Anna Carolina Fernandes da Silva

Os Teoremas de Ramsey e Freiman e suas Aplicações Envolvendo Conjuntos com Progressões Aritméticas

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade de Brasília, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Hemar Teixeira Godinho.

Brasília

2017

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Os Teoremas de Ramsey e Freiman e suas Aplicações Envolvendo Conjuntos com Progressões Aritméticas

por

Anna Carolina Fernandes da Silva *

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para obtenção do grau de

MESTRE EM MATEMÁTICA

Brasília, 17 de fevereiro de 2017.

Comissão Examinadora:

Prof. Hemar Teixeira Godinho – MAT/UnB (Orientador)

Profa. Daniela Amorim Amato– MAT/UnB (Membro)

Prof. Paulo Henrique de Azevedo Rodrigues - UFG (Membro)

* O autor foi bolsista do CNPq durante a elaboração desta dissertação.

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

FSI586t

Fernandes da Silva, Anna Carolina
Os Teoremas de Ramsey e Freiman e suas Aplicações em Conjuntos com Progressões Aritméticas / Anna Carolina Fernandes da Silva; orientador Hemar Teixeira Godinho. -- Brasília, 2017.
70 p.

Dissertação (Mestrado - Mestrado em Matemática) -- Universidade de Brasília, 2017.

1. Teoria de Ramsey. 2. Teorema de Freiman. 3. Progressões Aritméticas. I. Teixeira Godinho, Hemar, orient. II. Título.

Agradecimentos

Agradeço imensamente à Deus que me capacitou até aqui, me mantendo saudável e rodeada de anjos para enfrentar os obstáculos do caminho.

Aos meus pais, Marcos Pereira da Silva e Aparecida Fernandes Leite, por acreditarem em mim, mesmo quando nem eu mesma acreditava, por me educarem e principalmente por me amarem tanto.

Aos meus irmãos Jonatan Fernandes da Silva e Jhéssika Fernandes da Silva, por serem bem mais que irmãos nessa jornada, eles sempre serão meus melhores amigos. As minhas sobrinhas Maria Eduarda e Anna Heloísa que não precisaram fazer nada, mas foram minha força. Obrigada por existirem, sem vocês não seria possível.

Nesse caminho, além de minha família eu preciso agradecer muito o Jean Carlos, por estar ao meu lado em todos os momentos, foi ele que me fez ter coragem de sair da minha zona de conforto e vir a Brasília correr atrás do meu sonho. Será sempre lembrado com carinho e admiração.

As minhas Anna e Ana, por terem se tornado bem mais que parceiras de estudo e de noitada na UnB, fomos confidentes, amigas, um verdadeiro tripé de Anna's e Ana. Espero manter essa amizade para a vida(já estamos).

Aos amigos que conheci no mestrado, que compartilharam dúvidas e certezas, mostrando que eu não estava sozinha. Aos amigos do doutorado que me apoiavam, em especial a três queridos, Juliana Canella que me abrigou na sua casa antes mesmo de me conhecer, e mesmo depois de já alojada, ela me abrigava com o olhar de quem cuida, de quem dá apoio; ao Josimar Ramires que esteve ao meu lado, perdeu várias horas de "conversas vazias"no caminho de casa e sempre me dava aquela mão amiga nos momentos de sufoco; e a Alessandra Kreutz por ter me ajudado tanto na reta final deste trabalho, e ajudado das mais diversas formas, fico feliz por termos nos tornado amigas.

Agradeço a Laena Furtado que foi amiga de graduação e que mesmo de longe me salvou algumas vezes; aos amigos que não são da matemática, em especial Bruna Rodrigues, Layla Lorrayne que entenderam minha distância e me mandavam palavras de amor e carinho quando precisava; ao Halã Queiroz que assim como as meninas me deram suporte e que além disso se dispôs a ler essa dissertação para encontrar erros, mesmo não suportando matemática. Não é possível citar o nome de todos os amigos que me ajudaram, tenho muito sorte de ter todos vocês em minha vida, peço desculpas aos não citados e espero ter agradecido em algum momento.

Agradeço ao meu orientador Hemar Godinho, que com toda a bagagem e experiencia que têm, me ensinou muito. Além de ter um olhar de pai que acalma, que dá esperança ele é uma das pessoas mais bem humoradas que conheço.

Aos professores Daniela Amato e Paulo Henrique, que aceitaram com todo carinho o convite do Hemar para completar a banca examinadora. Confesso ficar muito feliz com a escolha do professor Hemar. Daniela por ter sido minha professora de Introdução à Álgebra e o Paulo Henrique por ser da UFG, lugar onde fiz graduação.

Por fim, agradeço ao CNPq, pelo apoio financeiro na realização desta pesquisa.

Resumo

Essa dissertação trata da Teoria combinatória dos números em conjuntos finitos de inteiros contendo progressões aritméticas, bem como da Teoria de Ramsey, do Teorema de Szemerédi e de alguns resultados adjacentes importantes. Além de apresentar o Teorema de Freiman e exibir uma demonstração de uma generalização do Teorema de Freiman, dada por Ruzsa, nós daremos duas importantes aplicações deste teorema, sendo que uma delas prova a versão quantitativa de uma conjectura de Erdös.

Palavras-chave: Conjuntos Soma, Progressões Aritmética, Teorema de Freiman e Teoria de Ramsey.

Abstract

This work is about Combinatorial number theory in finite sets of integers containing arithmetic progression. Also, we present Ramsey's theory, Szemerédi's theorem and some important adjacent results. Besides that, we introduce Freiman's theorem and exhibit a proof of its generalization, given two applications of this theorem, one of which proves the quantitative version of a conjecture of Erdös.

Keywords: Sumsets, Arithmetics Progression, Freiman's Theorem and Ramsey's Theory.

Sumário

Introdução

Teoria aditiva dos números é uma subárea de Teoria dos Números que estuda o comportamento de subconjuntos de inteiros sob a operação de soma. Problemas clássicos em teoria aditiva dos números inicia com um conjunto de inteiros A e uma h-ésima soma de cópias de A, que será denotado por $hA = \{a_1 + + a_h : a_i \in A\}$. Existe uma ligação entre essa Teoria e a Teoria Combinatória. Neste trabalho iremos abordar um pouco sobre essa ligação.

Um problema inverso em Teoria Aditiva dos Números é um problema em que tentamos deduzir propriedades de um conjunto finito de inteiros a partir de um conjunto soma. Existem vários teoremas inversos importantes, como os de Freiman, Kneser, Plunnecke e Vosper [13]. Em particular, Ruzsa descobriu uma generalização do teorema de Freiman. Um dos objetivos desta dissertação é apresentar esta bela prova de Ruzsa.

O segundo capítulo tratará da Teoria Combinatória de Ramsey, teoria que recebeu este nome em homenagem à Frank P. Ramsey que foi pioneiro nesta área, quando em 1930, em um artigo que ficou conhecido como "Um problema em lógica matemática", publicou um teorema conhecido hoje, o Teorema de Ramsey. Ainda nesse capítulo apresentaremos uma versão quantitativa do Teorema de Szemeredi que é fundamental na demonstração da primeira aplicação do Teorema de Freiman.

Em resumo o Teorema de Freiman diz que para um conjunto A não vazio, finito de inteiros com a soma dupla pequena, isto é, $|2A| \leqslant c|A|$, onde c é uma constante, têm-se que A está contido em uma P.A. multidimensional, isto é, uma progressão aritmética que têm mais de uma razão. Provaremos aqui uma generalização dada por I. Z. Ruzsa. Para esse fim, serão necessários: estabelecer o método de Plunnecke, onde definiremos grafo de Plunnecke e raio de magnitude para podermos demonstrar o Teorema de Plunnecke-Ruzsa; definir o conjunto de Bohr, para estabelecermos o Teorema de Bogolyubov e o isomorfismo

de Freiman, onde aqui o isomorfismo de Freiman é definido por uma propriedade especial, a de que a imagem de um conjunto finito B por um h-isomorfismo de Freiman é uma progressão aritmética n-dimensional própria se, e somente se, B é uma progressão aritmética n-dimensional própria. Todos estes conceitos serão melhor apresentados futuramente.

A primeira aplicação do teorema de Freiman que apresentaremos, refere-se à um conjunto $A \subset \mathbb{Z}$ com cardinalidade de A suficientemente grande e que possui conjunto soma pequena e pelo teorema de Freiman, tal conjunto contém uma progressão aritmética longa. A segunda trata-se de um conjunto finito de inteiros contendo "muitas"progressões aritméticas com três termos, isto é, progressões aritméticas com cardinalidade igual a três; contém uma progressão aritmética longa. este resultado é uma versão quantitativa de uma conjectura de Erdös. Para demonstrarmos este problema será necessário um outro resultado, o Teorema de Balog-Szemerédi.

Capítulo 1

Preliminares

Nesse capítulo, pretendemos introduzir os pré-requisitos básicos para o bom entendimento do trabalho, listando definições, exemplos e propriedades básicas de grafos, progressões aritméticas e conjuntos soma. Quando necessário, outros resultados e definições poderão ser citados ao longo do texto, para que tudo seja devidamente justificado.

1.1 Noções sobre Grafos

Objetivando uma notação mais precisa sobre problemas que podem ser modelados por meio de pontos ligados por arestas, introduzimos aqui a ideia de grafo. Esses conceitos nos auxiliarão no entendimento e na demonstração de alguns resultados posteriormente, por exemplo no teorema de Ramsey.

Definição 1.1. *Dados $V(G)$ e $E(G)$ conjuntos finitos não-vazios, define-se como* ***grafo*** *$G(V, E)$ a figura determinada por um conjunto $V(G)$ de pontos, denominados vértices e um conjunto $E(G)$ de linhas, denominadas arestas, de maneira que cada aresta seja determinado por um par não ordenado de vértices distintos.*

Exemplo 1.2. *Seja $G(V, E)$ um grafo, onde $V(G) = \{A, B, C, D, E, F, G, H\}$, $E(G) = \{(A, B), (A, D), (B, C), (B, F), (C, D), (D, E), (E, F), (F, G), (G, H)\}$. Assim, podemos representar graficamente $G(V, E)$ pela Figura 1.1.*

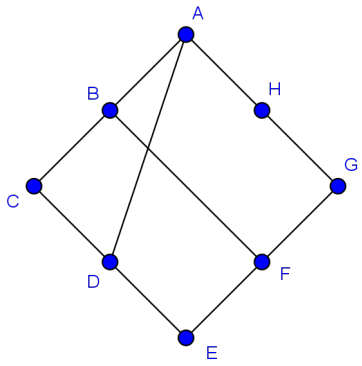

Figura 1.1: Exemplo de Grafo

Definição 1.3. *Um grafo $G(V, E)$ é dito* ***completo de ordem*** *n, desde que, $|V(G)| = n$ e para todos $i \neq j \in V(G)$ tenhamos que $(i, j) \in E(G)$.*

Exemplo 1.4. *No exemplo anterior $G(V, E)$ um grafo qualquer, consideramos o mesmo conjunto de vértices e o completando obtemos $G'(V, E)$, onde $E(G') = \{(x, y) : x, y \in V\}$. Sua representação pode ser dada pela figura 1.2.*

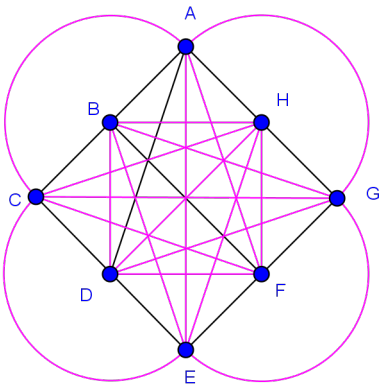

Figura 1.2: Exemplo de Grafo Completo de ordem 8

Definição 1.5. *Seja $G(V, E)$, se existem X e Y subconjuntos disjuntos de $V(G)$, tais que $X \cup Y = V(G)$ e para cada aresta de $(a, b) \in E(G)$ tivermos $a \in X$ e $b \in Y$ então, nós dizemos que G é um* ***grafo bipartido*** *com classes de vértices X e Y.*
Temos uma correspondência de X em Y se G é um grafo bipartido com $|X|$ arestas disjuntas.

Definição 1.6. *Um* ***grafo direcionado*** *é um grafo $G(V, E)$ onde cada aresta tem uma direção, isto é, se $(i, j) \in E(G)$, então existe uma aresta de i em j em G. Em um grafo direcionado, para dois vértices u e v, temos um caminho de u em v desde que existam uma sequência de vértices distintos $u = w_0, w_1, \ldots, w_l = v$, tais que, $(w_0, w_1), (w_1, w_2), \ldots, (w_{l-1}, w_l) \in E(G)$. Dois caminhos de u em v são ditos independentes se os únicos vértices em comum forem u e v.*

Exemplo 1.7. *Considere $G(V, E)$ um grafo direcionado, onde $V(G) = \{A, B, C, D, E, F\}$ e $E(G) = \{(A, B), (A, F), (B, E), (B, F), (C, B), (C, D), (C, F), (D, A), (D, E), (E, C), (F, E)\}$. Observe que existe um único caminho de F em A. Na figura 1.3*

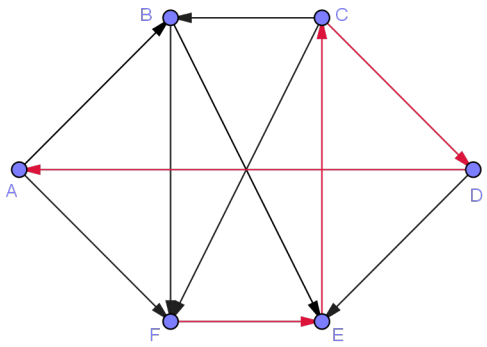

Figura 1.3: Exemplo de Grafo Direcionado

1.2 Conjuntos Soma

A questão que estamos abordando está relacionada com a teoria da adição de conjuntos. Portanto, é preciso primeiro definir o que é a adição de conjuntos e como ele funciona.

Definição 1.8. *Sejam $A_1, A_2, \ldots, A_n$ subconjuntos de números inteiros. Definimos o conjunto soma por:*

$$A_1 + \cdots + A_n = \{a_1 + \ldots + a_n : a_1 \in A_1, a_2 \in A_2, \ldots a_n \in A_n\}$$

e denotamos por nA quando $A_1 = A_2 = \cdots = A_n = A$.

Conjuntos somas podem ser também definidos sobre grupos abelianos e, de fato, em qualquer conjunto em que há uma operação binária . Por exemplo, devemos considerar

$\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ o grupo de congruências módulo m, ou ainda $\mathbb{Z}^n$ a rede de inteiros em $\mathbb{R}^n$. Assim como definimos conjuntos soma, podemos definir conjunto diferença. Sejam $A_1, A_2, \ldots, A_n$ subconjuntos de números inteiros.

$$A_1 - \cdots - A_n = \{a_1 - \ldots - a_n : a_1 \in A_1, a_2 \in A_2, \ldots a_n \in A_n\}$$

E

$$-nA = \{-a_1 - \ldots - a_n : a_i \in A\}$$

Definimos ainda,

$$k * A = \{ka : a \in A\}$$

E é claro que,

$$k * (A + B) = k * A + k * B.$$

1.3 Progressões Aritméticas

Progressão Aritmética é o nosso principal objeto de estudo nesse trabalho, dado que objetivamos dar aplicações ao teorema de Freiman, que tratam de hipóteses sobre conjuntos para que os mesmos contenham ou estejam contidos em progressões aritméticas.

Definição 1.9. *Sejam k e q inteiros positivos. Seja $a \in \mathbb{Z}$. Uma progressão aritmética P.A Q de tamanho k, razão q e termo inicial a é definida por*

$$Q = \{a, a + q, a + 2q, \cdots, a + (k-1)q\} = \{a + xq : x \in [0, k-1]\}$$

Podemos facilmente mostrar que

$$|A_1 + \cdots + A_n| \geqslant \sum_{i=1}^{n} |A_i| - n + 1,$$

A igualdade ocorre se, e somente se $A_1, \ldots, A_n$ são progressões aritméticas com mesma razão.

Podemos generalizar a definição de P.A. para uma P.A. n-dimensional. Sejam $l_1, \ldots, l_n$ e $q_1, \ldots, q_n$ inteiros positivos, seja a um inteiros qualquer. Uma P.A. n-dimensional de tamanho $l(Q) = l_1 \ldots l_n$ é dada por

$$Q = Q(a; q_1, \ldots, q_n; l_1, \ldots, l_n) = \{a + x_1 q_1 + \cdots + x_n q_n : x_i \in [0, l_i - 1]\}$$

Exemplo 1.10. *Sejam* $l_1 = l_2 = 2$, $q_1 = q_2 = 2$ *e* $a = 1$

$$\begin{aligned} Q' = Q'(a; q_1, \ldots, q_n; l_1, \ldots, l_n) &= Q(1; 2, 2; 2, 2) \\ &= \{1 + 2x_1 + 2x_2 : x_i \in [0, 1]\} \\ &= \{1, 3, 5\} \end{aligned}$$

Aqui, $|Q'| = 3$ *e* $l(Q') = 4$.

Observe ainda que podemos ver Q' *como uma P.A. 1-dimensional, basta tomar* $a = 1$, *a razão* $q = 2$ *e o tamanho* $k = 3$. *Daí*

$$Q' = \{a + xq : x \in [0, 2]\}$$

Isto nos diz que a representação de um conjunto, como uma progressão aritmética multidimensional não é único. Um conjunto pode ter mais de uma tal representação, e essas representações podem ter diferentes dimensões e comprimentos

Capítulo 2

Teoria de Ramsey

Desordem completa é impossível. Esta é a descrição da Teoria de Ramsey segundo T. S. Motzkin. Intuitivamente, essa teoria investiga a ordem inerente em algumas estruturas matemáticas. Nesta seção descrevemos alguns conceitos principais desta teoria.

Um resultado típico em Teoria de Ramsey começa com alguma estrutura matemática que é em seguida particionada. Quão grande deve ser a estrutura original de modo a assegurar que, pelo menos, uma das partes tenha uma dada propriedade? Antes de desvendarmos a clássica relação de Ramsey, ilustramos um resultado particular, simples mas emblemático. Assumimos aqui a simetria da relação "conhecer", ou seja, A conhece B se, e somente se, B conhece A.

Considere uma festa com n participantes. Dado s e t inteiros positivos, qual deve ser o tamanho mínimo de n para garantir que existem t pessoas que se conhecem ou existem s pessoas que não se conhecem?

Vamos inicialmente analisar um caso mais simples $t = s = 3$. Seja $V = \{P_1, \ldots, P_n\}$ o conjunto de n pessoas da festa e defina $[V]^2 = \{\{P_i, P_j\} : P_i, P_j \in V\}$. Considere o grafo completo $K_n = G(V, A)$ com vértices V e arestas $A = [V]^2$. Defina uma 2-coloração sobre A, como $f : A \to [1, 2]$ uma função definida tal que

$$f(\{P_i, P_j\}) = \begin{cases} 1, & \text{se } P_i \text{ e } P_j \text{ se conhecem,} \\ 2, & \text{caso contrário.} \end{cases}$$

Nesse caso nosso problema inicial pode ser reinterpretado como: encontre a menor cardinalidade de V que garanta que K_n tenha um subgrafo completo K_3, com todas as

arestas da mesma cor, ou seja, a função f restrita à $A(K_3)$ é estritamente 1 ou 2.

$$f\mid_{A(K_3)} = i \in [1,2].$$

Denotamos por $R_2(3,3)$ o número mínimo de vértices satisfazendo nosso problema. Ou seja a menor cardinalidade de V tal que, para qualquer 2-coloração f de A for possível encontrar um grupo de 3 pessoas tais que todos elas se conheçam ou um grupo de três pessoas tais que nenhuma delas se conheçam, onde o índice 2 representa os pares de V, o primeiro 3 representa um subgrafo de K_n com cardinalidade igual à 3 que possui todas as arestas da cor 1, e o segundo representa um subgrafo de K_n com cardinalidade igual à 3, onde todas suas arestas são da cor 2.

Lema 2.1. *$R_2(3,3) = 6$.*

Demonstração. Como K_n é completo $\{P_i, P_j\} \in A$ para todos $P_i, P_j \in V$. Queremos mostrar que $R_2(3,3) = 6$, isto é, que $n = 6$. Desta forma primeiro temos que mostrar que $n \geqslant 6$ satisfaz o problema e depois mostrar que $n = 5$ não satisfaz, e como $R_2(3,3)$ é definido como o menor inteiro positivo com essa propriedade, automaticamente teremos $R_2(3,3) = 6$. Temos que existem 5 arestas de K_n contendo P_1. E pelo Princípio da Casa dos Pombos, pelo menos 3 dessas arestas serão da mesma cor. Sem perda de generalidade assumiremos $\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_4\}$ são da cor 1.
Assim se $\{P_2, P_3\}$ ou, $\{P_2, P_4\}$ ou, $\{P_3, P_4\}$ forem da cor 1, obtemos um subgrafo K_3 com todas as arestas de cor 1. Se todos forem da cor 2, então teremos um subgrafo K_3' com todas as arestas de cor 2. Logo para $n \geqslant 6$ sempre se têm 3 pessoas se conhecendo mutuamente ou 3 pessoas que não se conhecem. Agora observe que $n = 5$ não é suficiente para garantir a existência de 3 pessoas se conhecerem ou 3 pessoas não se conhecerem. De fato, se $n = 5$, então $V = \{P_1, P_2, \ldots, P_5\}$ observe que podemos considerar $\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}, \{P_4, P_5\}$ *e* $\{P_5, P_1\}$ da cor 1 e $\{P_1, P_3\}, \{P_1, P_4\}, \{P_2, P_4\}$, $\{P_2, P_5\}$ *e* $\{P_3, P_4\}$ da cor 2, e ver que nesse caso não existe subgrafo de K_n com 3 vértices tais que todas as arestas são de mesma cor, em outras palavras, é possível que em uma festa com 5 pessoas não existam 3 pessoas se conhecendo mutuamente e não existam 3 pessoas que se desconhecem. Logo $R_2(3,3) > 5$. O resultado segue. □

Nossa pergunta original era encontrar $R_2(s,t)$, isto é, o número mínimo de pessoas em uma festa garantindo que sempre se tenha 3 pessoas se conhecendo ou 3 pessoas não

se conhecendo. Essa é uma pergunta em geral muito difícil. Erdös afirmou na década de 1930 que $R_2(5,5)$ seria possível calcular, mas que com as ferramentas que ele conhecia não seria possível encontrar $R_2(6,6)$. Até nos dias de hoje não se conhece o valor exato de $R_2(5,5)$, apenas se tem limitantes. Para mostrar a dificuldade de calcular esses valores segue uma tabela com alguns limitantes e valores conhecidos nos dias atuais.

$t\backslash s$	3	4	5	6	7	8	9	10
3	6	9	14	18	23	28	36	40 - 43
4		18	25	35 - 41	49 - 61	56 - 84	73 - 115	92 - 149
5			43 - 49	58 - 87	80- 143	101 - 216	125 - 316	143 - 442
6				102 - 165	113 - 298	130 - 495	169 - 780	179 - 1171
7					205 - 540	216 - 1031	237 - 1713	289 - 2826

Onde representamos nela os valores exatos quando aparecem apenas um termo e os limitantes inferior e superior quando há dois números. Sabendo-se da dificuldade de se encontrar o valor de $R_2(s,t)$, ficam as perguntas: esse número sempre existe? É possível generalizar este resultado para qualquer r-upla? A resposta afirmativa foi dada em 1930, conforme o seguinte resultado. Antes, uma definição necessária para o entendimento do enunciado.

Definição 2.2. *Seja S um conjunto não vazio. Denotamos por $[S]^r$ o conjunto de todos os subconjuntos de S com r elementos, chamados r-subconjuntos de S. Definimos n-coloração por uma função que vai de $[S]^r$ no intervalo de inteiros $[1,n]$.*

$$c : [S]^r \to [1,n]$$

Teorema 2.3 (Ramsey 1930)**.** *Sejam $r > 0$ e $q_1, q_2, ..., q_n \geq r$ inteiros. Existe um conjunto S com cardinalidade suficientemente grande, então para toda n-coloração de $[S]^r$, temos que existe $H \subseteq S$ com cardinalidade q_i e*

$$c\,|_{[H]^r} \equiv i$$

para algum $1 \leq i \leq n$.

A menor cardinalidade de S que satisfaz o Teorema de Ramsey é dito número de

Ramsey e denotado por

$$R_r(q_1, q_2, ..., q_n).$$

Para a demonstrar o Teorema de Ramsey, serão necessários dois lemas:

Lema 2.4. *$R_2(a, b)$ existe para todos $a, b \geq 2$.*

Demonstração. Seguiremos por indução sobre $a + b$.
Para $a + b = 2$ basta observarmos que $R_2(a, 2) = R_2(2, a) = a$. De fato, se um conjunto V tem cardinalidade igual à a então para toda 2-coloração de $[V]^2$, ou existe um par de V que têm imagem igual à 2, ou todos os pares têm imagem igual à 1. Analogamente para a outra igualdade.
Suponhamos a existência de $R_2(a-1, b)$ e de $R_2(a, b-1)$. Mostraremos que $R_2(a, b) \leqslant R_2(a-1, b) + R_2(a, b-1) + 1$, concluindo assim sua existência.

Seja $G(V, E)$ um grafo completo com $R_2(a-1, b) + R_2(a, b-1) + 1$ vértices. Tome $v \in V(G)$. Considere os subgrafos M e N, tais que $w \in V(G)$ está em M se, e somente se, (v, w) é da cor 1.

Pelo Princípio da Casa dos Pombos, $| V(M) | \geqslant R_2(a-1, b)$ ou $| V(N) | \geqslant R_2(a, b-1)$. Sem perda de generalidade, assuma $| V(M) | \geqslant R_2(a-1, b)$.

Daí existe $H \subseteq V(M)$ tal que $|H| = a - 1$ e o conjunto $[H]^2$ de arestas de H é da cor um, ou $|H| = b$ e $[H]^2$ é da cor dois.

No primeiro caso, basta observar que $[H \cup \{v\}]^2$ é pintado da cor 1 e $|H \cup \{v\}| = a$.

No segundo caso, não há o que mostrar. □

Lema 2.5. *$R_r(a, b)$ existe para todos $a, b \geqslant r$ e todo $r \geqslant 2$.*

Demonstração. Para $r = 2$ temos que $R_2(a, b)$ existe para todos $a, b \geq 2$ (Lema 2.4), temos também que $R_r(r, r) = r, \quad \forall r > 0$. Assuma por hipótese de Indução que $R_{r-1}(a, b)$ existe para todos $a, b \geq r - 1$ e que $R_r(a-1, b)$ e $R_r(a, b-1)$ existem para todo $r > 0$.

Mostraremos que $R_r(a, b) \leq R_{r-1}(R_r(a-1, b), R_r(a, b-1)) + 1$, para todos $r > 0$ e $a, b \geq r$.

Seja M um conjunto tal que,

$$|S| = R_{r-1}(R_r(a-1, b), R_r(a, b-1)) + 1$$

e considere

$$c : [S]^r \to [1, 2].$$

Seja $x \in S$, defina:

$$c_x : [S - \{x\}]^{r-1} \to [1, 2]$$

tal que, para todo $N \subseteq [S - \{x\}]^{r-1}$,

$$c_x(N) = c(N \cup \{x\}).$$

Por hipótese de indução, temos que $\exists H \subseteq S - \{x\}$ c_x-monocromático de cor um e $|H| = R_r(a - 1, b)$ ou de cor dois e $|H| = R_r(a, b - 1)$
Sem perda de generalidade, assuma que: $|H| = R_r(a - 1, b)$

Daí, existe $K \subseteq H$ tal que

$$c \mid_{[K]^r} \equiv 1 \text{ e } |K| = a - 1 \text{ ou}$$

$$c \mid_{[K]^r} \equiv 2 \text{ e } |K| = b.$$

No primeiro caso, como $c_x \mid_{[H]^{r-1}} \equiv 1$ e $K \subseteq H$, temos: $c_x \mid_{[K]^{r-1}} \equiv 1$.
Logo,

$$c \mid_{[K]^{r-1} \cup \{x\}} \equiv 1.$$

Assim,

$$c \mid_{[K \cup \{x\}]^r} \equiv 1.$$

No segundo caso, não há o que mostrar. O resultado segue.

□

2.0.1 Demonstração do Teorema de Ramsey

Com estes dois Lemas, podemos enfim demonstrar o Teorema de Ramsey.

Demonstração. Primeiro, observe que para $r = 1$ o resultado é válido para todo n e todos $q_1, ..., q_n$ e

$$R_1(q_1, ..., q_n) = q_1 + ... + q_n - n + 1.$$

De fato, se tomarmos S tal que $|S| = q_1 + ... + q_n - n + 1$ e considerarmos:

$$c : [S]^1 \to [1, n],$$

observamos que pelo Princípio da Casa dos Pombos, existirá um subconjunto $H \subseteq S$ tal que $c\,|_{[H]^1} = i$ e $|H| = q_i$.

Seguiremos por indução sobre n. Para $n = 2$ $R_r(q_1, q_2)$ existe. (Lema 2.5)

Suponhamos que $R_r(q_1, ..., q_{n-1})$ existe para todo $r > 0$ e todos $q_1, ..., q_n \geq r$.

Mostraremos que:

$$R_r(q_1, q_2, ..., q_n) \leq R_r(q_1, R_r(q_2, ..., q_n)).$$

Seja S um conjunto tal que $|S| = R_r(q_1, R_r(q_2, ..., q_n))$

Considere

$$c : [S]^r \to [1, n]$$

defina

$$p : [S]^r \to [1, 2]$$

$$p(H) = \begin{cases} 1, \text{se } c(H) = 1 \\ 2, \text{se } c(H) \neq 1 \end{cases}$$

Assim, existe $H \subseteq S$ tal que H é p-monocromático de cor 1 e

$$|H| = q_1,$$

ou de cor 2, e

$$|H| = R_r(q_2, ..., q_n).$$

No primeiro caso, não há o que demonstrar.

No segundo caso, $\exists K \subseteq H$ tal que para algum $2 \leq i \leq n$, temos $|K| = q_i$ e

$$c\,|_{[K]^r} \equiv i$$

O resultado segue. □

Conforme vimos, o Teorema de Ramsey garante a existência de $R_2(a, b)$, mas até o momento não foi criado um algoritmo para calculá-los. Para valores pequenos de a e b, o método normalmente utilizado é o da exaustão. No caso de $R_2(3, 3)$, por exemplo, verificamos que 4 e 5 são valores insuficientes. Somente após a análise do valor 6 foi verificada a

existência de triângulos monocromáticos, nos dando $R_2(3,3) = 6$. Contudo, para valores pouco maiores de a e b, a dificuldade aumenta consideravelmente, tornando inviável uma análise exaustiva. O problema torna-se ainda maior quando deseja-se conhecer números da forma $R_2(a_1, a_2, ..., a_k)$. Devido esta dificuldade, passou-se a investigar numerosas variantes e generalizações deste problema, despertando o interesse de pesquisadores de diversas áreas. A pesquisa relacionada à Teoria de Ramsey tem se expandido em várias direções. Conexões e aplicações foram estabelecidas com diversas áreas da matemática: teoria dos números, álgebra linear e multilinear, geometria, topologia, probabilidade e teoria dos conjuntos, além de áreas mais aplicadas. Atualmente, a Teoria de Ramsey é uma das áreas centrais de pesquisa em combinatória.

2.1 Aplicações do Teorema de Ramsey

Greenwood e Gleason encontraram uma cota superior para $R_2(3,3,...,3) \geq \lfloor n!e \rfloor + 1$, onde n é o número de cópias do número 3 (ver [10]). Com essa desigualdade e o Teorema de Ramsey em mãos, foi possível dar uma nova demonstração ao Teorema de Schur.

Teorema 2.6 (Schur, 1916)**.** *Se distribuirmos $M = \{1, 2, ..., \lfloor n!e \rfloor\}$ em n cores, então existirão $x,\ y,\ z \in M$ tais que x, y, z são da cor k e $x + y = z$ para algum $1 \leqslant k \leqslant n$.*

Demonstração. Seja $S = \{1, ..., \lfloor n!e \rfloor, \lfloor n!e \rfloor + 1\}$ e defina:

$$A_k = \{x \in S : x \neq \lfloor n!e \rfloor + 1 \text{ e x é da k-ésima cor}\}$$

$$\mathcal{A}_k = \{(i,j) : 1 \leq i < j \leq \lfloor n!e \rfloor + 1 \ e \ j - i \in A_k\}$$

Considere, $c : [S]^2 \to [1, n]$, definida como $c(s,t) = k$ sempre que $t - s$ é da cor k, isto é, $(s,t) \in \mathcal{A}_k$.

Como $|S| = \lfloor n!e \rfloor + 1 \geq R_2(3, ..., 3)$, existe $H = \{a, b, c\} \subset S$ tal que H é c-monocromático, ou seja, um conjunto que tem todos os elementos levados numa mesma cor.

Daí, $(a,b), (a,c), (b,c) \in \mathcal{A}_k$

Logo, $b - a = x,\ c - b = y,\ c - a = z \in A_k$ e $x + y = z$.

□

Teorema 2.7 (Erdos-Szekeres, 1935)**.** *Seja $m \geq 3$ inteiro. Existe um número suficientemente grande de pontos no plano, sem que se tenha 3 deles colineares, é possível selecionar m destes de modo a obter um polígono convexo com m lados.*

Demonstração. O caso $m = 3$ é trivial.
Para $m > 3$, tome $n \geq R_4(5, m)$. Seja $|S| = n$, considere $c : [S]^4 \to [1, 2]$ definida de modo que $\{P_i, P_j, P_k, P_l\}$ é levado na cor 1 se, e somente se, o polígono por eles formado é côncavo.

Como $n \geq R_4(5, m)$ pelo Teorema de Ramsey existe um subconjunto H monocromático de S da cor 1 tal que $|H| = 5$ e todos os 4-subconjuntos de H são constituídos por 4 vértices de um polígono côncavo, ou da cor 2 tal que $|H| = m$ e todos os 4-subconjuntos de H são formados por 4 vértices de um polígono convexo.

Mas em um conjunto com cinco pontos, sempre é possível selecionar quatro deles de modo a obter um polígono convexo. Logo o primeiro caso não ocorre. Isso conclui a demonstração.

□

O menor número de pontos necessários para garantir a existência de um polígono convexo de m lados no Teorema de Erdos e Szekeres será denotado por $ES(m)$ e chamado de número Erdos-Szekeres.

A melhor limitação para o número de Erdos-Szekeres [3] que temos, foi dada também por Erdor e Szekeres

$$2^{m-2} + 1 \leq ES(m) \leq \binom{2m-4}{m-2} + 1$$

E a conjectura mais famosa sobre o valor exato foi feita por Erdos: $ES(m) = 2^{m-2}$

Teorema 2.8 (van der Waerden)**.** *Para inteiros positivos, k e m, se n é suficientemente grande e distribuirmos 1,2,...,n objetos em k gavetas, então alguma gaveta irá conter uma progressão aritmética com m termos.*

Para demonstrarmos o Teorema de van der Waerden são necessários alguns resultados. Mas antes enunciaremos um resultado (ver [15]) provado por um dos alunos de Schur, R.Rado em 1933 que torna os teoremas de Schur e de van der Waerden em casos particulares.

Teorema 2.9 (Rado). *Seja $A = (a_{ij})_{1\leq i,j\leq n}$ uma matriz com entradas em $\mathbb{Z}$. Então a equação $A.(x_1, x_2, ..., x_n)^T = 0$ é uma partição regular (isto é, se distribuirmos todos os inteiros positivos em um número finito de cores a equação sempre tem solução em que $x_1, x_2, .., x_n$ ão da mesma cor) se, e somente se, pudermos renumerar os vetores coluna de A, de tal forma que os inteiros $1 \leq n_1 < n_2 < ... < n_l = n$, para os quais a soma dos primeiros n_k vetores coluna é uma combinação dos primeiros n_{k-1} vetores coluna. Denotamos $n_0 = 0$.*

Para $a_1, a_2, ..., a_m \in \mathbb{Z}^+$ com $m \geq 2$, definimos o número de Rado (2-cor) $R(a - 1, a_2, ..., a_m)$ o menor inteiro positivo N tal que para toda 2-coloração de um conjunto $[1, n]$ com $n \geq N$ então existe uma solução monocromática da equação $a_1x_1+a_2x_2+...+a_mx_m = x_0$ com $x_0, x_1, ..., x_m \in [1, n]$

Em 2005 S.Guo e Z. W. Sun determinaram o valor exato de $R(a - 1, a_2, ..., a_m)$, que havia sido conjecturado por B. Hopkins e D. Schaal. Neste trabalho não demonstraremos este resultado, para mais detalhes ver [11].

Teorema 2.10 (Guo-Sun). *Para todo $a_1, a_2, ..., a_m \in \mathbb{Z}^+$ com $m \geq 2$, temos*

$$R(a - 1, a_2, ..., a_m) = av^2 + v - a,$$

onde, $a = min\{a - 1, a_2, ..., a_m\}$ e $v = a - 1 + a_2 + ... + a_m$.

Teorema 2.11 (Princípio da Casa dos Pombos de Shelah). *Sejam $k, m, n \in \mathbb{Z}^+$ e $m \geq f(n, k)$, onde $f(1, k) = k + 1$ e $f(j + 1, k) = k^{f(j,k)^{2j}} + 1$, para $j = 1, 2, \ldots$. Então, para qualquer k-coloração $c_1, \ldots, c_n : [1, m] \times [1, m] \times \cdots \times [1, m] \to [1, k]$, existem $1 \leq a_1 < b_1 \leq m, \ldots 1 \leq a_n < b_n \leq m$ tais que,*

$$\begin{aligned} &c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, a_j, a_j, a_{j+1}, b_{j+1}, ..., a_n, b_n) = \\ &= c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, b_j, b_j, a_{j+1}, b_{j+1}, ..., a_n, b_n) \end{aligned} \tag{2.1}$$

para todo $j = 1, 2, ..., n$.

Demonstração. Seguiremos por Indução.
Para $n = 1$: Como $| \{(a, a) : a \in [1, m]\} | = m \geq f(1, k) = 1 + k > k$, pelo Princípio da Casa dos Pombos, existe $1 \leq a < b \leq m$, tais que, $c_1(a, a) = c_1(b, b)$.

Suponha por hipótese de indução que para $n \geq 1$ o resultado seja válido, isto é, se $m \geq f(n,k)$ para qualquer k-coloração $c_1, \ldots, c_n : [1,m] \times [1,m] \times \cdots \times [1,m] \to [1,k]$, existem $1 \leq a_1 < b_1 \leq m, \ldots 1 \leq a_n < b_n \leq m$ tais que,

$$c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, a_j, a_j, a_{j+1}, b_{j+1}, ..., a_n, b_n) =$$
$$= c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, b_j, b_j, a_{j+1}, b_{j+1}, ..., a_n, b_n)$$

para todo $j = 1, 2, ..., n$.

Mostraremos que o resultado vale para $n+1$,
Sejam $m \geq f(n+1,k) > k^{f(n,k)^{2n}}$ e $c_1, \ldots, c_{n+1}$ k-colorações de $[1,m] \times [1,m] \times \cdots \times [1,m]$. Para $a, b \in [1,m]$ definimos:

$$c_{a,b} : [1, f(n,k)])^{2n} = [1, f(n,k)] \times [1, f(n,k)] \times \cdots \times [1, f(n,k)] \to [1,k]$$

como

$$c_{a,b}(a_1, b_1, \ldots, a_n, b_n) = c_{n+1}(a_1, b_1, \ldots, a_n, b_n, a, b)$$

Como $m > k^{f(n,k)^{2n}} = |\{f : ([1, f(n,k)])^{2n} \to [1,k]\}|$, pelo Princípio da Casa dos Pombos, $\exists 1 \leq a_{n+1} < b_{n+1} \leq m$, tal que,

$$c_{an+1,an+1} = c_{bn+1,bn+1},$$

isto é, para algum $a_1, b_1, \ldots, a_n, b_n \in [1, f(n,k)]$, têm-se

$$c_{n+1}(a_1, b_1, \ldots, a_n, b_n, a_{n+1}, a_{n+1}) = c_{n+1}(a_1, b_1, \ldots, a_n, b_n, b_{n+1}, b_{n+1})$$

para algum $j = 1, 2, \ldots, n$, defina

$$c'_j : ([1, f(n,k)])^{2n} \to [1,k]$$

por, $c'_j(x_1, \ldots, x_{2n}) = c_j(x_1, \ldots, x_{2n}, a_{n+1}, b_{n+1})$
Por hipótese de indução, existem $1 \leq a_1 < b_1 \leq f(n,k), \ldots 1 \leq a_n < b_n \leq f(n,k)$ tais que,

$$c'_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, a_j, a_j, a_{j+1}, b_{j+1}, ..., a_n, b_n) =$$
$$= c'_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, b_j, b_j, a_{j+1}, b_{j+1}, ..., a_n, b_n)$$

isto é,

$$c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, a_j, a_j, a_{j+1}, b_{j+1}, ..., a_n, b_n, a_{n+1}, b_{n+1}) =$$

$$= c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, b_j, b_j, a_{j+1}, b_{j+1}, ..., a_n, b_n, a_{n+1}, b_{n+1})$$

Observe que $f(n,k) \leq f(n+1,k) \leq m$, ($f(n,k) = 2$ se $k = 1$).

□

Para $n, k \in \mathbb{Z}^+$, definimos o **número de Shelah** $S(n,k)$ como o menor, $m \in \mathbb{Z}^+$, tal que, para qualquer $c_1, \ldots, c_n \in ([1,m])^{2n} \to [1,k]$ existam, $1 \leq a_1 < b_1 \leq m, \ldots 1 \leq a_n < b_n \leq m$ tais que,

$$c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, a_j, a_j, a_{j+1}, b_{j+1}, ..., a_n, b_n) =$$

$$= c_j(a_1, b_1, ..., a_{j-1}, b_{j-1}, b_j, b_j, a_{j+1}, b_{j+1}, ..., a_n, b_n)$$

para todo $j = 1, 2, ..., n$..

Observe que $S(n,k) \leq f(n,k)$. Logo, $S(1,k) = k+1$ e $S(n+1,k) \leq k^{S(n,k)^{2n}} + 1$

Definição 2.12. *Seja S um conjunto não vazio, finito. Uma **linha combinatória** em S^n é da forma:*

$$L = \{(x_1, x_2, \ldots, x_n) \in S^n : \textit{todos os } x_i's \textit{ são iguais, se } i \in I$$

$$\textit{todos os } x_j \textit{ são fiixados, se } j \notin I\},$$

onde I é um subconjunto não vazio de $[1,n]$.

Em 1963 Hales e Jewett(ver [12]) mostraram um resultado tipo-Ramsey, que auxiliou na demonstração do Teorema de van der Waerden.

Teorema 2.13 (Hales-Jewett)**.** *Para quaisquer $m, k \in \mathbb{Z}^+$ se $n \in \mathbb{Z}^+$ é grande o suficiente, então para toda k-coloração de $[1,m]$, $[1,m]$ contém uma linha combinatória monocromática.*

Denotaremos o menor n inteiro positivo, satisfazendo o Teorema de Hales-Jewett por $HJ(m,k)$. Em 1988 Shelah usando Princípio da Casa dos Pombos mostrou que

$$HJ(m+1,k) \leq HJ(m,k)S(HJ(m,k), k^{(m+1)^{HJ(m,k)}})$$

2.1.1 Demonstração Teorema de van der Waerden

Demonstração. Seja $h = HJ(m,k)$. Para $x_1, x_2, \ldots, x_h \in [1,m]$ defina,

$$F(x_1, x_2, \ldots, x_h) = 1 + \sum_{i=1}^{h-1}(x_i - 1)m^i.$$

Assim, F é uma correspondência injetiva entre $[1,m]^h$ e $[1,m^h]$.
Qualquer distribuição de $1, 2, \ldots, m^h$ em k gavetas corresponde a distribuição das k-colorações. Pelo Teorema de Hales-Jewett, $[1,m]^h$ contém uma linha combinatória monocromática.

$$\{(x_1, x_2, \ldots, x_h) \in [1,m]^h : x_i's \text{ são iguais se, } i \in I, \text{ ou } x_j = a_j \text{ se } j \notin I\},$$

onde $\phi \neq I \subseteq [1,h]$ e $a_j \in [1,m]$, para $j \in \mathcal{I} = [1,h] - I$.
Assim, os números

$$1 + \sum_{j\in\mathcal{I}}(a_j - 1)m^{j-1} + \sum_{i\in I}(x-1)m^{i-1} \ (x = 1, \ldots, m)$$

estão na mesma gaveta. Em outras palavras, alguma gaveta contém uma progressão aritmética : $a, a+d, \ldots, a+(m-1)d$, onde

$$a = 1 + \sum_{j\in\mathcal{I}}(a_j - 1)m^{j-1} \text{ e } d = \sum_{i\in I} m^{i-1}.$$

O resultado segue.

□

Conjectura de Erdos-Graham, provada por Croot Se distribuirmos todos os inteiros maiores que um em n gavetas, então alguma gaveta contém $x_1, x_2, \ldots, x_n$ com, $\sum_{k=1}^{m} 1/x_k = 1$.

Abaixo uma conjectura geral, que faz do resultado de Croot um caso particular.

Conjectura 2.14 (Z. W. Sun, 2007)**.** *Se A é um subconjunto de $\{2,3,\ldots\}$ com densidade assintótica superior positiva, então existe um número finito de elementos distintos $a_1 < \cdots < a_n$ de A com $\sum_{k=1}^{m} 1/a_k = 1$.*

Em 1936, Erdos e Turán conjecturaram que qualquer conjunto de números inteiros com densidade positiva sobre os naturais contém infinitas progressões aritméticas com três termos. Esta conjectura foi comprovada por Klaus Roth em 1952. Este resultado foi generalizado para progressões aritméticas arbitrariamente longas. Isto é, conjuntos de números inteiros com densidade positiva têm infinitas progressões aritméticas de qualquer tamanho. Apenas em 1975 (ver [19]) Szemeredi conseguiu mostrar o caso geral em um artigo que foi considerado "uma obra prima do raciocínio combinatório"por R. L. Graham. Em 1977 H. Fustenberg deu um nova demonstração ao teorema de Szemeredi usando teoria ergótica. Finalmente em 2001 W. T. Gowers amplicando analise de Fourier e analise combinatória redemonstrou o teorema e conseguiu limites explícitos para a versão quantitativa deste teorema.

Teorema 2.15 (Szemerèdi-Versão Quantitativa)**.** *Seja $0 < \delta < 1$ e $k \in \{3, 4, \ldots\}$. Então existe $N(k, \delta)$, tal que, se $n \geq N(k, \delta)$ e $A \subset [1, n]$, com $|A| \geq \delta n$, então S contém uma P.A. de ordem k.*

Estes são os melhores limitantes para $N(k, \delta)$ conhecidos atualmente:

$$c^{\log(1/\delta)^{k-1}} \leq N(k, \delta) \leq 2^{2^{\delta - 2^{2^{k+9}}}},$$

onde o limite inferior é devido a Behrend (para $k = 3$) e Rankin em 1962, e o limite superior é devido à Gowers em 2001(ver [5]). Em 1999 J. Bourgain mostrou que:

$$N(3, \delta) \leq c^{\delta^{-2}\log(1/\delta)}.$$

Em 1976 Erdos na tentativa de melhorar ainda mais o resultado conjecturou,

Conjectura 2.16 (Erdos-Turán)**.** *Seja $a_1 < a_2 < \cdots$ uma sequência de inteiros positivos com $\sum_{n=1}^{\infty} 1/a_n$ divergente. Então, para qualquer $k = 3, 4, \ldots$ a sequência tem uma subsequência com uma PA de tamanho t k.*

Esta conjectura recebeu também o nome de Turán, em sua memória e em homenagem aos anos de trabalho em parceria com Erdos. Na época, Erdos ofereceu três mil dólares para quem a resolvesse. Ainda hoje, este é um problema em aberto, embora recentemente, em 2008 Green e Terence Tao (ver [9])obtiveram um grande avanço.

Teorema 2.17 (Green-Tao)**.** *Existem PA's arbitrariamente grandes de primos*

Claro que se a conjectura de Erdos-Turán for de fato comprovada, os teoremas de Szemeredi e de Green-Tao tornam-se corolários, já que conjuntos com densidade positiva têm a série de seus inversos divergente e a soma dos inversos de primos também é divergente.

Para Z. W. Sun (ver [18]) a conjectura Erdos-Turán é muito forte para ser verdade, ele acredita que essa conjectura deveria ser modificada para:

"Seja $a_1 < a_2 < \cdots$ uma sequência de inteiros positivos com $\sum_{n=1}^{\infty} 1/a_n$ divergente e $\sum_{i \in I} 1/a_i \in \mathbb{Z}^+$ Então, para qualquer subconjunto I de $\mathbb{Z}^+$ a sequência tem uma subsequência com uma PA arbitrariamente grande."

Capítulo 3

Teorema de Freiman

Um problema inverso em Teoria Aditiva dos Números é um problema em que tentamos deduzir propriedades de um conjunto finito de inteiros a partir de seu conjunto soma $hA = \{a_1 + \cdots + a_h : a_i \in A\}$. O teorema inverso mais importante que trataremos neste trabalho é o de Freiman [4], provado em 1964 sobre estruturas de conjuntos finitos de inteiros com conjunto soma pequeno, isto é, existe uma constante $c \geqslant 2$ tal que $|2A| \leqslant c|A|$, na verdade este teorema generaliza o seguinte resultado

Teorema 3.1. *Sejam A e B conjuntos não vazios, finitos de inteiros. Então*

$$|A + B| \geqslant |A| + |B| - 1.$$

A igualdade ocorre se, e somente se, A e B são progressões aritméticas de mesma razão.

Demonstração. Sejam A e B conjuntos finitos e não vazios de inteiros, podemos supor $A = \{a_1, \ldots, a_k\}$ e $B = \{b_1, \ldots, b_l\}$ e pelo princípio da boa ordenação podemos tomar $a_1 < \cdots < a_k$ e $b_1 < \cdots < b_l$.
Suponha ainda que $|A| \leqslant |B|$. Assim o conjunto soma $A + B$ contém uma sequência de elementos distintos:

$$\begin{aligned} a_1 + b_1 &< a_1 + b_2 < a_2 + b_2 < a_2 + b_3 < \cdots \\ &< a_i < b_i < a_i + b_{i+1} < a_{i+1} + b_{i+1} < \cdots \\ &< a_k + b_k < a_k + b_{k+1} < \cdots < a_k + b_l. \end{aligned}$$

E então, $|A + B| \geqslant (2k - 1) + (l - k) = k + l - 1 = |A| + |B| - 1$.
Se tivermos $|A + B| = |A| + |B| - 1$, mostraremos que A e B são progressões aritméticas

com razão q, para algum q inteiro. Primeiro vamos considerar o caso $|A| = |B| = k$. Assim como anteriormente teremos uma sequência de $2k-1$ termos distintos pertencentes à soma $A + B$. E como por hipótese $|A + B| = |A||B| - 1$, temos que,

$$\begin{aligned} a_1 + b_1 &< a_1 + b_2 < a_2 + b_2 < a_2 + b_3 < \cdots \\ &< a_i < b_i < a_i + b_{i+1} < a_{i+1} + b_{i+1} < \cdots \\ &< a_{k-1} + b_{k-1} < \cdots < a_k + b_k, \end{aligned}$$

são todos os elementos de $A + B$. Agora,

$$a_{i-1} + b_{i-1} < a_i + b_{i-1} < a_i + b_i$$
$$a_{i-1} + b_{i-1} < a_{i-1} + b_i < a_i + b_i,$$

logo, $a_i + b_{i-1} = a_{i-1} + b_i$, isto é, $a_i - a_{i-1} = b_i - b_{i-1}$, para todo $i = 1, \ldots, k$. Assim existe q inteiro tal que $a_i - a_{i-1} = b_i - b_{i-1} = q$. Portanto A e B são progressões aritméticas de mesma razão.

Se $|A| = k$ e $|B| = l$, com $l \geqslant k$ e então para $0 \leqslant t \leqslant l - k$.

Considere os conjuntos $B_0 = \{b_1, \ldots, b_{t-1}\}$, $B_1 = \{b_t, \ldots, b_{t+k-1}\}$ e $B_2 = \{b_{t+k}, \ldots, b_{l-1}\}$. Observe que

$$A + B \subseteq (a_1 + B_0) \cup (A + B_1) \cup (a_{k-1} + B_2),$$

e que,

$$\begin{aligned} a_1 + B_0 &\subseteq [a_1 + b_1, a_1 + b_{t-1}] \\ A + B_1 &\subseteq [a_1 + b_{t-1}, a_{k-1} + b_{t+k-1}] \\ a_{k-1} + B_2 &\subseteq [a_{k-1} + b_{t+k}, a_{k-1} + b_{l-1}], \end{aligned}$$

logo, $a_1 + B_0$, $A + B_1$ e $a_{k-1} + B_2$ são disjuntos, daí,

$$\begin{aligned} k + l - 1 &= |A + B| \\ &\geqslant |a_1 + B_0| + |A + B_1| + |a_{k-1} + B_2| \\ &\geqslant t + (2k - 1) + (l - t - k) \\ &= k + l - 1, \end{aligned}$$

assim, $|A+B_1| = 2k-1$, para $t = 1, \ldots l-k$ e assim, A e B_1 são progressões aritméticas de mesma razão. Quando $t = l - k$ temos, $B_1 = B$.

Por outro lado, se A e B forem progressões aritméticas de razão q, então existem a e b, tais que, $A = \{a + qx : x \in [0, k-1]\}$ e $B = \{b + qy : y \in [0, l-1]\}$.
Segue que,
$A + B = \{a + b + qz : z \in [0, l + k - 2]\}$, portanto, $|A + B| = k + l - 1$.

E o teorema está demonstrado.

□

Teorema 3.2 (Freiman)**.** *Seja A um subconjunto finito não vazio de números inteiros com $|2A| \leq c|A|$ para algum c constante. Então A está contido em uma progressão aritmética n-dimensional $Q = Q(a; q_1, \ldots, q_n; l_1, \ldots, l_n)$, onde $l_1, \ldots, l_n$ e $q_1, \ldots, q_n$ são inteiros positivos, a um inteiro qualquer, $|Q| \leq c'|A|$, com c' e n dependendo apenas de c.*

Esse resultado têm várias aplicações. Nós abordaremos duas delas no capítulo 3.

A primeira diz que dado um inteiro positivo t e A um conjunto finito de inteiros, não vazio com conjunto soma pequeno e cardinalidade suficientemente grande, então A contém uma progressão aritmética de tamanho pelo menos t.

A segunda é uma versão quantitativa de uma conjectura de Erdös, que diz que dado um inteiro positivo t e um conjunto A finito e não vazio de inteiros com conjunto soma pequeno contendo muitas progressões aritméticas com três termos, então A contém uma progressão aritmética de tamanho t

Apresentaremos a demonstração do resultado de Ruzsa que na verdade é uma generalização do teorema de Freiman.

Teorema 3.3 (Ruzsa)**.** *Sejam A e B subconjuntos finitos, não vazios de números inteiros, tais que, $|A + B| \leqslant c|A|$ e $\dfrac{|A|^2}{|B|^2} = \lambda$. Então B está contido numa progressão aritmética n-dimensional Q, com*

$$n \leq 2^8 c^{32}\lambda + c^{-11}(2^{10}c^{32}\lambda)^{2^8 c^{32}\lambda} \quad e \quad l(Q) \leq 2^n c^4 |A|.$$

De fato, basta tomar $B = A$ e $\lambda = 1$.

Como muitas das ideias que aparecem na demonstração desse teorema foram inspiradas na demonstração de Freiman, esse resultado é conhecido como Teorema Freiman-

Ruzsa. Para tal prova são necessários alguns resultados importantes como: Teorema de Plunnecke-Ruzsa e o Teorema de Bogolyubov.

Dessa forma precisaremos definir alguns conceitos e relacionar resultados, afim de conseguirmos justificar todos os passos da demonstração do Teorema de Freiman-Ruzsa. Assim, subdividiremos o capítulo em seções e somente no fim do capítulo será apresentado a demonstração desejada.

3.1 Teorema de Plunnecke-Ruzsa

Em 1969,(ver [14]) Plünnecke desenvolveu um método grafo-teórico para estimar a densidade de conjuntos soma. Ele construiu um grafo que lhe permitiu provar um importante teorema na teoria combinatória aditiva dos números, a desigualdade de Plünnecke. Com seu resultado, ele melhorou os limites apresentados por Erdös (ver [3]) em 1935, obtendo o melhor expoente possível. Essa desigualdade tem se tornado uma ferramenta básica da teoria de adição de conjuntos, sendo utilizados em muitas aplicações. Mas mais importante do que o resultado, é o método que ele desenvolveu para tal.

Definição 3.4. *Seja $G(V,E)$ um grafo direcionado. Suponha que exista uma partição de $V(G) = V_0 \cup V_1 \cup \cdots \cup V_h$ com $E(G) \subset \bigcup_{i=1}^{h}(V_{i-1} \times V_i)$. Então dizemos que $G(V,E)$ é um grafo direcionado de $h+1$ níveis. Se além disso $G(V,E)$ satisfazer:*

(a) *Dados $1 \leq i \leq h$, $u \in V_{i-1}, v \in V_i$ e distintos $w_1, \ldots, w_k \in V_{i+1}$, tais que, $(u,v),(v,w_1)$, $\ldots,(v,w_k) \in E(G)$. Então, existem distintos $v_1, \ldots, v_k \in V_i$ tais que, $(u,v_i),(v_i,w_i) \in E(G)$ para todo $i = 1, \ldots k$.*

(b) *Dados $1 \leq i \leq h$, $w \in V_{i+1}, v \in V_i$ e distintos $u_1, \ldots, u_k \in V_{i-1}$, tais que, $(v,w),(u_1,v)$, $\ldots,(u_k,v) \in E(G)$. Então, existem distintos $v_1, \ldots, v_k \in V_i$ tais que, $(u_i,v_i),(v_i,w) \in E(G)$ parra todo $i = 1, \ldots k$.*

dizemos que $G(V,E)$ é um ***grafo de Plunnecke****.*

Definição 3.5. *Seja $G(V,E)$ um grafo de Plunnecke de nível $h+1$. Definimos o* ***raio de magnitude*** *como*

$$D_i(G) = \min_{\emptyset \neq X \subset V_0} \frac{|im_G^{(i)}|}{|X|} \text{ para todo } i = 1, \ldots, h+1$$

onde,

$$im_G^{(i)}(X) = \{v \in V_i : \text{ existe um caminho de } x \in X \text{ em } v\}$$

Definição 3.6. *Seja $G(V, E)$ um grafo de Plunnecke de h níveis. Para cada $n \leq h$, $G(V, E)$ admite um subgrafo I_{nh}, dito grafo da somas independentes que satisfaz:*

$$\frac{n^j}{j!} \leq D_j(I_{nh}) \leq n^j$$

e também um subgrafo $\hat{I}_{nh}$ dito grafo das somas inversas que satisfaz:

$$n^{-j} \leq D_j(\hat{I}_{nh}) \leq h! n^{-j}.$$

Teorema 3.7. *Seja G um grafo de Plunnecke com níveis $V_0, V_1, \ldots, V_h$, e $|V_0| = m$. Se $D_h \geq 1$, então G contém m caminhos disjuntos de V_0 até V_h.*

(Para demonstração ver [1]).

Corolário 3.8. *Seja G um grafo de Plunnecke com níveis $V_0, V_1, \ldots, V_h$ tais que, $D_h(G) \geq 1$ então $D_j(G) \geq 1$ para todo $j \leq h$.*

Demonstração. Pelo Teorema anterior, temos $|V_0|$ caminhos direto de V_0 em V_h que iniciam em V_0. Para qualquer $Z \subset V_0$, o número de caminhos partindo de Z é maior que $|Z|$. Como G é grafo de Plunnecke, todo caminho para V_h passa por $V_|j$, $j = 1, 2, \ldots, h$. Daí, $|im_G^{(j)}(Z)| \geq |Z|$ para todo $Z \subset V_0$. Logo,

$$D_j(G) = \min_{\emptyset \neq Z \subset V_0} \frac{|im_G^{(j)}(Z)|}{|Z|} \geq 1$$

□

Lema 3.9. *O raio de magnitude é multiplicativo. Isto é, se G, G' e G'' são grafos de plunnecke e $G = G'G''$, então $D_j(G) = D_j(G')D_j(G'')$ para todo $j = 1, 2, \ldots, h$. Onde G, G' e G'' são grafos de Plunnecke de nível h*

Demonstração. Sejam $V_0', V_1', \ldots, V_{h-1}'$ e $V_0'', V_1'', \ldots, V_{h-1}''$ os níveis de G' e G'' respectivamente.

Considere $Z' \subset V_0'$ e $Z'' \subset V_0''$ os subconjuntos tais que

$$D_j(G') = \frac{|im_{G'}^{(j)}(Z')|}{|Z'|} \quad e \quad D_j(G'') = \frac{|im_{G''}^{(j)}(Z'')|}{|Z''|}$$

Observe que $im^{(j)}_{G'}(Z') \times im^{(j)}_{G''}(Z'') = im^{(j)}_{G}(Z' \times Z'')$

Assim,

$$\begin{aligned} D_j(G) \leq \frac{|im^{(j)}_{G}(Z' \times Z'')|}{|Z' \times Z''|} &= \frac{|im^{(j)}_{G'}(Z') \times im^{(j)}_{G''}(Z'')|}{|Z' \times Z''|} \\ &= \frac{|im^{(j)}_{G'}(Z')||im^{(j)}_{G''}(Z'')|}{|Z'||Z''|} \\ &= D_j(G')D_j(G'') \end{aligned}$$

Logo, $D_j(G) \leq D_j(G')D_j(G'')$.

Mostraremos agora $D_j(G) \geq D_j(G')D_j(G'')$. Para isso considere $X \subset V'_0 \times V''_0$. Podemos ecrever X como uma união disjunta

$$X = \bigcup_{a \in V'_0, X_a \neq \emptyset} (\{a\} \times X_a)$$

onde $X_a = v'' \in V''_0 : (a, v'') \in X$. Como a união é disjunta temos

$$\begin{aligned} |X| = \left| \bigcup_{a \in V'_0, X_a \neq \emptyset} (\{a\} \times X_a) \right| &= \sum_{a \in V'_0, X_a \neq \emptyset} |(\{a\} \times X_a)| \\ &= \sum_{a \in V'_0, X_a \neq \emptyset} |X_a|. \end{aligned}$$

Seja $Y \subset V'_0 \times V''_j$ definido de tal forma que para qualquer $(a, b) \in X$ em que, se tenha um caminho de b em $d \in V''_j$ então $(a, d) \in Y$. Para $(a, b) \in X$ fixado, temos $\{a\} \times im^{(j)}_{G''}(b) \subset Y$. Assim, $\{a\} \times im^{(j)}_{G''}(X_a) \subset Y$

Daí,

$$\begin{aligned} |Y| = \left| \bigcup_{a \in V'_0, X_a \neq \emptyset} (\{a\} \times im^{(j)}_{G''}(X_a) \right| &= \sum_{a \in V'_0, X_a \neq \emptyset} |\{a\} \times im^{(j)}_{G''}(X_a)| \\ &= \sum_{a \in V'_0, X_a \neq \emptyset} |im^{(j)}_{G''}(X_a)| \\ &\geqslant \sum_{a \in V'_0, X_a \neq \emptyset} D_j(G'')|X_a| \\ &= D_j(G'') \sum_{a \in V'_0, X_a \neq \emptyset} |X_a| = D_j(G'')|X| \end{aligned}$$

Agora considere uma partição de Y análoga a que fizemos para X.

$$Y = \bigcup_{d \in V_0', Y_d \neq \emptyset} (Y_d \times \{d\}),$$

onde $Y_d = \{v' \in V_0' : (v', d) \in Y\}$ e $|Y| = \sum_{d \in V_0', Y_d \neq \emptyset} |Y_d|$

Mas $im_{G'}^{(j)}(X) = \bigcup_{d \in V_0', Y_d \neq \emptyset} (im_{G'}^{(j)}(Y_d) \times \{d\})$

Então,

$$\begin{aligned} |im_{G'}^{(j)}(X)| &= \left| \bigcup_{d \in V_0', Y_d \neq \emptyset} (im_{G'}^{(j)}(Y_d) \times \{d\}) \right| \\ &= \sum_{d \in V_0', Y_d \neq \emptyset} |im_{G'}^{(j)}(Y_d)| \\ &\geqslant \sum_{d \in V_0', Y_d \neq \emptyset} D_j(G')|Y_d| \\ &= D_j(G') \sum_{d \in V_0', Y_d \neq \emptyset} |Y_d| \\ &\geqslant D_j(G')D_j(G'')|X|. \end{aligned}$$

Assim,

$$\frac{|im_G^{(j)}(X)|}{|X|} \geq D_j(G')D_j(G'').$$

Tome X o conjunto tal que $D_j(G) = \dfrac{|im_G^{(j)}(X)|}{|X|}$.

Daí, $D_j(G) \geq D_j(G')D_j(G'')$

Portanto, $D_j(G) = D_j(G')D_j(G'')$

□

3.1.1 Teorema de Menger

A primeira ferramenta forte usada no método de Plünnecke é o Teorema de Menger. Este resultado foi comprovado por Karl Menger em 1927. Existem muitas provas diferentes para este teorema. Aqui, apresentamos uma que não requer quaisquer definições mais do que as necessárias para o compreender. Mais sobre o teorema de Menger e alguns outros pode ser encontrados em [2].

O Teorema de Menger nos auxilia na demonstração da desigualdade de Plunnecke.

Teorema 3.10 (Menger)**.** *Seja $G(V, E)$ um grafo direcionado, e sejam a, b vértices distintos de $G(V, E)$ com $(a, b) \notin E(G)$. Então o número máximo de caminhos independentes de a em b é igual à menor cardinalidade de S, onde S é um conjunto de corte, isto é, todos os caminhos de a em b possuem vértice em S.*

Demonstração. Sejam $\gamma(G, a, b) = \{\sigma : \sigma$ é um caminho independente de a em $b\}$ e $\gamma = |\gamma(G, a, b)|$. Seja S um conjunto de corte de a e b.
Dado $\sigma \in \gamma(G, a, b)$ temos que existe um vértice $v \in \sigma$ tal que $v \in S$. Assim, $\gamma \leq |S|$ para todo conjunto de corte de a e b. Logo $\gamma \leq l = min\{|S| :$ S conj. de corte $\}$ Por outro lado, dado um conjunto de corte S_0 tal que $|S_0| = l$, temos que para todo $v \in S_0$ existe $\sigma \in \gamma(G, a, b)$ tal que $v \in \sigma$ caso contrário, $S_0 - v$ seria também um conjunto de corte, contrariando a minimalidade de S_0. Daí $l \leq \gamma$ Portanto $l = \gamma$.

□

3.1.2 Desigualdade de Plunnecke

O proximo resultado limita o tamanho do $|A + hB|$ e veio a ser conhecido como Desigualdade de Plünnecke, esta e muitas outras desigualdades relacionadas são uma parte de um ramo da matemática conhecida como a teoria combinatória aditiva.

Desigualdade de Plunnecke 3.11. *Seja G um grafo de Plunnecke de nível $h \geq 1$. Então a sequência $\{|D_j(G)^{1/j}|\}_{j=1}^{h}$ é não crescente. Onde $D_j(G)$ é o j-ésimo raio de magnitude de G.*

Demonstração. Observe que mostrar $D_1(G) \geq D_2(G)^{1/2} \geq \ldots \geq D_h(G)^{1/h}$, é equivalente a mostrar que $D_j(G)^{1/j} \leq D_h^{1/h}$ para todo $j \leq h$
Com efeito, se $D_j(G)^{1/j} \leq D_h(G)^{1/h}$ para todo $j \leq h$ é satisfeito, podemos considerar os grafos reduzidos de G é aplicar novamente o resultado.
Dividiremos a demonstração em 4 casos:

1. $D_h(G) = 0$.
   Temos $D_j(G)^{1/j} \geq 0$ para todo j por definição de raio de magnitude.
   Logo $D_j(G)^{1/j} \leq D_h(G)^{1/h}$ para todo $j \leq h$

2. $D_h(G) = 1$.

   No lema anterior vimos que se $D_h(G) \geq 1$ então, $D_j(G) \geq 1$, para todo $j \leq h$.
   Logo, $D_j(G)^{1/j} \leq D_h(G)^{1/h}$ para todo $j \leq h$

3. $0 < D_h(G) < 1$.

   Construa um grafo $G^* = G^k I_{nh}$ onde I_{nh} é a tal que $[D_h(G)]^k \dfrac{n^h}{h!} \geq 1$.
   Assim, $D_h(G^*) = D_h(G^k I_{nh})$
   como o raio de magnitude é multiplicativo têm-se
   $D_h(G^*) = [D_h(G)]^k D_h(I_{nh}) \geq [D_h(G)]^k \dfrac{n^h}{h!} \geq 1$, pois $D_h(I_{nh}) \geq \dfrac{n^h}{h!}$.
   Daí, $D_h(G^*) \geq 1$ e pelo corolário 3.8 temos, $D_j(G^*) \geq 1$, para todo $j \leq h$
   Agora, $1 \leq D_j(G^*) = [D_h(G)]^k D_h(I_{nh}) \leq D_j(G)^k n^j$
   Mas por construção, $[D_h(G)]^k \dfrac{n^h}{h!} \geq 1$, assim, $n \geq [h! d_h(G)^{-k}]^{1/h}$.
   Podemos tomar então, $n = 1 + \lfloor (h! D_h(G)^{-k})^{1/h} \rfloor$. Como $D_h(G) < 1$ teremos $n > 1$.
   Daí, $n \geq 2(h! D_h(G)^{-k})^{1/h}$
   Desta forma teremos,

$$1 \leq D_j(G)^k 2(h!)^{j/h} D_h(G)^{-kj/h}$$

   o que implica,

$$D_j(G)^k \geq 2(h!)^{-j/h} D_h(G)^{kj/h},$$

   assim,

$$D_j(G)^{1/j} \geq 2(h!)^{-1/hk} D_h(G)^{1/h}.$$

   Mandando k para o infinito teremos

$$D_j(G)^{1/j} \geq D_h(G)^{1/h}$$

   .

4. Construa um grafo $G' = G^k \hat{I}_{nh}$ e escolha n e h tais que $[D_h(G)]^k n^{-h} \geq 1$
   Assim, $D_h(G') = [D_h(G)]^k D^h(\hat{I}_{nh}) \geq [D_h(G)]^k n^{-h}$
   Logo $D_h(G') \geq 1$, pelo corolário 3.8, $D_j(G') \geq 1$ para todo $j \leq h$
   Agora, $1 \leq D_j(G') = [D_j(G)]^k [D_j(\hat{I}nh)] \leq [D_j(G)]^k n^{-j}$

Mas $[D_h(G)]^k n^{-h} \geq 1$, daí, $n \leq [D_h(G)]^{k/h}$

Otimizando o melhor valor inteiro de n e substituindo, obtemos,

$$1 \leq [D_j(G)]^k \{[D_h(G)]^{k/h}\}^{-j}$$

Daí, $[D_j(G)]^k \geq [D_h(G)]^{kj/h}$. Portanto $[D_j(G)]^{1/j} \geq [D_h(G)]^{1/h}$

O resultado segue

□

Apresentaremos agora o Teorema de Hall que é utilizado na demonstração do Teorema de Plunnecke-Ruzsa, objetivo desta sessão.

Definição 3.12. *Dada uma sequência $(A_i)_{i=1}^n$ de conjuntos , se $a_1 \in A_1, \ldots, a_n \in A_n$ e $a_i \neq a_j$ para todos $1 \leq i < j \leq n$, então nós dizemos que a sequência $(a_i)_{i=1}^n$ é um* ***sistema de representantes distintos - (SRD)*** *de $(A_i)_{i=1}^n$*

Teorema 3.13 (P. Hall, 1935)**.** *Sejam $A_1, \ldots, A_n$ conjuntos. Então $(A_i)_{i=1}^n$ têm uma SRD se, e somente se $|\cup_{i\in I} A_i| \geq |I|$ para todo $I \subset [1, n]$.*

Lema 3.14. *Sejam $A_1, A_2, \ldots, A_n$ subconjuntos de um conjunto qualquer X. Se $(a_i)_{i=1}^{n-1}$ é uma SRD de $(A_i)_{i=1}^{n-1}$, então para algum $J \subset [1, n]$ com $n \in J$, existem exatamente $|\cup_{j\in J} A_j| - |J| + 1$ elementos $x \in X$ tais que $\{a_1, a_2, \ldots, a_{n-1}, x\}$, são um SRD para $(A_i)_{i=1}^n$.*

Demonstração. Considere um grafo $G(V, E)$ com $V(G) = \{1, 2, \ldots, n\}$ vértices, definido de tal forma que existe uma aresta $(i, j) \in E(G)$ se, e somente se, $i \neq n$ e $a_i \in A_j$.
Defina $J = \{1 \leq j \leq n :$ existe um caminho de j em n $\}$ e $A = \cup_{j\in J} A_j$
Observe que para $i = 1, 2, \ldots, n-1$ têm-se:

$$\begin{aligned} a_i \in A &\Leftrightarrow a_i \in A_j, j \in J \\ &\Leftrightarrow (i, j) \in E(G) \text{ para algum } j \in J \\ &\Leftrightarrow \text{Existe um caminho de i em n} \\ &\Leftrightarrow i \in J \end{aligned}$$

Assim, $\{1 \leq i < n : a_i \in A\} = J - \{n\}$. Seja $B = A - \{a_i : i \in J - n\}$.
Então $B \cap \{a_1, \ldots, a_{n-1}\} = \emptyset$ e $|B| = |A| - |J| + 1$

Se $a \in B$ então $a \in A$, pois $B \subset A$. Então $a \in A_j, j \in J$.

Se $n = j$ então $(a_i)_{i=1}^n$ é um SRD.

Se $n \neq j$ então G contém um caminho de j em n digamos,

$$(j = j_0, j_1), (j_1, j_2), \ldots, (j_{r-1}, j_r = n) \in E(G)$$

Considere $I = \{j, j_1, \ldots, j_r\} \subset J$ e substitua $a, a_{j_0}, \ldots, a_{j_{r-1}}$ por $b_{j_0}, b_{j_1}, \ldots, b_{j_r}$ respectivamente.

$$(j_k, j_{k+1}) \in E(G) \Rightarrow a_{j_k} \in A_{j_{k+1}}$$

Daí cada b_i representa A_i e $(b_i)_{i=1}^n$ é um SDR de $(A_i)_{i=1}^n$ onde $b_i = a_i$ caso $i \notin I$.

Por outro lado se $x \in X$ é tal que juntamente com $a_1, \ldots, a_{n-1}$ formam um SRD com a_i representando A_i se $i \notin J$ então x deve representar A_j para algum $j \in J$, logo $x \in B$.

□

Com esse resultado, podemos dar uma demonstração via Indução do Teorema de Hall feita por Z. W. Sun em 2001.

Demonstração do Teorema de Hall. Suponha que dado $(A_i)_{i=1}^n$ tenhamos um SRD $(a_i)_{i=1}^n$ Assim, $a_i \in A_i$ para todo $i = 1, \ldots, n$ e $a_i \neq a_j$ se $i \neq j$. Mostraremos que $|\cup_{i \in I} A_i| \geq |I|$ para todo $I \subset [1, n]$.

Basta observar que dado $I \subset [1, n]$, $1 \leq |I| = k \leq n$, então podemos escrever $I + \{b_1, b_2, \ldots, b_k\}$ onde $b_i \neq b_j$ e assim $|\cup_{b_i \in I} A_{b_i}| \geqslant k$ pois pelo menos $a_{b_i} \in A_{b_i}$.

Reciprocamente se $|\cup_{i \in I} A_i| \geqslant |I|$ para todo $I \subset [1, n]$, mostraremos utilizando Indução que $(A_i)_{i=1}^n$ tenhamos um SRD $(a_i)_{i=1}^n$.

Para $n = 2$ $I \subset [1, 2] \Rightarrow I = 1, 2 ou 1, 2$. Logo $|A_1| \geqslant 1, |A_2| \geqslant 1 e |A_1 \cup A_2| \geqslant 2$ Então existem $a_1 \in A_1$ *e* $a_2 \in A_2 : a_1 \neq a_2$

Suponha verdade para $n - 1$ com $n > 2$, isto é,$(A_i)_{i=1}^{n-1}$ tem um SRD $(a_i)_{i=1}^{n-1}$.

Mostraremos válido para n.

Mas pelo Lema 3.14, temos que existem exatamente $|\cup_{j \in J} A_j| - |J| + 1$ elementos de $x \in X$ tais que $\{a_1, a_2, \ldots, a_{n-1}, x\}$, formam um SRD para $(A_i)_{i=1}^n$, como por hipótese $|\cup_{i \in I} A_i| \geq |I|$ para todo $I \subset [1, n]$, temos que $|\cup_{j \in J} A_j| \geqslant |J|$ logo $|\cup_{j \in J} A_j| - |J| + 1 \geqslant 1$ □

Sejam $A_1, \ldots, A_n$ conjuntos finitos. Então podemos escrever $\cup_{i=1}^n A_i = \{a_1, \ldots, a_m\}$. Construirmos um grafo bipartido G com classes de vértices $X = \{A_1, \ldots, A_n\}$ e

$Y = \{a_1, \ldots, a_m\}$ ligando A_i em a_j se $a_j \in A_i$. Assim, podemos reformular o teorema de Hall da seguinte forma.

Teorema 3.15 (Correspondência de Hall)**.** *Seja G um grafo bipartido qualquer, com classes de vértices X e Y. Então G têm uma correspondência de X em Y se, e somente se, $|\Gamma(S)| \geqslant |S|$ para todo $S \subset X$, onde $\Gamma(S) = \{y \in Y : (x, y) \in E(G)$ para algum $x \in X\}$.*

Demonstração da Correspondência de Hall. seja $G(V, E)$ um grafo bipartido com classes de vértices X e Y. Considere novos vértices a e b, tais que a juntamente com cada elemento de X formam uma nova aresta de $G' = G'(V, E)$. Analogamente, b juntamente como cada elemento de Y formam uma aresta de G'.

Suponha que $G(V, E)$ tenha uma correspondência de X em Y, então $G(V, E)$ é um grafo bipartido com $|X|$ arestas disjuntas, daí, $G(V, E)$ têm $|X|$ caminhos independentes de a em b. Pelo Teorema de Menger o número máximo de caminhos independentes de a em b é igual a menor cardinalidade de S, onde S é conjunto de corte. Assim, existe S conjunto de corte tal que $|X| = |S|$.
Queremos que $|\Gamma(T)| \geq |T|$ para todo $T \subset X$. De fato, se $|\Gamma(T)| < |T|$ para algum $T \subset X$, então existe $v_0 \in T$ tal que $(x_0, y) \notin E(G')$ para todo $y \in Y$, mas $(x_0, a) \in E(G')$ por construção. Contradição. Logo, $|\Gamma(T)| \geqslant |T|$ para todo $T \subset X$.

Reciprocamente, seja $S \subset V(G') - \{a, b\} = X \cup Y$ um conjunto de corte de a e b. Suponha $|\Gamma(T)| \geqslant |T|$, para todo $T \subset X$. Em particular $|\Gamma(X - S)| \geqslant |X - S|$. Agora observe que como S é conjunto de corte para todo $y \in \Gamma(X - S)$ tal que $(x, y) \in E(G')$ para algum $x \in X - S$ é necessário que $y \in S$ caso contrário S não seria conjunto de corte. Logo $|\Gamma(X - S)| \leq |S \cap Y|$
Daí, $|S \cap Y| \geqslant |X - S|$
Assim,

$$|S| = |S \cap X| + |S \cap Y| \geqslant |S \cap X| + |X - S| = |S \cap X| + |S^c \cap X| = |X|$$

E portanto, pelo Teorema de Menger existe $|X|$ caminhos independentes de a em b, isto é, têm-se uma correspondência de X em Y .

□

Teorema 3.16 (Plunnecke-Ruzsa)**.** *Sejam A e B subconjuntos finitos não vazios de um grupo abeliano com $|A+B| \leqslant c|A|$. Então para quaisquer $k, l \in \{0,1,2,\ldots\}$ temos,*

$$|kB - lB| \leqslant c^{k+l}|A|,$$

onde convenção denotamos por $0B = \{0\}$.

Demonstração. Para $k = l = 0$ $|0B - 0B| = |\{0\}| = 1 \leqslant |A|$. Assumiremos sem perda de generalidade que $k \leqslant l$ e $l \leqslant 1$

Defina $G = G_{A,B}$ um grafo direcionado de nível l como segue

$V(G) = \bigcup_{i=0}^{l} V_i$, $\quad V_i = A + Bi$ e $\quad E(G) = \{(v_i, v_{i+1}) : v_i \in V_i \ e \ v_{i+1} - v_i \in B\}$

Se $u \in V_{i-1}$, $v \in V_i$, $w_1, \ldots, w_m \in V_{i+1}$ são tais que $(u,v), (v,w_1), \ldots, (v,w_m) \in E(G)$ então para qualquer $1 \leqslant i \leqslant m$ temos $v_i = u + (w_j - v) \in V_{i-1} + B = V_i$ tal que $(u, v_i), (u_i, v_i) \in E(G)$, desde que $w_i - u = w_i - v \in B$ e $w_i - v_i = v - u \in B$

Analogamente, se $u_1, \ldots, u_m \in V_{i-1}$, $\quad v \in V_i \quad$ e $\quad w \in V_{i+1}$ são tais que $(u_1, v), \ldots, (u_m, v)$ e $(v,w) \in E(G)$ então para todo $1 \leqslant i \leqslant m$ têm-se $v_i = u_i + (w - v) \in V_{i-1} + B = V_i$ e $(u_i, v_i), (v_i, w) \in E(G)$ desde que $v_i - u_i = w - v \in B$ e $w - v_i = v - u_i \in B$.

Assim G é um grafo de Plunnecke de nível l. Se $k \geqslant 1$ então pela Desigualdade de Plunnecke existe $\emptyset \neq A' \subset V_0 = A$ tal que,

$$\begin{aligned} \frac{|im_G^{(k)}(A')|}{|A'|} &= D_k(G) \leqslant [D_1(G)]\ k \\ &\leqslant \left(\frac{|im_G^{(1)}(A)|}{|A|}\right)^k \\ &= \frac{|A+B|^k}{|A|^k} \leqslant c^k. \end{aligned}$$

Logo $|A' + kB| \leqslant c^k|A'|$

De fato,

$$im_G^{(1)}(A) = \{v \in V_1 : \exists x \in A \ e \ (x,v) \in E(G)\} = A + B.$$
$$im_G^{(k)}(A') = \{v \in V_k : \exists x \in A' \ e \ (x,v) \in E(G)\} = A' + kB.$$

Se $1 \leqslant k \leqslant l$ pela Desigualdade de Plunnecke, existe $A'' \subset A'$ tal que ,

$$\begin{aligned}
\frac{|im_G^{(l)}(A'')|}{|A''|} &= D_l(G_{A',B}) \\
&\leqslant [D_k(G_{A',B})]^{l/k} \\
&\leqslant \left(\frac{|im_G^{(k)}(A')|}{|A'|}\right)^{l/k} \\
&= \left(\frac{|A'+kB|}{|A'|}\right)^{l/k}
\end{aligned}$$

Daí,

$$\frac{|A''+lB|}{|A''|} = \frac{im_G^{(l)}(A'')}{|A''|} \leqslant \left(\frac{|A'+kB|}{|A'|}\right)^{l/k} \leqslant \left(\frac{c^k|A'|}{|A'|}\right)^{l/k} = c^l$$

Logo,

$$|A''+lB| \leqslant c^l|A''|.$$

Se $k=0$, então basta tomar $A'=A$ e daí, $|A'+kB| \leq c^k|A'|$. Como $l \geq 1$ repetindo o argumento acima $|A''+lB| \leq c^l|A''|$.

Agora sejam R, S e T subconjuntos finitos não vazios de um grupo abeliano. Para cada $d \in S-T$, podemos escrever $d = s(d) - t(d)$ onde $s(d) \in S$ e $t(d) \in T$

Se $(r,d),(r',d') \in R \times (S-T)$ e $(r+s(d), r+t(d)) = (r'+s(d'), r'+t(d'))$ então, $r+s(d) = r'+s(d')$ e $r+t(d) = r'+t(d')$

Logo, $d=d'$ e $r=r'$. Assim,

$$|R||S-T| \leq |\{(r+s(d), r+t(d)) : r \in R \ e \ d \in S-T\}| \leq |R+S||R+T|$$

Aplicando essa relação em nossas hipóteses obtemos

$$|A''||kB-lB| \leq |A''+lB||A''+lB| \leq |A'+kB||A''+lB| \leq c^k|A'|c^l|A''|$$

Desta maneira,

$$|kB-lB| \leq \frac{c^{k+l}|A'||A''|}{|A''|} = c^{k+l}|A'| \leq c^{k+l}|A|.$$

Consequentemente

$$|kB-lB| \leq c^{k+l}|A|.$$

□

Teorema 3.17 (Analogia de Ruzsa do Teorema de Freiman em grupos de torção)**.** *Seja G um grupo de torção abeliano, isto é, existe r tal que, todos os elementos de G têm ordem menor ou igual r. Sejam A e B subconjuntos finitos não vazios de G com $|A+B| \leq c|A|$. Então B está contido em um subgrupo de G com ordem menor ou igual à $c^2 r^{c^4|A|/|B|}|A|$.*

Demonstração. Pelo Teorema de Plunnecke-Ruzsa, nós temos $|B - B| \leq c^2|A|$ e $|2B - 2B| \leq c^4|A|$.

Seja $W = \{w_1, \ldots, w_k\}$ o subconjunto maximal de $2B - B$ tal que $w_1 - B, \ldots, w_k - B$ sejam dois-a-dois disjuntos. Então,

$$\begin{aligned} k|B| &= \sum_{i=1}^{k} |w_i - B| \\ &= \left| \bigcup_{i=1}^{k} (w_i - B) \right| \\ &\leqslant |(2B - B) - B| \\ &\leqslant c^4|A|. \end{aligned}$$

Logo $k \leq c^4|A|/|B|$.

Para todo $w \in 2B - B$ existe $1 \leq i \leq k$, tal que, $(w - B) \cap (w_i - B) \neq \emptyset$ (pois W é maximal)

Logo $w \in w_i - B + B \subset W - B + B$, daí $2B - B \subset W - B + B$ Segue que

$$3B - B \subset W + 2B - B \subset 2W + b - B \ \ e \ \ 4B - B \subset 2W + 2B - B \subset 3W + B - B$$

Assim, para $l \in \mathbb{Z}^+$ têm-se $lB - kB \subset (l-1)W + B - B \subset H(W) + B - B$, onde

$$H(W) = \{x_1 w_1 + \ldots + x_k w_k : x_i \in [0, r_i - 1], \ \text{ para } r_i \leq r \text{ e } i = 1, \ldots, k\}$$

é subgrupo de G gerado por W. E portanto

$$H(B) = \bigcup_{l=1}^{\infty} (lB - B) \subset H(W) + B - B$$

Portanto,

$$\begin{aligned} |H(B)| &\leqslant |H(W) + B - B| \\ &\leqslant |H(W)||B - B| \\ &\leqslant r^k c^2 |A| \\ &\leqslant r^{c^4|A|/|B|} c^2 |A| \end{aligned}$$

E o resultado segue.

□

3.2 Teorema de Bogolyubov

Nesta seção definiremos a distância de um número real à um inteiro e o conjunto de Bohr, posteriormente apresentaremos o teorema de Bogolyubov, que será importante na demonstração do Teorema de Freiman-Ruzsa. Seja $x \in \mathbb{R}$, definimos a distância de x ao inteiro mais próximo por

$$\|x\| = \min_{a\in\mathbb{Z}} |x-a| = \begin{cases} \{x\}, & se\ \{x\} \leq 1/2 \\ 1-\{x\}, & \text{caso contrário} \end{cases}$$

Onde, $\{x\}$ é a parte fracionária de x.

Para $m \in \mathbb{Z}^+$, inteiros distintos $r_1, \ldots, r_n \in [0, m-1]$ e $\varepsilon > 0$ dizemos que

$$B_m(r_1, \ldots, r_n; \varepsilon) = \{a + m\mathbb{Z} : \left\|\frac{ar_i}{m}\right\| \leq \varepsilon \text{ para todo } i = 1, \ldots, n\}$$

é um **conjunto de Bohr**.

Exemplo 3.18. *Considere $m = 2$ e $r_1 = 0, r_2 ='$. Desta forma o conjunto de Bohr para $\varepsilon = \frac{1}{3}$ é*

$$B_2(0, 1; \frac{1}{3}) = \{a + 2\mathbb{Z} : \left\|\frac{ar_i}{2}\right\| \leq \frac{1}{3} \ para \ \ i = 1, 2.\}.$$

Agora, se a é par, então $\left\|\frac{ar_i}{2}\right\| = 0 < \frac{1}{3}$ para todo r.

se a é ímpar então $a = 2n + 1$ para algum n inteiro.

Daí, $\left\|\frac{a}{2}\right\| = \left\|n + \frac{1}{2}\right\| = \frac{1}{2} > \frac{1}{3}$.

Logo,

$$B_2(0, 1; \frac{1}{3}) = 2\mathbb{Z}.$$

Teorema 3.19 (Bogolyubov,1939)**.** *Sejam $m \geq 2$ um inteiro e A um subconjunto não vazio de $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$. Então existem distintos $r_1, r_2, \ldots, r_n \in [0, m-1]$, com $r_1 = 0$ e $n \leq (m/|A|)^2$ tais que,*

$$B\left(r_1, \ldots, r_n; \frac{1}{4}\right) \subset 2A - 2A.$$

Demonstração. Seja $A = \{a_1 + m\mathbb{Z}, \ldots, a_k + m\mathbb{Z}\}$, onde $a_1, \ldots, a_k \in [0, m-1]$ distintos. Para cada $r \in [0, m-1]$ definimos:

$$S_A(r) = \sum_{s=1}^{k} \exp(2\pi i a_s r/m).$$

Para qualquer $g \in \mathbb{Z}$ asseguramos que

$$g + m\mathbb{Z} \in 2A + 2A \Leftrightarrow \sum_{r=0}^{m-1} |S_A(r)|^4 \chi_r(g) \neq 0,$$

onde $\chi_r(g) = \exp(2\pi i g r/m)$. De fato, considere $A_0 = \{a_1, \ldots, a_k\}$. Observe que

$$\begin{aligned}
\sum_{r=0}^{m-1} |S_A(r)|^4 \chi_r(g) \neq 0 &= \sum_{r=0}^{m-1} S_A(r)^2 \overline{S_A(r)}^2 \chi_r(g) \\
&= \sum_{r=0}^{m-1} \left(\sum_{s=1}^{k} e^{(2\pi i a_s r/m)} \right)^2 \overline{\left(\sum_{s=1}^{k} e^{(2\pi i a_s r/m)} \right)}^2 \chi_r(g) \\
&= \sum_{r=0}^{m-1} \left(\sum_{s=1}^{k} e^{(2\pi i a_s r/m)} \right)^2 \left(\sum_{s=1}^{k} e^{(-2\pi i a_s r/m)} \right)^2 \chi_r(g) \\
&= \sum_{r=0}^{m-1} \left(\sum_{a \in A_0}^{k} e^{(2\pi i a r/m)} \right)^2 \left(\sum_{d \in A_0}^{k} e^{(-2\pi i d r/m)} \right)^2 \chi_r(g) \\
&= \sum_{r=0}^{m-1} \left(\sum_{a,c \in A_0}^{k} e^{(2\pi i (a-c) r/m)} \right) \left(\sum_{b,d \in A_0}^{k} e^{(-2\pi i (d-b) r/m)} \right) \chi_r(g) \\
&= \sum_{r=0}^{m-1} \sum_{a,b.c,d \in A_0}^{k} e^{(2\pi i (a+b-c-d) r/m)} \chi_r(g) \\
&= \sum_{r=0}^{m-1} \sum_{a,b,c,d \in A_0}^{k} e^{(2\pi i (g+a+b-c-d) r/m)} \\
&= \sum_{a,b,c,d \in A_0}^{k} \sum_{r=0}^{m-1} e^{(2\pi i (g+a+b-c-d) r/m)}
\end{aligned}$$

Se $g \equiv -a - b + c + d(\mod m)$ então $e^{(2\pi i (g+a+b-c-d) r/m)} = 1$. Daí,

$$\sum_{r=0}^{m-1} e^{(2\pi i (g+a+b-c-d) r/m)} = m$$

Caso contrário, $e^{(2\pi i (g+a+b-c-d) r/m)} = e^{(2\pi i L r/m)}$ para algum L não múltiplo de m, contudo,

$$\begin{aligned}\sum_{r=0}^{m-1} e^{(2\pi i(g+a+b-c-d)r/m)} &= \sum_{r=0}^{m-1} e^{(2\pi iLr/m)} \\ &= e^0 + e^{(2\pi iL/m)} + \cdots + e^{(2\pi iL(m-1)/m)} \\ &= \frac{1-e^{(2\pi iLm/m)}}{1-2\pi iL/m} = 0\end{aligned}$$

Portanto,

$$\begin{aligned}\sum_{r=0}^{m-1} |S_A(r)|^4 \chi_r(g) \neq 0 &\Leftrightarrow g \equiv -a-b+c+d(\mod m) \\ &\Leftrightarrow g + m\mathbb{Z} \in 2A-2A\end{aligned}$$

Seja $\lambda = |A|/m \in (0,1]$, considere

$$R = \{r \in [0, m-1] : |S_A(r)| \geqslant \sqrt{\lambda}|A|\},$$

e

$$R' = \{r \in [0, m-1] : |S_A(r)| < \sqrt{\lambda}|A|\}.$$

Como $S_A(0) = |A| \geqslant \sqrt{\lambda}|A|$ temos, $0 \in R$ o que nos dá $|R'| < m$. Observe que

$$\begin{aligned}\left|\sum_{r\in R'} |S_A(r)|^4 \chi_r(g)\right| &= \left|\sum_{r\in R'} |S_A(r)|^2 |S_A(r)|^2 \chi_r(g)\right| \\ &\leqslant \sum_{r\in R'} |S_A(r)|^2 |S_A(r)|^2 \\ &< \sum_{r\in R'} (\sqrt{\lambda}|A|)^2 |S_A(r)|^2 \\ &= \lambda|A|^2 \sum_{r=0}^{m-1} |S_A(r)|^2 \\ &= \lambda|A|^2 \sum_{r=0}^{m-1} \sum_{a,b\in A_0} e^{(2\pi i(a-b)r/m)} \\ &= \lambda|A|^2 \sum_{a,b\in A_0} \sum_{r=0}^{m-1} e^{(2\pi i(a-b)r/m)}.\end{aligned}$$

Mas,

$$\sum_{r=0}^{m-1} \exp(2\pi i(a-b)r/m) \neq 0 \Leftrightarrow a-b \equiv 0(\mod m).$$

Como $a_1, \ldots, a_k \in [0, m-1]$, $a - b \equiv 0(\mod m) \Leftrightarrow a = b$. Temos,

$$\begin{aligned}\lambda|A|^2 \sum_{a,b\in A_0} \sum_{r=0}^{m-1} e\,(2\pi i(a-b)r/m) &= \lambda|A|^2 \sum_{a\in A_0} m \\ &= \lambda|A|^2|A_0|m \\ &= |A|^4\end{aligned}$$

Logo,

$$\left|\sum_{r\in R'} |S_A(r)|^4\chi_r(g)\right| < |A|^4.$$

Sabemos que $\mathfrak{Re}(z) \geqslant |z|$ para todo número complexo z, desta forma temos

$$|A|^4 + \mathfrak{Re}\left(\sum_{r\in R'} |S_A(r)|^4\chi_r(g)\right) > 0.$$

Para $x \in \mathbb{R}$, temos

$$\|x\| \leqslant \frac{1}{4} \Leftrightarrow \mathfrak{Re}(2\pi x) = \cos(2\pi x) \geqslant 0.$$

Pois a função cosseno é par, periódica e positiva entre zero e $\pi/2$. Com isso, se $r \in \mathbb{R}$ e $g \in \mathbb{Z}$ então, $\left\|\frac{gr}{m}\right\| \leqslant \frac{1}{4} \Leftrightarrow \mathfrak{Re}(\chi_r(g)) \geqslant 0$. Considere então, $r_1, \ldots, r_n$ todos os elementos de R, com $r_1 = 0$, e g um inteiro tal que $g + m\mathbb{Z} \in B_m\left(r_1, \ldots, r_n; \frac{1}{4}\right)$, isto é, $\left\|\frac{gr_j}{m}\right\| \leqslant \frac{1}{4}$. Então $\mathfrak{Re}(\chi_{r_j}(g)) \geqslant 0$ para todo $j = 1, \ldots, n$. Por consequência

$$\begin{aligned}\mathfrak{Re}\left(\sum_{r=0}^{m-1} |S_A(r)|^4\chi_r(g)\right) &= \mathfrak{Re}\left(\sum_{r\in R} |S_A(r)|^4\chi_r(g) + \sum_{r\in R'} |S_A(r)|^4\chi_r(g)\right) \\ &= \mathfrak{Re}\left(\sum_{r\in R} |S_A(r)|^4\chi_r(g)\right) + \mathfrak{Re}\left(\sum_{r\in R'} |S_A(r)|^4\chi_r(g)\right) \\ &= \sum_{1<j\leqslant n} |S_A(r_i)|^4\mathfrak{Re}(\chi_{r_i}(g)) + |S_A(0)|^4 + \mathfrak{Re}\left(\sum_{r\in R'} |S_A(r)|^4\chi_r(g)\right) \\ &\geqslant |A|^4 + \mathfrak{Re}\left(\sum_{r\in R'} |S_A(r)|^4\chi_r(g)\right) > 0.\end{aligned}$$

Logo,

$$\sum_{r=0}^{m-1} |S_A(r)|^4\chi_r(g)) \neq 0,$$

deste modo, $g + m\mathbb{Z} \in 2A - 2A$. Portanto,

$$B_m\left(r_1, \ldots, r_n; \frac{1}{4}\right) \subset 2A - 2A.$$

Finalmente observe que,

$$\begin{aligned} n(\sqrt{\lambda}|A|)^2 &\leqslant \sum_{r\in R}|S_A(r)|^2 \\ &\leqslant \sum_{r=0}^{m-1}|S_A(r)|^2 \leqslant \frac{|A|^2}{\lambda}, \end{aligned}$$

que nos leva em, $n \leqslant \lambda^{-2} = m^2/|A|^2$. Isto conclui a demonstração.

□

Lema 3.20 (Obtido Pelo Segundo Teorema de Minkowski)**.** *Seja $m \geq 2$ um inteiro, e sejam $r_1, \ldots, r_n \in [0, m-1]$, com $mdc(r_1, \ldots, r_n, m) = 1$. Então existe uma P.A. n-dimensional Q contida em $\mathbb{Z}_m$ tal que,*

$$Q \subset B_m\left(r_1, \ldots, r_n; \frac{1}{4}\right) \quad e \quad |Q| > \frac{m}{(4n)^n}.$$

Para ver demonstração consultar [13]

3.3 h-Isomorfismo de Freiman

O isomorfismo de Freiman é uma aplicação sobrejetiva que de certa forma "preserva"a soma. Ele será de fundamental importância na prova do teorema de Freiman-Ruzsa, e usaremos fortemente o fato de que a imagem de um conjunto A por um h-isomorfismo de Freiman é uma progressão aritmética própria se, e somente se, A também o for.

Definição 3.21. *Sejam G e H grupos abelianos e $h \geq 2$ um inteiro. Sejam $A \subset G$ e $B \subset H$. Uma aplicação $\phi : A \to B$ é dita h-**homomorfismo de Freiman** se tivermos*

$$\phi(a_1) + \cdots + \phi(a_h) = \phi(a_1') + \cdots + \phi(a_h')$$

sempre que

$$a_1 + \cdots + a_h = a_1' + \cdots + a_h',$$

para $a_1, a_1', \ldots, a_h, a_h' \in A$.

Se ϕ é sobrejetiva e para todos $a_1, a_1', \ldots, a_h, a_h' \in A$,

$$a_1 + \cdots + a_h = a_1' + \cdots + a_h' \Leftrightarrow \phi(a_1) + \cdots + \phi(a_h) = \phi(a_1') + \cdots + \phi(a_h'),$$

*e então, ϕ é um h- **isomorfismo de Freiman**.*

Observe que se ϕ é um h-isomorfismo de Freiman, então ϕ é injetiva.

$$\begin{aligned}\phi(a)=\phi(b) &\Rightarrow \phi(a)+(h-1)\phi(a)=\phi(b)+(h-1)\phi(a)\\ &\Rightarrow a+(h-1)a=b+(h-1)a\\ &\Rightarrow a=b.\end{aligned}$$

Para fixar o entendimento de isomorfismo de Freiman, considere $A=[0,k-1]$ e B uma P.A. de tamanho k, $B=\{a+qx_i : x_i\in[0,k-1]\}$. Defina $\phi : A\to B$ por $\phi(x)=a+qx$. Se tivermos

$$x_1+\cdots+x_h=x_1'+\cdots+x_h'$$

Então

$$\begin{aligned}\phi(x_1)+\cdots+\phi(x_h) &= a+qx_1+\cdots+a+qx_h\\ &= ha+q(x_1+\cdots+x_n)\\ &= ha+q(x_1'+\cdots+x_n')\\ &= a+qx_1'+\cdots+a+qx_h'\\ &= \phi(x_1')+\cdots+\phi(x_h')\end{aligned}$$

Do mesmo modo, se $\phi(x_1)+\cdots+\phi(x_h)=\phi(x_1')+\cdots+\phi(x_h')$, então $x_1+\cdots+x_h=x_1'+\cdots+x_h'$.

Logo, ϕ é um h-isomorfismo de Freiman.

Proposição 3.22. *Seja $\phi : A\to B$ um h-isomorfismo de Freiman, então A é uma P.A. n-dimensional própria se, e somente se B é uma P.A. n-dimensional própria.*

Demonstração. De fato, suponha A uma P.A. n-dimensional própria, então A pode ser reescrita como

$$A=\{a+x_1q_1+\cdots+x_nq_n : x_i\in[0,l_i-1]\}$$

Considere $A'=\{a'+x_1q_1'+\cdots+x_nq_n' : x_i\in[0,l_i-1]\}$,
onde, $a'=\phi(a)$, $q_i'=\phi(a+q_i)-\phi(a)$ para $i=1,\ldots,n$. Assim, A' é uma P.A. n-dimensional.
Mostraremos $A'=B$ e $\phi(a+x_1q_1+\cdots+x_nq_n)=a'+x_1q_1'+\cdots+x_nq_n'$ para todos $a+x_1q_1+\cdots+x_nq_n\in A$

Seguiremos por Indução sobre $m = \sum_{i=1}^{n} x_i$. Para $m = 0$ e $m = 1$ segue pela definição dos $q_i's$.

Suponha então que para $m \geq 1$ o resultado seja válido. Seja $r = a + x_1q_1 + \cdots + x_nq_n \in A$ com $m + 1 = \sum_{i=1}^{n} x_i$. Para algum j tal que $x_j \geq 1$ defina $r' = r - q_j$. Assim $r' = a + x_1q_1 + \cdots + x_{j-1}q_{j-1} + (x_j - 1)q_j + \cdots + x_nq_n$, logo por hipótese de indução

$$\begin{aligned} \phi(r') &= \phi(a + x_1q_1 + \cdots + x_{j-1}q_{j-1} + (x_j - 1)q_j + \cdots + x_nq_n) \\ &= a' + x_1q_1' + \cdots + x_{j-1}q_{j-1}' + (x_j - 1)q_j' + \cdots + x_nq_n' \end{aligned}$$

Observe que $a, r, r', a + q_j \in A$, e $r + a = r' + a + q_j$ daí

$$\begin{aligned} \phi(r) + \phi(a) &= \phi(r') + \phi(a + q_j) \\ &= \phi(r') + \phi(a + q_j) - \phi(a) \\ &= \phi(r') + q_j' \\ &= a' + x_1q_1' + \cdots + x_nq_n' \end{aligned}$$

Assim, $B = A'$ é uma P.A. n-dimensional. E como ϕ é uma bijeção e A é própria, $l(A) = |A| = |B|$. Logo B é própria. A recíproca é provada de maneira análoga.

□

Lema 3.23 (Ruzsa)**.** *Sejam A um subconjunto finito não vazio de números inteiros e $h \geq 2$ um inteiro. Então, para qualquer $m \geq |hA - hA|$ existe $A' \subset A$ com $|A'| \geq |A|/h$ tal que, A' é Freiman h-isomorfo à um subconjunto de $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$.*

Demonstração. Seja p um primo maior que o $\max hA - \min hA$. Para cada $d \in (hA - hA)\backslash\{0\}$, temos $p \nmid d$. Caso contrário p não seria maior que $\max hA - \min hA$. Temos ainda que

$$|\{q \in [1, p-1] : m \mid \{dq\}_p\}| = |\{r \in [1, p-1] : m \mid r\}| \leq \frac{p-1}{m}.$$

Onde $\{a\}_p$ é o menor inteiro não negativo congruente à a módulo p. Assim,

$$|\{q \in [1, p-1] : m \mid \{dq\}_p \text{para algum } d \in (hA - hA)\backslash\{0\}\}| < |hA - hA|\frac{(p-1)}{m} \leq p - 1.$$

E, portanto existe $q \in [1, p-1]$, tal que $m \nmid \{dq\}_p$ para todo $d \in (hA - hA)\backslash\{0\}$.

Defina $\phi : \mathbb{Z} \to \mathbb{Z}_m$ por $\phi(x) = \{qx\}_p + m\mathbb{Z}$. Para $j = 1, \ldots, h$ seja

$$S_j = \left\{ x \in A : \frac{j-1}{h}p \leq \{qx\}_p < \frac{j}{h}p \right\}.$$

Assim, $\sum_{j=1}^{h} |S_j| = |\bigcup_{j=1}^{h} S_j| = |A|$, então para algum $1 \leq j \leq h$ têm-se $|S_j| \geq |A|/h$.

De fato, se para todo $1 \leq j \leq h$ tivéssemos $|S_j| < |A|/h$ então $\sum_{j=1}^{h} |S_j| < \sum_{j=1}^{h} |A|/h = |A|$.

Absurdo.

Tome $A' = S_j$. Sejam $a_1, \ldots, a_h \in A'$, como

$$\frac{j-1}{h}p \leq \{qa_1\}_p, \ldots, \{qa_h\}_p < \frac{j}{h}p,$$

temos

$$\{qa_1\}_p + \cdots + \{qa_h\}_p = (j-1)p + \{q(a_1 + \cdots + a_h)\}_p$$

Daí

$$\{qa_1\}_p + \cdots + \{qa_h\}_p + m\mathbb{Z} = (j-1)p + \{q(a_1 + \cdots + a_h)\}_p + m\mathbb{Z}$$

Logo,

$$\phi(a_1) + \cdots + \phi(a_h) = (j-1)p + \{q(a_1 + \cdots + a_h)\}_p + m\mathbb{Z}.$$

Se $a'_1, \ldots, a'_h \in A'$ e $\{q(a_1 + \cdots + a_h)\}_p \geq \{q(a'_1 + \cdots + a'_h)\}_p$, então

$$\phi(a_1) + \cdots + \phi(a_h) = \phi(a'_1) + \cdots + \phi(a'_h) \Leftrightarrow$$

$$\{q(a_1 + \cdots + a_h - a'_1 - \cdots - a'_h)\}_p = \{q(a_1 + \cdots + a_h)\}_p - \{q(a'_1 - \cdots - a'_h)\}_p \in m\mathbb{Z}$$

$$\Leftrightarrow a_1 + \cdots + a_h - a'_1 - \cdots - a'_h = 0.$$

Portanto a restrição de ϕ em A' é um h-isomorfismo de Freiman, isto é, A' é Freiman h-isomorfo à um subconjunto de $\mathbb{Z}_m$

□

Enfim, estamos aptos para demonstrarmos o Teorema de Freima-Ruzsa.

3.3.1 Demonstração Freiman-Ruzsa

Demonstração. Observe que $|A + B| \geq |A|$, o que implica em $c \geq 1$. Pelo Teorema de Plunnecke-Ruzsa, $|B - B| \leq c^2|A|$ e $|8B - 8B| \leq c^{16}|A|$

Considere p primo, $p \in (c^{16}|A|, 2c^{16}|A|)$.

Como $p > c^{16}|A| \geq |8B - 8B|$ pelo Lema de Ruzsa, existe $B' \subset B$, tal que, $|B'| \geq \frac{|B|}{8}$ e

B' é Freiman 8-isomorfo à um subconjunto S de $\mathbb{Z}_p$

Pelo Teorema de Bogolyubov, existem $r_1, \ldots, r_{n_1} \in [0, p-1]$ inteiros distintos com $r_1 = 0$, tal que,

$$n_1 \leq \left(\frac{p}{|S|}\right)^2 = \left(\frac{p}{|B'|}\right)^2 \leq \left(\frac{2c^{16}|A|}{|B'|}\right)^2$$

Como $\dfrac{|A|^2}{|B|^2} = \lambda$ temos

$$n_1 \leq 2^8 c^{32} \lambda$$

E $B_p\left(r_1, \ldots, r_{n_1}; \dfrac{1}{4}\right) \subset 2S - 2S$

Pelo lema obtido pelo segundo Teorema de Minkowski, existe uma P.A $Q' \subset \mathbb{Z}_p$, tal que,

$$Q' \subset B_p\left(r_1, \ldots, r_{n_1}; \frac{1}{4}\right) \subset 2S - 2S$$

e

$$|Q'| \geq \frac{p}{(4n_1)^{n_1}} > \frac{c^{16}|A|}{(4n_1)^{n_1}}$$

Seja $\phi : B' \to S$ o h-isomorfismo de Freiman garantido pelo Lema de Ruzsa. Assim, para $a, b, c, d, a', b', c', d' \in B'$ têm-se

$$\phi(a) + \phi(b) - \phi(c) - \phi(d) = \phi(a') + \phi(b') - \phi(c') - \phi(d')$$

$$\Leftrightarrow \phi(a) + \phi(b) + \phi(c') + \phi(d') + 4\phi(a)$$

$$= \phi(a') + \phi(b') + \phi(c) + \phi(d) + 4\phi(a)$$

$$\Leftrightarrow a + b + c' + d' + 4a = a' + b' + c + d + 4a$$

$$\Leftrightarrow a + b - c - d = a' + b' - c' - d'$$

Assim, podemos introduzir uma aplicação bem definida e sobrejetiva $\psi : 2B' - 2B' \to 2S - 2S$, por $\psi(a + b - c - d) = \phi(a) + \phi(b) - \phi(c) - \phi(d)$ para todos $a, b, c, d \in B'$.

Para $a_1, b_1, \ldots, a_4, b_4, a_1', b_1', \ldots, a_4', b_4' \in S$.

$$\psi(a_1 + a_2 - a_3 - a_4) + \psi(b_1 + b_2 - b_3 - b_4)$$

$$= \psi(a_1' + a_2' - a_3' - a_4') + \psi(b_1' + b_2' - b_3' - b_4')$$

$$\Leftrightarrow \phi(a_1) + \phi(a_2) - \phi(a_3) - \phi(a_4) + \phi(b_1) + \phi(b_2) - \phi(b_3) - \phi(b_4)$$

$$= \phi(a'_1) + \phi(a'_2) - \phi(a'_3) - \phi(a'_4) + \phi(b'_1) + \phi(b'_2) - \phi(b'_3) - \phi(b'_4)$$

$$\Leftrightarrow \phi(a_1) + \phi(a_2) + \phi(b_1) + \phi(b_2) + \phi(a'_3) + \phi(a'_4) + \phi(b'_3) + \phi(b'_4)$$

$$= \phi(a'_1) + \phi(a'_2) + \phi(b'_1) + \phi(b'_2) + \phi(a_3) + \phi(a_4) + \phi(b_3) + \phi(b_4)$$

$$\Leftrightarrow a_1 + a_2 + b_1 + b_2 a'_3 + a'_4 + b'_3 + b'_4$$

$$= a'_1 + a'_2 + b'_1 + b'_2 a_3 + a_4 + b_3 + b_4$$

$$\Leftrightarrow (a_1 + a_2 - a_3 - a_4) + (b_1 + b_2 - b_3 - b_4)$$

$$= (a'_1 + a'_2 - a'_3 - a'_4) + (b'_1 + b'_2 - b'_3 - b'_4)$$

Portanto ψ é um 2-isomorfismo de Freiman de $2B' - 2B'$ em $2S - 2S$, e logo $Q_1 = \psi^{-1}(Q') \subset 2B' - 2B' \subset 2B - 2B$ é também uma P.A. própria n_1-dimensional com

$$l(Q_1) = |Q_1| = |Q'| > \frac{c^{16}|A|}{(4n_1)^{n_1}} \geqslant \frac{c^{16}|A|}{(2^{10}c^{32}\lambda)^{2^8 c^{32}\lambda}}.$$

Seja $B^* = \{b_1, \ldots, b_{n_2}\}$ o subconjunto maximal de B tal que, $b_1 + Q_1, \ldots, b_{n_2} + Q_1$ sejam dois-a-dois disjuntos . Então

$$n_2|Q_1| = \sum_{i=1}^{n_2} |b_i + Q_1| = |B^* + Q_1| \leqslant |B + (2B - 2B)| = |3B - 2B| \leqslant c^5|A|.$$

E, portanto

$$n_2 \leqslant \frac{c^5|A|}{|Q_1|} < c^{-11}(2^{10}c^{32}\lambda)^{2^8 c^{32}\lambda}.$$

Para cada $b \in B$, existe $1 \leqslant i \leqslant n_2$ tal que, $(b + Q_1) \cap (b_i + Q_1) \neq \emptyset$ e assim,

$$b \in b_i + Q_1 - Q_1 \subset B * + Q_1 - Q_1 \subset Q_2 + Q_1 - Q_1,$$

onde

$$Q_2 = \{\delta_1 b_1 + \cdots + \delta_{n_2} b_{n_2} : \delta_1, \ldots, \delta_{n_2} \in \{0, 1\}\},$$

é uma P.A. n_2-dimensional com $l(Q_2) = 2^{n_2}$. Observe que $Q_1 - Q_1$ é também uma P.A n_1-dimensional. De fato, Como Q_1 é uma P.A. n_1-dimensional, podemos escreve-la como

$$Q_1 = \{a + x_1 q_1 + \cdots + x_{n_1} q_{n_1} : x_i \in [0, l_i - 1]\}$$

dessa forma,

$$Q_1 - Q_1 = \{0 + (x_1 - x'_1)q_1 + \cdots + (x_{n_1} - x'_{n_1})q_{n_1} : x_i, x'_i \in [0, l_i - 1]\}.$$

E

$$l(Q_1 - Q_1) = 2^{n_1} l_1 \dots l_{n_1} = 2^{n_1} l(Q_1) = 2^{n_1} |Q_1| \leqslant 2^{n_1} |2B - 2B|$$

Pois $Q_1 \subset 2B - 2B$. Pelo Teorema de Plunnecke-Ruzsa $|2B - 2B| \leqslant c^4|A|$. Daí,

$$l(Q_1 - Q_1) \leqslant 2^{n_1} |2B - 2B| \leqslant 2^{n_1} c^4 |A|.$$

Assim, B está contido em $Q = Q_2 + Q_1 - Q_1$ uma P.A. n-dimensional com $n = n_1 + n_2$. Com efeito,

$$Q_2 + Q_1 - Q_1 = \{\delta_1 b_1 + \dots + \delta_{n_2} b_{n_2} : \delta_1, \dots, \delta_{n_2} \in \{0, 1\}\}$$

$$+\{(x_1 - x_1')q_1 + \dots + (x_{n_1} - x_{n_1}')q_{n_1} : x_i, x_i' \in [0, l_i - 1]\}$$

$$= \{\delta_1 b_1 + \dots + \delta_{n_2} b_{n_2} + (x_1 - x_1')q_1 + \dots + (x_{n_1} - x_{n_1}')q_{n_1} : \delta_1, \dots, \delta_{n_2} \in \{0, 1\} \, e \, x_i, x_i' \in [0, l_i - 1]\}.$$

Daí,

$$n = n_1 + n_2 \leqslant 2^8 c^{32} \lambda + c^{-11} (2^{10} c^{32} \lambda)^{2^8 c^{32} \lambda}$$

e

$$|Q| \leqslant l(Q) = l(Q_2) l(Q_1 - Q_1) \leqslant 2^{n_2} 2^{n_1} c^4 |A| = 2^n c^4 |A|$$

Isso conclui a demonstração. □

Capítulo 4

Aplicações do Teorema de Freiman

Para iniciarmos a apresentação das aplicações vamos relembrar o Teorema de Szemerédi que foi enunciado no capítulo 2, para podermos mostrar um lema importante na demonstração da primeira aplicação do Teorema de Freiman. Seja $0 < \delta < 1$ e $t \in \{3, 4, \ldots\}$. Então existe $l_0(\delta, t)$, tal que, se $n \geqslant l_0(\delta, t)$ e $A \subset [1, n]$, com $|A| \geqslant \delta n$, então S contém uma P.A. de ordem t.

Lema 4.1. *Seja $\delta > 0$ e $t \geq 3$. Se existe um inteiro $l_0(\delta, t)$ tal que para Q uma P.A. de tamanho l contida nos inteiros $\mathbb{Z}$ e um subconjunto B de Q com $|B| \geq \delta l$ e $l \geq l_0(\delta, t)$, então B contém uma progressão aritmética de tamanho t.*

Demonstração. Seja $l_0(\delta, t)$ o inteiro determinando pelo Teorema de Szemerédi. Seja Q a P.A. de tamanho l contida em $\mathbb{Z}$ dada por hipótese, existem elementos a e $q \neq 0$ em $\mathbb{Z}$ tais que,

$$Q = \{a + xq : x \in [0, l-1]\}.$$

Considere

$$A = \{x \in [0, l-1] : a + xq \in B\}.$$

Então $A \subset [0, l-1]$ e $|A| = |B| \geq \delta l$, assim pelo Teorema de Szemerédi A contém uma P.A. de tamanho t, isto é, existem a' e $q' \neq 0$ em $\mathbb{Z}$, tais que $a' + q'y \in A$ para todo $y \in [0, t-1]$.
Sejam $a'' = a + a'q$ e $q'' = q'q$, assim, $q'' \neq 0$. Daí,

$$a'' + yq'' = a + (a' + yq')q \in B \text{ para } y \in [0, t-1]$$

Logo, B contém uma P.A. de tamanho t.

□

Teorema 4.2 (Primeira Aplicação do Teorema de Freiman)**.** *Seja $c \geq 2$ e $t \geqslant 3$. Se existe $k_0 = k_0(c,t)$ tal que $|A| \geqslant k_0$, para $A \subset \mathbb{Z}$ com $|2A| \leqslant c|A|$, então A contém uma progressão aritmética de tamanho pelo menos t.*

Demonstração. Seja $|A| = k \geqslant k_0(c,t)$. Pelo Teorema de Freiman A está contida em uma P.A. n-dimensional $Q = \{a + x_1q_1 + \ldots x_nq_n : x_i \in [0, l_i - 1], i = 1, \ldots, n\}$, de tamanho $l(Q) = l_1 \ldots l_n$ e $|Q| \leqslant c'k$ onde n e c' dependem apenas de c. Daí, existe l inteiro positivo tal que $l(Q) \leqslant lk$, assim, $l_1 \ldots l_n \leqslant lk \Rightarrow \dfrac{k}{l_1 \ldots l_n} \geq \dfrac{l_n}{l}$
Assumiremos sem perda de generalidade que, $l_1 \leqslant \ldots \leqslant l_n$, e logo,

$$k = |A| \leqslant |Q| \leqslant l(Q) = l_1 \ldots l_n \leqslant l_n^n$$

Dessa forma, $l_n \geqslant k^{1/n}$.

Seja $Y = \{y = (y_1, \ldots, y_{n-1}) \in \mathbb{Z}^{n-1} : y_i \in [0, l_i - 1], i = 1, \ldots, n-1\}$ Daí, $|Y| = l_1 \ldots l_{n-1}$. Seja $Y = \{y = (y_1, \ldots, y_{n-1}) \in \mathbb{Z}^{n-1} : y_i \in [0, l_i - 1], i = 1, \ldots, n-1\}$. Assim, $|Y| = l_1 \ldots l_{n-1}$
Para cada $y \in Y$ defina

$$L(y) = \{a + y_1q_1 + \ldots + y_{n-1}q_{n-1} + x_nq_n : x_n \in [0, l_n - 1]\}$$

uma progressão aritmética de tamanho l_n contida em $\mathbb{Z}$.

□

4.1 Lema de Regularidade

Sejam A e B subconjuntos finitos, não vazios de um grupo abeliano livre de torção, com $|A| = |B| = k$. Para $W \subset A \times B$, seja

$$S(W) = \{a + b : (a,b) \in W\}.$$

Em particular,

$$S(A \times B) = A + B.$$

Assim, se $|S(A \times B)| \leqslant ck$ então pelo Teorema de Freiman, A está contida em uma P.A. n-dimensional. Balog e Szemerédi mostraram um resultado tipo-Freiman para subconjuntos longos em $A \times B$. Este resultado é importante para nós por nos permitir utilizar a primeira aplicação do Teorema de Freiman. Dessa forma nós apresentaremos alguns lemas para conseguirmos provar o Teorema de Balog-Szemerédi, e um dos lemas importantes é o Lema de Regularidade.

Definição 4.3. *Seja $G = G(V, E)$ um grafo não direcionado, com V finito e E um conjunto de arestas $e = \{v, v'\}$, com $v, v' \in V$ não necessariamente distintos. Uma aresta e é adjacente à v se $v \in e$. O grau de um vértice v é o número de arestas adjacentes a v.Se A e B são subconjuntos de V, denotamos por $e(A, B)$ o número de arestas com um ponto final em A e outro em B. Se A e B são disjuntos e não vazios, definimos a densidade de arestas por*

$$d(A, B) = \frac{e(A, B)}{|A||B|},$$

Como $0 \leqslant e(A, B) \leqslant |A||B|$, temos $0 \leqslant d(A, B) \leqslant 1$.

Para chegarmos ao Lema de Regularidade, precisaremos passar por alguns lemas.

Lema 4.4. *Seja $G = G(V, E)$ um grafo e sejam A e B subconjuntos disjuntos não vazios de V. Se $A' \subset A$ e $B' \subset B$ satisfazendo*

$$|A'| \geqslant (1 - \delta)|A|,$$

$$|B'| \geqslant (1 - \delta)|B|,$$

onde, $0 < \delta < 1$, então

$$|d(A, B) - d(A', B')| \leqslant \frac{2\delta}{(1 - \delta)^2}$$

$$|d(A, B)^2 - d(A', B')^2| \leqslant \frac{4\delta}{(1 - \delta)^2}$$

Em particular, se $\delta \leqslant \frac{1}{2}$, então

$$|d(A, B) - d(A', B')| \leqslant 8\delta,$$

$$|d(A, B)^2 - d(A', B')^2| \leqslant 16\delta.$$

Demonstração. Seja $A'' = A \backslash A'$ e $B'' = B \backslash B'$. Então $|A''| = |A| - |A'| \leqslant \delta|A|$ e $|B''| \leqslant \delta|B|$ e

$$\begin{aligned} e(A,B) &= e(A',B') + e(A',B'') + e(A'',B') + e(A'',B'') \\ &= e(A',B') + e(A',B'') + e(A'',B) \\ &\leqslant e(A',B') + e(A,B'') + e(A'',B) \\ &\leqslant e(A',B') + |A||B''| + |A''||B| \\ &\leqslant e(A',B') + 2\delta|A||B|. \end{aligned}$$

Pois $|A''| \leqslant \delta|A|$ e $|B''| \leqslant \delta|B|$. Assim, $e(A,B) \leqslant e(A',B') + 2\delta|A||B|$, logo,

$$\begin{aligned} d(A,B) &= \frac{e(A,B)}{|A||B|} \\ &\leqslant \frac{e(A',B')}{|A||B|} + 2\delta \leqslant \frac{e(A',B')}{|A'||B'|} + 2\delta \\ &= d(A',B') + 2\delta \leqslant d(A',B') + \frac{2\delta}{(1-\delta)^2}, \end{aligned}$$

consequentemente,

$$d(A,B) - d(A',B') \leqslant \frac{2\delta}{(1-\delta)^2}.$$

Analogamente,

$$\begin{aligned} d(A',B') &= \frac{e(A',B')}{|A'||B'|} \\ &\leqslant \frac{e(A,B)}{|A'||B'|} \leqslant \frac{e(A,B)}{(1-\delta)|A||B|} \\ &= \frac{d(A,B)}{(1-\delta)^2}, \end{aligned}$$

daí,

$$\begin{aligned} d(A',B') - d(A,B) &\leqslant d(A,B)\left(\frac{1}{(1-\delta)^2} - 1\right) \\ &\leqslant \frac{1}{(1-\delta)^2} - 1 = \frac{1 - 1 + 2\delta - \delta^2}{(1-\delta)^2} \\ &\leqslant \frac{1}{(1-\delta)^2}. \end{aligned}$$

Portanto,

$$|d(A,B) - d(A',B')| \leqslant \frac{2\delta}{(1-\delta)^2}$$

e,

$$|d(A,B)^2 - d(A',B')^2| = |d(A,B) + d(A',B')||d(A,B) - d(A',B')|$$

$$\leqslant 2|d(A,B) - d(A',B')|$$

$$\frac{4\delta}{(1-\delta)^2}.$$

Se $0 < \delta \leqslant \frac{1}{2}$, então $\frac{1}{(1-\delta)^2} \leqslant 4$. Isso completa a demonstração.

□

Lema 4.5 (Desigualdade de Schwarz)**.** *Seja $x_1, \ldots, x_n$ números reais. Então*

$$\sum_{i=1}^{n} x_i^2 \geqslant \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right)^2. \tag{4.1}$$

Para $m = 1, \ldots, n-1$, seja

$$\Delta = \frac{1}{m}\left(\sum_{i=1}^{m} x_i\right) - \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right).$$

Então,

$$\sum_{i=1}^{n} x_i^2 \geqslant \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right)^2 + \frac{mn\Delta^2}{n-m}. \tag{4.2}$$

Demonstração. Seja $S_1(n) = \sum_{i=1}^{n} x_i$ e $S_2(n) = \sum_{i=1}^{n} x_i^2$. Observe que

$$\begin{aligned}
0 &\leqslant \sum_{i=1}^{n}\left(x_i - \frac{S_1(n)}{n}\right)^2 \\
&= \sum_{i=1}^{n}\left(x_i^2 - \frac{2x_i S_1(n)}{n} + \frac{S_1(n)^2}{n^2}\right) \\
&= \sum_{i=1}^{n} x_i^2 - \frac{2S_i(n)}{n}\sum_{i=1}^{n} x_i + \sum_{i=1}^{n}\frac{S_1(n)^2}{n^2} \\
&= S_2(n) - \frac{2S_1(n)^2}{n} + \frac{nS_1(n)^2}{n^2} \\
&= S_2(n) - \frac{S_1(n)^2}{n},
\end{aligned}$$

Segue que,

$$S_2(n) \geqslant \frac{S_1(n)^2}{n},$$

o que prova a primeira desigualdade.

$$\begin{aligned} S_2(n) - S_2(m) &= \sum_{i=m+1}^{n} x_i^2 \\ &\geqslant \frac{1}{n-m}\left(\sum_{i=m+1}^{n} x_i\right)^2 \\ &= \frac{(S_1(n) - S_1(m))^2}{n-m}, \end{aligned}$$

e como,

$$\begin{aligned} S_2(n) &= S_2(m) + (S_2(n) - S_2(m)) \\ &\geqslant \frac{S_1(m)^2}{m} + \frac{(S_1(n) - S_1(m))^2}{n-m} \\ &= \frac{S_1(m)^2}{m} + \frac{S_1(n)^2 - 2S_1(n)S_1(m) + S_1(m)^2}{n-m} \\ &= \frac{S_1(n)^2}{n-m} - \frac{2S_1(n)S_1(m)}{n-m} + \frac{(n-m)S_1(m)^2 + mS_1(m)^2}{m(n-m)} \\ &= \frac{S_1(n)^2}{n-m} - \frac{2S_1(n)S_1(m)}{n-m} + \frac{nS_1(m)^2}{m(n-m)} \\ &= \frac{S_1(n)^2}{n} + \frac{mS_1(n)^2}{n(n-m)} - \frac{2S_1(n)S_1(m)}{n-m} + \frac{nS_1(m)^2}{m(n-m)} \\ &= \frac{S_1(n)^2}{n} + \frac{mn}{n-m}\left(\frac{S_1(n)^2}{n^2} - \frac{2S_1(n)S_1(m)}{mn} + \frac{S_1(m)^2}{m^2}\right) \\ &= \frac{S_1(n)^2}{n} + \frac{mn}{n-m}\left(\frac{S_1(n)}{n} - \frac{S_1(m)}{m}\right)^2 \\ &= \frac{S_1(n)^2}{n} + \frac{mn\Delta^2}{n-m}. \end{aligned}$$

E a segunda desigualdade está provada. □

Lema 4.6. *Seja $G = G(V, E)$ um grafo e sejam*

$$A = \bigcup_{i=1}^{q} A_i \subset V,$$

e

$$B = \bigcup_{j=1}^{r} B_j \subset V,$$

onde

$$|A_i| = a \geqslant 1 \quad \textit{disjuntos},$$

para $i = 1, \ldots, q$

$$|B_j| = b \geqslant 1, \quad \textit{disjuntos},$$

para $j = 1, \ldots, r$ *e*

$$A_i \cap B_j = \emptyset$$

para todos i *e* j*. Então*

$$\frac{1}{qr} \sum_{i=1}^{q} \sum_{j=1}^{r} d(A_i, B_j)^2 \geqslant d(A, B)^2. \tag{4.3}$$

Seja $0 < \theta < 1$*, e sejam* q', r' *inteiros tais que* $0 < \theta q \leqslant q' < q$ *e* $0 < \theta r \leqslant r' < r$*. Sejam* $A' = \cup_{i=1}^{q'}$ *e* $B' = \cup_{j=1}^{r'}$*. Então*

$$\frac{1}{qr} \sum_{i=1}^{q} \sum_{j=1}^{r} d(A_i, B_j)^2 \geqslant d(A, B)^2 + \theta^2 (d(A, B) - d(A', B'))^2. \tag{4.4}$$

Demonstração. Como os $A_i's$ e $B_j's$ são disjuntos e $|A_i| = a, |B_j| = b$ temos $|A| = aq$ e $|B| = rb$, segue que

$$\begin{aligned}
\frac{1}{qr} \sum_{i=1}^{q} \sum_{j=1}^{r} d(A_i, B_j) &= \frac{1}{qr} \sum_{i=1}^{q} \sum_{j=1}^{r} \frac{e(A - i, B_j)}{|A_i||B_j|} \\
&= \frac{1}{abqr} \left(\sum_{i=1}^{q} \sum_{j=1}^{r} e(A_i, B_j) \right) \\
&= \frac{1}{abqr} e(A, B) \\
&= \frac{e(A, B)}{|A||B|} \\
&= d(A, B).
\end{aligned}$$

Analogamente,

$$\frac{1}{q'r'} \sum_{i=1}^{q'} \sum_{j=1}^{r'} d(A_i, B_j) = d(A', B').$$

Então

$$\begin{aligned}
\Delta &= \frac{1}{qr} \sum_{i=1}^{q} \sum_{j=1}^{r} d(A_i, B_j) - \frac{1}{q'r'} \sum_{i=1}^{q'} \sum_{j=1}^{r'} d(A_i, B_j) \\
&= d(A, B) - d(A', B').
\end{aligned}$$

Segue de 4.1 do lema anterior que

$$\frac{1}{qr}\sum_{i=1}^{q}\sum_{j=1}^{r} d(A_i,B_j)^2 \geqslant \left(\frac{1}{qr}\right)^2 \left(\sum_{i=1}^{q}\sum_{j=1}^{r} d(A_i,B_j)\right)^2 = d(A,B)^2.$$

Isso prova a primeira desigualdade.

As condições $q' \geqslant \theta q$ e $r' \geqslant \theta r$ implicam em

$$\frac{q'r'}{qr-q'r'} \geqslant \frac{qr\theta^2}{qr-q'r'} \geqslant \theta^2.$$

Aplicando 4.2 para $n = qr, m = q'r'$ obtemos

$$\begin{aligned}\frac{1}{qr}\sum_{i=1}^{q}\sum_{j=1}^{r} d(A_i,B_j)^2 &\geqslant \left(\frac{1}{qr}\right)^2 \left(\sum_{i=1}^{q}\sum_{j=1}^{r} d(A_i,B_j)\right)^2 + \frac{q'r'\Delta^2}{qr-q'r'} \\ &\geqslant d(A,B)^2 + \theta^2\Delta^2 \\ &= d(A,B)^2 + \theta^2(d(A,B)-d(A',B'))^2.\end{aligned}$$

Isso completa a demonstração. □

Seja $G = G(V,E)$ um grafo, e seja $\mathcal{P}$ uma partição do conjunto V em $m+1$ conjuntos $C_0, C_1, \ldots, C_m$. A partição $\mathcal{P}$ é dita *equitativa* se tivermos $|C_s| = |C_t|$ para todos $1 \leqslant s < t \leqslant m$. O Conjunto C_0 é chamado de conjunto *excepcional* da partição. Definimos a *densidade de partição* de uma partição equitativa $\mathcal{P}$ por

$$d(\mathcal{P}) = \frac{1}{m^2}\sum_{1\leqslant s<t\leqslant m} d(C_s,C_t).$$

Observe que têm $m(m-1)/2$ parcelas no somatório, e cada parcela satisfaz $0 \leqslant d(C_s,C_t) \leqslant 1$. Segue que

$$0 \leqslant d(\mathcal{P}) < \frac{1}{2}.$$

Sejam A e B subconjuntos não vazios, disjuntos do conjunto de vértices V. Para $\varepsilon > 0$ o par (A,B) é dito *ε-regular* se as condições

$$X \subset A, |X| \geqslant \varepsilon|A|$$

e

$$Y \subset B, |Y| \geqslant \varepsilon |B|$$

Implicarem em

$$|d(A,B) - d(X,Y)| < \varepsilon.$$

Uma partição equitativa V em $m+1$ conjuntos dois-a-dois disjuntos $C_0, C_1, \ldots, C_m$ é *ε-regular* desde que

$$|C_0| \leqslant \varepsilon |V|$$

e se cada par (C_s, C_t) é ε-regular para no máximo εm^2 pares (C_s, C_t) com $1 \leqslant s < t \leqslant m$. O próximo lema é de fundamental importância na prova do Lema de Regularidade.

Lema 4.7. *Seja $0 < \varepsilon < 1$ e um inteiro m satisfazendo*

$$4^m \geqslant 2^{10}\varepsilon^{-5}.$$

Seja $G = G(V,E)$ um grafo com k vértices, e seja $\mathcal{P}$ uma partição equitativa de V em $m+1$ classes $C_0, C_1, \ldots, C_m$ tais que

$$|C_s| \geqslant 4^{2m}$$

para $s = 1, \ldots, m$. Se o ´número de pares ε-irregulares (C_s, C_t) com $1 \leqslant s < t \leqslant m$. é maior que εm^2, então existe uma partição equitativa $\mathcal{P}'$ de V em $m4^m + 1$ classes tais que o conjunto excepcional tem cardinalidade menor que

$$|C_0| + \frac{k}{4^m},$$

e a partição $\mathcal{P}'$ satisfaz

$$d(\mathcal{P}') \geqslant d(\mathcal{P}) + \frac{\varepsilon^{-5}}{32}.$$

Teorema 4.8 (O Lema de Regularidade)**.** *Seja $0 < \varepsilon < 1 e\ m' \geqslant 1$. Existem números $K = K(\varepsilon, m')$ e $M = M(\varepsilon, m')$ tais que, se $G = G(V,E)$ é um grafo com $|V| \geqslant K$ vértices, então existe uma partição ε-regular de V.*

Demonstração. Dado $t' = [16\varepsilon^{-5}]$. Construiremos uma sequência $m_0, m_1, m_2, \ldots$ de inteiros como segue. Considere

$$m_0 \geqslant m',$$

Sejam

$$4^{m_0} \geqslant \max\{2^{10}\varepsilon^{-5}, 2^{t'+2}\varepsilon^{-1}\}.$$

e

$$m_{t+1} = m_t 4^{m_t}$$

para $t = 0, 1, 2, \ldots$ Nós definimos M e K por

$$M = M(\varepsilon, m') = m_{t'}$$

e

$$K = K(\varepsilon, m') = \max\{2m_0/\varepsilon, m_{t'}16^{m_{t'}}/(1-\varepsilon)\}.$$

Seja $G = G(V, E)$ um grafo com $|V| = k \geqslant K$. Seja T um conjunto de inteiros não negativos t com a propriedade que existe uma partição $\mathcal{P}$ de V em $m_t + 1$ conjuntos tais que

$$d(\mathcal{P}) \geqslant \frac{t\varepsilon^5}{32} \tag{4.5}$$

e que o conjunto excepcional C_0 tenha cardinalidade

$$|C_0| < \varepsilon k(1 - 2^{-t-1}) \tag{4.6}$$

Considere uma partição $\mathcal{P}_\prime$ de V consistindo de m_0 conjuntos dois-a-dois disjuntos de tamanho $[k/m_0]$, juntamente com o conjunto excepcional C_0 de cardinalidade menor que m_0. Então

$$|C_0| < m_0 = \varepsilon K/2 \leqslant \varepsilon k/2 = \varepsilon k(1 - 1/2).$$

Como $d(\mathcal{P}_\prime) \geqslant 0$, segue que $t = 0$ satisfaz as condições 4.5 e 4.6. Assim, $0 \in T$. Além disso $d(\mathcal{P}) < 1/2$, se t satisfaz a condição 4.5, então

$$t \leqslant t' = [16\varepsilon^{-5}].$$

Segue que a condição 4.5 é satisfeita para uma quantidade finita de inteiros positivos. Assim o conjunto T é finito e existem um maior inteiro $t \leqslant t'$ satisfazendo 4.5 e 4.6 para

alguma partição $\mathcal{P}$ de V em $m+1$ conjuntos. Seja $\mathcal{P} = \{C_0, C_1, \ldots, C_m\}$. Então

$$\begin{aligned} |C_s| &= \frac{|V| - |C_0|}{m_t} \\ &> \frac{k(1-\varepsilon)}{m_t} \\ &\geqslant \frac{K(1-\varepsilon)}{m_{t'}} \\ &\geqslant 16^{m_{t'}} \\ &\geqslant 16^{m_t}, \end{aligned}$$

para $s = 1, \ldots, m_t$ e $4^{m_t} \geqslant 4^{m_0} > 2^{10}\varepsilon^{-5}$.

Como o conjunto excepcional de $\mathcal{P}$ satisfaz $|C_0| < \varepsilon k$, segue que, se a partição $\mathcal{P}$ é não ε-regular então o número de pares (C_s, C_t) é no máximo εm^2. Pelo Lema 4.7 temos que existe uma partição equitativa $\mathcal{P}'$ de V em $m_t 4^{m_t} + 1 = m_{t+1} + 1$ conjuntos tais que

$$d(\mathcal{P}') \geqslant d(\mathcal{P}) + \varepsilon^5/32 \geqslant (t+1)\varepsilon^5/32$$

e o conjunto excepcional C_0' de $\mathcal{P}'$ satisfaz

$$\begin{aligned} |C_0'| &< |C_0| + k/4^{m_t} \\ &< \varepsilon k(1 - 2^{-t-1}) + k/4^{m_t} \\ &\leqslant \varepsilon k(1 - 2^{-t-1} + \varepsilon^{-1}4^{-m_t}) \\ &\leqslant \varepsilon k(1 - 2^{-t-1} + \varepsilon^{-1}4^{-m_0}) \\ &\leqslant \varepsilon k(1 - 2^{-t-1} + 2^{-t'-2}) \\ &\leqslant \varepsilon k(1 - 2^{-t-1} + 2^{-t-2}) \\ &\leqslant \varepsilon k(1 - 2^{-t-1}). \end{aligned}$$

Isso implica que $t+1$ satisfaz as condições 4.5 e 4.6 o que contrária a máximalidade de t. Portanto $\mathcal{P}$ é ε-regular. □

Teorema 4.9 (Balog-Szemerédi)**.** *Sejam δ, σ, λ e μ números reais positivos. Existem números positivos c_1', c_2' e K dependendo de δ, σ, λ e μ com a propriedade de que se A e B forem subconjuntos de um grupo abeliano com*

$$\lambda k \leqslant |A| \leqslant \mu k$$

e

$$\lambda k \leqslant |B| \leqslant \mu k.$$

para W um subconjunto de $A \times B$ é tal que

$$|W| \geqslant \delta k \ 2$$

e

$$S = S(W) = \{a + b : (a, b) \in W\}$$

satisfaz

$$|S| \leqslant \sigma k.$$

Então existe um conjunto $A' \subset A$ tal que

$$|A'| \geqslant c_1' k$$

e

$$|2A'| \leqslant c_2' k.$$

Em particular,

$$|2A'| \leqslant c|A'|,$$

onde $c = c_2'/c_1'$.

Teorema 4.10 (Segunda Aplicação Teorema de Freiman)**.** *Seja $\delta > 0$ e $t \geq 3$. Existe um inteiro $k_1(\delta, t)$ tal que se A é um subconjunto de números inteiros com $|A| = k \geq k_1(\delta, t)$ e A contém pelo menos δk^2 progressões aritméticas com três termos, então A contém uma P.A. de tamanho t.*

Demonstração. Seja A um conjunto de k inteiros, e seja

$$\{\{a_i, b_i, c_i\} : i \in I\}$$

uma família de progressões aritméticas de três termos em A, onde I é um conjunto de índices com $|I| \geqslant \delta k^2$. Daí,

$$|\{\{a_i, b_i, c_i\} : i \in I\}| = |I| \geqslant \delta k^2$$

E $b_i - a_i = c_i - b_i > 0$ o que implica em

$$a_i + c_i = 2b_i$$

para $i \in I$, definimos

$$W = \{(a_i, c_i) : i \in A\}$$

Então,

$$|W| = |I| \geqslant \delta k^2.$$

Considere,

$$\begin{aligned} S(W) &= \{a_i + c_i = 2b_i : (a_i, c_i) \in W\} \\ &= \{2b_i : i \in I\} \\ &\subset \{2b : b \in A\} \\ &= 2 * A. \end{aligned}$$

Segue que

$$|S(W)| \leqslant |2 * A| = k.$$

Aplicando o Teorema 4.9 para $A = B$, $\lambda = \mu = \sigma = 1$. Se $k \geqslant K = K(\delta)$, então existe um conjunto $A' \subset A$ tal que $|A'| \geqslant c_1' k$ e $|2A'| \geqslant c|A'|$, onde c depende apenas de δ. E pelo Teorema 4.2, se $c_1' k \geqslant k_0(c, t)$, então A' contém uma progressão aritmética de tamanho t. Isso conclui a demonstração.

□

Referências Bibliográficas

[1] Dias, A. E., *Classical and modern approaches for Plunnecke-type inequalities*, MatemÃ tica Aplicada IV (2014).

[2] Diestel, R., *Graph Theory*, New York, Springer, 2000.

[3] Erdös, P. and Szekeres, G. *A combinatorial problem in geometry*, Compositio Math. 2 (1935), 463–470.

[4] Freiman, G. A., *Foundations of a Structural Theory of Set Addition*, Translations of Math. Monographs, Vol. 37, Amer. Math. Soc., Providence, R.I., 1973.

[5] Gowers, W. T., *A new proof of Szemerédi's theorem*, Geometry Functional Analytical **11** (2001), 465-588.

[6] Green, B. and Ruzsa, I. Z. *Freiman's Theorem in an arbitrary abelian group*, Journal ofthe London Mathematical Society **75.1** (2007), 163-175.

[7] Green, B. and Ruzsa, I. Z. *Sets with small sumset and rectification*, Bulletin of the London Mathematical Society **38.1** (2006), 43-52.

[8] Green, B. J., *Structure theory of set addition*, Lecture notes given at Edinburgh in (2002).

[9] Green, B. J. and Tao, T. *The Primes Contain Arbitrarity Long Arithmetic Progressions*, Annals of Mathematics Second Series, Vol 167, N. 2, (2008), 481-547.

[10] Greenwood, R. E. and Gleason, A. M., *Combinatorial Retation and Chromatic Graphs*, Canadian J. Math 7 (1955).

[11] Guo, S. and Sun, Z. W., *Determination of the 2-color Rado Number for* $ax_1 + \cdots + ax_m = x_0$, J. Combin, Theory Ser. A, 115 (2008) 345-353.

[12] Hales, A. W. and Jewett, R. I., *Regularity and Positional Games*,University of Oregon, (1961).

[13] Nathanson, M. B., *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* (Graduate texts in math.; 165), Springer, New York, (1996).

[14] Plunnecke, H., *Eine zahlentheoretische Anwendung der Graphentheorie*, Journal fur die reine und angewandte Mathematik **243** (1970), 171-183.

[15] Rado, R., *Studien zur Kombinstorik*, Math. Z.36 (1933), 424-480.

[16] Sampaio, P. C., *Combinatória Revisitada: Uma Introdução a Teoria de Ramsey*, Dissertação Mestrado IMPA, Rio de Janeiro (2014).

[17] Sun, Z. W., *Hall's theorem revisited*, Proc. American Mathematics Society **129** (2001), 3129-3131.

[18] Sun, Z. W., *Combinatorial Aspects of Szemerédi's Theorem*, Chinese Academy of Science(01-30), China (2007).

[19] Szemerédi, E. *On sets of integers containing no k elements in arithmetic progression*, Acta Arith.,27 (1975), 199-245.

[20] Tao, T. and Vu, V. H., *Additive Combinatorics*, Cambridge University Press, Cambridge, (2006).