamma \leq 1$. Fixe uma A-função $A = A(n)$, e sejam G, H e $J_l(H)$ grafos como os descritos antes do lema 49. Então, se $C \geq C_0 = 32/(\delta\rho\mu)^2$ e $0 < \varepsilon \leq \varepsilon_0 = \delta\rho/24$, temos $e(J_l[V_1, V_3]) \geq (1 - \delta)\gamma m^2$, desde que n seja suficientemente grande.*

Prova. Assumimos que n é grande, e, em particular, temos que G é η-uniforme para $\eta = \varepsilon\mu$ (veja o lema 26). Se G é um grafo, escrevemos $\delta(G)$ para denotar o grau mínimo entre os vértices de G. A prova do lema 50 segue de três fatos.

Fato 1 Existem conjuntos $V_i' \subset V_i$ com $|V_i'| \geq (1-2\varepsilon)m$ $(i = 1,2,3)$ tais que $H_{1,2} = H[V_1', V_2']$ e $H_{2,3} = H[V_2', V_3']$ têm grau mínimo $\delta(H_{1,2}) \geq (1-\delta/4)d_{1,2}pm$ e $\delta(H_{2,3}) \geq (1-\delta/4)d_{2,3}pm$

Prova. Este fato segue do lema 49. □

Fato 2 Para $(i,j) = (1,2)$ e $(i,j) = (2,3)$, o grafo bipartido $H_{i,j} = H[V_i', V_j']$ é $((1-\delta/2)d_{i,j}m/f, f)$-expansor para todo $0 < f \leq (\delta\rho\mu/4A)^2 d$.

Prova. Fixe $(i,j) \in \{(1,2),(2,3)\}$ e $\sigma \in \{i,j\}$, e suponha que $0 < f \leq (\delta\rho\mu/4A)^2 d$. Tome $U \subset V_\sigma'$ com $u = |U| \leq (1-\delta/2)d_{i,j}m/f$ e seja $W = \Gamma_{H_{i,j}}(U)$. Suponha por absurdo que $w = |W| < fu$. Então, pelo fato 1 e pela (p,A)-uniformidade de G, temos

$$\left(1-\frac{\delta}{4}\right)d_{i,j}pmu \leq e_{H_{i,j}}(U,W) \leq e_G(U,W)$$
$$\leq puw + A(duw)^{1/2} \leq \left(1-\frac{\delta}{2}\right)d_{i,j}pmu + A(duw)^{1/2}.$$

Logo $(\delta/4)d_{i,j}pmu \leq A(duw)^{1/2}$, e portanto $w \geq (\delta\rho\mu/4A)^2 du \geq fu$, o que é uma contradição. Logo $|\Gamma_{H_{i,j}}(U)| \geq f|U|$, como queríamos. □

Fato 3 Para todo $x \in V_1'$, temos $|\Gamma_{J_l}(x) \cap V_3'| \geq (1-3\delta/4)\gamma m$.

Prova. Note que $d = pn = CA^2 n^{1/2l}$, e portanto $H_{1,2}$ e $H_{2,3}$ são $((1-\delta/2)d_{i,j}m/f, f)$-expansores para $0 < f \leq 2n^{1/2l}$. Agora, fixe $x \in V_1'$, e seja $X_0 = \{x\}$. Escolha conjuntos $X_1, X_2, \ldots, X_{2l-1}$ tais que $n^{i/2l} \leq |X_i| \leq 2n^{i/2l}$ para $1 \leq i \leq 2l-1$, e $X_1 \subset \Gamma_{H_{1,2}}(X_0)$, $X_2 \subset \Gamma_{H_{1,2}}(X_1) \setminus X_0$,..., $X_{2l-1} \subset \Gamma_{H_{1,2}}(X_{2l-2}) \setminus (X_1 \cup \ldots \cup X_{2l-3})$. Finalmente, seja $X_{2l} = \Gamma_{H_{2,3}}(X_{2l-1})$. O resultado segue do fato 2. □

O lema 50 segue dos fatos 1 e 3, pois $e(J_l[V_1, V_3]) \geq (1-3\delta/4)\gamma m|V_1'| \geq (1-\delta)\gamma m^2$. □

Agora podemos provar o lema 47, dos pares proibidos.

Demonstração do lema 47. Fixe um inteiro $l \geq 1$, e fixe também reais $0 < \delta \leq 1$, $0 < \gamma_0 \leq 1$, além de uma A-função $A = A(n)$. Pela natureza do parâmetro δ, podemos assumir que $\delta \leq 15\gamma_0$. Seja $\varepsilon = \gamma_0\delta^2/2160$ e $k_0 = \lceil 1/\varepsilon \rceil$, e sejam $0 < \eta = \eta(\varepsilon, k_0) \leq 1$ e $K_0 = K_0(\varepsilon, k_0) \geq k_0$ valores

encontrados via teorema 45 (versão esparsa do lema de Szemerédi). Note que podemos assumir que $\eta \leq \varepsilon/(2K_0)$. Seja $\rho = \gamma_0\delta/15 \leq 1$, e, finalmente, seja $C_0 = C_0(l, \delta, \gamma_0) = 10^7(K_0/\delta^2\gamma_0)^2$. Mostraremos que esta escolha de C_0 é apropriada para o lema.

Sejam então H um subgrafo de um grafo (p, A)-uniforme $G = G^n$ com $\gamma = e(H)/e(G) \geq \gamma_0$ e $p = p(n) \geq C_0 A^2 n^{-1+1/2l}$. Podemos assumir que $V(H) = V(G)$, e que n é maior que uma certa constante grande, adequadamente escolhida. Pelo lema 26, temos que G é η-regular com densidade p. Aplicamos agora o teorema 45 a $H \subset G$ para obter uma partição $P = (V_i)_{i=0}^k$ de $V = V(G)$ que é (ε, H, G)-regular e (ε, k)-equitável, com $k_0 \leq k \leq K_0$. Seja $m = |V_i|$ $(1 \leq i \leq k)$. Note que $m \geq n(1-\varepsilon)/k$.

Usaremos agora as idéias de grafo reduzido e grafo limpo, adaptadas ao contexto da versão esparsa do Lema de Regularidade. Seguiremos a notação de [19], usando H^* para o grafo reduzido, e H' para o grafo limpo. Definimos o grafo reduzido H^* por $V(H^*) = [k]$ e $ij \in E(H^*)$ $(1 \leq i < j \leq k)$ se e só se (V_i, V_j) é um par (ε, H, G)-regular com $d_{H,G}(V_i, V_j) \geq \rho$. Para $e = ij \in E(H^*)$, seja $\gamma_e = d_{H,G}(V_i, V_j)$, e seja $\bar{\gamma} = (\gamma_e)_{e \in E(H^*)}$. Podemos supor que $\chi = (1, 2, \ldots, k)$ é uma ordenação que respeita $\bar{\gamma}$. Por último, definimos um grafo $H' \subset H$ com $V(H') = V(H)$ e tal que $xy \in E(H)$ é aresta de H' se e só se $x \in V_i$ e $y \in V_j$ para algum par $\{i, j\}$ com $1 \leq i < j \leq k$ e $ij \in E(H^*)$. Mostraremos que, a exemplo do que ocorre na versão original do Lema de Regularidade, o grafo limpo H' ainda tem grande parte das arestas de H. Note que o número de arestas de H é $e(H) = \gamma e(G) \sim \gamma p\binom{n}{2}$.

Fato 1 Temos $e(H') \geq (1 - \delta/6)\gamma p\binom{n}{2}$.

Prova. Estimaremos $|E(H) \setminus E(H')|$. Da (p, A)-uniformidade de G e dos lemas 26 e 28, segue que, para todo $W \subset V(G)$ com $|W| \geq 3\eta n$, temos $e(G[W]) \leq (1 + \eta)p\binom{|W|}{2}$, se n é suficientemente grande. Logo $e(H[V_0]) \leq \varepsilon^2 pn^2$.

Além disso, escrevendo como sempre $d = pn$, temos

$$e_G(V_0, V \setminus V_0) \leq p|V_0||V \setminus V_0| + A\sqrt{d|V_0||V \setminus V_0|} \leq \varepsilon pn^2 + An\sqrt{d} \leq 2\varepsilon pn^2$$

para n suficientemente grande. Note que $\sum e_G(V_i, V_j)$ com a soma sobre todos os $1 \leq i < j \leq k$ tais que (V_i, V_j) não é (ε, H, G)-regular é no máximo $\varepsilon\binom{k}{2}(1 + \eta)pm^2 \leq \varepsilon pn^2$. Já a soma $\sum e_H(V_i, V_j)$ sobre todos os $1 \leq i < j \leq k$ tais que $d_{H,G}(V_i, V_j) \leq \rho$ é no máximo $\rho\binom{k}{2}(1 + \eta)pm^2 \leq \rho pn^2$. Para n suficientemente grande, temos que $\sum_{1 \leq i \leq k} e(G[V_i]) \leq k(1 + \eta)p\binom{m}{2} \leq pn^2/k$. Portanto $|E(H) \setminus E(H')| \leq (4\varepsilon + \rho + 1/k)pn^2 \leq (5\varepsilon + \rho)pn^2$ se n é

suficientemente grande. Por outro lado, temos $e(H) = \gamma e(G) \geq \gamma(1-\eta)p\binom{n}{2}$, e então segue que

$$e(H') \geq \gamma(1-\eta)p\binom{n}{2} - 2(6\varepsilon+\rho)p\binom{n}{2} = \left(1-\eta-12\frac{\varepsilon}{\gamma}-2\frac{\rho}{\gamma}\right)\gamma p\binom{n}{2}$$
$$\geq \left(1-\frac{\delta}{6}\right)\gamma p\binom{n}{2}.$$

□

Aplicaremos agora o lema 48 a $(H^*, \bar{\gamma})$. Como no lema 48, seja $\bar{\gamma}(H^*) = \sum_{e\in E(H^*)} \gamma_e$.

Fato 2 Temos $\bar{\gamma}(H^*) \geq (1-\delta/2)\gamma k^2/2$.

Prova. Esta afirmação segue facilmente do fato 1. Note que

$$\left(1-\frac{\delta}{6}\right)\gamma p\binom{n}{2} \leq e(H') = \sum_{e=ij\in E(H^*)} e_H(V_i, V_j)$$
$$= \sum_{e=ij\in E(H^*)} \gamma_e e_G(V_i, V_j) \leq (1+\eta)pm^2\bar{\gamma}(H^*) \leq (1+\eta)p\frac{n^2}{k^2}\bar{\gamma}(H^*).$$

Logo

$$\bar{\gamma}(H^*) \geq \frac{1-\delta/6}{1+\eta}\left(1-\frac{1}{n}\right)\gamma\frac{k^2}{2} \geq \left(1-\frac{\delta}{2}\right)\gamma\frac{k^2}{2}.$$

□

Finalmente, mostraremos que $e(J_l(H)) \geq (1-\delta)\gamma\binom{n}{2}$. Fixe $1 \leq i < j \leq k$. Pelo lema 50, aplicado com $\delta/6$, temos que $e(J_l[V_i, V_j]) \geq (1-\delta/6)w(i,j)m^2$, onde $w(i,j) = w_{H^*,\bar{\gamma}}(i,j)$ foi definido antes do lema 48. Segue do fato 2 e do lema 48 que

$$e(J_l(H)) \geq \sum_{1\leq i<j\leq k} e(J_l[V_i, V_j])$$
$$\geq \left(1-\frac{\delta}{6}\right)m^2\left(w(H^*, \bar{\gamma}, x) - \sum_{1\leq i\leq k} w(i,i)\right)$$
$$\geq \left(1-\frac{\delta}{6}\right)m^2\bar{\gamma}(H^*) - km^2 \geq \frac{1}{2}\left(1-\frac{2\delta}{3}\right)\gamma k^2m^2 - \frac{n^2}{k}$$
$$\geq \frac{1}{2}(1-\varepsilon)^2\left(1-\frac{2\delta}{3}\right)\gamma n^2 - \varepsilon n^2 \geq (1-\delta)\gamma\binom{n}{2},$$

como queríamos. □

4.2 O teorema Schur(η)

Nosso objetivo nesta seção é provar o teorema 13. Vamos lembrar algumas definições dadas na seção 1. Dizemos que $S \subset \mathbb{Z}_n$ tem a propriedade Schur(η) se todo $D \subset S$ com $|D| \geq (1/2+\eta)|S|$ contém uma tripla de Schur. Lembramos que $\mathbb{Z}_{n,p}$ é um subconjunto aleatório de $\mathbb{Z}_n$ obtido por n sorteios independentes com probabilidade p.

Vamos agora discutir os parâmetros do enunciado do problema 12. Em primeiro lugar, observa-se que ao tratarmos da propriedade PA_3 (teorema 6), a densidade pode ser qualquer $\eta > 0$, enquanto que no problema 12 impomos a condição de que a densidade deve ser maior que $1/2$. O motivo disso é o seguinte. Fixe n par. Para pelo menos metade dos conjuntos $\mathbb{Z}_{n,p}$, vale que a quantidade de elementos ímpares é maior ou igual à quantidade de elementos pares (note que como n é par, podemos de fato falar em paridade em $\mathbb{Z}_n$). Se exigirmos apenas que $|D| = (1/2)|\mathbb{Z}_{n,p}|$, o enunciado do teorema torna-se falso, pois para cada um dos $\mathbb{Z}_{n,p}$ com mais ímpares que pares descritos acima, podemos tomar D como sendo os elementos ímpares de $\mathbb{Z}_{n,p}$ (logo $|D| \geq (1/2)|\mathbb{Z}_{n,p}|$), e não haverá solução em D da equação de Schur pois a soma de dois ímpares em $\mathbb{Z}_n$ (n par) dá sempre par. Assim, a probabilidade de $\mathbb{Z}_{n,p}$ ter a propriedade Schur(η) para $\eta = 0$ é no máximo $1/2$. Mesmo quando n é ímpar, não podemos permitir que a densidade seja qualquer real positivo; de fato, como ficará claro quando falarmos sobre a generalização deste problema para grupos abelianos finitos, a densidade sempre deverá ser um pouco maior que $2/7$.

Agora falemos sobre a probabilidade $p = p(n)$. Vamos mostrar que se $p(n)/n^{-1/2} \to 0$ quando $n \to \infty$, então quase certamente $\mathbb{Z}_{n,p}$ *não* tem a propriedade Schur(η). De fato, existem n^2 triplas (x, y, z) de $\mathbb{Z}_n$ que satisfazem $x + y = z$ (uma tripla assim é dita uma *tripla de Schur*), e, em média, p^3n^2 delas são tais que $x, y, z \in \mathbb{Z}_{n,p}$. Devido à hipótese imposta sobre p, temos que o número esperado de triplas de Schur em $\mathbb{Z}_{n,p}$, n^2p^3, é muito menor que np, o tamanho esperado de $\mathbb{Z}_{n,p}$. Assim, para quase todo $\mathbb{Z}_{n,p}$, podemos apagar no máximo $o(|\mathbb{Z}_{n,p}|)$ pontos de $\mathbb{Z}_{n,p}$ destruindo todas as triplas de Schur contidas em $\mathbb{Z}_{n,p}$. Daí segue que, com probabilidade tendendo a 1 quando $n \to \infty$, $\mathbb{Z}_{n,p}$ não tem a propriedade Schur(η).

Usaremos a seguir os conceitos de par proibido e elemento proibido. Vimos na seção anterior que um par proibido por H, ou, mais precisamente, um par l-proibido por H, é simplesmente um par $\{x, y\}$ tal que

$xy \in E(J_l(H))$. Ao longo desta seção, por "par proibido" entenda-se sempre "par 1-proibido". Ou seja, $\{x, y\}$ é um par proibido por H se existe $z \notin \{x, y\}$ tal que $xz, zy \in E(H)$.

Se $D \subset \mathbb{Z}_n$, dizemos que $x \in \mathbb{Z}_n$ é um elemento proibido por D, e que D proíbe x, se $x \in (D - D) = \{d_1 - d_2 \colon d_1, d_2 \in D\}$. O nome "elemento proibido" vem da seguinte observação. Se D não contém triplas de Schur, então $D \cap (D - D) = \emptyset$. De fato, se temos $x \in D \cap (D - D)$, então $x \in D$ escreve-se como $z - y$ com $y, z \in D$, e portanto $x + y = z$, absurdo. Logo, um elemento proibido por D não pode estar em D, se D não tem triplas de Schur.

Vamos agora dar algumas palavras sobre os próximos lemas. O lema 51 serve para mostrar que o grafo $\mathrm{CG}(\mathbb{Z}_{n,p}) = \mathrm{CG}_n^+(\mathbb{Z}_{n,p})$ é quase certamente (p, A)-uniforme (neste capítulo, estaremos sempre nos referindo ao grafo de Chung-Graham com adição). Isso será importante para podermos usar o lema dos pares proibidos na nossa demonstração. O lema 52 afirma, grosso modo, que se $D \subset R \subset \mathbb{Z}_n$, então $e(\mathrm{CG}_n(D))/e(\mathrm{CG}_n(R)) \geq |D|/|R|$. O lema 53 servirá para converter pares proibidos pelo grafo $\mathrm{CG}(D)$ em elementos proibidos por D. Finalmente, todos esses lemas serão usados para provar o principal resultado auxiliar da seção, o lema dos elementos proibidos (lema 54). Grosso modo, este lema nos diz que se $B \subset \mathbb{Z}_{n,p}$ e $|B|/|\mathbb{Z}_{n,p}| = \gamma_0$, então quase certamente B proíbe pelo menos $\gamma_0 n$ elementos de $\mathbb{Z}_n$. Vamos agora aos lemas.

O lema a seguir é o "ponto fraco" da nossa demonstração. É por causa dele que só conseguimos provar o teorema 13, em vez de resolver o problema 12. Nós só conseguimos mostrar que $\mathrm{CG}(\mathbb{Z}_{n,p})$ é (p, A)-uniforme para $A = \sqrt{24 \log n}$. O ideal (veja a próxima seção) seria provar isto para A igual a uma constante.

Lema 51. *Para todo $p = p(n)$, temos quase certamente que $\mathrm{CG}(\mathbb{Z}_{n,p}) = \mathrm{CG}_n(\mathbb{Z}_{n,p})$ é (p, A)-uniforme para $A = \sqrt{24 \log n}$.*

Prova. Daqui em diante, usaremos as letras especiais $\mathbb{P}$ e $\mathbb{E}$ para denotar probabilidade e esperança, respectivamente. Lembrando que o grafo $\mathrm{CG}_n^+(R)$ é (p, A)-uniforme se $\max_{j \neq 0} |\mathcal{T}(R)(j)| \leq A\sqrt{pn}$, o lema seguirá facilmente do fato abaixo.

Fato Para todo $j \neq 0$ e $0 < t \leq pn\sqrt{2}/2$, temos $\mathbb{P}(|\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq t) \leq 8e^{-t^2/12np}$.

Prova. Fixe $j \neq 0$. Se $z \in \mathbb{C}$, usaremos as notações $\mathrm{Re}(z)$ e $\mathrm{Im}(z)$ para denotar as partes real e imaginária de z. Note que se $|z| \geq t$, então ou

$|\operatorname{Re}(z)| \geq t/\sqrt{2}$ ou $|\operatorname{Im}(z)| \geq t/\sqrt{2}$. Logo

$$\begin{aligned}\mathbb{P}(|\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq t) \\ \leq \mathbb{P}\Big(|\operatorname{Re}\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq \frac{t}{\sqrt{2}}\Big) + \mathbb{P}\Big(|\operatorname{Im}\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq \frac{t}{\sqrt{2}}\Big). \quad (4.1)\end{aligned}$$

Sejam $(X_r)_{r\in\mathbb{Z}_n}$ variáveis aleatórias dadas por

$$X_r = \begin{cases} \operatorname{Re} e^{-2\pi ijr/n} = \cos(-2\pi jr/n) & \text{com probabilidade } p, \\ 0 & \text{com probabilidade } 1-p, \end{cases}$$

e, além disso, sejam $(X_r^+)_{r\in\mathbb{Z}_n}$ e $(X_r^-)_{r\in\mathbb{Z}_n}$ variáveis aleatórias dadas por $X_r^+ = \max\{X_r, 0\}$ e $X_r^- = -\min\{X_r, 0\}$. Segue que $0 \leq X_r^+ \leq 1$, $0 \leq X_r^- \leq 1$ e $X_r = X_r^+ - X_r^-$. Além disso, temos

$$X_r^+ = \frac{X_r + |X_r|}{2} \quad \text{e} \quad X_r^- = \frac{|X_r| - X_r}{2}.$$

Sejam também $X = \sum_{r\in\mathbb{Z}_n} X_r$, $X^+ = \sum_{r\in\mathbb{Z}_n} X_r^+$ e $X^- = \sum_{r\in\mathbb{Z}_n} X_r^-$. Temos

$$\mathbb{E}(X) = \sum_{r\in\mathbb{Z}_n} \mathbb{E}(X_r) = \sum_{r\in\mathbb{Z}_n} p \operatorname{Re}(e^{-2\pi ijr/n}) = p \operatorname{Re}(\sum_{r\in\mathbb{Z}_n} e^{-2\pi ijr/n}) = 0,$$

e

$$\mathbb{E}(X^+) = \sum_{r\in\mathbb{Z}_n} \mathbb{E}(X_r^+) = \frac{\sum_{r\in\mathbb{Z}_n} \mathbb{E}(X_r) + \sum_{r\in\mathbb{Z}_n} \mathbb{E}(|X_r|)}{2} = \frac{\sum_{r\in\mathbb{Z}_n} \mathbb{E}(|X_r|)}{2}.$$

Seja $\alpha = \mathbb{E}(X^+) = \sum_{r\in\mathbb{Z}_n} \mathbb{E}(|X_r|)/2$. É fácil ver que $\alpha = \mathbb{E}(X^-)$ e que $\alpha \leq pn/2$. Note também que

$$\begin{aligned}2\alpha = \sum_{r\in\mathbb{Z}_n} \mathbb{E}(|X_r|) = p \sum_{r\in\mathbb{Z}_n} |\cos(-2\pi jr/n)| \\ \geq p \sum_{r\in\mathbb{Z}_n} \cos(-2\pi jr/n)^2 = \frac{p}{2} \sum_{r\in\mathbb{Z}_n} (1 + \cos(-4\pi jr/n)) = pn/2,\end{aligned}$$

de onde segue que $\alpha \geq pn/4$. Pela desigualdade de Hoeffding (lema 23), para todo $0 < v < 1$, temos $\mathbb{P}\big(|X^+ - \alpha| \geq v\alpha\big) \leq 2\exp\big(-v^2\alpha/3\big)$ e $\mathbb{P}\big(|X^- - \alpha| \geq v\alpha\big) \leq 2\exp\big(-v^2\alpha/3\big)$, logo temos $\mathbb{P}\big(|X| \geq 2v\alpha\big) \leq 4\exp\big(-v^2\alpha/3\big)$. Equivalentemente, para todo $0 < t \leq 2\sqrt{2}\alpha$, temos $\mathbb{P}\big(|X| \geq t/\sqrt{2}\big) \leq$

$4\exp\big(-t^2/(24\alpha)\big)$. Como $\alpha \leq pn/2$, temos $\mathbb{P}\big(|X| \geq t/\sqrt{2}\big) \leq 4\exp\big(-t^2/(12pn)\big)$. Mas isto equivale a dizer que

$$\mathbb{P}\Big(|\operatorname{Re}\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq \frac{t}{\sqrt{2}}\Big) \leq 4\exp\big(-t^2/(12pn)\big).$$

Analogamente, provamos que

$$\mathbb{P}\Big(|\operatorname{Im}\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq \frac{t}{\sqrt{2}}\Big) \leq 4\exp\big(-t^2/(12pn)\big),$$

e a prova do fato está concluída, pela equação 4.1. □

Com isso, é fácil provar o lema 51, pois $\mathbb{P}(|\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq \sqrt{24pn\log n}) \leq 8e^{-2\log n} = 8/n^2$, e portanto

$$\mathbb{P}\Big(\max_{j\neq 0}|\mathcal{T}(\mathbb{Z}_{n,p})(j)| \geq \sqrt{24pn\log n}\Big) \leq 8/n,$$

o que conclui a prova. □

Lema 52. *Sejam D e R tais que $D \subset R \subset \mathbb{Z}_n$ e $|D| = c|R|$. Então $e(\mathrm{CG}_n(D)) \geq c(1-2/n)e(\mathrm{CG}_n(R))$.*

Prova. Vamos mostrar inicialmente que, para todo $D \subset \mathbb{Z}_n$, temos $|D|n/2 \leq e(\mathrm{CG}_n(D)) \leq (1+2/n)|D|n/2$. Dados $B \subset \mathbb{Z}_n$ e $x \in \mathbb{Z}_n \setminus B$, examinaremos as arestas que estão em $\mathrm{CG}_n(B\cup\{x\})$ e que não estão em $\mathrm{CG}_n(B)$ (note que $\mathrm{CG}_n(B)$ é subgrafo de $\mathrm{CG}_n(B\cup\{x\})$). Ao acrescentar x a B, incluímos as arestas $\{i,j\}$ com $i+j=x$. Suponha primeiramente que n é ímpar, $n=2m+1$. É fácil ver que incluiremos $m+1$ novas arestas. Se n for par $(n=2m)$, incluiremos m arestas se x for ímpar, e $m+1$ arestas se x for par. Note que, em todos os casos, o número de arestas que foram incluídas está entre $n/2$ e $n/2+1$.

Acrescentando um a um os $|D|$ elementos de D, teremos que o número total de arestas incluídas, $e(\mathrm{CG}_n(D))$, satisfaz

$$|D|\frac{n}{2} \leq e(\mathrm{CG}_n(D)) \leq |D|\frac{n}{2} + |D| = (1+\frac{2}{n})|D|\frac{n}{2}, \tag{4.2}$$

que é o que queríamos. Com isso, temos

$$\frac{e(\mathrm{CG}_n(D))}{e(\mathrm{CG}_n(R))} \geq \frac{|D|n/2}{(1+2/n)|R|n/2} = \frac{c}{(1+2/n)} \geq c\left(1-\frac{2}{n}\right).$$

□

Lema 53 (Lema de conversão). *Se a quantidade de pares proibidos por* $\mathrm{CG}_n(D)$*,* $e(J_1(\mathrm{CG}_n(D))$*, é maior ou igual a* $c\binom{n}{2}$*, para alguma constante* $0 < c \leq 1$*, então*

$$D - D = \{x - y \in \mathbb{Z}_n \colon x, y \in D\}$$

tem pelo menos $cn - 2$ *elementos.*

Prova. Há uma associação clara entre pares proibidos por $\mathrm{CG}_n(D)$ e elementos de $D - D$. Se $\{x, z\}$ é par proibido, existe $y \in \mathbb{Z}_n$ tal que $x + y \in D$ e $y + z \in D$. Mas então $x - z = (x + y) - (y + z) \in D - D$. O problema é que essa associação não é bijetora.

Para cada $m \in \mathbb{Z}_n$, definimos $\mathrm{rep}_n(m)$ como sendo o menor representante positivo da classe de m em $\mathbb{Z}_n$, isto é, o único elemento do conjunto $\{x \in \mathbb{Z} \colon x \equiv m \pmod{n}\} \cap \{0, 1, 2, \ldots, n-1\}$. Dado um par proibido $\{x, z\}$, definimos $d(x, z) = \min\{\mathrm{rep}_n(x - z), \mathrm{rep}_n(z - x)\}$ (é a menor distância entre as classes de x e z em $\mathbb{Z}_n$).

A função d acima descrita leva um par proibido $\{x, z\}$ em um elemento $d(x, z)$ de $(D - D) \cap \{1, 2, \ldots, \lfloor n/2 \rfloor\}$ (observe que estamos olhando para $\{1, 2, \ldots, \lfloor n/2 \rfloor\} = \{\bar{1}, \bar{2}, \ldots, \lfloor \bar{n/2} \rfloor\}$ como subconjunto de $\mathbb{Z}_n$ e não de $\mathbb{Z}$). Note que $\{x, z\}$ é par proibido em $\mathrm{CG}_n(D)$ se e só se existe $y \in \mathbb{Z}_n$ tal que $x + y \in D$ e $y + z \in D$. Mas isso equivale a dizer que para todo $t \in \mathbb{Z}_n$ temos $(x + t) + (y - t) \in D$ e $(y - t) + (z + t) \in D$. Com isso provamos que $\{x, z\}$ é par proibido se e só se $\{x + t, z + t\}$ é par proibido para todo t. Assim, para todo k pertencente à imagem de d, temos $|d^{-1}(k)| = n$, e segue que

$$|(D - D) \cap \{1, 2, \ldots, \lfloor n/2 \rfloor\}| \geq \frac{c\binom{n}{2}}{n} = \frac{c(n-1)}{2},$$

e analogamente temos $|(D - D) \cap \{\lceil n/2 \rceil, \ldots, n - 1\}| \geq c(n-1)/2$. Finalmente, somamos as duas últimas equações, obtendo

$$|D - D| \geq c(n-1) - 1 \geq cn - 2,$$

onde o "-1" certifica que, no caso em que n é par (e portanto $\lfloor n/2 \rfloor = \lceil n/2 \rceil = n/2$), não contamos duas vezes $|(D - D) \cap \{n/2\}|$.

□

O grafo $J = J_1$ que aparece na demonstração do lema abaixo é o grafo dos pares 1-proibidos.

Lema 54 (Lema dos elementos proibidos). *Dados reais* $0 < \delta \leq 1$ *e* $0 < \gamma_0 \leq 1$*, existe uma constante* $C_0 = C_0(\delta, \gamma_0) > 0$ *tal que, se* $p = p(n) \geq C_0 \log n/\sqrt{n}$*, então, para* n *suficientemente grande, vale o seguinte.*

Se $\mathrm{CG}_n(\mathbb{Z}_{n,p})$ *é* $(p, \sqrt{24 \log n})$*-uniforme e se* $B \subset \mathbb{Z}_{n,p}$ *é tal que* $|B| \geq \gamma_0 |\mathbb{Z}_{n,p}|$*, o número de elementos proibidos por* B *é pelo menos* $(1-\delta)(|B|/|\mathbb{Z}_{n,p}|)n$*.*

Prova. Seja $C^* = C^*(l, \delta, \gamma_0)$ a constante determinada pelo lema 47. Para provar o presente lema, escolha $C_0 = 24C^*(1, \delta/2, \gamma_0/2)$. Pelo lema 52, temos que

$$e(\mathrm{CG}_n(B))/e(\mathrm{CG}_n(\mathbb{Z}_{n,p})) \geq (1 - 2/n)|B|/|\mathbb{Z}_{n,p}|.$$

Pelo lema 47, e pela escolha de C_0, vemos que

$$\begin{aligned} e(J_1(\mathrm{CG}_n(B)) &\geq (1-\delta/2)\frac{e(\mathrm{CG}_n(B))}{e(\mathrm{CG}_n(\mathbb{Z}_{n,p}))}\binom{n}{2} \\ &\geq (1-\delta/2)\frac{|B|}{|\mathbb{Z}_{n,p}|}\left(1-\frac{2}{n}\right)\binom{n}{2}. \quad (4.3) \end{aligned}$$

Finalmente, segue do lema de conversão (lema 53) que

$$|B-B| \geq (1-\delta/2)\frac{|B|}{|\mathbb{Z}_{n,p}|}\left(1-\frac{2}{n}\right)n - 2 \geq (1-\delta)\frac{|B|}{|\mathbb{Z}_{n,p}|}n$$

para n suficientemente grande. □

Vamos agora falar sobre as linhas gerais da prova do teorema 13. Queremos mostrar que quase certamente $\mathbb{Z}_{n,p}$ tem a propriedade Schur(η). Fixe uma realização $\mathbb{Z}_{n,p}$ e seja $D \subset \mathbb{Z}_{n,p}$ tal que $|D| = (1/2+\eta)|\mathbb{Z}_{n,p}|$ e tal que D não contém triplas de Schur. Quebraremos $\mathbb{Z}_{n,p}$ em $k+1$ partes $(Z_i)_{i=1}^{k+1}$, sendo as k primeiras partes bem pequenas, e a última de tamanho aproximadamente $|\mathbb{Z}_{n,p}|/2$. Mostraremos que uma das partes menores é tal que $D \cap Z_i$ proíbe muitos elementos, o que implica que $|D-D| \geq |(D \cap Z_i) - (D \cap Z_i)|$ é grande. Olharemos em seguida para Z_{k+1} e concluiremos que, com alta probabilidade, há muitos elementos proibidos por D dentro de Z_{k+1}, e, como devemos ter $(D-D) \cap D = \emptyset$, não haverá "espaço" suficiente dentro de Z_{k+1} para os elementos de $D \cap Z_{k+1}$, o que é um absurdo. Vamos detalhar um pouco mais estas idéias, antes de demonstrar formalmente o teorema.

Prova do teorema 13 (esboço). Podemos imaginar que jogamos o seguinte jogo: nós sorteamos $\mathbb{Z}_{n,p}$, um adversário escolhe um subconjunto $D \subset \mathbb{Z}_{n,p}$ com densidade $1/2+\eta$ e aí nós temos que achar uma tripla de Schur em D para vencer o jogo. O que queremos provar é que para a enorme maioria dos $\mathbb{Z}_{n,p}$ sorteados, nós venceremos, por melhor que jogue nosso adversário.

Em primeiro lugar, observamos que basta nos concentrarmos no caso $p = o(1)$. Daremos uma prova "rascunhada" desta observação. Suponha que provamos o teorema para alguma função $p = p(n)$, e agora queremos prová-lo para uma função $p' = p'(n) \geq p(n)$. Fixe $D \subset \mathbb{Z}_{n,p'}$ com $|D| \geq (1/2 + \eta)|\mathbb{Z}_{n,p'}|$. Agora, sorteie um subconjunto $\mathbb{Z}^*_{n,p'} \subset \mathbb{Z}_{n,p'}$, colocando cada elemento de $\mathbb{Z}_{n,p'}$ em $\mathbb{Z}^*_{n,p'}$ com probabilidade p/p'.

Seja $\mathcal{Z}(n,p)$ o espaço de probabilidade formado pelos subconjuntos aleatórios de $\mathbb{Z}_n$ em que cada elemento $x \in \mathbb{Z}_n$ entra no subconjunto com probabilidade p (isto é, $\mathcal{Z}(n,p)$ é o espaço dos $\mathbb{Z}_{n,p}$). Então é claro que $\mathbb{Z}^*_{n,p'} \in \mathcal{Z}(n,p)$. Com alta probabilidade, temos que $D^* = D \cap \mathbb{Z}^*_{n,p'}$ tem cardinalidade aproximadamente $(p/p')|D|$, logo com alta probabilidade vale que $|D^*| \geq (1/2 + \eta/2)|\mathbb{Z}^*_{n,p'}|$, e, por hipótese, já sabemos que quase certamente D^* tem uma tripla de Schur. Mas isto implica que D contém uma tripla de Schur, que é o que queríamos.

Fixe então $p = p(n) = o(1)$. Escrevemos $\mathbb{Z}_{n,p} \in \mathcal{Z}(n,p)$ como uma união de dois subconjuntos aleatórios de $\mathcal{Z}(n,p_1)$, onde $(1-p) = (1-p_1)^2$:

$$\mathbb{Z}_{n,p} = \mathbb{Z}^{(1)}_{n,p_1} \cup \mathbb{Z}^{(2)}_{n,p_1},$$

e agora escrevemos $\mathbb{Z}^{(1)}_{n,p_1}$ como uma união de k elementos de $\mathcal{Z}(n,p_2)$, onde k é uma constante grande que será escolhida depois, e p_2 é tal que $(1-p_1) = (1-p_2)^k$. Temos

$$\mathbb{Z}^{(1)}_{n,p_1} = \bigcup_{i=1}^{k} Z_i = \bigcup_{i=1}^{k} \mathbb{Z}^{(i)}_{n,p_2},$$

onde $Z_i = \mathbb{Z}^{(i)}_{n,p_2}$. Como $p = o(1)$, temos $p_1 \sim p/2$ e $p_2 \sim p_1/k \sim p/2k$.

Basicamente, o que fizemos até aqui foi dizer ao nosso adversário: "Em vez de sortearmos $\mathbb{Z}_{n,p}$ de uma vez, iremos fazer isto em $k+1$ etapas, sendo que os k primeiros 'pedaços' serão pequenos e o último terá aproximadamente metade de $\mathbb{Z}_{n,p}$". Dado que o último pedaço sorteado tem só metade de $\mathbb{Z}_{n,p}$ e como o adversário deve escolher uma fração $1/2 + \eta$ de $\mathbb{Z}_{n,p}$, ele é obrigado a pegar alguns elementos entre os k primeiros pedaços. Iremos nos concentrar no pedaço j ($1 \leq j \leq k$) com maior densidade. Vamos agora tornar isto mais preciso.

Suponha que $D \subset \mathbb{Z}_{n,p}$ é tal que $|D| = (1/2+\eta)|\mathbb{Z}_{n,p}|$ mas D não contém soluções da equação de Schur. Sejam γ_1 e γ_2 as densidades de $D \cap \mathbb{Z}^{(1)}_{n,p_1}$ em $\mathbb{Z}^{(1)}_{n,p_1}$ e de $D \cap \mathbb{Z}^{(2)}_{n,p_1}$ em $\mathbb{Z}^{(2)}_{n,p_1}$, respectivamente. Ou seja, temos

$$|D \cap \mathbb{Z}^{(1)}_{n,p_1}| = \gamma_1 |\mathbb{Z}^{(1)}_{n,p_1}| \quad \text{e} \quad |D \cap \mathbb{Z}^{(2)}_{n,p_1}| = \gamma_2 |\mathbb{Z}^{(2)}_{n,p_1}|.$$

Com alta probabilidade, temos $\gamma_1 + \gamma_2 \sim 1 + 2\eta$.

Para $1 \leq i \leq k$, definimos os conjuntos D_i por $D_i = D \cap Z_i$ e as densidades $\gamma_i^{(2)}$ por $|D_i| = \gamma_i^{(2)}|Z_i|$. Seja j ($1 \leq j \leq k$) tal que $\gamma_j^{(2)} = \max_{1\leq i\leq k} \gamma_i^{(2)}$ e seja $\gamma^* = \gamma_j^{(2)}$. Observe que temos $\gamma^* \geq \gamma_1 > 2\eta$. Aplicando o lema 54 (juntamente com o lema 51) a $D_j \subset \mathbb{Z}_{n,p_2}^{(j)}$, temos quase certamente que

$$|D - D| \geq |D_j - D_j| \geq (1 - \delta)\gamma^* n.$$

Vamos lembrar que δ é tão pequeno quanto desejarmos, de modo que o resultado acima diz, grosso modo, que $|D - D| \geq \gamma^* n$. Já vimos que os elementos de $D - D$ são chamados de elementos proibidos justamente porque se $x \in D - D$, x não pode estar em D. Usaremos este fato ($(D - D) \cap D = \emptyset$) agora. Sabe-se que a distribuição binomial com parâmetros n e p vai ficando muito concentrada na média conforme n cresce. O número de elementos de $\mathbb{Z}_{n,p_1}^{(2)}$ que são elementos proibidos por D é uma variável aleatória com distribuição binomial. Os parâmetros desta binomial são $|D - D| \geq \gamma^* n$ (número de ensaios de Bernoulli) e p_1 (probabilidade), e portanto é extremamente improvável que tal número de elementos seja muito menor que $p_1\gamma^* n \sim \gamma^*|\mathbb{Z}_{n,p_1}^{(2)}|$. Como já observamos, $D \cap \mathbb{Z}_{n,p_1}^{(2)}$ não pode conter nenhum elemento proibido. Como, aproximadamente, uma proporção γ^* dos elementos de $\mathbb{Z}_{n,p_1}^{(2)}$ são proibidos, $D \cap \mathbb{Z}_{n,p_1}^{(2)}$ deve estar contido entre os $(1 - \gamma^*)|\mathbb{Z}_{n,p_1}^{(2)}|$ elementos restantes de $\mathbb{Z}_{n,p_1}^{(2)}$. Mas isto é muito improvável, já que $|D \cap \mathbb{Z}_{n,p_1}^{(2)}| = \gamma_2|\mathbb{Z}_{n,p_1}^{(2)}|$ e

$$\gamma_2|\mathbb{Z}_{n,p_1}^{(2)}| \sim (1 + 2\eta - \gamma_1)|\mathbb{Z}_{n,p_1}^{(2)}| \geq (1 + 2\eta - \gamma^*)|\mathbb{Z}_{n,p_1}^{(2)}| > (1 - \gamma^*)|\mathbb{Z}_{n,p_1}^{(2)}|,$$

e portanto "falta espaço" em $\mathbb{Z}_{n,p_1}^{(2)}$.

Com isso, mostramos que, dado um sorteio de $\mathbb{Z}_{n,p}$, e fixadas escolhas do adversário para uma etapa j (com $1 \leq j \leq k$) e para um subconjunto $D_j \subset \mathbb{Z}_{n,p_2}^{(j)}$, iremos perder com baixíssima probabilidade. Agora, se escolhemos k suficientemente grande, esta "baixíssima probabilidade" é tão pequena que, mesmo multiplicada pelo número de escolhas do adversário para a etapa j (com $1 \leq j \leq k$) e para um subconjunto $D_j \subset \mathbb{Z}_{n,p_2}^{(j)}$, ela ainda continua bastante pequena. De fato, o número de escolhas a que nos referimos acima é limitado por $k2^{|\mathbb{Z}_{n,p_2}^{(j)}|} \sim k2^{np_2} \sim k2^{np/(2k)}$ e o fato de aparecer um $1/k$ no expoente é crucial para nós. De fato, é exatamente por esta razão que fizemos o sorteio em $k + 1$ etapas: sem isso, teríamos um problema neste ponto.

Assim, com a escolha certa de k, esta "demonstração" está completa. □

Daremos agora a demonstração formal do teorema 13.

Prova do teorema 13. Seja $k = \lceil 54\eta^{-3} \rceil$, $\varepsilon = \eta/12$, $\delta = \eta/4$, $\gamma_0 = \eta$ e seja $C = C(\eta) = 2kC_0 > 0$, onde $C_0 = C_0(\delta, \gamma_0) > 0$ é dado pelo lema dos elementos proibidos. Mostraremos que esta escolha de C servirá no teorema 13. Fixemos $p = p(n) \geq C \log n/\sqrt{n}$. Iremos assumir que n é muito grande, e, como já foi observado, podemos nos deter no caso em que $p = p(n) = o(1)$.

Seja $\mathcal{Z}(n,p)$ o espaço de probabilidade formado pelos subconjuntos de $\mathbb{Z}_n$ em que cada elemento está no subconjunto com probabilidade p, e cada sorteio é independente dos demais.

Iremos gerar $\mathbb{Z}_{n,p} \in \mathcal{Z}(n,p)$ em $k+1$ rodadas. Sejam $0 < p_1 = p_1(n) < 1$, $0 < p_2 = p_2(n) < 1$ tais que $1-p = (1-p_1)^2$ e $1-p_1 = (1-p_2)^k$. Considere agora $k+1$ conjuntos aleatórios $Z_i = \mathbb{Z}^{(i)}_{n,p_2} \in \mathcal{Z}(n,p_2)$ $(1 \leq i \leq k)$ e $Z_{k+1} = \mathbb{Z}^{(2)}_{n,p_1} \in \mathcal{Z}(n,p_1)$. Note que o conjunto $\cup_{i=1}^{k+1} Z_i = (\cup_{i=1}^{k} \mathbb{Z}^{(i)}_{n,p_2}) \cup \mathbb{Z}^{(2)}_{n,p_1}$ é um elemento de $\mathcal{Z}(n,p)$.

Formalmente, trabalharemos com

$$\begin{aligned} Z &= (Z_1, \ldots, Z_k; Z_{k+1}) \\ &= (\mathbb{Z}^{(1)}_{n,p_2}, \ldots, \mathbb{Z}^{(k)}_{n,p_2}; \mathbb{Z}^{(2)}_{n,p_1}) \in \Omega = \left(\prod_{i=1}^{k} \mathcal{Z}(n,p_2) \right) \times \mathcal{Z}(n,p_1). \quad (4.4) \end{aligned}$$

Definimos ainda $\mathbb{Z}^{(1)}_{n,p_1} = \cup_{i=1}^{k} Z_i$ e $\mathbb{Z}_{n,p} = \mathbb{Z}^{(1)}_{n,p_1} \cup \mathbb{Z}^{(2)}_{n,p_1} = \mathbb{Z}^{(1)}_{n,p_1} \cup Z_{k+1}$.

O evento que queremos evitar, $\mathcal{B}$, é "existe $D \subset \mathbb{Z}_{n,p}$ com $|D| \geq (1/2 + \eta)|\mathbb{Z}_{n,p}|$ tal que D não contém triplas de Schur". Mostraremos que a probabilidade de $\mathcal{B}$ vai a zero quando $n \to \infty$.

Lembramos que escrevemos $O_1(x)$ para denotar um termo y tal que $|y| \leq x$. Seja $\Omega' \subset \Omega$ o conjunto dos $Z = (Z_1, \ldots, Z_k; Z_{k+1}) \in \Omega$ tais que: para todo $1 \leq i \leq k$, $\mathrm{CG}_n(Z_i)$ é $(p_2, \sqrt{24 \log n})$-uniforme e $|Z_i| = (1 + O_1(\varepsilon))np/2k$; para $i = 1, 2$, $|\mathbb{Z}^{(i)}_{p_1}| = (1 + O_1(\varepsilon))np/2$; e finalmente, $|\mathbb{Z}_{n,p}| = (1 + O_1(\varepsilon))np$. Pela desigualdade de Hoeffding (lema 23) e pelo lema 51, $\mathbb{P}(\Omega') = 1 - o(1)$ quando $n \to \infty$, e portanto podemos assumir que nosso Z está em Ω'. Por essa razão, vamos nos concentrar em calcular $\mathbb{P}(\mathcal{B}')$, onde $\mathcal{B}' = \mathcal{B} \cap \Omega'$.

Antes disso, fixemos mais algumas notações. Para cada $Z \in \mathcal{B}'$, fixe $D = D(Z) \subset \mathbb{Z}_{n,p}$ com $|D| \geq (1/2+\eta)|\mathbb{Z}_{n,p}|$ e tal que D não tem triplas de Schur. Para $i = 1, 2$, sejam $D^{(1)}_i = D^{(1)}_i(Z) = D \cap \mathbb{Z}^{(i)}_{n,p_1}$, $d^{(1)}_i = d^{(1)}_i(Z) = |D^{(1)}_i|$

e $\gamma_i^{(1)} = \gamma_i^{(1)}(Z) = d_i^{(1)}/|\mathbb{Z}_{n,p_1}^{(i)}|$. Para $1 \le i \le k$, sejam $D_i^{(2)} = D_i^{(2)}(Z) = D \cap Z_i$, $d_i^{(2)} = d_i^{(2)}(Z) = |D_i^{(2)}|$ e $\gamma_i^{(2)} = \gamma_i^{(2)}(Z) = d_i^{(2)}/|Z_i|$.

Agora fixe $Z \in \mathcal{B}'$. Note que $|D| = |D(Z)| \le d_1^{(1)} + d_2^{(1)}$, e portanto

$$\begin{aligned}\frac{1}{2} + \eta \le \frac{|D|}{|\mathbb{Z}_{n,p}|} &\le \gamma_1^{(1)} \frac{|\mathbb{Z}_{n,p_1}^{(1)}|}{|\mathbb{Z}_{n,p}|} + \gamma_2^{(1)} \frac{|\mathbb{Z}_{n,p_1}^{(2)}|}{|\mathbb{Z}_{n,p}|} \\ &\le \gamma_1^{(1)} \frac{(1+\varepsilon)np_1}{(1-\varepsilon)np} + \gamma_2^{(1)} \frac{(1+\varepsilon)np_1}{(1-\varepsilon)np} \le (\gamma_1^{(1)} + \gamma_2^{(1)}) \frac{(1+3\varepsilon)}{2},\end{aligned}$$

donde concluímos que $\gamma_1^{(1)} + \gamma_2^{(1)} \ge (1+2\eta)/(1+3\varepsilon)$.

Note que $d_1^{(1)} \le d_1^{(2)} + d_2^{(2)} + \cdots + d_k^{(2)}$, e portanto temos que $\gamma_1^{(1)} \le ((1+3\varepsilon)/k) \sum_{1 \le i \le k} \gamma_i^{(2)}$. Logo, se $\gamma^* = \gamma^*(Z) \colon = \max_{1 \le i \le k} \gamma_i^{(2)}$, temos $(1+3\varepsilon)\gamma^* \ge (1+3\varepsilon)((\sum_{1 \le i \le k} \gamma_i^{(2)})/k) \ge \gamma_1^{(1)}$. Com isso, vemos que $\gamma^* + \gamma_2^{(1)} \ge (\gamma_1^{(1)} + \gamma_2^{(1)})/(1+3\varepsilon) \ge (1+2\eta)/(1+3\varepsilon)^2 \ge 1 + \eta$. Em particular, $\gamma^* \ge \eta$.

Para $1 \le j \le k$, seja $\mathcal{B}'_j = \{Z \in \mathcal{B}' \colon \gamma_j^{(2)} = \gamma^*\}$. Como $\mathcal{B}' = \cup_{j=1}^k \mathcal{B}'_j$, é suficiente mostrarmos que $\mathbb{P}(\mathcal{B}'_j) = o(1)$ quando $n \to \infty$, para todo $1 \le j \le k$. Fixemos a partir de agora algum j com $1 \le j \le k$, e consideremos $Z \in \mathcal{B}'_j$. Temos

$$\begin{aligned}\mathbb{P}(\mathcal{B}'_j) &= \sum_{Z_0} \mathbb{P}(\mathcal{B}'_j \cap \{Z \colon Z_j = Z_0\}) \\ &= \sum_{Z_0} \mathbb{P}(\mathcal{B}'_j \mid Z_j = Z_0)\mathbb{P}(Z_j = Z_0) \le \max_{Z_0} \mathbb{P}(\mathcal{B}'_j \mid Z_j = Z_0), \quad (4.5)\end{aligned}$$

onde Z_0 varre todos os elementos de $\mathcal{Z}(n, p_2)$ de tamanho $(1 + O_1(\varepsilon))np/2k$ e tais que $\mathrm{CG}_n(Z_j)$ é (p_2, A)-uniforme. Iremos agora fixar um certo Z_0 e mostrar que $\mathbb{P}(\mathcal{B}'_j \mid Z_j = Z_0)$ é pequeno.

Para $D_0 \subset Z_0$, seja $P(j, Z_0, D_0) = \mathbb{P}(Z \in \mathcal{B}'_j \text{ e } D_j^{(2)}(Z) = D_0 \mid Z_j = Z_0)$. Então,

$$\begin{aligned}\mathbb{P}(\mathcal{B}'_j \mid Z_j = Z_0) &= \sum_{D_0 \subset Z_0} P(j, Z_0, D_0) \\ &\le 2^{(1+\varepsilon)(p/2k)n} \max_{D_0 \subset Z_0} P(j, Z_0, D_0). \quad (4.6)\end{aligned}$$

Vamos fixar $D_0 \subset Z_0$ com $P(j, Z_0, D_0) > 0$. Note que $\gamma^* = |D_0|/|Z_0| \ge \eta = \gamma_0$. Segue do lema dos elementos proibidos (lema 54) que $|D_0 - D_0| \ge (1-\delta)\gamma^* n$.

Agora, para cada $Z \in \Omega$, definimos $D' = D'(Z) = Z_{k+1} \cap (D_0 - D_0) = \mathbb{Z}^{(2)}_{n,p_1} \cap (D_0 - D_0)$, e $d' = d'(Z) = |D'|$. Observe que $d' = d'(Z)$ $(Z \in \Omega)$ tem distribuição binomial $\mathrm{Bi}(|D_0 - D_0|, p_1)$ com parâmetros $|D_0 - D_0|$ e p_1. Suponha que $Z \in \mathcal{B}'_j$, $Z_j = Z_0$ e $D^{(2)}_j(Z) = D_0$. Como D não contém triplas de Schur, temos $D'(Z) \cap D^{(1)}_2(Z) = \emptyset$. Como $(D'(Z) \cup D^{(1)}_2(Z)) \subset Z_{k+1}$, temos $d'(Z) + \gamma^{(1)}_2 |Z_{k+1}| \leq |Z_{k+1}|$, e portanto $d'(Z) \leq (1 - \gamma^{(1)}_2)|Z_{k+1}|$. Com isso,

$$P(j, Z_0, D_0) \leq \mathbb{P}\Big(Z \in \Omega' \text{ e } d'(Z) \leq (1 - \gamma^{(1)}_2)|Z_{k+1}|\Big) \\ \leq \mathbb{P}\Big(d'(Z) \leq (1 - \gamma^{(1)}_2)(1+\varepsilon)\frac{pn}{2}\Big) \quad (4.7)$$

Estimaremos esta probabilidade usando o fato que $d' = d'(Z) \sim \mathrm{Bi}(|D_0 - D_0|, p_1)$ e mostrando que $(1 - \gamma^{(1)}_2)(1+\varepsilon)\frac{pn}{2}$ é significantemente menor que a esperança de d', $\mathbb{E}(d')$. Claramente, $\mathbb{E}(d') \leq p_1 n \leq pn$. Além disso, lembrando que $\gamma^* + \gamma^{(1)}_2 \geq 1 + \eta$, temos

$$\mathbb{E}(d') - (1 - \gamma^{(1)}_2)(1+\varepsilon)\frac{pn}{2} \geq \Big((1-\delta)\gamma^* - (1+\varepsilon)(1 - \gamma^{(1)}_2)\Big)\frac{pn}{2} \geq \\ (\eta - \delta - \varepsilon)\frac{pn}{2} \geq \frac{\eta}{3}pn \geq \frac{\eta}{3}\mathbb{E}(d'), \quad (4.8)$$

e é fácil ver que $\mathbb{E}(d') \geq (\eta p/3)n$. Pela desigualdade de Hoeffding (lema 23), $d'(Z) \leq (1 - \gamma^{(1)}_2)(1+\varepsilon)\frac{pn}{2}$ ocorre com probabilidade no máximo

$$\mathbb{P}\Big(d'(Z) \leq (1 - \frac{\eta}{3})\mathbb{E}(d')\Big) \leq \exp\big(-\frac{\eta^3}{54}pn\big).$$

Da equação acima, e das equações 4.6 e 4.7, vemos que

$$\mathbb{P}\big(\mathcal{B}'_j \,|\, Z_j = Z_0\big) \leq 2^{(1+\varepsilon)(p/2k)n} \exp\Big(-\frac{\eta^3}{54}pn\Big) \\ = \exp\Big\{\log 2(1+\varepsilon)(p/2k)n - \frac{\eta^3}{54}pn\Big\},$$

e isso vai a zero quando $n \to \infty$, pois

$$\log 2(1+\varepsilon)(p/2k)n - \frac{\eta^3}{54}pn \leq pn\Big(\frac{1}{2k} - \frac{\eta^3}{54}\Big) \leq \\ pn\Big(\frac{\eta^3}{108} - \frac{\eta^3}{54}\Big) = -pn\frac{\eta^3}{108} \leq -C\log n\sqrt{n}\frac{\eta^3}{108} \quad (4.9)$$

e $-C \log n \sqrt{n} \eta^3/108 \to -\infty$ quando $n \to \infty$. □

4.3 O problema Schur(η)

É fácil ver que toda a demonstração do teorema 13 pode ser usada para resolver o problema 12, caso um resultado mais forte que o lema 51 seja provado. Conforme vimos, seria suficiente provar a seguinte conjectura.

Conjectura 55. *Existe $A > 0$ tal que para todo $p = p(n)$, com probabilidade tendendo a 1 quando $n \to \infty$, temos*

$$\left(\max_{j \neq 0} \mathcal{T}(\mathbb{Z}_{n,p})(j) \right) \leq A\sqrt{pn}.$$

Há uma última observação que gostaríamos de fazer sobre o Teorema de Schur. Para provar algo sobre a equação $x + y = z$, usamos o lema dos pares proibidos com $l = 1$. Usando o lema com $l \geq 1$, obtemos uma generalização do resultado. Seja $\sum_{j=1}^{l} a_j = \sum_{j=1}^{l+1} b_j$ a *equação de Schur l-generalizada*. Note que obtemos a equação de Schur original fazendo $l = 1$. Então, podemos provar uma generalização do teorema 13:

Teorema 56 (Teorema Schur(η) **generalizado).** *Para todos $l \in \mathbb{N}^*$ e $0 < \eta \leq 1/2$, existe uma constante $C = C(\eta, l)$ tal que, se $p = p(n) \geq C \log n \, n^{-1+1/(2l)}$, então, com probabilidade tendendo a 1 quando $n \to \infty$, qualquer subconjunto de $\mathbb{Z}_{n,p}$ com densidade $1/2 + \eta$ tem uma solução da equação de Schur l-generalizada.*

Toda a prova do teorema original pode ser facilmente adaptada ao teorema referente à equação de Schur generalizada. O único ponto da prova que poderia apresentar algum problema é o lema de conversão (lema 53). No entanto, sua adaptação também é fácil, como esboçaremos a seguir. Falaremos somente sobre o caso $l = 2$ unicamente para não carregar a notação.

Lema 57 (Lema de conversão generalizado). *Se o número de pares 2-proibidos por $\mathrm{CG}_n(D)$, $e(J_2(\mathrm{CG}_n(D))$, é maior ou igual a $c\binom{n}{2}$, para alguma constante $0 < c \leq 1$, então*

$$D - D + D - D = \{x - y + z - w \in \mathbb{Z}_n \colon x, y, z, w \in D\}$$

tem pelo menos $cn - 2$ elementos.

Prova. Construiremos uma associação entre pares 2-proibidos por $\mathrm{CG}_n(D)$ e elementos de $D - D + D - D$. Se $\{x, y\}$ é par 2-proibido, existem $a, b, c \in \mathbb{Z}_n$ tais que $x + a \in D$, $a + b \in D$, $b + c \in D$ e $c + y \in D$. Mas então

$x - y = (x + a) - (a + b) + (b + c) - (c + y) \in D - D + D - D$. Além disso, é fácil ver que $\{x, y\}$ é um par 2-proibido se e só se $\{x + t, y + t\}$ é um par 2-proibido para todo t.

Para $m \in \mathbb{Z}_n$, lembramos que $\mathrm{rep}_n(m)$ é o único inteiro contido em $\{x \in \mathbb{Z} \colon x \equiv m \pmod{n}\} \cap \{0, 1, 2, \ldots, n-1\}$. Dado um par 2-proibido $\{x, z\}$, definimos $d(x, z) = \min\{\mathrm{rep}_n(x - z), \mathrm{rep}_n(z - x)\}$. Note que a função d leva pares 2-proibidos em elementos de $(D - D + D - D) \cap \{1, 2, \ldots, \lfloor n/2 \rfloor\}$, e, além disso, para todo k pertencente à imagem de d, temos $d^{-1}(k) = n$.

Logo,

$$|(D - D + D - D) \cap \{1, 2, \ldots, \lfloor n/2 \rfloor\}| \geq \frac{c\binom{n}{2}}{n} = \frac{c(n-1)}{2},$$

e analogamente temos $|(D - D + D - D) \cap \{\lceil n/2 \rceil, \ldots, n-1\}| \geq c(n-1)/2$. Segue daí que

$$|D - D| \geq c(n-1) - 1 \geq cn - 2,$$

como queríamos.

□

Naturalmente, a veracidade da conjectura 55 nos levaria a uma demonstração do seguinte:

Problema 58 (Problema Schur(η) **generalizado).** *Para todos $l \in \mathbb{N}^*$ e $0 < \eta \leq 1/2$, existe uma constante $C = C(\eta, l)$ tal que, se $p = p(n) \geq Cn^{-1+1/(2l)}$, então, com probabilidade tendendo a 1 quando $n \to \infty$, qualquer subconjunto de $\mathbb{Z}_{n,p}$ com densidade $1/2+\eta$ tem uma solução da equação de Schur l-generalizada.*

O mesmo tipo de argumento dado para o problema Schur(η) original nos mostra que o enunciado acima é "ótimo": ele é falso se $p = o(n^{-1+1/(2l)})$, ou se trocarmos "$1/2 + \eta$" por "$1/2$".

Capítulo 5

Herança de regularidade

Neste capítulo, enunciaremos um resultado recente de Gerke, Kohayakawa, Rödl e Steger, ainda não publicado [12]. A partir deste resultado (teorema 60), desenvolvemos uma versão mais conveniente para nossos propósitos (teorema 64) e depois provaremos o teorema 14.

Começamos relembrando algumas definições. Dado um certo grafo $G = (V, E)$, e dois subconjuntos disjuntos $U, W \subset V$, definimos $E(U, W)$ como o conjunto das arestas entre U e W no grafo G, e colocamos $e(U, W) = e_G(U, W) = |E(U, W)|$. Denotamos ainda por $G[U, W]$ o grafo bipartido com vértices $U \dot\cup W$ e arestas $E(U, W)$.

Definição 59. *Sejam $0 < \varepsilon, d \leq 1$. Um grafo bipartido $B = (V_1 \dot\cup V_2, E)$ é (ε, d)-bipartido-regular se para todos $V_1' \subset V_1$, $V_2' \subset V_2$ com $|V_1'| \geq \varepsilon|V_1|$ e $|V_2'| \geq \varepsilon|V_2|$, temos*

$$|E(V_1', V_2')| \geq (1 - \varepsilon)d|V_1'||V_2'|.$$

Com isso, podemos enunciar o resultado principal de [12]. Basicamente, o teorema abaixo afirma que, dado um grafo bipartido $B = (V_1 \dot\cup V_2, E)$ que é (ε, d)-bipartido-regular, e dado um certo inteiro apropriado q, então quase todos os subconjuntos de tamanho q de V_1 induzem um grafo (ε', d)-bipartido-regular com V_2, desde que ε seja suficientemente pequeno. Ou seja, estes subconjuntos de tamanho q "herdam" a propriedade de regularidade de V_1.

Teorema 60 (Herança de regularidade). *Para todos $0 < \beta, \varepsilon' < 1$, existem $\varepsilon_0 = \varepsilon_0(\beta, \varepsilon') > 0$ e $C = C(\varepsilon')$ tais que para todo $0 < \varepsilon \leq \varepsilon_0$ e todo $0 < d < 1$, qualquer grafo $G = (V_1 \dot\cup V_2, E)$ bipartido e (ε, d)-bipartido-regular tem a seguinte propriedade. O número de subconjuntos $Q \subset V_1$ com*

$q = |Q| \geq C/d$ que formam um grafo (ε', d)-bipartido-regular com V_2 é pelo menos

$$(1 - \beta^q)\binom{|V_1|}{q}.$$

5.1 Versão interna de herança de regularidade

Usaremos agora o teorema 60 para deduzir uma outra versão de herança de regularidade. Começamos com uma observação simples: aplicando o teorema 60 duas vezes, obtemos o corolário abaixo. Note que, ao contrário do que ocorre no teorema anterior, aqui a constante C depende de β.

Corolário 61 (Herança de regularidade, versão 2). *Para todos $0 < \beta, \varepsilon' < 1$, existem $\varepsilon_0 = \varepsilon_0(\beta, \varepsilon') > 0$ e $C = C(\beta, \varepsilon')$ tais que para todo $0 < \varepsilon \leq \varepsilon_0$ e todo $0 < d < 1$, qualquer grafo $G = (V_1 \dot\cup V_2, E)$ bipartido e (ε, d)-bipartido-regular tem a seguinte propriedade. O número de pares (X, Y) com $X \subset V_1$, $Y \subset V_2$ e $q = \min\{x, y\} \geq C/d$ (onde $x = |X|$ e $y = |Y|$) tais que o grafo $G[X, Y]$ é (ε', d)-bipartido-regular é pelo menos*

$$(1 - \beta^q)\binom{|V_1|}{x}\binom{|V_2|}{y}.$$

Note que quando dizemos que $G[X, Y]$ é (ε', d)-bipartido-regular, estamos afirmando algo sobre as arestas entre X e Y, mas não dizemos nada sobre as arestas contidas em X ou Y. Para nossos interesses, é necessária uma versão que afirme algo sobre as arestas internas. Veremos agora uma versão "interna" dos teoremas anteriores, e que é aplicável a grafos não necessariamente bipartidos. Antes disso, precisamos de um lema simples.

Lema 62. *Sejam n e $q = q(n)$ inteiros positivos com $3 \leq q \leq n/2$. Existe uma constante absoluta n_0 tal que, para $n \geq n_0$, temos*

$$2\frac{\binom{n}{\lfloor n/2 \rfloor}}{\binom{n-q}{\lfloor (n-q)/2 \rfloor}} \leq 3^q.$$

Prova. Vamos usar uma estimativa padrão para $\binom{k}{\lfloor k/2 \rfloor}$, que segue facilmente da fórmula de Stirling. A estimativa é a seguinte (veja o lema 95 de [29]):

$$\binom{k}{\lfloor k/2 \rfloor} = (1 + o(1))\sqrt{\frac{2}{\pi k}}2^k.$$

Com isso, para n suficientemente grande, temos

$$2\frac{\binom{n}{\lfloor n/2\rfloor}}{\binom{n-q}{\lfloor (n-q)/2\rfloor}} = (2+o(1))\sqrt{\frac{2}{\pi n}}2^n\sqrt{\frac{\pi(n-q)}{2}}\frac{1}{2^{n-q}}$$
$$= (2+o(1))\sqrt{\frac{n-q}{n}}2^q \leq 3^q.$$

□

Definimos abaixo um conceito parecido com a (ε, d)-bipartido-regularidade, mas que se aplica a grafos gerais (não só aos bipartidos):

Definição 63. *Sejam $0 < \varepsilon, d \leq 1$. Um grafo $G = (V, E)$ é (ε, d)-inf-regular se para todos $U, W \subset V$ com $U \cap W = \emptyset$, $|U| \geq \varepsilon|V|$ e $|W| \geq \varepsilon|V|$, temos*

$$|E(U,W)| \geq (1-\varepsilon)d|U||W|.$$

Agora podemos enunciar e provar a "versão interna de herança de regularidade". Lembramos apenas que $G[Q]$ é o subgrafo de G induzido pelo subconjunto de vértices $Q \subset V(G)$. Estará implícito o tempo todo que $n = |V| = |V(G)|$.

Teorema 64 (Versão interna de herança de regularidade). *Para todos $0 < \alpha, \tilde{\varepsilon} < 1$, existem $\tilde{\varepsilon}_0 = \tilde{\varepsilon}_0(\alpha, \tilde{\varepsilon}) > 0$ e $\tilde{C} = \tilde{C}(\alpha, \tilde{\varepsilon})$ tais que para todo $0 < \varepsilon \leq \tilde{\varepsilon}_0$ e todo $0 < d < 1$, qualquer grafo $G = (V, E)$ (ε, d)-inf-regular com $n = |V(G)|$ suficientemente grande (isto é, maior que uma certa constante absoluta) tem a seguinte propriedade. Seja q um inteiro maior ou igual a $\tilde{C}/d$. Então, o número de subconjuntos $Q \subset V$ com $|Q| = q$ e tais que $e(G[Q]) \geq (1-\tilde{\varepsilon})d\binom{q}{2}$ é pelo menos*

$$(1-\alpha^q)\binom{|V|}{q}.$$

Prova. Dados α e $\tilde{\varepsilon}$, escolhemos $\beta = (\alpha/3)^3$ e usamos o corolário 61 com esta escolha de β e com $\varepsilon' = \tilde{\varepsilon}$ para obter ε_0 e C. Por fim, escolhemos $\tilde{\varepsilon}_0(\alpha, \tilde{\varepsilon}) = \varepsilon_0/3$ e $\tilde{C}(\alpha, \tilde{\varepsilon}) = 3C$, e agora mostraremos que o teorema é verdadeiro com esta escolha de $\tilde{\varepsilon}_0$ e de $\tilde{C}$. Suponha agora que $0 < \varepsilon \leq \tilde{\varepsilon}_0 = \varepsilon_0/3$, $0 < d < 1$ e seja G um grafo (ε, d)-inf-regular. Se $q > n/2$, o teorema segue do lema 28. Assim, fixe um inteiro $\tilde{C}/d \leq q \leq n/2$ e observe que $\lfloor q/2 \rfloor \geq \tilde{C}/3d = C/d$.

Dizemos que $\{U, W\}$ é uma bipartição equilibrada de $V = V(G)$ se $U \dot{\cup} W = V$ e $||U| - |W|| \leq 1$. Seja $A = \binom{V}{q}$ o conjunto dos subconjuntos

de V de tamanho q, e seja B o conjunto das bipartições equilibradas de V. Note que

$$|B| = \binom{n}{\lfloor n/2 \rfloor}.$$

Montaremos agora um grafo bipartido H com vértices $A \dot\cup B$. Se $Q \in A$ e $\{U, W\} \in B$, $(Q, \{U, W\})$ será uma aresta de H se e só se $\{U \cap Q, W \cap Q\}$ for uma bipartição equilibrada de Q (isto é, se e só se $(U \cap Q) \dot\cup (W \cap Q) = Q$ e $\Big||U \cap Q| - |W \cap Q|\Big| \leq 1$).

Diremos que uma aresta $(Q, \{U, W\}) \in E(H)$ é especial se

$$e_G(U \cap Q, W \cap Q) < (1 - \tilde\varepsilon) d \lfloor q/2 \rfloor \lceil q/2 \rceil.$$

Por fim, diremos que $Q \subset A$ é um conjunto ruim se

$$e(G[Q]) < (1 - \tilde\varepsilon) d \binom{q}{2}.$$

Mostraremos que conjuntos ruins são muito raros. A estratégia da prova é contar o número de arestas especiais do grafo H de duas formas diferentes. Primeiro estimaremos quantas destas arestas saem de A, e depois, quantas saem de B. Da comparação destas estimativas seguirá o resultado.

Fixe $Q \in A$. Se $e_G(U \cap Q, W \cap Q) \geq (1 - \tilde\varepsilon) d \lfloor q/2 \rfloor \lceil q/2 \rceil$ para todo $\{U, W\} \in \Gamma_H(Q)$, segue do lema 28 que Q não é um conjunto ruim. Logo, se Q é ruim, existe $\{U, W\} \in \Gamma_H(Q)$ tal que $e_G(U \cap Q, W \cap Q) < (1 - \tilde\varepsilon) d \lfloor q/2 \rfloor \lceil q/2 \rceil$, ou seja, tal que a aresta $(Q, \{U, W\})$ é especial. Note que se $(Q, \{U, W\})$ é uma aresta especial e se $\{U', W'\} \in B$ é tal que $\{U' \cap Q, W' \cap Q\} = \{U \cap Q, W \cap Q\}$, então a aresta $(Q, \{U', W'\})$ também é especial. Como existem pelo menos $\binom{n-q}{\lceil n/2 \rceil - \lceil q/2 \rceil}$ modos de estender uma bipartição equilibrada de Q para uma bipartição equilibrada de V, temos que

$$\text{(Número de arestas especiais)} \geq \binom{n-q}{\lceil n/2 \rceil - \lceil q/2 \rceil} \times \text{(Número de conjuntos ruins)}. \quad (5.1)$$

Fixe agora $\{U, W\} \in B$ e considere o grafo bipartido $G[U, W]$. Como G é (ε, d)-inf-regular, segue que $G[U, W]$ é $(3\varepsilon, d)$-bipartido-regular. Como $3\varepsilon \leq 3\tilde\varepsilon_0 = \varepsilon_0$, temos pelo corolário 61 que o número de pares (X, Y) com $X \subset U$, $Y \subset W$, $x = |X| = \lfloor q/2 \rfloor$ e $y = |Y| = \lceil q/2 \rceil$ tais que o grafo $G[X, Y]$ não é $(\tilde\varepsilon, d)$-bipartido-regular é no máximo

$$\beta^{q/3} \binom{|U|}{x} \binom{|W|}{y} \leq \beta^{q/3} \binom{\lceil n/2 \rceil}{\lceil q/2 \rceil}^2.$$

Analogamente, o número de pares (X, Y) com $X \subset U$, $Y \subset W$, $x = |X| = \lceil q/2 \rceil$ e $y = |Y| = \lfloor q/2 \rfloor$ tais que o grafo $G[X, Y]$ não é $(\tilde{\varepsilon}, d)$-bipartido-regular é no máximo

$$\beta^{q/3}\binom{|U|}{x}\binom{|W|}{y} \leq \beta^{q/3}\binom{\lceil n/2 \rceil}{\lceil q/2 \rceil}^2.$$

Logo, o número de conjuntos $Q \in \Gamma_H(\{U, W\})$ tais que $e_G(U \cap Q, W \cap Q) < (1 - \tilde{\varepsilon})d\lfloor q/2 \rfloor \lceil q/2 \rceil$ é no máximo $2\beta^{q/3}\binom{\lceil n/2 \rceil}{\lceil q/2 \rceil}^2$, e portanto, o número de arestas especiais que saem de $\{U, W\}$ é no máximo $2\beta^{q/3}\binom{\lceil n/2 \rceil}{\lceil q/2 \rceil}^2$. Com isso, temos que

$$\begin{aligned}(\text{Número de arestas especiais}) &\leq 2\beta^{q/3}\binom{\lceil n/2 \rceil}{\lceil q/2 \rceil}^2 |B| \\ &= 2\beta^{q/3}\binom{\lceil n/2 \rceil}{\lceil q/2 \rceil}^2\binom{n}{\lfloor n/2 \rfloor}. \quad (5.2)\end{aligned}$$

Daqui em diante, ignoraremos pisos e tetos ($\lfloor x \rfloor$, $\lceil x \rceil$). Das desigualdades 5.1 e 5.2, temos que

$$\binom{n-q}{(n-q)/2} \times (\text{Número de conjuntos ruins}) \leq 2\beta^{q/3}\binom{n/2}{q/2}^2\binom{n}{n/2},$$

ou seja,

$$(\text{Número de conjuntos ruins}) \leq 2\beta^{q/3}\frac{\binom{n/2}{q/2}^2\binom{n}{n/2}}{\binom{n-q}{(n-q)/2}} \leq 2\beta^{q/3}\binom{n}{q}\frac{\binom{n}{n/2}}{\binom{n-q}{(n-q)/2}}.$$

Por fim, segue do lema 62 que, para n suficientemente grande, o número de conjuntos ruins é no máximo

$$3^q\beta^{q/3}\binom{n}{q} = (3\beta^{1/3})^q\binom{n}{q} = \alpha^q\binom{n}{q}.$$

□

5.2 Uma versão probabilística do Teorema de Sárközy

Iremos agora aplicar o teorema anterior dando uma prova do teorema 14. Na verdade, provaremos resultados mais gerais, a saber, os teoremas 67 e 68. Vamos começar estabelecendo algumas notações.

Convencionemos que $\mathbb{N} = \{1, 2, 3 \ldots\}$. Seja $M = \{m_1, m_2, \ldots\}$ um subconjunto infinito de $\mathbb{N}$ com $1 \leq m_1 < m_2 < \ldots$.

Definição 65. *Dizemos que $\mathcal{S}_M$ é uma M-sequência se $\mathcal{S}_M$ for uma sequência de conjuntos indexada por M, $\mathcal{S}_M = (S_{m_i})_{i\in\mathbb{N}}$, tal que, para todo i, $S_{m_i} \subset \mathbb{Z}_{m_i}$.*

Denotaremos a densidade de um grafo G por $d(G) = e(G)/\binom{n}{2}$, onde $n = |V(G)|$.

Definição 66. *Seja $\mathcal{S}_M$ uma M-sequência. Dizemos que $\mathcal{S}_M$ é adição-regular se para todo $\varepsilon > 0$ existe $i_0 \in \mathbb{N}$ tal que, se $i \geq i_0$, o grafo $\mathrm{CG}^+_{m_i}(S_{m_i})$ é $(\varepsilon, d(\mathrm{CG}^+_{m_i}(S_{m_i})))$-inf-regular. Analogamente, dizemos que $\mathcal{S}_M$ é subtração-regular se para todo $\varepsilon > 0$ existe $i_0 \in \mathbb{N}$ tal que, se $i \geq i_0$, o grafo $\mathrm{CG}^-_{m_i}(S_{m_i})$ é $(\varepsilon, d(\mathrm{CG}^-_{m_i}(S_{m_i})))$-inf-regular.*

Usaremos a seguir as notações definidas pelas equações 1.10 e 1.11. Os teoremas principais desta seção são os seguintes:

Teorema 67. *Suponha que $\mathcal{S}_M = (S_{m_i})_{i\in\mathbb{N}}$ é uma M-sequência adição-regular. Para todos $0 < \eta, \gamma < 1$, existem constantes $C = C(\eta, \gamma)$ e $i_0 = i_0(\eta, \gamma)$ tais que, se $i \geq i_0$ e se $p\colon M \to [0, 1]$ satisfaz $p = p(m_i) \geq C/|S_{m_i}|$, então, com probabilidade pelo menos $1 - \gamma$, temos que*

$$\mathbb{Z}_{m_i,p} \to_\eta \mathit{Soma}(S_{m_i}).$$

Teorema 68. *Suponha que $\mathcal{S}_M = (S_{m_i})_{i\in\mathbb{N}}$ é uma M-sequência subtração-regular. Para todos $0 < \eta, \gamma < 1$, existem constantes $C = C(\eta, \gamma)$ e $i_0 = i_0(\eta, \gamma)$ tais que, se $i \geq i_0$ e se $p\colon M \to [0, 1]$ satisfaz $p = p(m_i) \geq C/|S_{m_i}|$, então, com probabilidade pelo menos $1 - \gamma$, temos que*

$$\mathbb{Z}_{m_i,p} \to_\eta \mathit{Diferença}(S_{m_i}).$$

Dado que as demonstrações dos teoremas acima são extremamente parecidas, provaremos apenas o primeiro deles.

Prova do teorema 67. Fixe reais $0 < \eta, \gamma < 1$. Sejam $e = \exp(1)$ e $\alpha = \gamma\eta/\big(2e(2 + \gamma)\big)$. Note que $0 < \alpha < 1$ e que $\sum_{t=1}^{\infty}(2\alpha e/\eta)^t = 2\alpha e/(\eta - 2\alpha e) = \gamma/2$. Seja $\tilde{\varepsilon} = 10^{-2}$ e use o teorema 64 para achar $\tilde{C} = \tilde{C}(\alpha, \tilde{\varepsilon})$ e $\tilde{\varepsilon}_0 = \tilde{\varepsilon}_0(\alpha, \tilde{\varepsilon}) = \tilde{\varepsilon}_0(\alpha, 10^{-2}) > 0$. Tome $C = C(\eta, \gamma) = 4\tilde{C}(\alpha, \tilde{\varepsilon})/\eta$. Podemos supor sem perda que C é tal que $2\exp(-C/12) \leq \gamma/2$. Como $\mathcal{S}_M$ é adição-regular, existe $i_0 = i_0(\tilde{\varepsilon}_0) = i_0(\gamma, \eta)$ tal que, se $i \geq i_0$, o grafo $G = \mathrm{CG}^+_{m_i}(S_{m_i})$ é $(\tilde{\varepsilon}_0/2, d(\mathrm{CG}^+_{m_i}(S_{m_i})))$-inf-regular.

Veremos que, com esta escolha de C e de i_0, o teorema 67 é verdadeiro. Fixe $i \geq i_0$. Vamos provar que

$$\mathbb{P}\Big(\mathbb{Z}_{m_i,p} \to_\eta \text{Soma}(S_{m_i})\Big) \geq 1 - \gamma.$$

Lembramos que $\mathcal{Z}(n,p)$ é o espaço de probabilidade dos subconjuntos de $\mathbb{Z}_n$ em que cada elemento está no subconjunto com probabilidade p. Seja $\mathcal{Z}(n,p)'$ o subconjunto de $\mathcal{Z}(n,p)$ formado pelos conjuntos $\mathbb{Z}_{n,p}$ que satisfazem $np/2 \leq |\mathbb{Z}_{n,p}| \leq 3np/2$. Pela desigualdade de Hoeffding (lema 23),

$$\mathbb{P}(\mathcal{Z}(m_i,p)') \geq 1 - 2\exp(-m_i p/12) \geq 1 - 2\exp(-C/12) \geq 1 - \gamma/2$$

Vamos supor daqui em diante que $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)'$. Note que isto implica que, ao escolhermos $D \subset \mathbb{Z}_{m_i,p}$ com $|D| = \eta|\mathbb{Z}_{m_i,p}|$, teremos $\eta m_i p/2 \leq |D| \leq 3\eta m_i p/2$.

Seja G o grafo $\text{CG}^+_{m_i}(S_{m_i})$. Diremos que um conjunto $Q \subset \mathbb{Z}_{m_i}$ com $|Q| = q$ é indesejável se

$$e(G[Q]) = e(\text{CG}^+_{m_i}(S_{m_i})[Q]) < (1-\tilde{\varepsilon})d(\text{CG}^+_{m_i}(S_{m_i}))\binom{q}{2}.$$

Vamos mostrar que a probabilidade de $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)'$ conter um subconjunto de densidade η e indesejável é no máximo $\gamma/2$.

Seja q um inteiro positivo com $\eta m_i p/2 \leq q \leq 3\eta m_i p/2$. Note que, da equação 4.2 (na demonstração do lema 52), segue que

$$q \geq \frac{\eta m_i p}{2} \geq \frac{4\eta\tilde{C}(\alpha,\tilde{\varepsilon})m_i}{2\eta|S_{m_i}|} \geq \frac{\tilde{C}(\alpha,\tilde{\varepsilon})}{d(\text{CG}^+_{m_i}(S_{m_i}))}.$$

Com isso, podemos aplicar o teorema 64 ao grafo $\text{CG}^+_{m_i}(S_{m_i})$ e ao inteiro q para concluir que o número de conjuntos $Q \subset \mathbb{Z}_{m_i}$ de tamanho exatamente q com $e(G[Q]) < (1-\tilde{\varepsilon})d(\text{CG}^+_{m_i}(S_{m_i}))\binom{q}{2}$ é no máximo $\alpha^q\binom{m_i}{q}$.

O número esperado de conjuntos indesejáveis de tamanho exatamente q e contidos em $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)'$ é no máximo o número de conjuntos indesejáveis de tamanho q vezes a probabilidade de um destes conjuntos indesejáveis estar contido em $\mathbb{Z}_{m_i,p}$, e isto é limitado por

$$\alpha^q\binom{m_i}{q}p^q \leq \left(\alpha\frac{m_i e}{q}p\right)^q \leq \left(\frac{2\alpha e}{\eta}\right)^q,$$

onde usamos o fato que $\binom{m_i}{q} \leq (m_i e/q)^q$ (para uma prova disto, veja o lema 94 de [29]). Portanto, o número esperado de conjuntos indesejáveis em $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)'$ com tamanho entre $\eta m_i p/2$ e $3\eta m_i p/2$ é no máximo

$$\sum_{q=\eta m_i p/2}^{3\eta m_i p/2} \left(\frac{2\alpha e}{\eta}\right)^q \leq \sum_{q=1}^{\infty} \left(\frac{2\alpha e}{\eta}\right)^q = \gamma/2.$$

Com isso, segue da desigualdade de Markov que a probabilidade de $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)'$ não conter nenhum conjunto indesejável com cardinalidade entre $\eta m_i p/2$ e $3\eta m_i p/2$ é pelo menos $1-\gamma/2$.

Voltemos a $\mathcal{Z}(m_i,p)$. Vimos que, com probabilidade pelo menos $1-\gamma$, nenhum conjunto D com densidade η em $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)$ é indesejável. Isto implica que, com probabilidade pelo menos $1-\gamma$, $\mathbb{Z}_{m_i,p} \in \mathcal{Z}(m_i,p)$ é tal que, se D é uma η-fração de $\mathbb{Z}_{m_i,p}$, temos $e(G[D]) \geq (1-\tilde{\varepsilon})d(\mathrm{CG}^+_{m_i}(S_{m_i}))\binom{|D|}{2} \geq 1$. Finalmente, observe que cada uma destas arestas representa uma solução de $x+y \in S_{m_i}$ com $x,y \in D$. □

O teorema 14 segue imediatamente do teorema 68, bastando tomar M igual ao conjunto dos primos e $\mathcal{S}_M = (S_{m_i})_{i\in\mathbb{N}}$ com $S_{m_i} = \mathrm{Quad}(m_i)$, onde $\mathrm{Quad}(n) \subset \mathbb{Z}_n$ é o conjunto dos quadrados não-nulos módulo n. É fácil ver que, se n é primo, $|\mathrm{Quad}(n)| = n(1+o(1))/2$. A última coisa que falta verificar é que $\mathcal{S}_M$ é subtração-regular. Veremos que isto é bem simples. Usaremos o fato abaixo, que é um resultado clássico da teoria dos números, provado por Gauss.

Fato 69. *Seja m um primo e seja $j \in \mathbb{Z}_m$, $j \neq 0$. Então*

$$S(m) = \sum_{x=1}^{m-1} e^{-2\pi i j x^2/m} = O(\sqrt{m}).$$

Prova. A demonstração pode ser encontrada em vários textos de teoria dos números. Por exemplo, veja [2]. □

Corolário 70. *Seja m um primo. Então, temos para todo $j \neq 0$ que*

$$\mathcal{T}(\mathrm{Quad}(m))(j) = \sum_{x\in\mathrm{Quad}(m)} e^{-2\pi i j x/m} = O(\sqrt{m}). \tag{5.3}$$

Prova. Seja $\mathbb{Z}^*_m = \mathbb{Z}_m \setminus \{0\}$ e considere $f\colon \mathbb{Z}^*_m \to \mathbb{Z}^*_m$ dada por $f(x) = x^2$ e m é primo. É fácil ver que para cada y na imagem de f, $|f^{-1}(y)| = 2$. Desta observação, segue que

$$\sum_{x \in \mathrm{Quad}(m)} e^{-2\pi i j x/m} = \frac{1}{2} \sum_{x=1}^{m-1} e^{-2\pi i j x^2/m},$$

e o resultado segue do fato 69. □

Pelo lema 33, segue que $\mathcal{S}_M = (\mathrm{Quad}(m_i))_{i \in \mathbb{N}}$ é adição-regular, onde M é a subsequência dos primos. É fácil ver agora que $\mathcal{S}_M$ também é subtração-regular, e com isso provamos o teorema 14.

Observe que, "no meio do caminho", provamos também o seguinte teorema:

Teorema 71. *Para todos $0 < \eta, \gamma < 1$, existem constantes $C = C(\eta, \gamma)$ e $n_0 = n_0(\eta, \gamma)$ tais que, se $p = p(n) \geq C/n$ e se n é um primo com $n \geq n_0$, então, com probabilidade pelo menos $1 - \gamma$, temos que*

$$\mathbb{Z}_{n,p} \rightarrow_\eta \mathit{Soma}(\mathrm{Quad}(n)).$$

Como observação final, note que a propriedade essencial de $\mathrm{Quad}(n)$ que utilizamos foi a adição-regularidade (e a subtração-regularidade). Por sua vez, isto seguiu do fato que para $j \neq 0$, o j-ésimo coeficiente de Fourier de $\mathrm{Quad}(n)$ é $o(|\mathrm{Quad}(n)|)$. Na próxima seção, veremos mais alguns exemplos de M-sequências com esta propriedade, e, com isso, daremos novas aplicações dos teoremas 67 e 68.

5.3 Outras aplicações dos teoremas 67 e 68

Nesta seção, mostraremos que os teoremas 67 e 68 têm algumas outras aplicações, além dos teoremas 14 e 71.

Vimos que os quadrados módulo n (n primo) formam uma M-sequência adição-regular. Fixe $f(z)$, um polinômio com coeficientes inteiros não constante. Provaremos que a imagem de $f(z)$ módulo n (n primo) é adição-regular. Com isso, obteremos um teorema para a equação $x + y = f(z)$.

Começamos observando que existem extensões do fato 69 para polinômios gerais. Enunciamos uma destas extensões, que é um resultado devido a Hua [20, 21].

Teorema 72 (L. K. Hua). *Sejam m um inteiro positivo e $f(x) = a_k x^k + \ldots + a_1 x + a_0$ um polinômio com coeficientes inteiros. Se $\mathrm{mdc}(a_k, \ldots, a_1, m) = 1$, então para todo $\theta > 0$, existe uma constante $c_1(k, \theta)$ que só depende de k e de θ tal que*

$$\Big| \sum_{x \in \mathbb{Z}_m} e^{-2\pi i f(x)/m} \Big| \leq c_1(k, \theta) m^{1 - \frac{1}{k} + \theta}.$$

Note que foi fácil passar do fato 69 ao corolário 70 porque, se m é primo e $f\colon \mathbb{Z}_m^* \to \mathbb{Z}_m^*$ é dada por $f(x) = x^2$, cada elemento da imagem de f tem o mesmo número de pré-imagens (a saber, 2). Isto é, para todo k na imagem de f, $|f^{-1}(k)|$ é constante. Isto não vale para polinômios quaisquer, e, portanto, será necessário desenvolver outro método para aplicar o teorema 72.

No que segue, usaremos grafos de Chung-Graham com pesos. Vamos definir este conceito. Seja R um multiconjunto finito contido em $\mathbb{Z}_n$, isto é, um conjunto com elementos de $\mathbb{Z}_n$ em que permitimos elementos repetidos (finitas vezes). Por exemplo, $S = \{1, 1, 1, 1, 3, 5, 5, 6, 6, 6\}$ é um multiconjunto contido em $\mathbb{Z}_7$. A função característica de um multiconjunto R contido em $\mathbb{Z}_n$, que também denotaremos por R, é a função $R\colon \mathbb{Z}_n \to \mathbb{N}$ tal que $R(j)$ é a multiplicidade do elemento j em R. Assim, a função característica do multiconjunto $S = \{1, 1, 1, 1, 3, 5, 5, 6, 6, 6\}$ contido em $\mathbb{Z}_7$ é o vetor $(S(j))_{j=0}^6$ tal que $(S(j)) = (0, 4, 0, 1, 0, 2, 3)$.

Com isso, podemos falar de grafos de Chung-Graham com pesos. No grafo de Chung-Graham "tradicional", $\mathrm{CG}_n^+(R)$, vale que $\{i, j\}$ é aresta se e só se existe $r \in R$ tal que $i + j \equiv r \pmod{n}$. No grafo de Chung-Graham com pesos, R deve ser um multiconjunto, e para cada $r \in R$ e para cada $i, j \in \mathbb{Z}_n$ com $i+j = r$, colocaremos $R(r)$ arestas ligando i a j (ou uma aresta com peso $R(r)$, equivalentemente). Denotaremos este grafo por $\mathrm{PCG}_n^+(R)$. Três últimas convenções que faremos são: (1) se $U, W \subset V(\mathrm{PCG}_n^+(R)) = \mathbb{Z}_n$ e $U \cap W = \emptyset$, cada aresta $\{i, j\}$ entre U e W entrará k vezes no cômputo de $e(U, W)$, onde $k = R(i + j)$ é o peso da aresta $\{i, j\}$; (2) as multiplicidades das arestas são levadas em conta no cálculo de $e(\mathrm{PCG}_n^+(R))$; e (3) por "$|R|$", deve-se entender "$\sum_r R(r)$".

Dito isto, é fácil verificar que os lemas da seção 3.2 ainda valem neste contexto com pesos. As provas podem ser adaptadas de maneira evidente. Em particular, o lema 33 é válido, e ele será usado na prova do teorema 73.

Faremos agora uma observação simples, mas importante: suponha que o grafo $\mathrm{PCG}_n^+(R)$ é (ε, d)-inf-regular (podemos ter $d \geq 1$ neste contexto!) e $\max_{r \in \mathbb{Z}_n} R(r) = L > 0$. Então o grafo de Chung-Graham "tradicional", $\mathrm{CG}_n^+(R)$, que é obtido de modo trivial a partir de $\mathrm{PCG}_n^+(R)$ (apagando arestas múltiplas ou transformando todos os pesos $R(r) > 1$ em $R(r) = 1$), é $(\varepsilon, d/L)$-inf-regular.

Vamos fixar algumas notações. Começamos definindo a função aritmética $\Delta\colon \mathbb{N} \to \mathbb{N}$, do seguinte modo: para $n > 1$, $\Delta(n)$ é o menor primo que divide n, e $\Delta(1) = 1$. Além disso, se $f\colon \mathbb{Z}_m \to \mathbb{Z}_m$ é um polinômio, denotaremos a imagem de f por $\mathrm{Im}_m f(x)$. Observe que $\mathrm{Im}_m f(x)$ é um subconjunto ordinário de $\mathbb{Z}_m$. Definimos $\mathrm{Im}_m^* f(x)$ como o multiconjunto $\{f(0), f(1), \ldots, f(m-1)\}$ contido em $\mathbb{Z}_m$. Finalmente, definimos $\phi_m(f) =$

$\max_{j\in\mathbb{Z}_m} |f^{-1}(j)|$. O teorema abaixo é o resultado mais importante desta seção.

Teorema 73. *Seja $f(x)$ um polinômio com coeficientes inteiros, não constante. Seja $M = \{m_1, m_2, \ldots\}$ um subconjunto infinito de $\mathbb{N}$ com $1 \leq m_1 < m_2 < \ldots$ e $\lim_{i\in\mathbb{N}} \Delta(m_i) = \infty$. Suponha ainda que existe $L > 0$ tal que $\phi_{m_i}(f) \leq L$ para todo $m_i \in M$. Então, para todo $\varepsilon > 0$, existe $i_0 > 0$ tal que, se $i \geq i_0$, o grafo de Chung-Graham ordinário $\mathrm{CG}^+_{m_i}(\mathrm{Im}_{m_i} f(x))$ é $(\varepsilon, 1/L)$-inf-regular.*

Prova. Com o auxílio do teorema 72, mostraremos que os grafos de Chung-Graham com pesos $\mathrm{PCG}^+_{m_i}(\mathrm{Im}^*_{m_i} f(x))$ têm propriedades de regularidade.

Fixe $m_i \in M$, $j \in \mathbb{Z}^*_{m_i}$. Seja $t = \mathrm{mdc}(j, m_i)$ e sejam $j' = j/t$ e $m'_i = m_i/t$. Seja k o grau de f e defina $\theta = 1/(2k)$. Pelo teorema da divisão euclideana, para cada $0 \leq x < m_i$, existem $0 \leq y < t$ e $0 \leq r < m'_i$ com $x = ym'_i + r$. Logo,

$$\begin{aligned}\sum_{x\in\mathbb{Z}_{m_i}} e^{-2\pi i j f(x)/m_i} &= \sum_{x\in\mathbb{Z}_{m_i}} e^{-2\pi i j' f(x)/m'_i} \\ &= \sum_{y\in\mathbb{Z}_t} \sum_{r\in\mathbb{Z}_{m'_i}} e^{-2\pi i j' f(ym'_i+r)/m'_i} = t \sum_{r\in\mathbb{Z}_{m'_i}} e^{-2\pi i j' f(r)/m'_i}, \quad (5.4)\end{aligned}$$

e, pelo teorema 72, isto é limitado, em módulo, por

$$\begin{aligned}t c_2(k,\theta)(m'_i)^{1-\frac{1}{k}+\theta} &= t c_2(k,\theta)(m'_i)^{1-\frac{1}{2k}} \\ &= t^{1/(2k)} c_2(k,\theta)(m'_i t)^{1-\frac{1}{2k}} = t^{1/(2k)} c_2(k,\theta)(m_i)^{1-\frac{1}{2k}}.\end{aligned}$$

Como $t \leq m_i/\Delta(m_i)$, temos que

$$\Big| \sum_{x\in\mathbb{Z}_{m_i}} e^{-2\pi i j f(x)/m_i} \Big| \leq \frac{c_2(k,\theta) m_i}{\sqrt[2k]{\Delta(m_i)}},$$

e isto é $o(m_i)$, pois, por hipótese, $\Delta(m_i) \to \infty$.

Segue do lema 33 (adaptado a grafos com pesos) que, para todo $\varepsilon > 0$, existe $i_0 > 0$ tal que, se $i \geq i_0$, o grafo com pesos $\mathrm{PCG}^+_{m_i}(\mathrm{Im}^*_{m_i} f(x))$ é ε-regular com densidade 1, e em particular, é $(\varepsilon, 1)$-inf-regular. Como vimos, isto implica que o grafo de Chung-Graham ordinário $\mathrm{CG}^+_{m_i}(\mathrm{Im}_{m_i} f(x))$ é $(\varepsilon, 1/L)$-inf-regular, para todo $i \geq i_0$, como queríamos. □

Seja M a subsequência dos primos. O teorema 73 mostra que a M-sequência $\mathcal{S}_M = (F_{m_i})_{i\in\mathbb{N}}$ dada por $F_{m_i} = \mathrm{Im}_{m_i} f(x) \subset \mathbb{Z}_{m_i}$ é "praticamente" adição-regular. O único problema é que a densidade não está correta.

Apesar deste pequeno problema, a prova do teorema 67 pode ser facilmente adaptada para provar o seguinte teorema:

Teorema 74. *Seja f um polinômio de coeficientes inteiros, não constante. Para todos $0 < \eta, \gamma < 1$, existem constantes $C = C(\eta, \gamma)$ e $n_0 = n_0(\eta, \gamma)$ tais que, se $p = p(n) \geq C/n$ e se n é um primo com $n \geq n_0$, então, com probabilidade pelo menos $1-\gamma$, temos que qualquer η-fração de $\mathbb{Z}_{n,p}$ contém x, y tais que existe $z \in \mathbb{Z}_n$ com $x - y = f(z)$.*

Para a próxima aplicação, usaremos um outro teorema de Hua, que trata de somas trigonométricas parciais. A prova deste resultado pode ser vista no capítulo 1 de [20].

Teorema 75 (L. K. Hua). *Sejam m um inteiro positivo e $f(x) = a_k x^k + \ldots + a_1 x + a_0$ um polinômio com coeficientes inteiros. Se $\mathrm{mdc}(a_k, \ldots, a_1, m) = 1$, então para todo $\theta > 0$, existe uma constante $c_3(k, \theta)$ que só depende de k e de θ tal que para todo t com $1 \leq t \leq m$, temos*

$$\Big| \sum_{x=1}^{t} e^{-2\pi i f(x)/m} \Big| \leq c_2(k, \theta) m^{1-\frac{1}{k}+\theta}.$$

Com isto, poderemos exibir um exemplo de uma M-sequência $\mathcal{S}_M = (S_{m_i})_{i \in \mathbb{N}}$ esparsa (isto é, $|S_{m_i}|/m_i \to 0$), adição-regular e subtração-regular. Seja M o conjunto dos primos, e para todos $m_i \in M$, $\mu > 0$, seja $Q(m_i, \mu)$ o subconjunto de $\mathbb{Z}_{m_i}$ dado por

$$Q(m_i, \mu) = \{x^2 \bmod m_i \colon 1 \leq x \leq m_i^{1/2+\mu}\}.$$

O corolário abaixo segue imediatamente do teorema 75 e do lema 33.

Corolário 76. *Fixe $0 < \mu < 1/2$ e considere a M-sequência $\mathcal{S}_M = (S_{m_i})_{i \in \mathbb{N}}$, onde M é o conjunto dos primos e para todo $i \in \mathbb{N}$, $S_{m_i} = Q(m_i, \mu)$. Então $\mathcal{S}_M$ é adição-regular e subtração-regular.*

Nossos dois últimos teoremas seguem do corolário acima, e dos teoremas 67 e 68.

Teorema 77. *Para todos $0 < \mu < 1/2$, $0 < \eta, \gamma < 1$, existem constantes $C = C(\mu, \eta, \gamma)$ e $n_0 = n_0(\mu, \eta, \gamma)$ tais que, se $p = p(n) \geq C/n^{1/2+\mu}$ e se n é um primo com $n \geq n_0$, então, com probabilidade pelo menos $1 - \gamma$, temos que*

$$\mathbb{Z}_{m_i,p} \to_\eta \mathit{Soma}(Q(m_i, \mu)).$$

Teorema 78. *Para todos $0 < \mu < 1/2$, $0 < \eta, \gamma < 1$, existem constantes $C = C(\mu, \eta, \gamma)$ e $n_0 = n_0(\mu, \eta, \gamma)$ tais que, se $p = p(n) \geq C/n^{1/2+\mu}$ e se n é*

um primo com $n \geq n_0$*, então, com probabilidade pelo menos* $1 - \gamma$*, temos que*

$$\mathbb{Z}_{m_i,p} \rightarrow_\eta \textit{Diferença}(Q(m_i, \mu)).$$

O teorema 75 pode ser usado para achar outros exemplos de M-sequências esparsas, adição-regulares e subtração-regulares, mas não prosseguiremos nesta direção.

Capítulo 6

Conclusão

Para encerrar o presente trabalho, desejamos mencionar alguns problemas relacionados às versões probabilísticas dos teoremas de Schur e Särkozy.

Começamos falando sobre problemas relacionados à versão probabilística do Teorema de Schur. Em primeiro lugar, seria interessante verificar a validade da conjectura 55. Mesmo que ela seja falsa, seria interessante provar isto.

Outro problema, muito mais interessante, seria fazer uma versão probabilística para o Teorema de Schur para grupos abelianos. O enunciado abaixo, por exemplo, é uma generalização natural do Problema de Schur em $\mathbb{Z}_n$.

Problema 79 (Schur probabilístico em grupos abelianos). *O teorema* Schur(η) *é verdadeiro se trocarmos* $\mathbb{Z}_n$ *por uma classe qualquer de grupos abelianos finitos* $\mathcal{G} = (G_j)_{j=1}^{\infty}$ *com* $|G_j| \to \infty$.

A demonstração do teorema 13 pode ser adaptada para o problema acima. É claro que, no caso de a conjectura 55 ser verdadeira, poderíamos trocar a hipótese $p > C \log n/\sqrt{n}$ (que é o que sabemos fazer) por $p > C/\sqrt{n}$ (que é o valor "certo").

O problema acima fica mais difícil se quisermos considerar a "densidade correta". Vamos explicar isto. Recordemos que, em $\mathbb{Z}_n$, o motivo pelo qual exigimos inicialmente no enunciado do problema que a densidade seja maior que $1/2$ é a existência, para n par, de conjuntos livres de somas (ou seja, sem soluções de $x + y = z$) com densidade $1/2$. Quando consideramos um grupo abeliano em geral, nem sempre haverá um subconjunto livre de somas com metade dos elementos do grupo. Por exemplo, em $\mathbb{Z}_7$, pode-se verificar que a cardinalidade do maior subconjunto livre de somas é 2.

Seja G um grupo abeliano e seja $\mu(G)$ a densidade do maior subconjunto

livre de somas de G. Sabe-se, por exemplo, que $\mu(\mathbb{Z}_{2n}) = 1/2$ e que $\mu(\mathbb{Z}_7) = 2/7$. Recentemente, Green e Rusza [16] determinaram o valor de $\mu(G)$ para todo G finito. Enunciaremos o resultado deles abaixo.

Teorema 80 (Green, Rusza, 2004). *Seja G um grupo abeliano de ordem n.*

- *Se n é divisível por algum primo congruente a 2 mod 3, então $\mu(G) = \frac{1}{3} + \frac{1}{3p}$, onde p é o menor primo congruente a 2 mod 3 que divide n;*
- *Se n não é divisível por nenhum primo congruente a 2 mod 3, mas $3 \mid n$, então $\mu(G) = \frac{1}{3}$;*
- *Se n só tem fatores primos congruentes a 1 mod 3, então $\mu(G) = \frac{1}{3} - \frac{1}{3m}$, onde m é o expoente de G (a máxima ordem de um elemento do grupo).*

Em particular, para todo G abeliano finito, $2/7 \leq \mu(G) \leq 1/2$.

É natural tentar resolver o problema 79 trocando a densidade $1/2 + \eta$ pela densidade "correta", $\mu(G) + \eta$. Daremos um exemplo. Sabemos, pelo teorema acima, que $\mu(\mathbb{Z}_3^n) = \mu(\mathbb{Z}_3 \times \ldots \times \mathbb{Z}_3) = 1/3$. Seja $(\mathbb{Z}_3^n)_p$ um subconjunto aleatório de $\mathbb{Z}_3^n$ obtido por 3^n sorteios independentes, cada um com probabilidade p. Seria interessante resolver o seguinte problema:

Problema 81 (Schur para grupos com densidade corrigida). *Para todo $\eta > 0$, existe uma constante $C = C(\eta)$ tal que, se $p = p(m)$ é tal que $p(3^n) > C3^{-n/2}$, então, com probabilidade tendendo a 1 quando $n \to \infty$, qualquer subconjunto de $(\mathbb{Z}_3^n)_p$ com densidade pelo menos $1/3+\eta$ tem triplas de Schur.*

Naturalmente, pode-se formular uma versão com outra classe de grupos, no lugar de $(\mathbb{Z}_{3^n})_n$.

Uma outra área de problemas é a de versões probabilísticas do Teorema de Schur com coloração (e não mais densidade). Por exemplo, vimos no capítulo introdutório (teorema 20, referência [14]) que Graham, Rödl e Ruciński provaram que se $N = N(n)$ satisfaz $N/n^{1/2} \to \infty$, então $[n]_N \to (\text{Schur})_2$ com probabilidade tendendo a 1 quando $n \to \infty$ (estas notações foram definidas pelas equações 1.5 e 1.8). No entanto, a generalização disto para $m > 2$ está em aberto.

Sobre a versão probabilística do Teorema de Sárközy, um desafio interessante seria investigar a versão difícil do problema de Sárközy. Lembramos que tratamos da equação $x - y = z^2$ no nosso resultado (teorema 14), e a exigência sobre os termos da equação é que x e y estejam no subconjunto

de densidade η de $\mathbb{Z}_{n,p}$, enquanto que z pode ser qualquer elemento de $\mathbb{Z}_n$. A proposta é investigar o que acontece se exigirmos que z (ou z^2) também esteja no subconjunto de densidade η de $\mathbb{Z}_{n,p}$.

Outro problema, mais humilde, é achar outras M-sequências interessantes (não muito artificiais) que sejam adição-regulares ou subtração-regulares. Evidentemente, para cada nova M-sequência adição- ou subtração-regular, teremos um novo corolário do teorema 67 ou do teorema 68.

Bibliografia

[1] M. Aigner and G. Ziegler, *Proofs from The Book*, second ed., Springer-Verlag, Berlin, 2001, Including illustrations by Karl H. Hofmann. MR MR1801937 (2001j:00001)

[2] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976, Undergraduate Texts in Mathematics. MR 55 #7892

[3] B. Bollobás, *Modern graph theory*, Springer-Verlag, New York, 1998. MR 99h:05001

[4] ———, *Random graphs*, second ed., Cambridge Studies in Advanced Mathematics, vol. 73, Cambridge University Press, Cambridge, 2001. MR 2002j:05132

[5] F. R. K. Chung and R. L. Graham, *Quasi-random subsets of Z_n*, J. Combin. Theory Ser. A **61** (1992), no. 1, 64–86. MR 94b:05168

[6] F. R. K. Chung, R. L. Graham, and R. M. Wilson, *Quasi-random graphs*, Combinatorica **9** (1989), no. 4, 345–362. MR 91e:05074

[7] P. Erdős and M. Simonovits, *A limit theorem in graph theory*, Studia Scientiarum Mathematicarum Hungarica **1** (1966), 51–57.

[8] P. Erdős and A. H. Stone, *On the structure of linear graphs*, Bulletin of the American Mathematical Society **52** (1946), 1087–1091.

[9] P. Erdős and P. Turán, *On some sequences of integers*, Journal of the London Mathematical Society **11** (1936), no. 2, 261–264.

[10] P. Frankl, R. L. Graham, and V. Rödl, *Quantitative theorems for regular systems of equations*, J. Combin. Theory Ser. A **47** (1988), no. 2, 246–261. MR 89d:05020

[11] H. Furstenberg, *Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions*, J. Analyse Math. **31** (1977), 204–256. MR 58 #16583

[12] S. Gerke, Y. Kohayakawa, V. Rödl, and A. Steger, *Small subsets inherit sparse ε-regularity*, in preparation, 2004.

[13] S. Gerke, T. Schickinger, and A. Steger, *K^5-free subgraphs of random graphs*, Random Structures and Algorithms **24** (2004), no. 2, 194–232.

[14] R. L. Graham, V. Rödl, and A. Ruciński, *On Schur properties of random subsets of integers*, J. Number Theory **61** (1996), no. 2, 388–408. MR 98c:05013

[15] R. L. Graham, B. L. Rothschild, and J. H. Spencer, *Ramsey theory*, second ed., John Wiley & Sons Inc., New York, 1990, A Wiley-Interscience Publication. MR 90m:05003

[16] B. Green and I. Z. Ruzsa, *Sum-free sets in abelian groups.*

[17] P. E. Haxell, Y. Kohayakawa, and T. Łuczak, *The induced size-Ramsey number of cycles*, Combin. Probab. Comput. **4** (1995), no. 3, 217–239. MR 96h:05140

[18] ———, *Turán's extremal problem in random graphs: forbidding even cycles*, J. Combin. Theory Ser. B **64** (1995), no. 2, 273–287. MR 96e:05151

[19] ———, *Turán's extremal problem in random graphs: forbidding odd cycles*, Combinatorica **16** (1996), no. 1, 107–122. MR 97k:05180

[20] L. K. Hua, *Additive theory of prime numbers*, Translations of Mathematical Monographs, Vol. 13, American Mathematical Society, Providence, R.I., 1965. MR MR0194404 (33 #2614)

[21] ———, *Introduction to number theory*, Springer-Verlag, Berlin, 1982. MR MR665428 (83f:10001)

[22] S. Janson, T. Łuczak, and A. Ruciński, *Random graphs*, Wiley-Interscience, New York, 2000. MR 2001k:05180

[23] Y. Kohayakawa, *Szemerédi's regularity lemma for sparse graphs*, Foundations of computational mathematics (Rio de Janeiro, 1997), Springer, Berlin, 1997, pp. 216–230. MR 99g:05145

[24] Y. Kohayakawa, T. Łuczak, and V. Rödl, *Arithmetic progressions of length three in subsets of a random set*, Acta Arith. **75** (1996), no. 2, 133–163. MR 97b:11011

[25] ———, *On K^4-free subgraphs of random graphs*, Combinatorica **17** (1997), no. 2, 173–213. MR 98h:05166

[26] Y. Kohayakawa and V. Rödl, *Szemerédi's regularity lemma and quasi-randomness*, Recent advances in algorithms and combinatorics, CMS Books Math./Ouvrages Math. SMC, vol. 11, Springer, New York, 2003, pp. 289–351. MR MR1952989 (2003j:05065)

[27] J. Komlós and M. Simonovits, *Szemerédi's regularity lemma and its applications in graph theory*, Combinatorics, Paul Erdős is eighty, Vol. 2 (Keszthely, 1993), János Bolyai Math. Soc., Budapest, 1996, pp. 295–352. MR 97d:05172

[28] C. McDiarmid, *On the method of bounded differences*, Surveys in combinatorics, 1989 (Norwich, 1989), London Math. Soc. Lecture Note Ser., vol. 141, Cambridge Univ. Press, Cambridge, 1989, pp. 148–188. MR 91e:05077

[29] C. G. Moreira and Y. Kohayakawa, *Tópicos em combinatória contemporânea*, Publicações Matemáticas do IMPA. [IMPA Mathematical Publications], Instituto de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2001, 23º Colóquio Brasileiro de Matemática. [23rd Brazilian Mathematics Colloquium]. MR MR1846391 (2002e:05003)

[30] R. Rado, *Studien zur Kombinatorik.*, Math. Z. **36** (1933), 424–480 (German).

[31] V. Rödl and A. Ruciński, *Threshold functions for Ramsey properties*, J. Amer. Math. Soc. **8** (1995), no. 4, 917–942. MR 96h:05141

[32] ———, *Rado partition theorem for random subsets of integers*, Proc. London Math. Soc. (3) **74** (1997), no. 3, 481–502. MR 98d:05147

[33] A. Sárkőzy, *On difference sets of sequences of integers. I*, Acta Math. Acad. Sci. Hungar. **31** (1978), no. 1–2, 125–149. MR 57 #5942

[34] E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245, Collection of articles in memory of Juriĭ Vladimirovič Linnik. MR 51 #5547

[35] ———, *Regular partitions of graphs*, Problèmes combinatoires et théorie des graphes (Colloq. Internat. CNRS, Univ. Orsay, Orsay, 1976), CNRS, Paris, 1978, pp. 399–401. MR 81i:05095

[36] P. Turán, *Eine Extremalaufgabe aus der Graphentheorie*, Mat. Fiz. Lapok **48** (1941), 436–452, in Hungarian, with German summary.

[37] B. L. van der Waerden, *Beweis einer Baudetschen Vermutung*, Nieuw Archief voor Wiskunde **15** (1927), 212–216.