Monografia do Projeto de Formatura – MAC499

Domingos Dellamonica Jr.

Orientador: Yoshiharu Kohayakawa

15 de novembro de 2004

Resumo

Esta monografia pretende abordar uma boa parte dos assuntos estudados por mim durante a minha iniciação científica, cujo título é "Métodos Probabilísticos e Algébricos em Combinatória". Espero poder exemplificar diversas técnicas sofisticadas empregadas em problemas combinatórios numa abordagem simples porém completa.

Sumário

1 A Iniciação Científica

Descreverei nesta seção, de forma breve, as atividades da minha inciação científica, que é também o meu trabalho de formatura. Meu orientador foi o Prof. Yoshiharu Kohayakawa. Gostaria de agradecê-lo por guiar a pesquisa da minha IC, em particular, por escolher assuntos que foram muito interessantes e despertaram meu interesse em pesquisa científica.

Os assuntos estudados foram muitos. As referências básicas são o livro de N. Alon e J. Spencer, *The Probabilistic Method* [1] e o pré-release do livro *Linear Algebra Methods in Combinatorics* [2], de L. Babai e P. Frankl. Além deles, alguns artigos sofisticados foram estudados. Resolvi incluir nesta monografia o conteúdo de uma monografia submetida à *Jornada de Iniciação Científica do IMPA*. O trabalho foi selecionado para uma apresentação oral no IMPA e estará concorrendo a participação num colóquio em 2005.

Os motivos para incluir este conteúdo vão além do orgulho de um trabalho bem feito. Este trabalho inclui muitas técnicas sofisticadas, envolvendo várias áreas da matemática para construir um objeto combinatório. Além disso, ele contém uma porção substancial do conteúdo estudado nesta iniciação científica.

1.1 Metodologia de Estudo

Durante a iniciação científica, eu e meu orientador nos reuníamos semanalmente. Basicamente eu estudava algum assunto específico ou resolvia algum problema relacionado e então preparava uma apresentação oral. Este esquema foi muito produtivo. Por exemplo, a monografia que está inclusa neste trabalho surgiu a partir de diversas apresentações.

Inicialmente só havia um texto pouco estruturado. A partir dos comentários e opiniões expressados durante as apresentações, esse texto foi remodelado e deu origem a monografia entregue. Um outro exemplo foi um problema proposto, resolvido por mim de uma maneira peculiar. Elaborei um pequeno artigo contendo uma generalização da solução e submeti tal artigo para para publicação na RMU (Revista de Matemática Universitária). O artigo foi aceito e será publicado na próxima edição da revista. A seguir, descrevo brevemente a solução para tal problema.

2 Conjuntos Livres de Somas - Problema Resolvido

Dizemos que um conjunto S é livre de somas quando não existem $a, b, c \in S$, tais que $a + b = c$. Vamos apresentar um teorema, provado por Erdős em 1965.

Teorema 2.1. *Todo conjunto $B = \{b_1, \ldots, b_n\}$ de inteiros não nulos contém um subconjunto A, livre de somas, de tamanho $|A| > n/3$.*

Demonstração. Seja $p = 3k + 2$ um primo satisfazendo $p > 2\max_{1\leq i\leq n} |b_i|$ e defina $C = \{k + 1, k + 2, \ldots, 2k + 1\} \subset \mathbb{Z}_p$. Veja que C é livre de somas em $\mathbb{Z}_p$ e que

$$\frac{|C|}{p-1} = \frac{k+1}{3k+1} > \frac{1}{3}.$$

Escolha um elemento aleatório x, de $\mathbb{Z}_p^*$, conforme uma distribuição uniforme. Defina $d_i = xb_i \mod p$, $1 \leq i \leq n$. Note que como p é primo e $b_i \not\equiv 0 \pmod p$, $\varphi_i(x) = xb_i$ é uma função bijetiva e, portanto, $\mathbb{P}[d_i \in C] = |C|/(p-1) > 1/3$. O número esperado de elementos b_i tais que $d_i \in C$ é maior que $n/3$. Logo, existe um $x \in \mathbb{Z}_p^*$ e $A \subset B$ de cardinalidade $|A| > n/3$ tal que $xy \mod p \in C$ para todo $y \in A$. Mas A é livre de somas, pois se $a_1, a_2, a_3 \in A$ são tais que $a_1 + a_2 = a_3$, então $xa_1 + xa_2 \equiv xa_3 \pmod p$, o que contradiz o fato de que C é livre de somas. □

Um dos problemas propostos no livro *Probabilistic Method* [1] consistia em demonstrar uma generalização do teorema de Erdős. Queremos mostrar que todo conjunto $B = \{b_1, \ldots, b_n\}$ de *reais* não nulos contém um subconjunto A, livre de somas, de tamanho $|A| > n/3$.

Seja $B = \{b_1, \ldots, b_n\}$ um conjunto de n números reais. Sejam $x_1, \ldots, x_n$, variáveis. Para cada $1 \leq i, j, k \leq n$ com $b_i + b_j = b_k$, adicione a equação $x_i + x_j - x_k = 0$ a um sistema de equações lineares. Se não existem i, j, k dessa forma, então B é livre de somas e o enunciado é satisfeito.

Caso o sistema tenha pelo menos uma equação, podemos definir uma matriz $\mathbf{T}$, correspondente ao sistema linear homogêneo formado. Note que as entradas de $\mathbf{T}$ são elementos de $\{0, 1, -1\}$, que são racionais.

Denotamos $\ker(\mathbf{T}) = \{\mathbf{x} \mid \mathbf{Tx} = \mathbf{0}\}$ (alguns autores definem o núcleo de uma transformação linear $\mathbf{T}$ como $\mathrm{Null}(\mathbf{T})$). Como $\mathbf{b} = (b_1, \ldots, b_n)$ é solução do sistema por definição, $\mathbf{b} \in \ker(\mathbf{T})$, ou seja, $\ker(\mathbf{T}) \neq \emptyset$ e, portanto, deve haver uma base de $\ker(\mathbf{T})$ com vetores de coordenadas racionais (pois $\mathbf{T}$ tem coordenadas racionais).

Seja $\mathbf{u} \in \ker(\mathbf{T}) \cap \mathbb{Q}^n$ com o menor número de coordenadas repetidas, ou seja, $\#\{(i, j) \mid u_i = u_j\}$ é mínimo. Vamos mostrar que $\mathbf{u}$ não tem coordenadas repetidas.

Suponha que $u_i = u_j$. Existe um vetor $\mathbf{v} \in \ker(\mathbf{T}) \cap \mathbb{Q}^n$ com $v_i \neq v_j$. Caso contrário, todos os vetores da base de $\ker(\mathbf{T})$ teriam as coordenadas i e j iguais, mas como $\mathbf{b}$ é uma combinação linear dos vetores de tal base (com coeficientes reais), teríamos $b_i = b_j$, o que é absurdo.

Vamos mostrar que para algum $\lambda \in \mathbb{Q}^*$, $\mathbf{u} + \lambda\mathbf{v}$ tem estritamente menos coordenadas repetidas que $\mathbf{u}$. Para isso, veja que

$$u_i + \lambda v_i \neq u_j + \lambda v_j.$$

Além disso, $u_k + \lambda v_k = u_l + \lambda v_l$ somente se $u_k - u_l = \lambda(v_k - v_l)$. Então, ou $u_k - u_l = v_k - v_l = 0$, ou

$$\lambda = \frac{u_k - u_l}{v_k - v_l}.$$

Como há um número finito de pares (k, l), os valores que λ não pode assumir formam um conjunto finito e, portanto, para infinitos valores de λ, $\mathbf{u} + \lambda\mathbf{v}$ possui menos coordenadas repetidas que $\mathbf{u}$, o que contradiz a definição de $\mathbf{u}$.

Para concluir a demonstração, tome $U = \{u_1, \ldots, u_n\}$, que é um conjunto de n números racionais. Pelo teorema 2.1, existe $U' \subset U$, de cardinalidade $|U'| > n/3$, livre de somas. Mas se $U' = \{u_{i_1}, \ldots, u_{i_r}\}$, o conjunto $A = \{b_{i_1}, \ldots, b_{i_r}\} \subset B$ deve ser livre de somas.

3 Introdução - Cotas para Números de Ramsey

O número de Ramsey, $R(m, s)$ é, na linguagem de teoria dos grafos, o menor inteiro n tal que todo grafo com n vértices possue um clique de tamanho s ou um conjunto independente de tamanho m. Um clique é um conjunto de vértices tal que cada par de vértices é ligado por uma aresta. Um conjunto independente é formado por vértices que não são ligados por nenhuma aresta entre si.

Numa abordagem informal, o número $R(m, s)$ pode ser introduzido como o menor número de pessoas que devem estar presentes em uma festa para que existam s pessoas que se conhecem mutuamente (um clique!) ou existam m pessoas que não se conhecem entre si (um conjunto independente).

Ramsey (1930) mostrou que os números $R(m, s)$ são finitos. Desde então, determinar o valor numérico e o comportamento assintótico desses números tem sido objeto de estudo de muitos pesquisadores. O problema, no entanto, tem se mostrado difícil.

Na próxima seção, mostraremos como um método probabilístico pode ser usado para determinar cotas superiores para os números de Ramsey. Nas seções seguintes, apresentaremos construções explícitas de grafos que provam cotas inferiores para os números de Ramsey. É interessante notar que as cotas obtidas dessa forma são muito mais fracas que as cotas obtidas probabilisticamente.

No desenvolvimento das idéias que seguem, são utilizadas as mais diversas ferramentas matemáticas: conceitos estatísticos como probabilidades e esperanças, álgebra linear, teoria dos corpos, representação de grupos através de caracteres, teoria dos códigos e teoria dos grafos etc. É impressionante como áreas tão diversas se combinam harmoniosamente para produzir resultados combinatórios. Esperamos que o leitor possa compartilhar nosso entusiasmo em uma leitura agradável deste trabalho.

3.1 Aplicações da Teoria de Ramsey na Computação

A teoria de Ramsey tem diversas aplicações em Ciência da Computação. Um exemplo interessante é o artigo [3], que mostra um algoritmo de aproximação para encontrar conjuntos independentes num grafo. O algoritmo trabalha incrementando, ao mesmo tempo, um conjunto de vértices independentes do grafo e um conjunto de vértices formando um clique. Para demonstrar a qualidade da aproximação (e também demonstrar que os algoritmos mostrados são, dentro da sua categoria, os melhores possíveis) são utilizadas idéias da teoria de Ramsey.

Uma lista de artigos relacionados a teoria de Ramsey pode ser encontrado na página `http://www.cs.umd.edu/~gasarch/ramsey/ramsey.html`.

4 Cotas Probabilísticas

Nesta seção apresentaremos diversas cotas para os números de Ramsey. O leitor interessado pode consultar [4, cap. 12] para demonstrações detalhadas e mais informações técnicas.

4.1 Método Probabilístico

O método probabilístico é um método não construtivo usado para demonstrar a existência de objetos matemáticos com certas propriedades. O pioneiro desta técnica foi Paul Erdős. A idéia do método consiste em estabelecer um espaço finito de probabilidades relacionado a estrutura cuja existência queremos constatar. Se, ao escolhermos aleatoriamente um objeto desse espaço, a probabilidade do objeto possuir as características desejadas for positiva então existe um objeto com as propriedades desejadas. Com os exemplos que seguem, estes conceitos ficarão mais claros.

Definição. *3 Definimos o espaço de probabilidades $\mathcal{G}(n,p)$ como o espaço de todos os grafos com n vértices no qual dois vértices são ligados por uma aresta com probabilidade p.*

4.2 Algumas Cotas Probabilísticas

Teorema 4.1. *Suponha que $3 \leq s \leq m$, $0 < p < 1$ e*

$$\binom{n}{s} p^{\binom{s}{2}} + \binom{n}{m} (1-p)^{\binom{m}{2}} < 1.$$

Então $R(m,s) \geq n+1$.

Demonstração. Considere um grafo escolhido aleatoriamente no espaço $\mathcal{G}(n,p)$. Seja Y_s o número de cliques de tamanho s no grafo escolhido e seja $\overline{Y_m}$ o número de conjuntos

independentes de tamanho m no mesmo grafo. Temos

$$\mathbb{P}[Y_s + \overline{Y_m} = 0] = 1 - \sum_{r>0} \mathbb{P}[Y_s + \overline{Y_m} = r]$$
$$\geq 1 - \sum_{r>0} r \times \mathbb{P}[Y_s + \overline{Y_m} = r] = 1 - \mathbb{E}[Y_s + \overline{Y_m}] > 0,$$

pois, pela linearidade da esperança, temos

$$\mathbb{E}[Y_s + \overline{Y_m}] = \mathbb{E}[Y_s] + \mathbb{E}[\overline{Y_m}] = \binom{n}{s} p^{\binom{s}{2}} + \binom{n}{m}(1-p)^{\binom{m}{2}} < 1.$$

□

Lema 4.1. *Para todo $s \leq n$, temos*

$$\sum_{k=0}^{s} \binom{n}{k} \leq \left(\frac{en}{s}\right)^s,$$

onde e é a base do logaritmo natural.

Demonstração. Como $s \leq n$, vale

$$\left(\frac{s}{n}\right)^s \sum_{k=0}^{s} \binom{n}{k} \leq \sum_{k=0}^{s} \binom{n}{k} \left(\frac{s}{n}\right)^k \leq \left(1 + \frac{s}{n}\right)^n.$$

Utilizando a desigualdade

$$1 + x < e^x, \text{ para todo } x \neq 0 \text{ real}, \tag{1}$$

verificamos que

$$\left(\frac{s}{n}\right)^s \sum_{k=0}^{s} \binom{n}{k} \leq (e^{s/n})^n = e^s.$$

Logo $\sum_{k=0}^{s} \binom{n}{k} \leq \left(\frac{en}{s}\right)^s$. □

Lema 4.2. *Para todo $3 \leq s \leq n$, temos*

$$\binom{n}{s} < \frac{1}{2}\left(\frac{en}{s}\right)^s.$$

Demonstração. Basta verificar (por exemplo, usando indução) que

$$\sum_{k=0}^{s} \binom{n}{k} > 2\binom{n}{s}.$$

Aplicando o lema 4.1, obtemos a desigualdade desejada. □

Teorema 4.2. *Seja* $3 \leq s \leq m$ *e*

$$\Big(\frac{s}{en}\Big)^{2/(s-1)} + \Big(\frac{m}{en}\Big)^{2/(m-1)} > 1.$$

Então $R(m,s) \geq n+1$.

Demonstração. Seja $p = (m/en)^{2/(m-1)}$ e $q = (s/en)^{2/(s-1)}$. Como $p+q > 1$, é evidente que $1-p < q$. Sejam Y_s e $\overline{Y_m}$ como no teorema 4.1. Temos

$$\mathbb{E}[\overline{Y_m}] = \binom{n}{m} p^{\binom{m}{2}} < \frac{1}{2}\Big(\frac{en}{m}\Big)^m p^{m(m-1)/2} = \frac{1}{2}, \text{ e}$$

$$\mathbb{E}[Y_s] = \binom{n}{s}(1-p)^{\binom{s}{2}} < \binom{n}{s} q^{\binom{s}{2}} < \frac{1}{2}\Big(\frac{en}{s}\Big)^s q^{s(s-1)/2} = \frac{1}{2}.$$

Como na demonstração do teorema 4.1, temos

$$\mathbb{P}[Y_s + \overline{Y_m} = 0] \geq 1 - \mathbb{E}[Y_s + \overline{Y_m}] > 0.$$

□

Teorema 4.3. *[4, Corolário 12.9] Para* $3 \leq s \leq m$, *temos*

$$R(m,s) \geq \frac{1}{e} m^{(s-1)/2} s^{(3-s)/2} (\log m)^{(1-s)/2}. \tag{2}$$

Demonstração. Defina $n = \lfloor (1/e) m^{(s-1)/2} s^{-(s-3)/2} (\log m)^{-(s-1)/2} \rfloor$. Note que

$$\frac{m}{en} \geq m^{-(s-3)/2} s^{(s-3)/2} (\log m)^{(s-1)/2} > m^{-s/2+3/2} > m^{-s/2+s/2m} = m^{-s(m-1)/2m}.$$

Observe também que

$$\Big(\frac{s}{en}\Big)^{2/(s-1)} \geq [m^{-(s-1)/2} s^{(s-1)/2} (\log m)^{(s-1)/2}]^{2/(s-1)} = (\log m)\frac{s}{m}.$$

Usando a desigualdade (1), concluimos que

$$\Big(\frac{m}{en}\Big)^{\frac{2}{m-1}} \geq m^{-s/m} = e^{-(\log m)s/m} > 1 - (\log m)s/m \geq 1 - \Big(\frac{s}{en}\Big)^{\frac{2}{s-1}}.$$

Agora basta aplicar o teorema 4.2 para concluir a demonstração. □

Podemos expressar o teorema acima da seguinte forma. Existe uma função $\alpha(m,s)$ tal que $\lim_{m\to\infty} \alpha(m,s) = 0$ para todo $s \geq 3$ e

$$R(m,s) \geq m^{[s-1-\alpha(m,s)]/2}. \tag{3}$$

Também temos cotas superiores para números de Ramsey fora da diagonal:

Teorema 4.4. *[4, 12.17] Existem constantes $c_3, c_4, \ldots$ tais que para todo $s \geq 3$ temos $c_s < 2.(20)^{s-3}$ e, se m é suficientemente grande,*

$$R(m,s) < \frac{c_s m^{s-1}}{(\log m)^{s-2}}. \tag{4}$$

Existem cotas probabilísticas mais sofisticadas para grafos livres de triângulo [4, 12.15]. Quando $m \to \infty$, temos

$$\Big(\frac{1}{162} + o(1)\Big)\frac{m^2}{\log m} \leq R(m,3) \leq (1+o(1))\frac{m^2}{\log m}. \tag{5}$$

5 Cotas Construtivas

5.1 Resultado Principal

Teorema 5.1. *Existe uma constante $\varepsilon > 0$ e uma construção explícita de grafos tal que para todo s e todo m suficientemente grande, tal construção produz um grafo com pelo menos $m^{\varepsilon\sqrt{\log s/\log\log s}}$ vértices que não contém nem um clique de tamanho s nem um conjunto independente de tamanho m. Isso mostra uma cota inferior construtiva para $R(m,s)$.*

Definição (Grafo de Cliques). *3 Seja G um grafo. O grafo $\mathrm{CQ}(G)$ tem como vértices os cliques de G de tamanho pelo menos 2. Dois vértices de $\mathrm{CQ}(G)$ são ligados por uma aresta se o conjunto de vértices dos cliques associados a tais vértices são K e L e há uma aresta $(u,v) \in E_G$ com $u \in K \setminus L$ e $v \in L \setminus K$. Chamamos $\mathrm{CQ}(G)$ de* grafo de cliques *de G. Definimos $\mathrm{CQ}_k(G)$ como o grafo de k- cliques de G.*

5.2 Lemas Preliminares

Lema 5.1. *Para todo grafo G e todo k, temos $\alpha(\mathrm{CQ}_k(G)) \leq \alpha(G)$.*

Demonstração. Seja X um conjunto independente de $\mathrm{CQ}_k(G)$ de tamanho máximo. Se $|X| = 2$, então tome dois cliques diferentes de X e veja que deve existir um vértice em um dos cliques e outro vértice no outro clique sem uma aresta entre eles, caso contrário, eles não formariam um conjunto independente em $\mathrm{CQ}_k(G)$, mas então esses dois vértices formam um conjunto independente em G e o lema está provado.

Se $|X| > 2$, sejam $L_1, L_2, K \in X$ os conjuntos de vértices de três cliques diferentes. As intersecções $L_1 \cap K$ e $L_2 \cap K$ são comparáveis por inclusão, caso contrário, haveria $u \in L_1 \setminus L_2$ e $v \in L_2 \setminus L_1$ com $u, v \in K$, mas então u e v são ligados por uma aresta (pois estão no clique K) e deve haver uma aresta ligando L_1 e L_2, contradição.

Portanto, para cada membro K de X existe uma intersecção maximal da forma $K \cap L$, onde $L \in X$ e $L \neq K$. Sendo assim, para todo K fixado, existe um elemento $v \in K$ que não aparece em nenhum outro clique de X, ou seja, v é um vértice exclusivo de K. Se tomarmos um vértice exclusivo de cada clique de X vemos que estes formam um conjunto independente em G (caso contrário, os cliques estariam ligados por uma aresta em

$\mathrm{CQ}_k(G)$). Isso mostra que há um conjunto independente em G com tamanho pelo menos $\alpha(\mathrm{CQ}_k(G))$ e isso conclui a demonstração do lema.

□

Definição (Girassol). *3 Um* girassol *com $l > 1$* pétalas *e um* centro *Y é uma coleção de conjuntos $S_1, \ldots, S_l$ tal que $S_i \cap S_j = Y$ para todo $i \neq j$. Os conjuntos $S_i \setminus Y$ são as pétalas.*

Lema 5.2. *Seja $\mathcal{F}$ uma família de conjuntos de cardinalidade k. Se $|\mathcal{F}| > k!(l-1)^k$ então $\mathcal{F}$ contém um girassol com l pétalas.*

Demonstração. A demonstração segue por indução em k. Para $k = 1$, devemos ter pelo menos l conjuntos unitários (distintos) em $\mathcal{F}$, mas quaisquer l conjuntos unitários distintos formam um girassol com centro vazio.

Seja $k \geq 2$ e $\mathcal{A} = \{A_1, \ldots, A_t\}$ uma família maximal de elementos dois a dois disjuntos. Se $t \geq l$, $\mathcal{A}$ é um girassol com centro vazio e não há nada a demonstrar. Se $t < l$, defina $B = A_1 \cup \cdots \cup A_t$. Temos que $|B| = kt \leq k(l-1)$. Pela maximalidade de $\mathcal{A}$, o conjunto B intercepta todo membro de $\mathcal{F}$. Pelo princípio da casa dos pombos, algum $x \in B$ deve estar contido em pelo menos

$$\frac{|\mathcal{F}|}{|B|} > \frac{k!(l-1)^k}{k(l-1)} = (k-1)!(l-1)^{k-1}$$

membros da família $\mathcal{F}$.

Defina $\mathcal{F}_x = \{S \setminus \{x\} \mid S \in \mathcal{F}, x \in S\}$. Pela hipótese de indução, $\mathcal{F}_x$ contém um girassol com l pétalas. Adicionando x a cada um dos conjuntos desse girassol, obtemos um girassol de $\mathcal{F}$.

□

Lema 5.3. *Suponha que $\mathrm{CQ}_k(G)$ tenha um clique de tamanho $> k!(l-1)^k$. Então existe em G um subconjunto de kl vértices com pelo menos $\binom{l}{2}$ arestas.*

Demonstração. Seja X um clique com tamanho $> k!(l-1)^k$. Se encararmos X como um sistema de conjuntos — onde cada membro de X é um conjunto de vértices de um k-clique em G — então, pelo lema 5.2, há um girassol com l pétalas. Como os l cliques do girassol estão conectados em $\mathrm{CQ}_k(G)$, há pelo menos $\binom{l}{2}$ arestas em G entre os vértices das pétalas (kl vértices).

□

Definição (Grafos Norma - Kollár, Rónyai, Szabó). *3 Sejam q uma potência de um primo, $t > 1$ e N a norma dos elementos do corpo GF_{q^t} sobre GF_q, ou seja, $N(x) = x^{(q^t-1)/(q-1)}$. Definimos o* grafo norma $\mathrm{NG}_{q,t}$ *como o grafo cujos vértices são elementos de GF_{q^t} e dois vértices a, b são ligados por uma aresta se e somente se $N(a+b) = 1$. Estamos considerando grafos com laços, ou seja, se $N(2a) = 1$, a possui um laço.*

5.3 Propriedades dos Grafos Norma

1. **O número de vértices é $n = q^t$.**
   Decorre imediatamente de $|\,\mathrm{GF}_{q^t}\,| = q^t$.

2. **O grafo é regular de grau $(q^t-1)/(q-1)$ (que é $n^{1-1/t}$ assintoticamente).**
   Primeiramente, note que $\mathrm{Im}(N) \subset \mathrm{GF}_q$. Todo elemento não-nulo $y = N(x)$ satisfaz $y^{q-1} = x^{q^t-1} = 1$. Mas as raízes de $y^{q-1} - 1 = 0$ são precisamente os elementos de GF_q^*, ou seja, $y \in \mathrm{GF}_q^*$.

   Veja que para cada $b \in \mathrm{GF}_q$ fixado, há no máximo $(q^t-1)/(q-1)$ valores de x com $N(x) = b$, pois o polinômio $x^{(q^t-1)/(q-1)} - b$ tem no máximo $(q^t-1)/(q-1)$ raízes em $\mathrm{GF}_{q,t}$. Se $b = 0$, então só há uma raiz ($x = 0$).

   Há $q^t - 1$ elementos em $\mathrm{GF}_{q^t}^*$ e $q - 1$ elementos em GF_q^*, logo, como cada elemento de $\mathrm{GF}_{q^t}^*$ é levado a um elemento de GF_q^*, para cada $b \in \mathrm{GF}_q^*$ devemos ter exatamente $(q^t-1)/(q-1)$ valores de $x \in \mathrm{GF}_{q^t}^*$ com $N(x) = b$.

   Fixe um vértice a. O grau de a é dado pelo número de soluções de $N(x + a) = 1$. Pelo argumento acima, há $(q^t-1)/(q-1)$ valores de x que satisfazem a igualdade e, portanto, a tem $(q^t-1)/(q-1)$ vizinhos.

3. $\mathrm{NG}_{q,t}$ **não contém um $K_{t,t!+1}$.**
   São utilizadas técnicas de geometria algébrica para provar esse resultado (tal prova está fora do escopo deste trabalho).

4. **O maior auto-valor do grafo é $(q^t-1)/(q-1)$ e o valor absoluto de todos os demais auto-valores é limitado superiormente por $q^{t/2}(q-2)/(q-1)$ (que é $< \sqrt{n}$).**

5.4 Caracteres de Grupos

Definição (caractere). *3 Se G é um grupo, e $\chi : G \to \mathbb{C}^*$ é um homomorfismo de G no grupo multiplicativo dos números complexos, χ é um* caractere *do grupo G.*

Algumas propriedades de caracteres de um grupo G:

(a) Todo elemento $s \in G$ é levado a uma raiz n-ésima da unidade, onde $n = |G|$. Para ver isso, note que $s^n = 1$ em G e que todo caractere χ é um homomorfismo. Então devemos ter $\chi(s)^n = \chi(s^n) = \chi(1) = 1$.

(b) Se G é abeliano há exatamente $|G|$ caracteres distintos de G, e eles são dois a dois ortogonais (em relação ao produto interno em $\mathbb{C}^{|G|}$).

Vamos demonstrar a propriedade 4b. Sejam χ_j e χ_k dois caracteres distintos de G e $s \in G$ tal que $\chi_j(s) \neq \chi_k(s)$. Seja n a ordem de s. A partir da propriedade 4a, podemos assumir que $\chi_j(s) = \zeta^j$ e $\chi_k(s) = \zeta^k$, onde $\zeta = e^{2\pi \boldsymbol{i}/n}$. Temos

$$\sum_{l=1}^{n} \chi_j(s^l)\overline{\chi_k(s^l)} = \sum_{l=1}^{n} \zeta^{jl}\overline{\zeta^{kl}} = \sum_{l=1}^{n} \zeta^{l(j-k)} = \sum_{l=1}^{n} (\zeta^{j-k})^l = 0.$$

É sabido que G pode ser particionado em classes laterais de $H = \langle s \rangle$ (grupo gerado pelo elemento s). Sendo assim, sejam $a_1, \ldots, a_t$ representantes das classes laterais $C_1, \ldots, C_t$, onde $t = [G : H]$. Temos

$$\begin{aligned}\langle \boldsymbol{\chi}_j, \boldsymbol{\chi}_k \rangle = \sum_{r=1}^{t} \sum_{u \in C_r} \chi_j(u)\overline{\chi_k(u)} &= \sum_{r=1}^{t} \sum_{l=1}^{n} \chi_j(a_r s^l)\overline{\chi_k(a_r s^l)} \\ &= \sum_{r=1}^{t} \chi_j(a_r)\overline{\chi_k(a_r)} \sum_{l=1}^{n} \chi_j(s^l)\overline{\chi_k(s^l)} = 0.\end{aligned}$$

Note que ao provarmos que dois caracteres distintos são ortogonais, mostramos que todos eles são linearmente independentes nos complexos e, portanto, não podemos ter mais do que $|G|$ caracteres (que é a dimensão do espaço).

Para mostrarmos que há exatamente $|G|$ caracteres distintos, vamos utilizar o Teorema Fundamental de Grupos Abelianos Finitos. Este teorema nos diz que um grupo G, abeliano e finito, é isomorfo ao produto cartesiano de grupos cíclicos cujas ordens são potências de primos, então

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k},$$

com $n_1 \times \cdots \times n_k = |G|$ e $n_i | n_{i+1}$ para $i = 1, \ldots, k-1$. Seja $\psi : G \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ o isomorfismo caracterizado acima.

Veja que podemos definir caracteres φ_i para $\mathbb{Z}_{n_i}$ e há exatamente n_i opções para φ_i, já que $\mathbb{Z}_{n_i}$ é cíclico de ordem n_i. Se $a \in G$, podemos definir um caractere de G como

$$\chi(a) = \varphi_1(\psi(a)_1) \ldots \varphi_k(\psi(a)_k).$$

É simples ver que χ é bem definida e é um homomorfismo.

Para cada escolha possível dos φ_i temos um único caractere χ de G. Podemos ver isso verificando que

$$\chi(\psi^{-1}(1, \ldots, 1, b, 1, \ldots, 1)) = \varphi_1(1) \ldots \varphi_j(b) \ldots \varphi_k(1) = \varphi_j(b),$$

pois cada φ_i é um homomorfismo. Sendo assim, se mudarmos qualquer um dos caracteres φ_i teremos mudado o caractere χ.

Como há n_i opções para cada φ_i e podemos escolher cada uma delas independentemente, temos um total de $n_1 \times \cdots \times n_k = |G|$ caracteres possíveis para G. Na verdade, podemos provar algo mais forte usando a idéia acima: se G' é o grupo de caracteres de G então $G \cong G'$.

Vamos limitar os auto-valores de $\mathrm{NG}_{q,t}$ e demonstrar a propriedade 4. Sejam χ um caractere do grupo aditivo de GF_{q^t} e A a matriz de adjacência de $\mathrm{NG}_{q,t}$. Vendo $\boldsymbol{\chi}$ como um vetor coluna (indexado pelos elementos de GF_{q^t}, assim como as linhas e colunas de A), temos

$$(A\boldsymbol{\chi})_a = \sum_{N(a+b)=1} \chi(b) = \sum_{N(c)=1} \chi(c-a) = \sum_{N(c)=1} \chi(c)\chi(-a) = \sum_{N(c)=1} \chi(c)\overline{\chi(a)}.$$

Logo, $A\boldsymbol{\chi} = (\sum_{N(c)=1} \chi(c))\overline{\boldsymbol{\chi}}$ e então

$$A^2\boldsymbol{\chi} = \sum_{N(c)=1} \chi(c) A\overline{\boldsymbol{\chi}} = \sum_{N(c)=1} \chi(c) \overline{\sum_{N(c)=1} \chi(c)}\boldsymbol{\chi} = \left|\sum_{N(c)=1} \chi(c)\right|^2 \boldsymbol{\chi}, \text{ pois}$$

$$(A\overline{\boldsymbol{\chi}})_a = \sum_{N(a+b)=1} \overline{\chi(b)} = \sum_{N(a+b)=1} \chi(-b) = \sum_{N(c)=1} \chi(a-c)$$
$$= \sum_{N(c)=1} \overline{\chi(c)}\chi(a) = \overline{\sum_{N(c)=1} \chi(c)}\chi(a).$$

A partir da propriedade 4b, sabemos que os vetores dos caracteres são ortogonais e geram todo o espaço (pois há n caracteres distintos), logo todos os auto-vetores e auto-valores estão determinados.

É simples ver que se H é um grafo d-regular, o maior auto-valor de H é d e um auto-vetor correspondente é $(1, 1, \ldots, 1)$. Para demonstrar tal fato, basta tomar $\mathbf{x}$ com $|x_i| \leq 1$ para $i = 1, \ldots, n$, $|x_j| = \max\{|x_1|, \ldots, |x_n|\}$ e verificar que se $\mathbf{A}$ é a matriz de incidência do grafo, temos

$$|(\mathbf{Ax})_j| = \left|\sum_k A_{j,k}x_k\right| \leq \sum_k |A_{i,k}||x_k| \leq |x_j| \sum_k |A_{i,k}| = d|x_j|. \tag{6}$$

A partir da observação acima, vemos que o maior auto-valor do grafo é $\sum_{N(c)=1} 1 = (q^t - 1)/(q - 1)$, correspondento ao caractere trivial. Os demais (que são reais, pois $\mathbf{A}$ é simétrica) estão entre $\pm|\sum_{N(c)=1} \chi(c)|$.

Teorema 5.2. *Para um caractere aditivo (não trivial) χ de GF_{q^t}, $a \neq 0$ em GF_{q^t} e $d \geq 1$, temos*

$$\left|\sum_{x \in \mathrm{GF}_{q^t}} \chi(ax^d)\right| \leq (d-1)\sqrt{q^t}.$$

A demonstração se encontra no Apêndice (teorema A.1).

Note que para todo valor $c \in \mathrm{GF}_q^*$, existem exatamente $q-1$ valores d satisfazendo $d^{q-1} = c$. Além disso, $N(d^{q-1}) = d^{q^t-1} = 1$. O polinômio $f(x) = x^{q-1}$ claramente se encaixa nas condições do teorema 5.2. A partir das observações acima, temos

$$\left|\sum_{N(c)=1} \chi(c)\right| = \left|\frac{1}{q-1}\sum_{d\in \mathrm{GF}_{q^t}} \chi(f(d))\right| \leq \frac{q-2}{q-1} q^{t/2}.$$

5. $\alpha(\mathrm{NG}_{q,t}) = O(n^{1/2+1/t})$ **(estamos omitindo os laços de** $\mathrm{NG}_{q,t}$**).**

6. **Para cada** $k \leq \lceil t/2 \rceil$**, o número de cliques de tamanho** k **em** $\mathrm{NG}_{q,t}$ **é**

$$(1+o(1))\frac{1}{k!} n^{k-\binom{k}{2}/t}.$$

5.5 Mais Lemas Preliminares

Os dois lemas a seguir são apresentados em [1, cap. 9].

Lema 5.4. *Seja $G = (V, E)$ um grafo d-regular com n vértices. Suponha que o valor absoluto de todos os auto-valores (exceto o maior) seja no máximo λ. Para um vértice $v \in V$ e $B \subset V$, denotamos por $N(v)$ o conjunto de todos os vizinhos de v em G. Seja $N_B(v) = N(v) \cap B$. Então, para cada conjunto $B \subset V$ de cardinalidade $|B| = bn$,*

$$\sum_{v\in V} (|N_B(v)| - bd)^2 \leq \lambda^2 b(1-b)n.$$

Demonstração. Seja $\mathbf{A}$ a matriz de adjacência de G. Primeiro vamos mostrar que para todo vetor $\mathbf{u}$ com $\sum_i u_i = 0$, temos $\langle \mathbf{Au}, \mathbf{Au}\rangle \leq \lambda^2 \langle \mathbf{u}, \mathbf{u}\rangle$. Como $\mathbf{A}$ é simétrica, ela é diagonalizável e, portanto, existe uma base de n auto-vetores de $\mathbf{A}$. A partir da observação em (6), sabemos que o maior auto-valor de A corresponde a auto-valores cujas coordenadas são todas iguais.

Então temos que $\mathbf{u}$ é ortogonal ao auto-vetor correspondente a d. Seja $\mathbf{X} = [\mathbf{x}_1 \ldots \mathbf{x}_n]$ uma base ortonormal de auto-vetores de $\mathbf{A}$. Podemos expressar $\mathbf{u}$ como $\mathbf{u} = \sum_k \langle \mathbf{x}_k, \mathbf{u}\rangle \mathbf{x}_k$; basta ver que $\mathbf{X}^{-1} = \mathbf{X}^T$ (pois $\mathbf{X}$ é ortonormal) e, se $\mathbf{u} = \sum_k w_k \mathbf{x}_k = \mathbf{Xw}$, então $\mathbf{w} = \mathbf{X}^{-1}\mathbf{u} = \mathbf{X}^T\mathbf{u}$, ou seja, $w_k = \langle \mathbf{x}_k, \mathbf{u}\rangle$, como queríamos.

Sejam λ_k os auto-valores associados aos $\mathbf{x}_k$. Temos $\langle \mathbf{Au}, \mathbf{Au}\rangle = (\mathbf{Au})^T\mathbf{Au} = \mathbf{u}^T\mathbf{A}^T\mathbf{Au} = \mathbf{u}^T\mathbf{A}^2\mathbf{u}$. Expressando $\mathbf{u}$ da forma acima, utilizando a linearidade de transformações lineares e os auto-valores associados a cada auto-vetor, temos

$$\begin{aligned}\langle \mathbf{Au}, \mathbf{Au}\rangle &= \mathbf{u}^T \sum_k \langle \mathbf{x}_k, \mathbf{u}\rangle \mathbf{A}^2\mathbf{x}_k = \mathbf{u}^T \sum_k \langle \mathbf{x}_k, \mathbf{u}\rangle \lambda_k^2 \mathbf{x}_k \\ &= \sum_k \langle \mathbf{x}_k, \mathbf{u}\rangle \lambda_k^2 \mathbf{u}^T\mathbf{x}_k = \sum_k \langle \mathbf{x}_k, \mathbf{u}\rangle^2 \lambda_k^2.\end{aligned}$$

O maior auto-valor, d, não aparece na soma pois $\mathbf{u}$ é ortogonal ao auto-vetor correspondente a d, sendo assim

$$\langle \mathbf{Au}, \mathbf{Au} \rangle = \sum_k \langle \mathbf{x}_k, \mathbf{u} \rangle^2 \lambda_k^2 \leq \lambda^2 \sum_k \langle \mathbf{x}_k, \mathbf{u} \rangle^2 \leq \lambda^2 \sum_k w_k^2 = \lambda^2 \mathbf{w}^T \mathbf{w}.$$

Agora basta trocar $\mathbf{w}$ por $\mathbf{u}$, já que

$$\langle \mathbf{Au}, \mathbf{Au} \rangle \leq \lambda^2 \mathbf{w}^T \mathbf{w} = \lambda^2 \mathbf{w}^T \mathbf{X}^T \mathbf{X} \mathbf{w} = \lambda^2 (\mathbf{Xw})^T \mathbf{Xw} = \lambda^2 \mathbf{u}^T \mathbf{u} = \lambda^2 \langle \mathbf{u}, \mathbf{u} \rangle.$$

Defina $\mathbf{f}$ (indexado por V) tal que $f_v = 1 - b$ se $v \in B$ e $f_v = -b$ se $v \notin B$. É simples ver que $\sum_{v \in V} f_v = |B|(1-b) - b(n - |B|) = 0$, lembrando que $|B| = bn$ por definição. Pelo que foi provado acima, temos $\langle \mathbf{Af}, \mathbf{Af} \rangle \leq \lambda^2 \langle \mathbf{f}, \mathbf{f} \rangle$. Note que o lado direito é igual a $\lambda^2(bn(1-b)^2 + (1-b)nb^2) = \lambda^2 b(1-b)n$, já o lado esquerdo é igual a

$$\sum_{v \in V} ((1-b)|N_B(v)| - b(d - |N_B(v)|))^2 = \sum_{v \in V} (|N_B(v)| - bd)^2.$$

□

Lema 5.5. *Sejam $G = (V, E)$, d, n e λ como no enunciado do lema 5.4. Então para quaisquer conjuntos B, C, defina $e_{B,C} = \#\{\{u, v\} \mid u \in B, v \in C, \{u, v\} \in E\}$. Temos*

$$\left| e_{B,C} - \frac{d}{n} |B||C| \right| \leq \lambda \sqrt{|B||C|}.$$

Demonstração. Seja $|B| = bn$ e $|C| = cn$. Pelo lema 5.4, sabemos que

$$\sum_{v \in C} (|N_B(v)| - bd)^2 \leq \sum_{v \in V} (|N_B(v)| - bd)^2 \leq \lambda^2 b(1-b)n.$$

Como $e_{B,C} - |B||C|d/n = e_{B,C} - cbdn = \sum_{v \in C} (|N_B(v)| - bd)$, temos, por Cauchy-Schwarz,

$$\Big[\sum_{v \in C} (|N_B(v)| - bd) \Big]^2 \leq |C| \sum_{v \in C} (|N_B(v)| - bd)^2 \leq |C| \lambda^2 b(1-b)n \leq \lambda^2 |B||C|,$$

o que demonstra a desigualdade deste lema.

□

A propriedade 5 segue do lema acima, já que $e_{B,B} \leq |B|$ (B pode possuir laços), como $|e_{B,B} - |B|^2 d/n| \geq |B|^2 d/n - |B|$, temos $|B|^2 d/n - |B| \leq \sqrt{n}|B|$ com $d = (1 + o(1))n^{1-1/t}$. Logo, $|B| \leq O(n^{1/2+1/t})$, como queríamos.

Definição. *3 Seja G um grafo. Considere mapas injetores aleatórios do conjunto de vértices de G no conjunto de vértices de $\mathrm{NG}_{q,t}$. Definimos f como uma* imersão *de G se f leva cada aresta de G a uma aresta de $\mathrm{NG}_{q,t}$. Denotamos por $A(G)$ o evento em que toda aresta de G é levada a uma aresta de $\mathrm{NG}_{q,t}$.*

Lema 5.6. *Seja G um grafo com menos de $1 + t/2$ vértices e r arestas. Então*

$$\mathbb{P}[A(G)] = (1 + o(1))n^{-\frac{r}{t}}.$$

Demonstração. Precisaremos de alguns resultados simples de manipulação assintótica:

(i) Se $x = (1 + o(1))f(n)$ e $y = (1 + o(1))g(n)$, onde $o(1) \to 0$ quando $n \to \infty$, vale que $xy = (1 + o(1))f(n)g(n)$ e $x/y = (1 + o(1))f(n)/g(n)$.

Para ver isso, note que existem seqüências $\{a_n\}_{n=1}^{\infty}$ e $\{b_n\}_{n=1}^{\infty}$ tais que $x = (1+a_n)f(n)$ e $y = (1 + b_n)g(n)$, onde $a_n, b_n \to 0$ quando $n \to \infty$. Defina $c_n = (1 + a_n)(1 + b_n) - 1$ e $d_n = (1 + a_n)/(1 + b_n) - 1$. É simples ver que $c_n, d_n \to 0$ quando $n \to \infty$. Temos

$$xy = (1 + c_n)f(n)g(n) \text{ e } x/y = (1 + d_n)f(n)/g(n),$$

ou seja, $xy = (1 + o(1))f(n)g(n)$ e $x/y = (1 + o(1))f(n)/g(n)$.

(ii) Se $x = (1 + o(1))n^p + O(n^q)$, com $q < p$ então $x = (1 + o(1))n^p$, ou seja, o termo $O(n^q)$ pode ser desprezado.

Como no item anterior, $x = (1 + a_n)n^p + O(n^q)$. Temos $x = (1 + a_n + O(n^{q-p}))n^p$. Mas claramente o termo $O(n^{q-p}) \to 0$ quando $n \to \infty$. Logo, $x = (1 + o(1))n^p$, como queríamos.

Vamos demonstrar o lema usando indução no número de vértices e arestas. O caso $n = 1$ é trivial. Suponha que o lema valha para todo grafo menor que G, com r arestas e $s < 1+t/2$ vértices. Seja $G_{u,v}$ o grafo obtido de G eliminando-se a aresta $\{u, v\}$. Seja $G_u = G - v$ (G_v é definido analogamente). Além disso, defina $G' = G - u - v$. Seja r' o número de arestas de G'. Note que $r - r' < t - 1$, pois os vértices u e v poderiam possuir, no total $(s - 1) + (s - 2)$ arestas.

Utilizando as regras de probabilidade condicional, podemos afirmar que $\mathbb{P}[A(G_{u,v})] = \mathbb{P}[A(G_{u,v})|A(G')].\mathbb{P}[A(G')]$. Por hipótese, $\mathbb{P}[A(G_{u,v})] = (1 + o(1))n^{(1-r)/t}$ e $\mathbb{P}[A(G')] = (1 + o(1))n^{-r'/t}$, então

$$\mathbb{P}[A(G_{u,v})|A(G')] = (1 + o(1))n^{-\frac{r-r'-1}{t}}.^{\dagger}$$

Defina $\nu(u, f')$ como o número de extensões de f' a uma imersão de G_u; $\nu(v, f')$ é o análogo para v. Podemos construir uma extensão de f' a uma imersão de $G_{u,v}$ escolhendo valores para $f'(u)$ e $f'(v)$. Há exatamente $\nu(u, f')$ valores permitidos a $f'(v)$ e $\nu(v, f')$ valores permitidos a $f'(u)$. Como desejamos que f' seja injetora, não podemos ter $f'(u) = f'(v)$. Sendo assim, como $\{u, v\}$ não está em $G_{u,v}$, há entre $\nu(u, f')\nu(v, f') - \min(\nu(u, f'), \nu(v, f'))$

[†]Note que podemos fazer n crescer arbitrariamente quando t está fixado (aumentando o valor de q). Sendo assim, podemos considerar que $n \to \infty$ sem qualquer preocupação com o parâmetro t e aplicar o resultado de (i).

e $\nu(u,f')\nu(v,f')$ maneiras de extendermos f' a uma imersão de $G_{u,v}$. No total existem $(n-s+2)(n-s+1)$ maneiras de valorar $f'(u)$ e $f'(v)$. Logo,

$$\frac{\nu(u,f')\nu(v,f') - \min(\nu(u,f'),\nu(v,f'))}{(n-s+2)(n-s+1)} \leq \mathbb{P}[A(G_{u,v})|f'] \leq \frac{\nu(u,f')\nu(v,f')}{(n-s+2)(n-s+1)}. \quad (7)$$

Vamos calcular a seguinte esperança

$$\begin{aligned}
&\mathbb{E}[\mathbb{P}[A(G_{u,v})|f']|A(G')] = \sum_{f'} \mathbb{P}[A(G_{u,v})|f']\,\mathbb{P}[f'|A(G')] \\
=&\sum_{f'} \mathbb{P}[A(G_{u,v})|f'] \frac{\mathbb{P}[f' \wedge A(G')]}{\mathbb{P}[A(G')]} = \frac{1}{\mathbb{P}[A(G')]} \sum_{f'} \mathbb{P}[A(G_{u,v})|f']\,\mathbb{P}[f'] \\
=&\frac{\mathbb{P}[A(G_{u,v})]}{\mathbb{P}[A(G')]} = \mathbb{P}[A(G_{u,v})|A(G')] = (1+o(1))n^{-\frac{r-r'-1}{t}}.
\end{aligned}$$

Evidentemente, $\min(\nu(u,f'),\nu(v,f')) \leq n$. A partir de (7), obtemos

$$\mathbb{E}[\nu(u,f')\nu(v,f')|A(G')] = (1+o(1))n^{\frac{r'-r+1}{t}}(n-s+2)(n-s+1) + O(n).$$

Note que $(r'-r+1)/t > -1$ e que $(n-s+2)(n-s+1) = (1+o(1))n^2$. Então, de acordo com (ii), temos

$$\mathbb{E}[\nu(u,f')\nu(v,f')|A(G')] = (1+o(1))n^{2-\frac{r-r'-1}{t}}.$$

Seja f um mapa injetor aleatório de V_G no conjunto de vértices de $\mathrm{NG}_{q,t}$. Seja f' uma imersão de G' fixado. Então $\mathbb{P}[A(G)|f\big|_{V_G\setminus\{u,v\}} = f']$ é o número de extensões de f' a uma imersão de G dividido pelo número de escolhas possíveis para as imagens de u e v.

Seja B o conjunto das possíveis imagens de u nas quais a extensão obtida é uma imersão de G_v; C é definido de forma análoga para v. Note que $|B| = \nu(u,f')$ e $|C| = \nu(v,f')$.

Sabemos que $\mathrm{NG}_{q,t}$ é regular, seu grau é $(q^t-1)/(q-1)$ (assintoticamente $n^{1-1/t}$) e o valor absoluto de todos os seus auto-valores (exceto o maior) é limitado por $\sqrt{n}$. Temos as condições necessárias para aplicar o lema 5.5, portanto,

$$|e_{B,C} - n^{-\frac{1}{t}}|B||C|| \leq \sqrt{n|B||C|}.$$

O número de arestas entre B e C é dado por

$$e_{B,C} = n^{-\frac{1}{t}}\nu(u,f')\nu(v,f') + \delta, \text{ com } |\delta| \leq \sqrt{n.\nu(u,f')\nu(v,f')}.$$

Para obtermos uma extensão de f' a uma imersão de G na qual $u \mapsto x$ e $v \mapsto y$, devemos ter $x \in B$, $y \in C$, $x \neq y$ e $\{x,y\} \in E(\mathrm{NG}_{q,t})$.

Portanto o número de possíveis extensões de f' a uma imersão de G é dado por $e_{B,C}$ menos o número de laços em $B \cap C$. Como $|B \cap C| \leq \min(\nu(u,f'),\nu(v,f')) \leq \sqrt{\nu(u,f')\nu(v,f')}$ vemos que os casos contados em $e_{B,C}$ que não são extensões válidas são poucos e podem ser incluídos num fator de erro bem limitado, ou seja,

$$\mathbb{P}[A(G)|f\big|_{V_G\setminus\{u,v\}} = f'] = \frac{n^{-\frac{1}{t}}\nu(u,f')\nu(v,f') + \delta}{(n-s+2)(n-s+1)},$$

com $|\delta| \leq \sqrt{n.\nu(u,f')\nu(v,f')}$.

Agora repetimos a idéia anterior e vamos calcular a esperança de $\mathbb{P}[A(G)|f\big|_{V_G\setminus\{u,v\}} = f']$ sobre todas as imersões f'. Ao fazer isso, obtemos $\mathbb{P}[A(G)|A(G')]$ no lado esquerdo e, no lado direito, obtemos $(1+o(1))n^{(r-r')/t}$ mais a esperança dos erros, que pode ser limitada, pela desigualdade de Jensen, em

$$\frac{\sqrt{n\,\mathbb{E}[\nu(u,f')\nu(v,f')|A(G')]}}{(n-s+2)(n-s+1)} = (1+o(1))n^{-\frac{t-1+r-r'}{2t}}$$

Como para a nossa escolha de parâmetros, $t-1+r-r' > 2(r-r')$, podemos utilizar (ii) para concluir que $\mathbb{P}[A(G)|A(G')] = (1+o(1))n^{(r'-r)/t}$ e, por (i), $\mathbb{P}[A(G)] = (1+o(1))n^{-r/t}$. □

A partir do lema acima, concluimos que o número de k-cliques, com $k \leq \lceil t/2 \rceil$ em $\mathrm{NG}_{q,t}$ é

$$\binom{n}{k}\mathbb{P}[A(K_k)] = \binom{n}{k}(1+o(1))n^{-\binom{k}{2}/t} = (1+o(1))\frac{n^{k-\binom{k}{2}/t}}{k!},$$

que é precisamente a propriedade 6.

Retornando a demonstração do teorema principal, tomamos $k = \lceil t/2 \rceil$ (pois queremos uma construção com o maior número possível de vértices). Vamos limitar o tamanho de um clique em $\mathrm{CQ}_k(\mathrm{NG}_{q,t})$. Para isso, usaremos o seguinte lema.

Lema 5.7. *Para todo t, existe uma constante C_t tal que todo grafo com m vértices e pelo menos $C_t m^{2-1/t}$ arestas contém $K_{t,t!+1}$ como subgrafo.*

Demonstração. Vamos contar, para cada vértice $x \in V_G$ o número de t-conjuntos de vértices, onde cada vértice do conjunto é um vizinho de x. Esse número é dado por

$$\sum_{x\in V_G}\binom{d(x)}{t},$$

onde $d(x)$ é o grau do vértice x e convencionamos que quando $t > d(x)$ o valor da binomial é 0.

Podemos nos perguntar quantas vezes um t-conjunto foi contado na soma acima. Se algum conjunto foi contado pelo menos $t! + 1$ vezes, então temos um $K_{t,t!+1}$. Se

$$\sum_{x \in V_G} \binom{d(x)}{t} \geq \binom{m}{t}(t! + 1),$$

algum t-conjunto foi contado pelo menos $t! + 1$ vezes.

Se $f(k) = \binom{k}{t}$, então f é uma função convexa. Então podemos aplicar a desigualdade de Jensen na soma acima, obtendo

$$\sum_{x \in V_G} f(d(x)) \geq mf\left(\frac{\sum_{x \in V_G} d(x)}{m}\right) = mf(C_t m^{1-1/t}/2).$$

Quando $k \geq t$, as seguintes desigualdades valem (veja o lema 4.1)

$$\left(\frac{k}{t}\right)^t \leq f(k) \leq \left(\frac{ke}{t}\right)^t,$$

onde e é a base do logaritmo natural.

Reunindo todas as proposições acima, temos

$$\sum_{x \in V_G} \binom{d(x)}{t} \Big/ \binom{m}{t} \geq m\left(\frac{C_t m^{1-1/t}}{2t}\right)^t \Big/ \left(\frac{me}{t}\right)^t = m\left(\frac{C_t m^{1-1/t}}{2me}\right)^t = \left(\frac{C_t}{2e}\right)^t,$$

e é imediato verificar que tomando, por exemplo, $C_t = 2te$, [†] temos

$$\sum_{x \in V_G} \binom{d(x)}{t} \geq \binom{m}{t}(t! + 1).$$

□

Se tomarmos $l(1 - t/l) > (2C_t)^t k^{2t-1}$, então $\binom{l}{2} > C_t(kl)^{2-1/t}$. Para ver isso, note que $(1 - 1/l)^t \geq 1 - t/l$ (o resultado sai facilmente por indução em t). Agora basta ver que $l(1 - 1/l)^t > (2C_t)^t k^{2t-1}$, e

$$\binom{l}{2} = \frac{1}{2} l^{2-1/t}\left[l\left(1 - \frac{1}{l}\right)^t\right]^{\frac{1}{t}} > \frac{1}{2} l^{2-1/t} 2C_t k^{2-1/t} = C_t(kl)^{2-1/t}.$$

A partir do lema 5.3, concluimos que $\mathrm{CQ}_k(\mathrm{NG}_{q,t})$ não pode ter um clique de tamanho $> k!(l-1)^k$ já que $\mathrm{NG}_{q,t}$ não possui um $K_{t,t!+1}$.

[†]Para simplificar a demonstração, fomos um pouco generosos na constante, de fato, bastaria tomar $C_t = (1 + o(1))t/2e$.

5.6 Analisando Assintoticamente os Parâmetros

Como $k = \lceil t/2 \rceil$, a partir da propriedade 6, concluimos que o grafo $\mathrm{CQ}_k(\mathrm{NG}_{q,t})$ tem $n^{t \times c_{q,t}}$ vértices, onde $c_{q,t} \to 3/8$ quando $q, t \to \infty$. Conseguimos obter um grafo com $n^{\Omega(t)}$ vértices, sem conjuntos independentes maiores que $O(n^{1/2+1/t})$ (propriedade 5 e 5.1) e sem cliques de tamanho $s = k!l^k$, para algum $l < t^{3t}$.

Vamos encerrar com uma análise dos parâmetros m e s. Temos

$$s = \left\lceil \frac{t}{2} \right\rceil ! (t^{\Theta(t)})^{\lceil t/2 \rceil}.$$

Utilizando a aproximação de Stirling e eliminado os tetos para simplificar, obtemos

$$s = \sqrt{t\pi} \left(\frac{t}{2} \right)^{\frac{t}{2}} (t^{\Theta(t)})^{\frac{t}{2}} = t^{\Theta(t^2)}.$$

Aplicando $\log$ em ambos os lados, temos $\log s = \Theta(t^2) \log t$. Tirando a raiz quadrada, chegamos em $\sqrt{\log s} = \Theta(t)\sqrt{\log t}$. Concluimos que

$$\sqrt{\frac{\log s}{\log t}} = \Theta(t).$$

Portanto, $t = c\sqrt{\log s / \log t}$ para alguma constante c. Sendo assim,

$$\frac{\log s}{\log t} = \frac{\log s}{1/2 \times \log \frac{\log s}{\log t} + O(1)} = \frac{\log s}{1/2 \times (\log\log s - \log\log t) + O(1)}.$$

Como $s \gg t$,

$$\sqrt{\frac{\log s}{\log\log s}} = \Theta(t).$$

Dado um inteiro $s > 0$, podemos obter um valor inteiro para t (a partir das várias equações acima que relacionam s, t e l). Com t fixado, basta determinar um valor para q e assim obter n. Precisamos de q (potência de primo) suficientemente grande para que o lema 5.6 possa ser usado na contagem de cliques de $\mathrm{NG}_{q,t}$. Sendo assim, para algum q suficientemente grande, a construção possui $n^{\Omega(t)}$ vértices.

Tomamos $m = O(n^{1/2+1/t})$ (a prop. 5 nos diz que o grafo construído não tem conjuntos independentes maiores que $O(n^{1/2+1/t})$). Portanto, $n^{\Omega(t)} = m^{\Omega(t)}$ e

$$R(s,m) \geq m^{\Omega\left(\sqrt{\frac{\log s}{\log\log s}}\right)},$$

para infinitos valores de m. Como potências de primos são abundantes, podemos afirmar que o teorema 5.1 vale para todo m suficientemente grande.

6 Construções de grafos de Ramsey evitando triângulos

6.1 Resultado Principal

Podemos obter construções melhores do que a construção geral acima para o caso em que queremos evitar apenas triângulos (cliques com 3 vértices) e limitar o tamanho dos conjuntos independentes. Essa construção obtém uma grafo com $\Omega(m^{3/2})$ vértices sem triângulos e sem conjuntos independentes de tamanho m, fornecendo uma cota construtiva para $R(m, 3)$. Esta seção é baseada no artigo [5].

6.2 A Construção

Vamos utilizar a seguinte definição que será importante para o desenvolvimento das idéias que seguem.

Definição (Grafo de Cayley). *3 Seja Γ um grupo (aqui estamos utilizando grupos finitos e abelianos) e A um conjunto simétrico $A = -A$. Definimos o* grafo de Cayley $G(\Gamma, A)$ *como um grafo cujos vértices são elementos de Γ e dois vértices u e v estão ligados se e somente se $u - v \in A$.*

Vamos mostrar a idéia de construção de um grafo livre de triângulos que evita conjuntos independentes grandes. Seja $F_k = \mathrm{GF}(2^k)$ o corpo com 2^k elementos. Podemos representar cada elemento desse corpo como um vetor binário de k bits. Suponha que 3 não divida k e seja $n = 2^{3k}$. Definimos W_0 como o conjunto dos elementos $\alpha \in F_k^*$ tais que o bit mais a esquerda da representação binária de α^7 é 0. O conjunto W_1 é formado pelos elementos $\alpha \in F_k^*$ tais que o bit mais a esquerda da representação binária de α^7 é 1.

Como 3 não divide k, temos $|F_k^*| = 2^k - 1 \not\equiv 0 \pmod 7$ e o mapa $\alpha \mapsto \alpha^7$ é bijetor. Suponha que s seja o gerador de F_k^*. Se $\alpha, \beta \in F_k^*$, então $\alpha = s^i$ e $\beta = s^j$ para algum par de inteiros i e j. Então $\alpha^7 = s^{7i}$ e $\beta^7 = s^{7j}$, concluimos que $\alpha^7 = \beta^7$ se e somente se $s^{7(i-j)} = 1$, mas isso ocorre se e somente se $2^k - 1$ divide $7(i - j)$, o que acontece se e somente se $\alpha = \beta$.

É simples ver que $|W_0| = 2^{k-1} - 1$ e $|W_1| = 2^{k-1}$. Definimos G_n como um grafo cujos vértices são vetores binários de comprimento $3k$ e dois vértices u e v são ligados por uma aresta se e somente se existe $w_0 \in W_0$ e $w_1 \in W_1$ tais que $u+v = (w_0, w_0^3, w_0^5)+(w_1, w_1^3, w_1^5)$, onde as potências são calculadas no corpo F_k e a soma é feita módulo 2. Veja que tal soma corresponde a soma no corpo F_k, pois $F_k \cong \mathrm{GF}(2)[X]/\langle q(X)\rangle$, onde $q(X)$ é algum polinômio irredutível de grau k.

Note que G_n é o grafo de Cayley para o grupo aditivo $\mathbb{Z}_2^{3k}$ em relação ao conjunto gerador $S = U_0 + U_1 = \{u_0 + u_1 \mid u_0 \in U_0, u_1 \in U_1\}$, onde $U_0 = \{(w_0, w_0^3, w_0^5) \mid w_0 \in W_0\}$ e U_1 é definido de forma análoga.

Para limitar o tamanho dos conjuntos independentes do grafo G_n faremos uso da função ϑ de Lovász. Esta função é definida como segue. Se $G = (V, E)$ é um grafo, uma *rotulação ortonormal* de G é uma família $(\mathbf{b}_v)_{v\in V}$ de vetores unitários num espaço Euclidiano tal que

se u e v são vértices distintos não adjacentes, então $\langle \mathbf{b}_u, \mathbf{b}_v \rangle = 0$. Definimos $\vartheta(G)$ como o mínimo, sobre todas as rotulações ortonormais e todos os vetores unitários $\mathbf{c}$, de

$$\max_{v \in V} \frac{1}{\langle \mathbf{c}, \mathbf{b}_v \rangle^2}. \tag{8}$$

Um resultado simples (veja [6]) relaciona a função ϑ e o número de independência $\alpha(G)$.

Lema 6.1. *Para todo grafo G, temos $\alpha(G) \leq \vartheta(G)$.*

Demonstração. Seja $\mathbf{c}$ um vetor unitário e $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ uma rotulação ortonormal que minimiza (8). Suponha que os vértices do grafo são $\{1, 2, \ldots, n\}$ e que $\{1, \ldots, k\}$ seja um conjunto independente de tamanho máximo. Os vetores $\{\mathbf{u}_1, \ldots, \mathbf{u}_k\}$ são dois a dois ortogonais por hipótese. Note que podemos construir uma matriz unitária (ortonormal) $\mathbf{U}$, cujas k primeiras linhas são os vetores $(\mathbf{u}_i)_{i=1}^k$. É simples ver que $\|\mathbf{Uc}\| = \|\mathbf{c}\| = 1$. Sendo assim,

$$1 \geq \sum_{i=1}^{k} (\mathbf{Uc})_i^2 = \sum_{i=1}^{k} \langle \mathbf{c}, \mathbf{u_i} \rangle^2.$$

Por hipótese, $\vartheta(G) \geq 1/\langle \mathbf{c}, \mathbf{u_i} \rangle^2$ para todo $1 \leq i \leq n$. Portanto, $1/\vartheta(G) \leq \langle \mathbf{c}, \mathbf{u_i} \rangle^2$, donde concluimos que

$$1 \geq \sum_{i=1}^{k} \langle \mathbf{c}, \mathbf{u_i} \rangle^2 \geq \frac{k}{\vartheta(G)} = \frac{\alpha(G)}{\vartheta(G)}.$$

Portanto, $\alpha(G) \leq \vartheta(G)$. □

6.3 Propriedades do grafo G_n

Se 3 não divide k e $n = 2^{3k}$, vale

1. G_n é d_n-regular, onde $d_n = 2^{k-1}(2^{k-1} - 1)$;
2. G_n é livre de triângulos;
3. todo autovalor μ de G_n satisfaz

$$-9 \times 2^k - 3 \times 2^{k/2} - 1/4 \leq \mu \leq 4 \times 2^k + 2 \times 2^{k/2} + 1/4;$$

4. a função ϑ de G_n satisfaz

$$\vartheta(G_n) \leq n \frac{36 \times 2^k + 12 \times 2^{k/2} + 1}{2^k(2^k - 2) + 36 \times 2^k + 12 \times 2^{k/2} + 1} \leq (36 + o(1))n^{2/3}.$$

Observe que o grafo G_n é o grafo de Cayley $G(\mathbb{Z}_2^{3k}, S)$, onde $S = S_n = U_0 + U_1$.

Seja $\mathbf{A} = [\mathbf{A}_0 | \mathbf{A}_1]$ a matriz $3k \times 2^k - 1$, onde $\mathbf{A}_0$ tem como colunas os $2^{k-1} - 1$ vetores de U_0 e $\mathbf{A}_1$ é definida de forma análoga. Vamos mostrar que quaisquer 6 colunas de $\mathbf{A}$ são linearmente independentes. Podemos simplificar a representação da matriz e utilizar

elementos de F_k em vez de utilizar a representação binária (lembrando que as somas dos vetores binários correspondem a soma dos elementos no corpo). Se α é um gerador do grupo multiplicativo de F_k, podemos re-arranjar as colunas de $\mathbf{A}$ e obter

$$\mathbf{A} = \begin{bmatrix} \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \alpha^5 & \alpha^{10} & \dots & \alpha^{5(n-1)} \end{bmatrix}.$$

Suponha que existam 6 colunas de $\mathbf{A}$ linearmente dependentes. Sejam $i_1, \dots, i_6$ os índices de tais colunas. Então existe um vetor $\mathbf{c} = (c_1, \dots, c_6) \in \mathrm{GF}(2)^6$, com $\mathbf{c} \neq \mathbf{0}$, tal que

$$\begin{bmatrix} \alpha^{i_1} & \dots & \alpha^{i_6} \\ \alpha^{3i_1} & \dots & \alpha^{3i_6} \\ \alpha^{5i_1} & \dots & \alpha^{5i_6} \end{bmatrix} \mathbf{c} = \mathbf{0}.$$

Note que se $c_1\alpha^{i_1} + \dots + c_6\alpha^{i_6} = 0$ então $c_1\alpha^{2i_1} + \dots + c_6\alpha^{2i_6} = (c_1\alpha^{i_1} + \dots + c_6\alpha^{i_6})^2 = 0$. Aplicando essa idéia repetidamente, verificamos que

$$\begin{bmatrix} \alpha^{i_1} & \dots & \alpha^{i_6} \\ \alpha^{2i_1} & \dots & \alpha^{2i_6} \\ \vdots & & \vdots \\ \alpha^{6i_1} & \dots & \alpha^{6i_6} \end{bmatrix} \mathbf{c} = \mathbf{0}.$$

A matriz 6×6 formada deve ter determinante igual a 0. Podemos então dividir colunas (ou linhas) por escalares sem alterar o determinante. Dividindo a primeira coluna por α^{i_1}, a segunda por α^{i_2} e assim consecutivamente, obtemos a matriz

$$\begin{bmatrix} 1 & \dots & 1 \\ \alpha^{i_1} & \dots & \alpha^{i_6} \\ \vdots & & \vdots \\ \alpha^{5i_1} & \dots & \alpha^{5i_6} \end{bmatrix}.$$

Esta é (a transposta de) uma matriz de Vandermonde, cujo determinante é

$$\prod_{1 \leq j < k \leq 6} (\alpha^{i_j} - \alpha^{i_k}).$$

Note que este produto não pode ser nulo, pois todos os fatores são diferentes de 0. Chegamos a uma contradição.

Então temos que quaisquer 6 colunas de $\mathbf{A}$ são linearmente independentes. Como conseqüência, toda soma $u_0 + u_1$ com $u_0 \in U_0$ e $u_1 \in U_1$ é distinta. Isso mostra que $|S| = |U_0||U_1|$. Fixe um vértice x de G_n. Os vizinhos de x são elementos $x + y$ com $y \in S$, portanto, o grau de x é $|S|$, isso mostra a propriedade 1.

Suponha que G_n possua um triângulo formado por vértices u, v e w. Então temos que $u+v$, $v+w$ e $w+u$ são 3 elementos distintos de S, mas isso é absurdo pois $(u+v)+(v+w)+(w+u)=0$. A propriedade 2 está provada.

Teorema 6.1. *Seja χ um caractere de um grupo finito abeliano Γ, seja A um conjunto simétrico ($A=-A$) e seja $G=G(\Gamma,A)$. Defina*

$$\lambda(\chi)=\sum_{a\in A}\chi(a).$$

Todo auto-valor de G é dado por $\lambda(\chi)$ para algum caractere χ.

Demonstração. Seja $\mathbf{v}=\mathbf{v}(\chi)$ um vetor indexado por Γ tal que $\mathbf{v}_\gamma=\chi(\gamma)$. Seja $\mathbf{M}$ a matriz de adjacência de G. Temos

$$(\mathbf{Mv})_\gamma=\sum_{a\in A}\chi(\gamma-a)=\sum_{a\in A}\chi(\gamma+a)=\Big(\sum_{a\in A}\chi(a)\Big)\chi(\gamma)=\lambda(\chi)\mathbf{v}_\gamma.$$

Isso mostra que $\lambda(\chi)$ é auto-valor de $\mathbf{M}$. Como há $|\Gamma|$ caracteres (linearmente independentes) e a dimensão do espaço é $|\Gamma|$, o teorema está demonstrado. □

Vamos aplicar o teorema acima para obter os auto-valores de G_n. Para um caractere χ fixado, temos

$$\sum_{s\in S}\chi(s)=\Big(\sum_{u_0\in U_0}\chi(u_0)\Big)\Big(\sum_{u_1\in U_1}\chi(u_1)\Big).$$

Note que χ é um caractere aditivo de $\mathbb{Z}_2^{3k}$ e, logo, $\chi(b_1,\ldots,b_{3k})=\phi_1(b_1)\ldots\phi_{3k}(b_{3k})$, onde cada ϕ_i é um caractere de $\mathbb{Z}_2$. Como ϕ_i é caractere de $\mathbb{Z}_2$, temos $\phi_i(0)=1$ e $\phi_i(1)\in\{1,-1\}$. Defina o mapa $\chi\leftrightarrow\boldsymbol{\chi}=(\delta_{\phi_1(1),-1},\ldots,\delta_{\phi_{3k}(1),-1})$, onde $\delta_{i,j}$ é 1 se $i=j$ e 0 se $i\neq j$.

Com esta definição, fica claro que

$$\chi(b_1,\ldots,b_{3k})=\begin{cases}-1, & \text{caso } \langle\boldsymbol{\chi},\mathbf{b}\rangle=1,\\ 1, & \text{caso } \langle\boldsymbol{\chi},\mathbf{b}\rangle=0,\end{cases}\tag{9}$$

onde o produto interno é sobre $\mathbb{Z}_2^{3k}$. Denotamos por $w(\mathbf{u})$ o *peso* de um vetor binário (o número de coordenadas não-nulas do vetor). Se $x=w(\boldsymbol{\chi}^T\mathbf{A}_0)$ então $\sum_{u_0\in U_0}\chi(u_0)=|U_0|-2x$. Analogamente, se $y=w(\boldsymbol{\chi}^T\mathbf{A}_1)$, então $\sum_{u_1\in U_1}\chi(u_1)=|U_1|-2y$. Isso segue diretamente de (9).

O mapa $\chi\leftrightarrow\boldsymbol{\chi}$ é uma bijeção e cada auto-valor de G_n corresponde a um caractere. Então todos os auto-valores de G_n são da forma

$$(|U_0|-2x)(|U_1|-2y)=(2^{k-1}-1-2x)(2^{k-1}-2y),$$

onde $x+y$ é o peso de uma combinação linear das linhas de $\mathbf{A}$, x é o peso dessa combinação restrito aos índices de $\mathbf{A}_0$ e y é o peso dessa combinação restrito aos índices de $\mathbf{A}_1$. Queremos então limitar esses valores para demonstrar a propriedade 3.

Para isso, faremos uso da teoria de códigos (veja [7]). As linhas da matriz $\mathbf{A}$ geram o código dual do código BCH que tem $\mathbf{A}$ como matriz de paridade. O seguinte teorema nos fornece cotas para o peso das palavras desse código dual e, portanto, cotas para o peso das combinações lineares das linhas de $\mathbf{A}$.

Teorema 6.2. *[7, 9.18] Suponha que $\mathcal{C}$ seja um código BCH binário com tamanho $n = 2^m - 1$ e distância projetada $\delta = 2t+1$, onde $2t-1 < 2^{\lceil m/2 \rceil}+1$. Então o peso de qualquer palavra $\mathbf{c}$ (não nula) do código $\mathcal{C}^\perp$ (código dual) é limitada por*

$$2^{m-1} - (t-1)2^{m/2} \leq w(\mathbf{c}) \leq 2^{m-1} + (t-1)2^{m/2}.$$

O tamanho do código BCH cuja matriz de paridade é $\mathbf{A}$ é $n = 2^k - 1$. Como já demonstramos, quaisquer 6 colunas de $\mathbf{A}$ são linearmente independentes. É possível verificar (por contagem) que existem 8 colunas linearmente dependentes em $\mathbf{A}$. Para códigos definidos em corpos de característica 2, podemos assumir, sem perda de generalidade, que a distância projetada é ímpar (veja [7, cap. 7, pg. 203]), portanto, temos $\delta = 7 = 2 \times 3 + 1$ e então

$$2^{k-1} - 2^{1+k/2} \leq x + y \leq 2^{k-1} + 2^{1+k/2}. \tag{10}$$

Seja $\mathbf{p}$ um vetor indexado pelos elementos não nulos de F_k, com $p_v = 1$, se $v \in W_1$ e $p_v = 0$, se $v \in W_0$. Seja $\mathbf{A}'$ uma matriz cuja i-ésima coluna é dada por $(\mathbf{w}, \mathbf{w}^3, \mathbf{w}^5, \mathbf{w}^7)$, onde a i-ésima coluna de $\mathbf{A}$ é $(\mathbf{w}, \mathbf{w}^3, \mathbf{w}^5)$. Pela definição dos conjuntos W_0 e W_1, temos que $\mathbf{p}$ é uma das linhas de $\mathbf{A}'$. Além disso, a matriz $\mathbf{A}'$ gera o código dual de um código BCH de distância projetada $\delta' = 9 = 2 \times 4 + 1$ (o argumento é o mesmo usado para determinar a distância projetada do código cuja matriz de paridade é $\mathbf{A}$). A soma de $\mathbf{p}$ com a combinação linear das linhas de $\mathbf{A}$ considerada anteriormente tem peso $x + (2^{k-1} - y)$. Aplicando a cota de Carlitz-Uchiyama, obtemos

$$2^{k-1} - 3 \times 2^{k/2} \leq x + 2^{k-1} - y \leq 2^{k-1} + 3 \times 2^{k/2}. \tag{11}$$

Agora usamos o fato que para quaisquer reais a e b, temos

$$-\Big(\frac{a-b}{2}\Big)^2 \leq ab \leq \Big(\frac{a+b}{2}\Big)^2.$$

Concluimos, a partir de (10), que

$$\begin{aligned}(2^{k-1} - 1 - 2x)(2^{k-1} - 2y) &\leq \frac{(2^k - 1 - 2(x+y))^2}{4} \\ &\leq \frac{(2^k - 1 - 2(2^{k-1} + 2^{1+k/2}))^2}{4} \\ &\leq \frac{-1 - 2^{2+k/2}}{4} = 4 \times 2^k + 2 \times 2^{k/2} + \frac{1}{4}.\end{aligned}$$

Analogamente, a partir de (11), temos

$$\begin{aligned}(2^{k-1}-1-2x)(2^{k-1}-2y) &\geq -\frac{(1+2(x-y))^2}{4}\\ &\geq -\frac{(1+2\times 3\times 2^{k/2})^2}{4}\\ &= -9\times 2^k - 3\times 2^{k/2} - 1/4.\end{aligned}$$

E a propriedade 3 acaba de ser demonstrada.

6.4 A Função ϑ de Lovász

Teorema 6.3. *[6] Seja G um grafo com n vértices, $\{1,\ldots,n\}$. O valor $\vartheta(G)$ é definido como em (8). Podemos caracterizar $\vartheta(G)$ como o mínimo entre o maior auto-valor de cada matriz simétrica $\mathbf{A}=(a_{ij})_{i,j=1}^n$, com*

$$a_{ij}=1 \text{ se } i=j \text{ ou se os vértices } i \text{ e } j \text{ não são adjacentes.} \tag{12}$$

Demonstração. Sejam $\mathbf{c}$ um vetor unitário e $\mathbf{u}_1,\ldots,\mathbf{u}_n$ uma representação ortonormal de G que seja ótima (em relação a $\vartheta(G)$). Defina

$$a_{ij}=1-\frac{\langle \mathbf{u}_i,\mathbf{u}_j\rangle}{\langle \mathbf{c},\mathbf{u}_i\rangle\langle \mathbf{c},\mathbf{u}_j\rangle}, \text{ se } i\neq j \text{ e } a_{ii}=1.$$

É simples ver que $\mathbf{A}=(a_{ij})_{i,j=1}^n$ é uma matriz que satisfaz as propriedades do teorema. Seja $\mathbf{x}_i=\mathbf{c}-\mathbf{u}_i/\langle \mathbf{c},\mathbf{u}_i\rangle$. Note que

$$-a_{ij}=\langle \mathbf{x}_i,\mathbf{x}_j\rangle, \text{ se } i\neq j \text{ e } -a_{ii}=\|\mathbf{x}_i\|^2-\frac{1}{\langle \mathbf{c},\mathbf{u}_i\rangle^2}.$$

Seja λ o maior auto-valor de $\mathbf{A}$ e $\mathbf{v}$ um auto-vetor correspondente. Seja $\mathbf{X}$ a matriz cujas linhas são os vetores $\mathbf{x}_i$. Seja $\mathbf{D}=\operatorname{diag}(\langle \mathbf{c},\mathbf{u}_1\rangle^{-2},\ldots,\langle \mathbf{c},\mathbf{u}_n\rangle^{-2})$. Temos que $\mathbf{X}\mathbf{X}^T=\mathbf{D}-\mathbf{A}$. Para todo vetor $\mathbf{y}$, vale $\mathbf{y}^T\mathbf{X}\mathbf{X}^T\mathbf{y}\geq 0$, em particular

$$\mathbf{v}^T\mathbf{X}\mathbf{X}^T\mathbf{v}=\mathbf{v}^T\mathbf{D}\mathbf{v}-\mathbf{v}^T\mathbf{A}\mathbf{v}=\frac{v_1^2}{\langle \mathbf{c},\mathbf{u}_1\rangle^2}+\cdots+\frac{v_n^2}{\langle \mathbf{c},\mathbf{u}_n\rangle^2}-\lambda(v_1^2+\cdots+v_n^2)\geq 0.$$

Isso mostra que $\lambda\leq\vartheta(G)$.

Vamos mostrar que a desigualdade vale no sentido contrário. Seja $\mathbf{A}$ uma matriz que satisfaz (12) e seja λ seu maior auto-valor. Então $\mathbf{B}=\lambda\mathbf{I}-\mathbf{A}$ é simétrica positiva semidefinida (SPSD). Basta verificar que se μ é auto-valor de $\mathbf{B}$ então $\det(\mathbf{B}-\mu\mathbf{I})=\det(-\mathbf{A}-(\mu-\lambda)\mathbf{I})=0$. Mas então $\lambda-\mu$ é auto-valor de $\mathbf{A}$ e, por hipótese, $\lambda-\mu\leq\lambda$. Logo, $\mu\geq 0$, o que é equivalente a dizer que $\mathbf{B}$ é SPSD.

Se uma matriz real é SPSD, ela pode ser expressa como produto $\mathbf{X}\mathbf{X}^T$, onde $\mathbf{X}$ é uma matriz real. Se $\mathbf{x}_i$ é a i-ésima linha de $\mathbf{X}$, temos

$$\lambda\delta_{ij} - a_{ij} = \langle \mathbf{x}_i, \mathbf{x}_j \rangle.$$

Sejam $\hat{\mathbf{x}}_i = (\mathbf{x}_i, 0)$ e $\mathbf{c} = (\mathbf{0}, 1)$. Defina $\mathbf{u}_i = (\mathbf{c} + \hat{\mathbf{x}}_i)/\sqrt{\lambda}$. Note que $\langle \hat{\mathbf{x}}_i, \hat{\mathbf{x}}_j \rangle = \langle \mathbf{x}_i, \mathbf{x}_j \rangle$, que $\langle \hat{\mathbf{x}}_i, \mathbf{c} \rangle = 0$ e que $\|\mathbf{c}\| = 1$. Portanto,

$$\|\mathbf{u}_i\|^2 = \frac{1}{\lambda}(\|\mathbf{c}\|^2 + 2\langle \hat{\mathbf{x}}_i, \mathbf{c} \rangle + \|\mathbf{x}_i\|^2) = \frac{1}{\lambda}(1 + \|\mathbf{x}_i\|^2) = \frac{1}{\lambda}(1 + \lambda - a_{ii}) = 1,$$

e, para i e j não adjacentes, temos

$$\langle \mathbf{u}_i, \mathbf{u}_j \rangle = \frac{1}{\lambda}(\|\mathbf{c}\|^2 + \langle \hat{\mathbf{x}}_i, \mathbf{c} \rangle + \langle \hat{\mathbf{x}}_j, \mathbf{c} \rangle + \langle \hat{\mathbf{x}}_i, \hat{\mathbf{x}}_j \rangle) = \frac{1}{\lambda}(1 + \langle \mathbf{x}_i, \mathbf{x}_j \rangle) = \frac{1}{\lambda}(1 - a_{ij}) = 0.$$

Então $\{\mathbf{u}_1, \ldots, \mathbf{u}_n\}$ é uma representação ortonormal para G e $\mathbf{c}$ é um vetor unitário. Além disso, $\langle \mathbf{c}, \mathbf{u}_i \rangle = 1/\sqrt{\lambda}$. Logo, $\vartheta(G) \leq \lambda$ e assim completamos a demonstração do teorema. □

Teorema 6.4. *[6] Seja G um grafo d-regular e sejam $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ os auto-valores da matriz de adjacência $\mathbf{A}$. Então*

$$\vartheta(G) \leq -n\frac{\lambda_n}{\lambda_1 - \lambda_n}.$$

Demonstração. Sejam $\mathbf{J}$ a matriz $n \times n$ onde todas as entradas tem valor 1 e $\mathbf{j}$ um vetor linha de $\mathbf{J}$. Claramente, $\mathbf{j}$ é auto-vetor de $\mathbf{J}$ e de $\mathbf{A}$ (os auto-valores são n e d, respectivamente). Sejam $\mathbf{j} = \mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ os auto-vetores correspondentes aos auto-valores $\lambda_1, \ldots, \lambda_n$.

Observe que todo auto-vetor de $\mathbf{J}$ que não é múltiplo de $\mathbf{j}$ tem auto-valor correspondente 0. Suponha que $\lambda_1 = \cdots = \lambda_k = d$ para algum $k \geq 1$ e que $\lambda_l < d$ para todo $l > k$. Verifique que $\mathbf{J}\mathbf{A} = \mathbf{A}\mathbf{J} = d\mathbf{J}$ e, portanto, $\mathbf{J}(\mathbf{A}\mathbf{v}_l) = \lambda_l \mathbf{J}\mathbf{v}_l$. Por outro lado, $(\mathbf{J}\mathbf{A})\mathbf{v}_l = d\mathbf{J}\mathbf{v}_l$ e então $d\mathbf{J}\mathbf{v}_l = \lambda_l \mathbf{J}\mathbf{v}_l$. Para $l > k$, devemos ter $\mathbf{J}\mathbf{v}_l = \mathbf{0}$.

Sabemos que toda matriz simétrica e real possui uma base ortogonal de auto-vetores que gera todo o espaço. Para algum x real positivo, defina $\mathbf{B} = \mathbf{J} - x\mathbf{A}$. Note que $\mathbf{B}$ é simétrica e real. Além disso, a proposição acima mostra que $\mathbf{v}_{k+1}, \ldots, \mathbf{v}_n$ são auto-vetores de $\mathbf{B}$. Seja $\mathbf{w}$ um auto-vetor de $\mathbf{B}$ que não é combinação linear de $\{\mathbf{v}_{k+1}, \ldots, \mathbf{v}_n\}$ e seja μ o auto-valor correspondente. Então $\mathbf{w}$ é combinação linear de $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$. Logo, $\mathbf{B}\mathbf{w} = \mathbf{J}\mathbf{w} - x\mathbf{A}\mathbf{w} = \mathbf{J}\mathbf{w} - xd\mathbf{w} = \mu\mathbf{w}$. E assim obtemos $\mathbf{J}\mathbf{w} = (\mu - xd)\mathbf{w}$. Pelo que vimos acima, ou $\mathbf{w} = \mathbf{j}$ ou $\mathbf{J}\mathbf{w} = \mathbf{0}$.

Sendo assim, os auto-valores de $\mathbf{B}$ são $n - x\lambda_1, -x\lambda_2, \ldots, -x\lambda_n$. O maior desses auto-valores pode ser o primeiro ou o último (pois $-x\lambda_i \leq -x\lambda_n$). A escolha de x que minimiza o máximo entre os dois é $x = n/(\lambda_1 - \lambda_n)$, quando ambos são iguais a $-n\lambda_n/(\lambda_1 - \lambda_n)$. A matriz $\mathbf{J} - x\mathbf{A}$ satisfaz as condições do teorema 6.3, logo $\vartheta(G) \leq -n\lambda_n/(\lambda_1 - \lambda_n)$. □

Agora basta utilizar a propriedade 3 e o teorema 6.4 para obter a propriedade 4. Primeiramente, observe que $\vartheta(G) \leq -n\lambda_n/(\lambda_1 - \lambda_n) = n[1 - \lambda_1/(\lambda_1 - \lambda_n)]$. Fica claro que quanto menor o valor de λ_n, maior o valor do lado direito da desigualdade. Então, pela propriedade 3, temos

$$\vartheta(G) \leq -n\frac{\lambda_n}{\lambda_1 - \lambda_n} \leq n\frac{36 \times 2^k + 12 \times 2^{k/2} + 1}{2^k(2^k - 2) + 36 \times 2^k + 12 \times 2^{k/2} + 1}.$$

Multiplicando o numerador e o denominador por 2^{-k}, obtemos

$$\vartheta(G) \leq n\frac{36 + 12 \times 2^{-k/2} + 2^{-k}}{2^k + 34 + 12 \times 2^{-k/2} + 2^{-k}} \leq 2^{2k}(36 + 12 \times 2^{-k/2} + 2^{-k}) = (36 + o(1))n^{2/3}.$$

Corolário. *3 Se k não é divisível por 3 e $n = 2^{3k}$, o grafo $G = G_n$ é livre de triângulos e o lema 6.1 nos garante que $\alpha(G) \leq \vartheta(G) \leq (36 + o(1))n^{2/3}$. Isso mostra que é possível construir um grafo com $\Omega(m^{3/2})$ vértices, sem triângulos e sem conjuntos independentes de tamanho m.*

A Demonstrando um caso particular do Teorema de Weil

O estudo de somas de caracteres desenvolvido neste apêndice segue os passos do livro *Equations over Finite Fields* [8].

A.1 Definições e Lemas Preliminares

Definição (expoente). *3 Se χ é um caractere multiplicativo e $\chi^d = \chi_0$, onde χ_0 é o caractere trivial, dizemos que χ tem* expoente *d. Lembrando que a multiplicação de caracteres é dada por $(\chi_1\chi_2)(x) = \chi_1(x)\chi_2(x)$.*

Lema A.1. *Seja G um grupo abeliano finito.*

1. *Dado um caractere χ,*

$$\sum_{x \in G} \chi(x) = \begin{cases} |G|, & \text{se } \chi = \chi_0, \\ 0, & \text{caso contrário.} \end{cases}$$

2. *Dado um elemento $x \in G$*

$$\sum_{\chi} \chi(x) = \begin{cases} |G|, & \text{se } x = 1, \\ 0, & \text{caso contrário.} \end{cases}$$

Demonstração. Se $\chi = \chi_0$, a soma é trivial. Se $\chi \neq \chi_0$, tome $s \in G$ com $\chi(s) \neq 1$. Temos

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xs) = \chi(s) \sum_{x \in G} \chi(x).$$

Logo $\sum_{x \in G} \chi(x) = 0$. A segunda parte segue por raciocínio análogo, lembrando que os caracteres de um grupo G (abeliano e finito) formam um grupo G' isomorfo a G. □

Lema A.2. *Se d divide $|F^*|$, existe um isomorfismo natural entre o grupo de caracteres de F^* de expoente d e o grupo de caracteres de $F^*/(F^*)^d$. Em particular, há exatamente d caracteres com expoente d.*

Demonstração. Como F^* é um grupo cíclico, podemos tomar s como gerador. É simples verificar que $(F^*)^d = \{s^d, s^{2d}, s^{3d}, \dots\}$. Seja χ um caractere multiplicativo de F de expoente d. É bem claro que para todo elemento $a \in (F^*)^d$, temos $\chi(a) = 1$. Note que as d classes laterais de $(F^*)^d$ são $(F^*)^d, s(F^*)^d, s^2(F^*)^d, \dots, s^{d-1}(F^*)^d$. Portanto o valor de $\chi(x)$ depende somente da classe lateral a qual x pertence. Concluimos que todo caractere de expoente d induz um caractere de $F^*/(F^*)^d$ e vice-versa. Este é o isomorfismo desejado. □

Lema A.3. *Seja F um corpo e suponha que d divide $|F^*|$. Então*

$$\sum_{\chi\,:\,\chi^d=\chi_0} \chi(x) = \begin{cases} d, & \text{se } x \in (F^*)^d, \\ 0, & \text{se } x \notin (F^*)^d, x \neq 0, \\ 1, & \text{se } x = 0. \end{cases}$$

Demonstração. A partir do lema A.2, podemos encarar os caracteres de expoente d como caracteres de $F^*/(F^*)^d$. Podemos então utilizar o lema A.1 para os dois primeiros casos. Se χ é um caractere tal que $\chi(0) \neq 0$ então $\chi = \chi_0$ e $\chi_0(0) = 1$, e isso mostra o último caso. □

Definição (Soma Gaussiana). *3 Seja F um corpo, χ um caractere multiplicativo de F e ψ um caractere aditivo de F. A soma Gaussiana é dada por*

$$G(\chi, \psi) = \sum_{x \in F} \chi(x)\psi(x).$$

Lema A.4. *Se $\chi \neq \chi_0$ e $\psi \neq \psi_0$, então $|G(\chi, \psi)| = \sqrt{|F|}$.*

Demonstração.

$$|G(\chi, \psi)|^2 = \sum_{x \in F} \sum_{y \in F} \chi(x)\psi(x)\overline{\chi(y)}\,\overline{\psi(y)}.$$

Como $\chi(0) = 0$, podemos somar apenas nos valores de y diferentes de 0. Assim $\overline{\chi(y)} = \chi(y^{-1})$ e $\overline{\psi(y)} = \psi(-y)$. Colocando $x = ay$, obtemos

$$\begin{aligned} |G(\chi, \psi)|^2 &= \sum_{a \in F} \sum_{y \in F^*} \chi(ay)\psi(ay)\chi(y^{-1})\psi(-y) \\ &= \sum_{a \in F} \chi(a) \sum_{y \in F^*} \psi((a-1)y) \\ &= \sum_{a \in F} \chi(a) \sum_{y \in F} \psi((a-1)y) - \sum_{a \in F} \chi(a) \\ &= \sum_{a \in F} \chi(a) \sum_{y \in F} \psi((a-1)y). \end{aligned}$$

Pelo Lema A.1, a soma interna é $|F|$, se $t = 1$ e 0, caso contrário. Portanto,

$$|G(\chi, \psi)|^2 = \chi(1)|F| = |F|.$$

□

Lema A.5. *Se $\psi \neq \psi_0$ é um caractere aditivo, d divide $|F^*|$ e $a \in F^*$, então*

$$\sum_{y \in F} \psi(ay^d) = \sum_{\chi \,:\, \chi^d = \chi_0} \overline{\chi(a)} G(\chi, \psi).$$

Demonstração. Para um dado $x \in F$, o número de elementos $y \in F$ tais que $x = y^d$ é d, se $x \in (F^*)^d$, é 1, se $x = 0$ e é 0, se $x \notin (F^*)^d$ e $x \neq 0$. Sendo assim, pelo lema A.3,

$$\sum_{y \in F} \psi(ay^d) = \sum_{x \in F} \psi(ax) \sum_{\chi \,:\, \chi^d = \chi_0} \chi(x).$$

Substituindo x por $a^{-1}x$ e notando que $\chi(a^{-1}x) = \overline{\chi(a)}\chi(x)$, obtemos

$$\sum_{x \in F} \psi(x) \sum_{\chi \,:\, \chi^d = \chi_0} \overline{\chi(a)}\chi(x) = \sum_{\chi \,:\, \chi^d = \chi_0} \overline{\chi(a)} \sum_{x \in F} \chi(x)\psi(x) = \sum_{\chi \,:\, \chi^d = \chi_0} \overline{\chi(a)} G(\chi, \psi).$$

□

A.2 Teorema Principal

Teorema A.1. *Para um caractere aditivo $\psi \neq \psi_0$, $a \in F^*$ e $d \geq 1$,*

$$\left| \sum_{x \in F} \psi(ax^d) \right| \leq (d-1)\sqrt{|F|}.$$

Demonstração. Seja $d' = \mathrm{mdc}(d, |F^*|)$, com $d = d' \times m$. Seja s o gerador de F^*. Note que

$$\sum_{x \in F} \psi(ax^d) = \psi(0) + \sum_{j=1}^{|F^*|} \psi(as^{jmd'}) = \psi(0) + \sum_{j=1}^{|F^*|} \psi(as^{jd'}) = \sum_{x \in F} \psi(ax^{d'}),$$

pois como m é relativamente primo com $|F^*|$, jm assume todos os valores módulo $|F^*|$. Podemos então assumir sem perda de generalidade que d divide $|F^*|$. A partir do lema A.5, temos

$$\sum_{x \in F} \psi(ax^d) = \sum_{\chi \,:\, \chi^d = \chi_0} \overline{\chi(a)} G(\chi, \psi).$$

Há precisamente d caracteres de expoente d. Um deles é χ_0 e $G(\chi_0, \psi) = 0$. Os outros $d-1$ caracteres são tais que $|G(\chi, \psi)| = \sqrt{|F|}$ (pelo lema A.4). Como $\overline{\chi(a)}$ é uma raiz da unidade, $|\overline{\chi(a)}| = 1$. Então,

$$\left| \sum_{x \in F} \psi(ax^d) \right| \leq \sum_{\chi \,:\, \chi^d = \chi_0} |\overline{\chi(a)}||G(\chi, \psi)| = (d-1)\sqrt{|F|}.$$

□

Referências

[1] N. Alon and J. Spencer, *The Probabilistic Method*. New York: John Wiley and Sons, 2nd ed., 2000.

[2] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics*. preliminary version 2 ed., 1992.

[3] R. Boppana and M. M. Halldórsson, "Approximating maximum independent sets by excluding subgraphs," in *SWAT 90 2nd Scandinavian Workshop on Algorithm Theory* (J. R. Gilbert and R. Karlsson, eds.), vol. 447, pp. 13–25, 1990.

[4] B. Bollobás, *Random Graphs*. Cambridge University Press, 2nd ed., 2001.

[5] N. Alon, "Explicit Ramsey graphs and orthonormal labelings," *The Electronic J. Combinatorics 1*, no. R12, 1994.

[6] L. Lovász, "On the Shannon capacity of a graph," *IEEE Transactions on Information Theory*, vol. 25, no. 1, 1979.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, vol. 1. North-Holland, 1977.

[8] W. M. Schmidt, *Equations over Finite Fields*. Springer-Verlag, 1976.