



**Gabriel
Simões Cardoso**

**Grafos de Ramanujan em Teoria dos Códigos e
Criptografia**



**Gabriel
Simões Cardoso**

Grafos de Ramanujan em Teoria dos Códigos e Criptografia

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Matemática e Aplicações, realizada sob a orientação científica do Professor Doutor *Paulo José Fernandes Almeida*, Professor Auxiliar do Departamento de Matemática da Universidade de Aveiro e da Professora Doutora *Sofia Alexandra Marques Jorge Pinheiro*, Professora Auxiliar do Departamento de Matemática da Universidade de Aveiro.

o júri / the jury

presidente / president

Prof^a. Doutora Maria Raquel Rocha Pinto

Professora Auxiliar da Universidade de Aveiro

vogais / examiners committee

Prof. Doutor José Pedro Miranda Mourão Patrício

Professor Auxiliar da Universidade do Minho

Prof. Doutor Paulo José Fernandes Almeida

Professor Auxiliar da Universidade de Aveiro

**agradecimentos /
acknowledgements**

Em primeiro lugar agradeço a toda a minha família pelo apoio incondicional demonstrado ao longo destes dois anos de mestrado, em particular pelo amor demonstrado nos últimos meses.

Agradeço às minhas amigas e aos meus amigos que possibilitaram a realização desta dissertação, estando sempre ao meu lado com uma enorme paciência.

Um grande obrigado ao Doutor Paulo José Fernandes Almeida e à Doutora Sofia Alexandra Marques Jorge Pinheiro pela forma como me acompanharam na realização desta dissertação, pelo apoio, pela sempre boa disposição e por todos os momentos de debate saudável que me permitiram crescer cientificamente.

Palavras-chave

grafo expensor, grafo de Ramanujan, código LDPC, função de síntese

Resumo

Nesta dissertação são estudadas propriedades de uma certa família de grafos, os grafos de Ramanujan. São ainda apresentadas e exemplificadas algumas aplicações destes, nomeadamente à Teoria dos Códigos e à Criptografia. Em particular, é apresentada e demonstrada uma propriedade dos grafos regulares com base no seu espectro, propriedade extremal para a família dos grafos de Ramanujan. Existindo outras construções possíveis, esta família pode ser construída, por exemplo, tal como é feito nesta dissertação, enquanto um caso particular de uma família de grafos de Cayley. Os grafos daquela família, caracterizando-se pelo facto de possuírem uma cintura grande, possibilitam, enquanto grafos expansores, a construção de códigos LDPC com uma grande distância e a construção de funções de síntese resistentes a colisões.

Key-words

expander graph, Ramanujan graph, LDPC code, cryptographic hash function

Abstract

In this thesis are studied the properties of a certain family of graphs, the Ramanujan graphs, and are presented and exemplified some of their applications, namely in Code Theory and Cryptography. Particularly, is presented and proved a regular graphs property based on their spectrum, which is extreme for the Ramanujan graphs family. There are many possible constructions for this family. In this thesis, the Ramanujan graphs are constructed as Cayley graphs. The graphs on that family, because of their large girth as expander graphs, are suitable to apply in constructions of LDPC codes and collision-resistant cryptographic hash functions.

Conteúdo

Conteúdo	i
1 Introdução	1
2 Conceitos e resultados preliminares	5
2.1 Teoria dos Grafos	5
2.2 Álgebra Linear	9
2.3 Teoria dos Números e Combinatória	13
3 Grafos de Ramanujan	17
3.1 Caracterização dos grafos de Ramanujan	17
3.2 Grafos de Cayley	22
3.3 Construção LPS	22
3.4 Cintura de grafos de Ramanujan bipartidos	28
4 Aplicação à Teoria dos Códigos	37
4.1 Construção de um código LDPC	38
4.2 Detecção e correção de erros	41
5 Aplicação à Criptografia	45
5.1 Função de síntese	45
5.2 Minimização da probabilidade de colisão	46
5.3 Construção de uma função de síntese resistente a colisões	49
6 Conclusão	53

Capítulo 1

Introdução

Numa era cada vez mais digital torna-se ainda mais estimulante a continuação da investigação, ensino e aprendizagem nas ditas ciências exatas, sendo a matemática uma delas. Ao longo da sua história, e em particular das últimas décadas da sua existência, o ser humano tem provado que é pela ciência, e em particular pela matemática, que se tem vindo a contribuir decisivamente e de forma construtiva para o aprofundamento do seu desenvolvimento cognitivo e para importantes aplicações no âmbito das tecnologias da informação e da comunicação.

Na primeira metade do século XX, o matemático inglês Alan Turing, que ficou conhecido como pai da Teoria da Computação, desenvolveu a famosa Máquina de Turing e formalizou o conceito de algoritmo, ambos cruciais para a construção do computador moderno. Algo que no tempo de vida de Turing seria impensável é hoje absolutamente banal: o contacto possível e permanente por meio de conversações virtuais. Nessas mesmas conversações qualquer mensagem poderá ser enviada com erros que se pretendem detetar (e eventualmente corrigir) através do que se designará, nesta dissertação, por código.

Alguns anos após a morte de Alan Turing, em 1985, surgem em Portugal os primeiros doze terminais de multibanco, apenas no Porto e em Lisboa, estendendo-se a milhares por todo o país nos dias de hoje. Num terminal de multibanco é possível efetuar um conjunto de operações, contando com a proteção de uma senha sendo que esta ao ser inserida num destes terminais é protegida, pelo que se denominará nesta dissertação, por uma função de síntese, havendo uma probabilidade muito reduzida

de que a inserção de uma senha diferente da verdadeira seja considerada igualmente válida.

Esta dissertação foi impulsionada pela relevância das aplicações dos grafos que ao longo dela serão estudados, em particular, à Teoria dos Códigos e à Criptografia. Neste sentido procura-se desenvolver esta temática ao longo deste trabalho introduzindo conceitos e resultados importantes para o estudo das suas aplicações. Comece-se por enunciar alguns contributos decisivos para o estudo da família dos grafos de Ramanujan.

Alon, em [2], relaciona o espectro de um grafo com a possibilidade de este ser ou não expensor, estabelece um majorante para o número de independência de um grafo de Ramanujan não bipartido (ver [17]) e apresenta também um minorante para o segundo menor valor próprio de um grafo regular.

Margulis, em [19], apresenta uma construção de uma família de grafos de Cayley assim como anos mais tarde apresenta, em [20], uma construção para uma família de grafos de Ramanujan baseada na prévia construção de grafos de Cayley em [19].

Lubotzky, Phillips e Sarnak, em [17], além de apresentarem um minorante para a cintura dos grafos de Ramanujan estudam também outros parâmetros destes grafos tais como o seu diâmetro, caso sejam ou não bipartidos, e o seu número cromático (caso não sejam bipartidos). Além disso, os autores deste artigo enunciam e demonstram uma propriedade comum a todos os grafos regulares, indo mais longe e apresentando uma construção dos grafos de Ramanujan baseada na construção de Margulis em [19], provando que essa mesma construção conduz a uma família infinita de grafos de Ramanujan.

Em [5], Biggs e Boshier apresentam um majorante para a cintura dos grafos de Ramanujan assim como um valor exato para a cintura destes no caso de serem bipartidos.

Em [26], Rosenthal e Vontobel, partindo de [19], constroem uma família de grafos de Cayley sem ciclos de comprimento pequeno, ou seja grafos com cintura grande, com o objetivo de construir bons códigos LDPC a partir destes grafos. Também em [26] é referida a construção de Margulis dos grafos de Ramanujan e é estabelecida uma ligação entre a construção de grafos de Ramanujan a partir de grafos de Cayley feita em [17] e códigos LDPC sendo também graficamente comparados os desempenhos de dois códigos LDPC $(3, 6)$ -regular (de razão $\frac{1}{2}$) baseados, um deles num grafo de Ramanujan

$(3, 6)$ -biregular construído em [17] e o outro num grafo de Cayley $(3, 6)$ -biregular.

Apresentando a família dos grafos de Cayley, da qual a família de grafos de Ramanujan construídos em [17] faz parte, em [29], Vontobel comenta, à semelhança de Biggs e Boshier e também de Lubotzky, Phillips e Sarnak, a existência de um valor exato para a cintura destes últimos grafos. Em [29] é também referido que o resultado obtido em [17] para o minorante da cintura de um grafo de Ramanujan pode ser estendido a quaisquer p e q primos, e não apenas a p e q primos, onde $p, q \equiv 1 \pmod{4}$. Vontobel explora a construção de Margulis de grafos de Cayley e define os grupos essenciais à construção de grafos de Ramanujan feita em [17] demonstrando inclusivamente as suas respetivas cardinalidades. Em [29] avança-se também para conceitos fundamentais da Teoria dos Códigos, como é o caso da razão de um código, particularmente dos códigos LDPC.

No próximo capítulo são apresentados alguns conceitos e resultados preliminares essenciais para o estudo e para uma construção da família dos grafos de Ramanujan assim como para as aplicações destes que serão estudadas nos dois últimos capítulos, nomeadamente a construção de códigos LDPC e de funções de síntese.

No terceiro capítulo estuda-se a teoria da família dos grafos regulares e dos grafos de Ramanujan em particular, elaborando uma das suas construções (ver [5] e [17]) e termina-se o capítulo com diversos resultados acerca da cintura destes grafos, no caso de serem bipartidos.

De seguida, no quarto capítulo, é feita a construção de códigos LDPC e é apresentado um exemplo que clarifica essa mesma construção além da explicitação da deteção e possível correção de erros.

No quinto capítulo, de forma muito semelhante ao capítulo anterior, são apresentadas construções de duas funções de síntese, uma com base num qualquer grafo expensor (regular) e outra partindo de um grafo de Ramanujan.

Finalmente, no sexto capítulo, são apresentadas as conclusões desta dissertação.

Capítulo 2

Conceitos e resultados preliminares

Neste capítulo introduzem-se definições, notações e resultados preliminares de Teoria dos Grafos, de Álgebra Linear e de Teoria dos Números e Combinatória, respetivamente, que serão relevantes ao longo desta dissertação.

2.1 Teoria dos Grafos

Inicia-se este segundo capítulo de conceitos e resultados preliminares com uma secção inteiramente dedicada à Teoria dos Grafos. Nesta secção apresentam-se diversas definições encadeadas e também dois lemas essenciais para a propriedade espectral dos grafos regulares que se apresenta no terceiro capítulo (ver [8]).

Designa-se por *grafo* não orientado um terno $G = (V(G), E(G), \phi_G)$, onde o conjunto de *vértices* $V = V(G)$ é um conjunto numerável, o conjunto de *arestas* $E = E(G)$ é um conjunto disjunto de V e a *função de incidência* ϕ_G é tal que, para cada aresta $e \in E$, $\phi_G(e)$ denota um par não ordenado de elementos, não necessariamente distintos, de V . Se $e \in E(G)$ é a aresta que une os vértices $u, v \in V(G)$ escreve-se $\phi_G(e) = uv = vu$ e diz-se que u e v são os *vértices extremos* de e . Diz-se que G tem *ordem* n se $|V(G)| = n$. Dadas duas arestas $e_1, e_2 \in E(G)$ diferentes diz-se que e_1 e e_2 são *arestas paralelas* se têm os mesmos vértices extremos. Diz-se que e é um *lacete* de G se existe $v \in V(G)$ tal que $\phi_G(e) = vv$. Um grafo diz-se *simples* se não contém arestas paralelas nem lacetes. Daqui em diante, nesta dissertação, consideram-se apenas

grafos simples, logo identifica-se uma aresta do grafo com os seus vértices extremos, isto é, $e = uv$.

Dado um grafo G , designa-se por *passeio* em G toda a sequência não vazia

$$P = v_0 e_1 v_1 e_2 \dots e_k v_k,$$

tal que $v_0, v_1, \dots, v_k \in V(G)$ e $e_1, e_2, \dots, e_k \in E(G)$, onde os vértices v_{i-1} e v_i são os vértices extremos da aresta e_i , para $i = 1, \dots, k$. O vértice v_0 designa-se por *vértice inicial*, os vértices v_1, \dots, v_{k-1} designam-se por *vértices intermédios* e o vértice v_k designa-se por *vértice final* do passeio P . Se todas as arestas de P são distintas então P diz-se um *trajeto* e se, adicionalmente, todos os vértices são distintos então P diz-se um *caminho*. Se um trajeto é tal que os vértices inicial e final coincidem então designa-se por *circuito*. A um circuito sem repetição de vértices, com a exceção de que $v_0 = v_k$, designa-se por *ciclo*. Designa-se por *comprimento* de um passeio P , e denota-se por $comp(P)$, o número de arestas que o constituem, com eventual repetição, e diz-se que um circuito ou um ciclo com m arestas tem comprimento m . Um grafo diz-se *conexo* se entre qualquer par de vértices existe um caminho que os une e diz-se *acíclico* se não contém qualquer ciclo.

Seja $v \in V(G)$, designa-se por *grau* de v , e denota-se por $d_G(v)$, o número de arestas incidentes no vértice v e designa-se por *vizinhança* de v o conjunto dos vizinhos de v , ou seja, o conjunto $N_G(v) = \{u \in V(G) : uv = vu \in E(G)\}$. Diz-se que u e v são vértices *adjacentes* se existe uma aresta $e \in E(G)$ tal que u e v são vértices extremos de e . Um grafo diz-se *k-regular* se todos os seus vértices têm grau k e diz-se uma *árvore* se é conexo e acíclico. Uma árvore diz-se *infinita k-regular* se é uma árvore k -regular e se tem um número infinito de vértices.

Diz-se que uma aplicação $f : V(H) \rightarrow V(G)$ é um *homomorfismo* de um grafo H para um grafo G se f é tal que se $xy \in E(H)$ então $f(x)f(y) \in E(G)$ (ver [31]), isto é, f preserva as relações de adjacência. Dado f um homomorfismo de um grafo conexo H para um grafo G , diz-se que f é um *homomorfismo de cobertura* se para qualquer vértice v de H , a restrição de f a $N_H(v)$ é injetiva. Nesse caso, diz-se que H é uma *cobertura* de G ou que H *cobre* G . Dado um vértice $x_0 \in V(G)$, denota-se por $T_G(x_0)$ a árvore que tem x_0 como vértice raiz e que é obtida da seguinte forma:

seja $N_G(x_0) = \{v_1, v_2, \dots, v_k\}$ tem-se que as arestas de $T_G(x_0)$ que têm x_0 como vértice extremo são as arestas da forma $e_i = x_0 v_i, i \in \{1, \dots, k\}$. Iterativamente, as arestas que têm v_i como vértice extremo (e não têm x_0 como vértice extremo) são da forma $e_j = v_i v_j$, onde $j \notin \{1, \dots, k\}$, evitando-se a formação de ciclos nesta construção. Caso seja escolhido para vértice raiz um outro vértice x_1 de G obtém-se uma árvore isomorfa, isto é $T_G(x_0) \cong T_G(x_1)$. Assim sendo, por simplicidade de linguagem, designa-se esta árvore, daqui por diante, por T_G . A T_G chama-se *cobertura universal* de G (ver [13]).

Dado um grafo G , designa-se por *cintura de G* e denota-se por $g(G)$ o comprimento do circuito de menor comprimento em G , caso tal circuito exista. Caso contrário, diz-se que o grafo possui cintura infinita e escreve-se $g(G) = \infty$. Diz-se que G é *bipartido* se existe uma partição do seu conjunto de vértices em dois conjuntos X e Y tal que não existem arestas entre qualquer par de vértices de X nem entre qualquer par de vértices de Y , sendo que G é bipartido se e só não admite circuitos de comprimento ímpar. Adicionalmente, se G é bipartido e se cada vértice de X tem grau d_1 e cada vértice de Y tem grau d_2 , diz-se que G é (d_1, d_2) -*biregular* (ver [3]).

Se G é tal que $V(G) = \{v_1, \dots, v_n\}$ então designa-se por *matriz de adjacência* dos vértices de G , ou simplesmente matriz de adjacência de G , e denota-se por $A_G = (a_{ij})$, a matriz quadrada e simétrica de ordem n , tal que $a_{ij} = 1$, se $v_i v_j \in E(G)$ e $a_{ij} = 0$, caso contrário.

Dois grafos $G = (V(G), E(G), \phi_G)$ e $H = (V(H), E(H), \phi_H)$ dizem-se *isomorfos*, denotando-se essa relação de isomorfismo por $G \cong H$, se existem duas bijeções $\varphi : V(G) \rightarrow V(H)$ e $\psi : E(G) \rightarrow E(H)$ tais que:

$$\phi_G(e) = uv \text{ se e só se } \phi_H(\psi(e)) = \varphi(u)\varphi(v),$$

isto é, dois grafos dizem-se isomorfos se existe uma bijeção entre os respetivos conjuntos de vértices e uma bijeção entre os respetivos conjuntos de arestas que preservam as relações de adjacência e de incidência, respetivamente.

O próximo resultado é relevante na obtenção de um minorante do valor absoluto do segundo maior valor próprio (em valor absoluto) de um grafo regular e conexo que será enunciado e provado no próximo capítulo. Daqui em diante, denote-se por I_n a matriz identidade de ordem n .

Lema 2.1 [28] *Seja G um grafo de ordem n , A_G a sua matriz de adjacência e l um inteiro não negativo. Então $A_G^l = (\delta_{ij}^{(l)})$, onde $\delta_{ij}^{(l)}$ é o número de passeios distintos de comprimento l que unem o vértice i ao vértice j em G .*

Demonstração. Seja $\delta_{ij}^{(l)}$ a entrada (i, j) da matriz A_G^l e seja $p_{ij}(l)$ o número de passeios de comprimento l entre os vértices i e j do grafo G .

Fazendo a prova por indução sobre l , comece-se por observar que o resultado se verifica trivialmente para $l = 0$ pois $A_G^0 = I_n$ e que, para $l = 1$, pela definição de matriz de adjacência de um grafo o resultado também se verifica.

Suponha-se que o resultado é verdade para $l \geq 1$ e considere-se que $A_G^{l+1} = A_G^l A_G$. Assim, para qualquer aresta $v_i v_j$ tem-se que:

$$\begin{aligned} \delta_{ij}^{(l+1)} &= \sum_{r=1}^n \delta_{ir}^{(l)} \delta_{rj}^{(1)} \\ &= \sum_{r=1}^n p_{ir}(l) \delta_{rj}^{(1)} \\ &= p_{ij}(l+1), \end{aligned}$$

pois o número de passeios distintos de comprimento $l+1$ de v_i para v_j é igual à soma do número de passeios distintos de comprimento l de v_i para os vértices v_r que são adjacentes a v_j .

□

Denotando por $\det(Q)$ o determinante de uma matriz quadrada Q de ordem n , diz-se que $p_A(\lambda) = \det(A - \lambda I_n)$ é o *polinómio característico* de ordem n de A (ver [21]) e diz-se que um valor próprio de A_G é um *valor próprio do grafo G* , isto é, todo o $\lambda \in \mathbb{C}$ que verifica $p_{A_G}(\lambda) = 0$, definindo-se o *espectro* de G , e denotando-se por $\sigma(G)$, o conjunto de todos os valores próprios de G (ver [7]).

Por forma a demonstrar que todo o valor próprio da matriz de adjacência de um grafo é real, considere-se que a matriz \bar{P} e que o vetor \bar{x} representam respetivamente a matriz conjugada da matriz P e o vetor conjugado do vetor x .

Lema 2.2 [9] *Sejam G um grafo e λ um valor próprio de G então λ é real.*

Demonstração. Seja λ um valor próprio de A_G e seja x um vetor próprio de A_G associado a λ , isto é, x diferente do vetor nulo que verifica $A_G x = \lambda x$. Assim, identificando x como um vetor coluna cujas entradas são as coordenadas de x , tem-se que:

$$\begin{aligned}
\lambda \bar{x}^T x &= \bar{x}^T \lambda x \\
&= \bar{x}^T A_G x \\
&= (A_G^T \bar{x})^T x \\
&= (A_G \bar{x})^T x && (A_G \text{ é simétrica}) \\
&= (\overline{A_G x})^T x && (A_G \text{ é igual à sua conjugada}) \\
&= (\bar{\lambda} \bar{x})^T x \\
&= \bar{\lambda} \bar{x}^T x
\end{aligned}$$

Uma vez que x é diferente do vetor nulo conclui-se que $\lambda = \bar{\lambda}$, logo λ é real.

□

Como, pelo Lema 2.2, todos os valores próprios de um grafo são reais, estes podem ser ordenados da seguinte forma:

$$\lambda_0 \leq \lambda_1 \leq \dots \leq \lambda_{n-1}.$$

Ainda relativamente ao espectro de um grafo G , tem-se que se G contém pelo menos uma aresta e é bipartido então $\sigma(G)$ é simétrico relativamente a zero, isto é, se $\lambda \in \sigma(G)$ então $-\lambda \in \sigma(G)$. Se G é um grafo k -regular então $k \in \sigma(G)$ (ver [9] e [30]).

Depois de introduzidos alguns conceitos e resultados fundamentais da Teoria dos Grafos seguem-se algumas definições e resultados da Álgebra Linear também eles essenciais no decorrer deste trabalho.

2.2 Álgebra Linear

Nesta secção são apresentados alguns conceitos e resultados no âmbito da Álgebra Linear, como por exemplo o traço de uma matriz e o Primeiro Teorema do Isomorfismo, fundamentais na demonstração da Proposição 3.1 e numa construção de uma família de grafos de Ramanujan (ver [23] e [29]), respetivamente.

Definição 2.3 Define-se o *traço* de uma matriz quadrada A , e denota-se por $tr(A)$, a soma dos elementos da sua diagonal principal.

Depois de definido, veja-se uma propriedade importante do traço de uma matriz (quadrada).

Proposição 2.4 [10] *Seja V um espaço vetorial de dimensão n . Se M é a matriz de uma aplicação linear $\varphi : V \rightarrow V$ numa base B de V e se M' é uma matriz de $\varphi : V \rightarrow V$ numa base B' de V então $tr(M) = tr(M')$.*

Demonstração. Seja $m_{i,j}$ a entrada (i, j) da matriz M e considere-se $p_M(\lambda)$, o polinómio característico da matriz M , onde:

$$\begin{aligned} p_M(\lambda) &= \det(M - \lambda I_n) \\ &= \det \begin{bmatrix} m_{1,1} - \lambda & m_{2,1} & \dots & m_{n,1} \\ m_{1,2} & m_{2,2} - \lambda & \dots & m_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ m_{1,n} & m_{2,n} & \dots & m_{n,n} - \lambda \end{bmatrix} \end{aligned}$$

Por definição de determinante, $p_M(\lambda) = (m_{1,1} - \lambda)(m_{2,2} - \lambda) \dots (m_{n,n} - \lambda) + r_\lambda$, onde r_λ é um polinómio em λ de ordem inferior ou igual a $n - 2$, concluindo-se que:

$$p_M(\lambda) = (-1)^n \lambda^n + (-1)^{n-1} (m_{1,1} + m_{2,2} + \dots + m_{n,n}) \lambda^{n-1} + \tilde{r}_\lambda,$$

onde \tilde{r}_λ é um polinómio em λ de ordem inferior ou igual a $n - 2$. O traço de M é, a menos de uma mudança de sinal, o coeficiente associado ao termo de ordem $n - 1$ de $p_M(\lambda)$. Além disso, existe uma matriz S de mudança de base tal que é possível escrever $M' = S^{-1}MS$.

Assim,

$$\begin{aligned}
p_{M'}(\lambda) &= \det(M' - \lambda I_n) \\
&= \det(S^{-1}MS - \lambda I_n) \\
&= \det(S^{-1}MS - S^{-1}\lambda I_n S) \\
&= \det(S^{-1}(M - \lambda I_n)S) \\
&= \det(S^{-1}) \cdot \det(M - \lambda I_n) \cdot \det(S) \\
&= \det(M - \lambda I_n) \\
&= p_M(\lambda).
\end{aligned}$$

Concluindo-se que o polinómio característico é independente da base utilizada para a escrita de uma matriz de uma dada aplicação linear, tem-se que, em particular, os coeficientes associados ao termo de ordem $n - 1$ de $p_M(\lambda)$ e de $p_{M'}(\lambda)$ são iguais. Logo $tr(M) = tr(M')$.

□

Introduz-se agora o Primeiro Teorema do Isomorfismo fundamental na correspondência entre a construção de grafos de Ramanujan elaborada a partir de inteiros de Lipschitz e na construção de grafos de Ramanujan feita a partir de matrizes do grupo $PGL_2(\mathbb{Z}_q)$, cuja definição se encontra imediatamente depois deste teorema.

Teorema 2.5 [12] (*Primeiro Teorema do Isomorfismo*) Se $\varphi : G \rightarrow H$ é um homomorfismo de grupos, então φ induz um isomorfismo $G/Nuc \varphi \cong Im \varphi$.

De seguida definem-se quatro grupos e apresentam-se as suas ordens, essenciais para a construção apresentada da família de grafos de Ramanujan em [17].

Denote-se por \mathbb{F}_q o corpo finito com q elementos e por \mathbb{F}_q^* o conjunto $\mathbb{F}_q \setminus \{0\}$.

Definição 2.6 1. Define-se o grupo linear geral de ordem 2, denotado por $GL_2(\mathbb{F}_q)$, como o grupo das matrizes de ordem 2 invertíveis sobre \mathbb{F}_q .

2. O grupo linear geral projetivo de ordem 2, denotado por $PGL_2(\mathbb{F}_q)$, é o grupo

quociente $GL_2(\mathbb{F}_q)/D$, onde

$$D = \left\{ \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} : x \in \mathbb{F}_q^* \right\}.$$

3. Define-se o *grupo linear especial de ordem 2*, denotado por $SL_2(\mathbb{F}_q)$, como o grupo das matrizes de ordem 2 invertíveis sobre \mathbb{F}_q , cujo determinante é igual a 1.

4. O *grupo linear especial projetivo de ordem 2*, denotado por $PSL_2(\mathbb{F}_q)$, é o grupo quociente $SL_2(\mathbb{F}_q)/D'$, onde $D' = \{I_2, -I_2\}$.

O grupo $GL_2(\mathbb{F}_q)$ pode ser visto como a união disjunta de dois conjuntos:

$$GL_2(\mathbb{F}_q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a \neq 0, b, c, d \in \mathbb{F}_q, d \neq a^{-1}bc \right\} \cup \left\{ \begin{bmatrix} 0 & b \\ c & d \end{bmatrix} : b, c \neq 0, d \in \mathbb{F}_q \right\}.$$

O grupo $SL_2(\mathbb{F}_q)$ também pode ser visto como a união disjunta de dois conjuntos:

$$SL_2(\mathbb{F}_q) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a \neq 0, b, c, d \in \mathbb{F}_q, d = a^{-1}(1 + bc) \right\} \cup \left\{ \begin{bmatrix} 0 & b \\ c & d \end{bmatrix} : b \neq 0, c = -b^{-1}, d \in \mathbb{F}_q \right\}.$$

Proposição 2.7 [29] *Sejam $GL_2(\mathbb{F}_q)$ o grupo linear geral de ordem 2, $PGL_2(\mathbb{F}_q)$ o grupo linear projetivo de ordem 2, $SL_2(\mathbb{F}_q)$ o grupo linear especial de ordem 2 e $PSL_2(\mathbb{F}_q)$ o grupo linear especial projetivo de ordem 2, então a cardinalidade de cada um destes grupos é, respetivamente:*

$$\begin{aligned} |GL_2(\mathbb{F}_q)| &= q(q-1)(q^2-1). \\ |PGL_2(\mathbb{F}_q)| &= q(q^2-1). \\ |SL_2(\mathbb{F}_q)| &= q(q^2-1). \\ |PSL_2(\mathbb{F}_q)| &= \frac{q(q^2-1)}{2}. \end{aligned}$$

Demonstração. Pela união disjunta de dois conjuntos e pelos valores que a, b, c e d podem tomar respetivamente, a cardinalidade de $GL_2(\mathbb{F}_q)$ é

$$(q-1) \cdot q \cdot q \cdot (q-1) + 1 \cdot (q-1) \cdot (q-1) \cdot q = q(q-1)(q^2-1).$$

Como a cardinalidade de um grupo quociente G/N é o quociente entre a cardinalidade de G e a cardinalidade de N então a cardinalidade de $PGL_2(\mathbb{F}_q)$ é

$$\frac{q(q-1)(q^2-1)}{q-1} = q(q^2-1).$$

Pela união disjunta de dois conjuntos e pelos valores que a, b, c e d podem tomar respectivamente, a cardinalidade de $SL_2(\mathbb{F}_q)$ é

$$(q-1) \cdot q \cdot q \cdot 1 + 1 \cdot q \cdot (q-1) \cdot 1 = q(q^2-1).$$

Como a cardinalidade de um grupo quociente G/N é o quociente entre a cardinalidade de G e a cardinalidade de N então a cardinalidade de $PSL_2(\mathbb{F}_q)$ é $\frac{q(q^2-1)}{2}$.

□

2.3 Teoria dos Números e Combinatória

Nesta secção são apresentadas duas definições que serão úteis ao longo do texto, fundamentalmente na construção dos códigos LDPC (ver [1] e [29]). Apresenta-se também a fórmula de Stirling para uma aproximação de $n!$, observa-se que -1 é resíduo quadrático de qualquer primo da forma $4n+1$ e o teorema de Jacobi que dá o número de representações de um número ímpar positivo como soma de quatro quadrados. Todos estes resultados serão relevantes no próximo capítulo para a obtenção de um resultado sobre o espectro de um grafo regular (Proposição 3.1) e na construção dos grafos de Ramanujan feita em [17].

Definição 2.8 Sejam a inteiro e p primo. Diz-se que a é um *resíduo quadrático módulo p* se a congruência $x^2 \equiv a \pmod{p}$ tem exatamente duas soluções distintas. Se a congruência não tem soluções então diz-se que a é um *não resíduo quadrático módulo p* .

Definição 2.9 Sejam a inteiro e p primo. Define-se o símbolo de Legendre como:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{se } p \mid a \\ 1, & \text{se } a \text{ é resíduo quadrático módulo } p \\ -1, & \text{se } a \text{ é não resíduo quadrático módulo } p \end{cases}$$

Teorema 2.10 (Fórmula de Stirling) [8] Para cada inteiro $n \geq 1$ verificam-se as seguintes desigualdades:

$$\sqrt{2\pi n} n^n e^{-n} < n! < \sqrt{2\pi n} n^n e^{-n+\frac{1}{12n}}.$$

Corolário 2.11 Para cada inteiro $m \geq 1$, verificam-se as seguintes desigualdades:

$$\frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{-\frac{1}{6m}} < \binom{2m}{m} < \frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{\frac{1}{24m}}.$$

Demonstração. Pelo Teorema 2.10 tem-se que:

$$\sqrt{4\pi m} (2m)^{2m} e^{-2m} < (2m)! < \sqrt{4\pi m} (2m)^{2m} e^{-2m+\frac{1}{24m}} \quad (2.1)$$

e

$$\sqrt{2\pi m} m^m e^{-m} < m! < \sqrt{2\pi m} m^m e^{-m+\frac{1}{12m}}. \quad (2.2)$$

De (2.2) tem-se que:

$$2\pi m m^{2m} e^{-2m} < m!m! < 2\pi m m^{2m} e^{-2m+\frac{1}{6m}}. \quad (2.3)$$

Assim, de (2.1) e de (2.3) vem que:

$$\frac{\sqrt{4\pi m} (2m)^{2m} e^{-2m}}{2\pi m m^{2m} e^{-2m+\frac{1}{6m}}} < \frac{(2m)!}{m!m!} = \binom{2m}{m} < \frac{\sqrt{4\pi m} (2m)^{2m} e^{-2m+\frac{1}{24m}}}{2\pi m m^{2m} e^{-2m}}.$$

Logo, tal como pretendido, tem-se que:

$$\frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{-\frac{1}{6m}} < \binom{2m}{m} < \frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{\frac{1}{24m}}.$$

□

Teorema 2.12 [9] Seja p um primo ímpar. A congruência $x^2 \equiv -1 \pmod{p}$ tem duas soluções distintas se e só se $p \equiv 1 \pmod{4}$.

Teorema 2.13 (Teorema de Jacobi) [22] Se n é inteiro ímpar positivo então o número de representações de n como soma de quatro quadrados é $r_4(n) = 8 \sum_{\substack{d|n \\ 4 \nmid d}} d$.

Considere-se agora \mathbb{Z} , o conjunto dos números inteiros. Define-se

$$\mathbb{L}(\mathbb{Z}) = \{\alpha = a_0 + a_1i + a_2j + a_3k \mid a_t \in \mathbb{Z}, t = 0, 1, 2, 3\}$$

o conjunto dos inteiros de Lipschitz, onde

$$i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ik = -j, kj = -i \text{ e } ji = -k.$$

Diz-se que

$$\alpha = a_0 + a_1i + a_2j + a_3k \in \mathbb{L}(\mathbb{Z})$$

é congruente com

$$\beta = b_0 + b_1i + b_2j + b_3k \in \mathbb{L}(\mathbb{Z})$$

módulo n , e escreve-se $\alpha \equiv \beta \pmod{n}$, se

$$a_l \equiv b_l \pmod{n}, \text{ para } l \in \{0, 1, 2, 3\}.$$

Definição 2.14 Diz-se que $\epsilon \neq 0$ é uma *unidade* de $L(\mathbb{Z})$ se existe $\alpha \in L(\mathbb{Z})$ tal que $\epsilon\alpha = 1$.

Nota 2.15 Note-se que se ϵ é uma unidade de $\mathbb{L}(\mathbb{Z})$ e $\alpha \in \mathbb{L}(\mathbb{Z})$ então existe uma unidade ϵ' de $\mathbb{L}(\mathbb{Z})$ tal que $\epsilon\alpha = \alpha\epsilon'$, onde $\epsilon, \epsilon' \in \mathbb{L}(\mathbb{Z})$. Um inteiro de Lipschitz ϵ é uma unidade se e só se $N(\epsilon) = 1$.

Concluído que está o segundo capítulo, tendo já apresentado os conceitos e resultados essenciais para estudar os grafos de Ramanujan, avança-se para uma propriedade espectral dos grafos de Ramanujan, para a construção feita em [17] e para o estudo da cintura dos grafos de Ramanujan bipartidos.

Capítulo 3

Grafos de Ramanujan

Neste capítulo, começa-se por enunciar e demonstrar uma proposição transversal a todos os grafos regulares e de seguida, contando com o auxílio de diversos lemas enunciados ao longo da própria construção, é construída uma família de grafos de Ramanujan partindo da família dos grafos de Cayley. É ainda apresentado um resultado que determina um minorante e um majorante para a cintura destes grafos. Como consequência são deduzidos resultados exatos para a sua cintura (ver [5] e [17]). Inicia-se este capítulo, partindo do espectro de um grafo conexo e regular, com uma secção dedicada a uma condição verificada por estes grafos, condição essa verificada de forma extremal pelos grafos de Ramanujan sendo estes últimos considerados como ótimos no seu comportamento enquanto grafos expansores. Além disso, os grafos de Ramanujan têm uma cintura grande originando por isso bons códigos LDPC regulares.

3.1 Caracterização dos grafos de Ramanujan

Nesta secção apresenta-se uma propriedade transversal a todos os grafos regulares sobre o segundo maior valor próprio (em valor absoluto). Os grafos de Ramanujan são os grafos regulares que verificam o caso extremo desta propriedade.

Considere-se $X = X_{n,k}$ um grafo conexo, k -regular e de ordem n e considerem-se também todos os seus valores próprios (ver [16]):

$$k = \lambda_0 > \lambda_1 \geq \dots \geq \lambda_{n-1}, \text{ com } |\lambda_i| \leq k, \forall i \in \{0, 1, \dots, n-1\}.$$

Note-se que na ordenação dos valores próprios de X estabelece-se a desigualdade estrita $\lambda_0 > \lambda_1$ pois X é conexo (ver [9]).

Seja $\lambda(X) = \max_{0 \leq i \leq n-1} \{|\lambda_i| : |\lambda_i| \neq k\}$. Apresente-se a propriedade referida no início desta secção.

Proposição 3.1 [17] *Se X é um grafo k -regular de ordem n então verifica-se a seguinte desigualdade:*

$$\lim_{n \rightarrow +\infty} \lambda(X) \geq 2\sqrt{k-1}.$$

Demonstração. Seja A_X a matriz de adjacência de X . Então, pelo Lema 2.1, $A_X^l = (\delta_{ij}^{(l)})$, onde $\delta_{ij}^{(l)}$ é o número de passeios distintos de comprimento l que unem o vértice i ao vértice j em X . Sejam $k = \lambda_0 > \lambda_1 \geq \dots \geq \lambda_{n-1}$ os valores próprios de A_X . Pela Proposição 2.4 podem escolher-se os vetores próprios associados aos valores próprios de A_X para a constituição de uma base de \mathbb{R}^n (ver [7]) de tal forma que:

$$\sum_{j=0}^{n-1} \lambda_j^l = \sum_j \delta_{jj}^{(l)}. \quad (3.1)$$

Seja T^k a árvore k -regular que é cobertura universal de X . Assim, tem-se que

$$\delta_{jj}^{(l)} \geq \rho(l), \forall j \in \{0, \dots, n-1\}, \quad (3.2)$$

onde $\rho(l)$ é o número de passeios distintos de tamanho l em T^k que unem um vértice x_0 arbitrário a ele próprio.

Por (3.1) e (3.2) tem-se que

$$\sum_{j=0}^{n-1} \lambda_j^l \geq n\rho(l). \quad (3.3)$$

Removendo os dois maiores valores próprios em valor absoluto, $\lambda_0 = k$ e λ_{n-1} ou $\lambda_0 = k$ e λ_1 , tem-se que $\lambda(X)^{2l} \geq \lambda_i^{2l}$, onde $i \in \{1, \dots, n-2\}$ ou $i \in \{2, \dots, n-1\}$, respetivamente.

Assim,

$$(n-2)\lambda(X)^{2l} \geq \sum_{j=0}^{n-1} \lambda_j^{2l} - \lambda_0^{2l} - \lambda_t^{2l},$$

onde $t = 1$ ou $t = n-1$.

Como $\lambda_{n-1} \leq \lambda_0$ e $\lambda_{n-1} \geq -\lambda_0$ (ver [32]) então

$$\lambda_{n-1}^{2l} \leq \lambda_0^{2l}.$$

Além disso $\lambda_1 < \lambda_0$. Assim,

$$\lambda_0^{2l} + \lambda_1^{2l} \leq 2\lambda_0^{2l} = 2k^{2l}$$

e

$$\lambda_0^{2l} + \lambda_{n-1}^{2l} \leq 2\lambda_0^{2l} = 2k^{2l},$$

concluindo-se, por isso, que

$$(n-2)\lambda(X)^{2l} \geq \sum_{j=0}^{n-1} \lambda_j^{2l} - 2k^{2l}. \quad (3.4)$$

De (3.3) e (3.4) tem-se que:

$$\begin{aligned} \lambda(X)^{2l} &\geq \frac{n}{n-2}\rho(2l) - \frac{2k^{2l}}{n-2} \\ &\geq \rho(2l) - \frac{2k^{2l}}{n-2}. \end{aligned}$$

Obviamente $\rho(2l) \geq \rho'(2l)$, onde $\rho'(2l)$ é o número total de passeios distintos de comprimento $2l$ em T^k que começam e terminam em x_0 pela primeira vez, para qualquer vértice arbitrário x_0 .

Considere-se, em T^k , o passeio $v_0, y_1, v_1, \dots, y_{2l}, v_{2l}$ de comprimento $2l$ onde y_m é uma aresta, $\forall m \in \{1, \dots, 2l\}$. Partindo de v_0 , sem perda de generalidade, existem k possibilidades de escolha de um vértice v_1 adjacente a v_0 . Escolhido v_1 , existem agora $k-1$ possibilidades de escolha de um outro vértice da vizinhança de v_1 , com exceção de v_0 , pois existe uma e uma só possibilidade de voltar imediatamente a v_0 . Tal como em v_1 , em todos os outros vértices $v_t, t \in \{2, \dots, 2l\}$, do passeio (com exceção de v_0) existem $k-1$ possibilidades de escolha de um vértice adjacente caso não se pretenda a repetição da aresta y_t já percorrida ou existe apenas uma possibilidade caso se percorra de novo a aresta y_t . Assim sendo, existem $k \cdot (k-1)^{l-1} \cdot 1^l$ possibilidades de escolha dos vértices para um passeio de comprimento $2l$ que comece em v_0 e termine em v_{2l} . Como se pretende um passeio de v_0 a v_{2l} é possível associar cada um destes passeios a um perfil montanhoso (ver [8], página 150, exercício 6.5) da seguinte forma: a v_0 faz-se

corresponder o ponto de coordenadas $(0, 0)$ e a v_{2l} faz-se corresponder o ponto de coordenadas $(2l, 0)$. Além disso, considerando $y_0 = v_{-1}v_0$ uma aresta artificial onde v_{-1} é um vértice artificial, se em T^k é percorrida uma aresta $y_m = v_{m-1}v_m$ no sentido de v_{m-1} para v_m então é desenhado, no perfil montanhoso, um segmento de reta entre o ponto $(m-1, m-1)$ e o ponto (m, m) . Caso seja percorrida, em T^k , a aresta $y_m = v_{m-1}v_m$ no sentido de v_m para v_{m-1} então é desenhado, no perfil montanhoso, um segmento de reta entre o ponto de coordenadas (m, m) e o ponto de coordenadas $(m+1, m-1)$ existindo por isso $C_{l-1} = \frac{1}{l} \binom{2l-2}{l-1}$ perfis montanhosos diferentes de comprimento $2l$, onde C_{l-1} denota o número de Catalan de ordem $l-1$. Assim,

$$\rho'(2l) = \frac{1}{l} \binom{2l-2}{l-1} k(k-1)^{l-1}.$$

Deste modo, uma vez que $\rho(2l) \geq \rho'(2l)$ e que $\lambda(X)^{2l} \geq \rho(2l) - \frac{2k^{2l}}{n-2}$ tem-se que:

$$\begin{aligned} \lambda(X)^{2l} &\geq \rho'(2l) - \frac{2k^{2l}}{n-2} \\ &= \frac{1}{l} \binom{2l-2}{l-1} k(k-1)^{l-1} - \frac{2k^{2l}}{n-2}. \end{aligned}$$

Para $k > 1$, $k(k-1) > (k-1)(k-1)$, logo:

$$\lambda(X)^{2l} > \frac{1}{l} \binom{2l-2}{l-1} (\sqrt{k-1})^{2l} - \frac{2k^{2l}}{n-2}, \forall l \in \mathbb{N}.$$

Para qualquer $l \in \mathbb{N}$ vem que,

$$\lim_{n \rightarrow +\infty} \lambda(X)^{2l} \geq \frac{1}{l} \binom{2l-2}{l-1} (\sqrt{k-1})^{2l}. \quad (3.5)$$

Por outro lado, pelo Corolário 2.11, tem-se que, para $m \in \mathbb{N}$,

$$\frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{-\frac{1}{6m}} < \binom{2m}{m} < \frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{\frac{1}{24m}}. \quad (3.6)$$

Como

$$\lim_{m \rightarrow +\infty} \left[\left(\frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{-\frac{1}{6m}} \right)^{\frac{1}{2m+2}} \right] = 2 \quad \text{e} \quad \lim_{m \rightarrow +\infty} \left[\left(\frac{\sqrt{\pi m}}{\pi m} 2^{2m} e^{\frac{1}{24m}} \right)^{\frac{1}{2m+2}} \right] = 2,$$

então

$$\binom{2m}{m}^{\frac{1}{2m+2}} \rightarrow 2 \quad \text{quando} \quad m \rightarrow +\infty. \quad (3.7)$$

Para $m = l - 1$ tem-se que $2m = 2l - 2$. Logo $\frac{1}{2m+2} = \frac{1}{2l}$. Assim, e também por (3.7), tem-se que:

$$\left(\frac{2l-2}{l-1}\right)^{\frac{1}{2l}} \rightarrow 2 \quad \text{quando } l \rightarrow +\infty. \quad (3.8)$$

Por (3.6), prova-se que a função $f(x) := \left(\frac{1}{x}\right)^{\frac{1}{2x}} \left(\frac{2x-2}{x-1}\right)^{\frac{1}{2x}}$ é crescente. Por outro lado, intui-se que esta função tende para $g(x) := 2$ por valores inferiores. Ilustra-se esta tendência na figura 3.1.

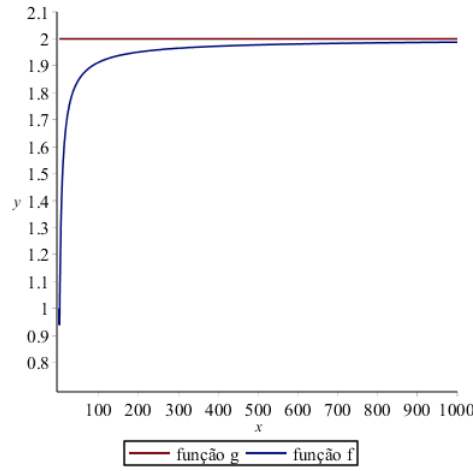


Figura 3.1: Gráficos das funções f e g

Assim, por (3.5) e (3.8), tem-se que

$$\lim_{n \rightarrow +\infty} \lambda(X) \geq \lim_{l \rightarrow +\infty} \left[\left(\frac{1}{l}\right)^{\frac{1}{2l}} \left(\frac{2l-2}{l-1}\right)^{\frac{1}{2l}} \sqrt{k-1} \right] = 2\sqrt{k-1}.$$

□

Dentro da família dos grafos regulares existem grafos que verificam uma condição extremal, grafos esses que se definem de seguida (ver [17]).

Definição 3.2 Seja X um grafo k -regular. Diz-se que X é um *grafo de Ramanujan* se $\lambda(X) \leq 2\sqrt{k-1}$.

Além da definição é possível explicitar uma construção de uma família de grafos de Ramanujan partindo dos grafos de Cayley.

3.2 Grafos de Cayley

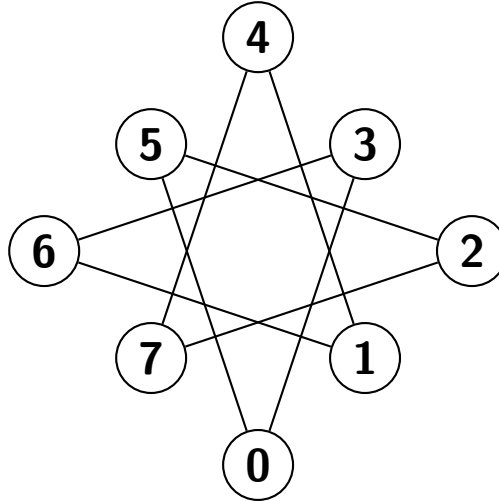
Nesta secção serão definidos e exemplificados os grafos de Cayley. Com base nestes será construída uma família de grafos de Ramanujan (ver [17]), construção essa que será apresentada na secção seguinte.

Seja S um conjunto e $\langle H, * \rangle$ um grupo, onde H é um conjunto e $*$ é uma operação binária. Diz-se que $S \subseteq H$ é *gerador* de H se $\forall h \in H \ h = s_1 \dots s_t$, com $s_1, \dots, s_t \in S$. S é *gerador simétrico* de H se S é gerador de H e se $S = S^{-1}$, onde S^{-1} denota o conjunto constituído por todos os inversos dos elementos de S . Define-se *grafo de Cayley* $X(H, S)$ como um grafo que admite $V = H$ como o seu conjunto de vértices e $E = \{v(v * s) \mid v \in V, s \in S\}$ como o seu conjunto de arestas (ver [29]).

Exemplo 3.3 Considere-se o grupo $\langle H, * \rangle = \langle \mathbb{Z}_8, + \rangle$ e o conjunto $S = \{-3, 3\}$. Assim:

$$V_{X(H,S)} = \mathbb{Z}_8 \text{ e } E_{X(H,S)} = \{h(h + s) : h \in \mathbb{Z}_8, s \in S\}$$

Desta forma, obtém-se o seguinte grafo de Cayley $X(H, S)$ 2-regular:



3.3 Construção LPS

Nesta secção propõe-se uma construção de uma família de grafos de Ramanujan, com base na família dos grafos de Cayley, proposta em [17] por Lubotzky, Phillips e

Sarnak. Denominar-se-á esta construção, daqui por diante, por construção LPS. Para esta construção recorre-se a conceitos e resultados preliminares do segundo capítulo.

Considerem-se dois primos p e q distintos tais que $p, q \equiv 1 \pmod{4}$.

Vão ser construídos grafos de Ramanujan, que se denotarão daqui por diante por $X^{p,q}$, enquanto grafos de Cayley $(p+1)$ -regulares. Prova-se que se $\left(\frac{p}{q}\right) = 1$ então $X^{p,q}$ não é bipartido e a sua ordem é $\frac{q(q^2-1)}{2}$ e que se $\left(\frac{p}{q}\right) = -1$ então $X^{p,q}$ é bipartido e a sua ordem é $q(q^2-1)$.

Por forma a iniciar a construção LPS de $X^{p,q}$ relembre-se o conjunto dos inteiros de Lipschitz:

$$\mathbb{L}(\mathbb{Z}) = \{\alpha = a_0 + a_1i + a_2j + a_3k \mid a_t \in \mathbb{Z}, t = 0, 1, 2, 3\},$$

$$\text{onde } i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ik = -j, kj = -i \text{ e } ji = -k.$$

Dado $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathbb{L}(\mathbb{Z})$, o seu conjugado e a sua norma são

$$\bar{\alpha} = a_0 - a_1i - a_2j - a_3k \text{ e } N(\alpha) = \alpha\bar{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

respetivamente, definindo-se como *componentes* de α os a_t com $t \in \{0, 1, 2, 3\}$.

Por simplicidade de linguagem denomina-se, daqui por diante, um inteiro de Lipschitz por quaternião.

Lema 3.4 [17] *Seja $\alpha = a_0 + a_1i + a_2j + a_3k \in \mathbb{L}(\mathbb{Z})$ tal que $N(\alpha) = p$ e $p \equiv 1 \pmod{4}$. Então exatamente uma das componentes de α é ímpar.*

Demonstração. Claramente o quadrado de um número ímpar é um número ímpar congruente com $1 \pmod{4}$ e o quadrado de um número par é um número par congruente com $0 \pmod{4}$. Como $p \equiv 1 \pmod{4}$ e $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$ então exatamente uma das componentes de α é ímpar.

□

Continue-se a considerar p e q primos distintos, com $p, q \equiv 1 \pmod{4}$ e seja i tal que $i^2 \equiv -1 \pmod{q}$. Note-se que, pelo Teorema 2.12, existe i que verifica esta condição pois $q \equiv 1 \pmod{4}$. Pelo Teorema 2.13, tem-se que existem $8(p+1)$ formas diferentes

de escrever p como soma de quatro quadrados. A cada uma dessas formas associa-se um quaternião cuja norma é p . Se α é um desses quaterniões então existe uma unidade $\epsilon \in \mathbb{L}(\mathbb{Z})$ tal que $\epsilon\alpha \equiv 1 \pmod{2}$, isto é, a sua parte real é um inteiro ímpar positivo.

Assim, existem exatamente $p + 1$ quaterniões com a_0 inteiro ímpar positivo e com a_1, a_2, a_3 inteiros pares. Seja $S = \{\alpha_1, \bar{\alpha}_1, \alpha_2, \bar{\alpha}_2, \dots, \alpha_s, \bar{\alpha}_s\}$ o conjunto destes $p + 1$ quaterniões. A cada um destes quaterniões da forma $\alpha = a_0 + a_1i + a_2j + a_3k$ associa-se a matriz

$$A = \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix} \pmod{q},$$

onde $\det(A) = p$.

Tendo quaterniões de norma p , procura-se de seguida, no Lema 3.6, escrever um quaternião com norma p^k , de forma única, como um produto de quaterniões de norma p . Para isso comece-se por definir palavra reduzida e por estabelecer o próximo resultado.

Diz-se que u é uma *palavra reduzida* de comprimento m em S se u é o produto de m elementos de S sem fatores da forma $\alpha_i \bar{\alpha}_i$ nem da forma $\bar{\alpha}_i \alpha_i$, onde $1 \leq i \leq s$, e denota-se por $R_m(\alpha_1, \dots, \bar{\alpha}_s)$ o conjunto de todas as palavras reduzidas de comprimento m , em S .

Teorema 3.5 [15] *Seja $\alpha \in \mathbb{L}(\mathbb{Z})$. Se $a \mid N(\alpha)$ então existe $\gamma \in \mathbb{L}(\mathbb{Z})$ tal que $N(\gamma) = a$ e $\gamma \mid \alpha$.*

Lema 3.6 [17] *Todo o $\alpha \in \mathbb{L}(\mathbb{Z})$ que verifica $N(\alpha) = p^k$ pode ser escrito de forma única como:*

$$\alpha = \epsilon p^r r_m,$$

onde ϵ é uma unidade de $\mathbb{L}(\mathbb{Z})$, $2r + m = k$, e $r_m \in R_m(\alpha_1, \dots, \bar{\alpha}_s)$.

Demonstração.

Seja $S = \{\alpha_1, \dots, \bar{\alpha}_s\}$ o conjunto dos quaterniões com norma p e $R_m(\alpha_1, \dots, \bar{\alpha}_s)$ o conjunto das palavras reduzidas de comprimento m , em S .

Fazendo a prova deste lema por indução sobre k comece-se por provar que é verdadeiro para $k = 1$.

Seja α tal que $N(\alpha) = p$, logo $\alpha = \epsilon_\alpha \alpha'$, onde ϵ_α é uma unidade de $\mathbb{L}(\mathbb{Z})$ e $\alpha' \in S$.

Assim, como $2r + m = 1$ e $r, m \geq 0$ inteiros então $r = 0$ e $m = 1$, logo α pode ser escrito como

$$\begin{aligned}\alpha &= \epsilon_\alpha \alpha' \\ &= \epsilon_\alpha \cdot p^0 \cdot \alpha'\end{aligned}$$

e $\alpha' \in R_1(\alpha_1, \dots, \bar{\alpha}_s)$.

Assumindo que o resultado se verifica para $k - 1$, mostre-se que também se verifica para k .

Seja α tal que $N(\alpha) = p^k$. Como $p^{k-1} \mid p^k$, então, pelo Teorema 3.5, existe $\gamma \in \mathbb{L}(\mathbb{Z})$ tal que $N(\gamma) = p^{k-1}$ e $\gamma \mid \alpha$.

Assim, por hipótese de indução, $\gamma = \epsilon \cdot p^r \cdot r_m$, onde ϵ é uma unidade de $\mathbb{L}(\mathbb{Z})$, $2r + m = k - 1$, e $r_m \in R_m(\alpha_1, \dots, \bar{\alpha}_s)$.

Além disso, como $\gamma \mid \alpha$ então existe β tal que $\alpha = \gamma\beta$, onde $N(\beta) = p$. Assim, $\beta = \epsilon_\beta \cdot \beta'$, onde $\beta' \in S$ e

$$\begin{aligned}\alpha &= \gamma\beta \\ &= \epsilon \cdot p^r \cdot r_m \cdot \epsilon_\beta \cdot \beta' \\ &= \epsilon' \cdot p^r \cdot r_m \cdot \beta',\end{aligned}$$

por m aplicações da Nota 2.15, onde ϵ' é uma unidade de $\mathbb{L}(\mathbb{Z})$.

Pode escrever-se r_m como o produto de uma palavra reduzida de comprimento $m - 1$ por uma palavra reduzida de comprimento 1, isto é,

$$r_m = r'_{m-1} \cdot r'_1,$$

com $r'_{m-1} \in R_{m-1}(\alpha_1, \dots, \bar{\alpha}_s)$ e $r'_1 \in R_1(\alpha_1, \dots, \bar{\alpha}_s)$. Tem-se duas possibilidades para r'_1 :

(i) $r'_1 = \bar{\beta}'$: Neste caso,

$$\begin{aligned}\alpha &= \epsilon' \cdot p^r \cdot r'_{m-1} \cdot \beta' \cdot \beta \\ &= \epsilon' \cdot p^{r+1} \cdot r'_{m-1},\end{aligned}$$

e

$$\begin{aligned}
2(r+1) + m - 1 &= (2r + m) + 1 \\
&= k - 1 + 1 && \text{(por hipótese de indução)} \\
&= k.
\end{aligned}$$

(ii) $r'_1 \neq \overline{\beta'}$: Neste caso,

$$\begin{aligned}
\alpha &= \epsilon' \cdot p^r \cdot r'_{m-1} \cdot r'_1 \cdot \beta' \\
&= \epsilon' \cdot p^r \cdot r'_{m+1},
\end{aligned}$$

onde $r'_{m+1} \in R_{m+1}(\alpha_1, \dots, \overline{\alpha}_s)$ e

$$\begin{aligned}
2r + (m+1) &= k - 1 + 1 && \text{(por hipótese de indução)} \\
&= k.
\end{aligned}$$

□

Como consequência, tem-se o seguinte corolário.

Corolário 3.7 [17] *Se $\alpha \equiv 1 \pmod{2}$ e $N(\alpha) = p^k$ então pode representar-se α de forma única, onde:*

$$\alpha = \pm p^r r_m, \quad 2r + m = k.$$

Depois destes dois últimos resultados prossegue-se este trabalho com a concretização da construção de uma família de grafos de Ramanujan enquanto grafos de Cayley (ver [5] e [17]).

Considere-se $\Lambda'(2)$ o conjunto de todos os $\alpha \in \mathbb{L}(\mathbb{Z})$ tais que:

$\alpha \equiv 1 \pmod{2}$, $a_0 > 0$ e $N(\alpha) = p^\nu$, para algum $\nu \in \mathbb{Z}$ não negativo, e seja $\Lambda(2)$ o conjunto das classes de equivalência obtidas de $\Lambda'(2)$ identificando α com β sempre que é possível escrever $\pm p^{\nu_1} \alpha = p^{\nu_2} \beta$, para alguns $\nu_1, \nu_2 \in \mathbb{Z}$ não negativos. Assim, as classes de equivalência que formam o grupo $\Lambda(2)$ verificam:

$$[\alpha][\beta] = [\alpha\beta] \text{ e } [\alpha][\bar{\alpha}] = [\alpha\bar{\alpha}] = [N(\alpha)] = [p^\nu \cdot 1] = [1].$$

Deste modo, o grafo de Cayley $Y^{p,q} = X_1(H, S)$ que tem como grupo $H = \Lambda(2)$ e como conjunto simétrico $S = \{\alpha \in \mathbb{L}(\mathbb{Z}) : N(\alpha) = p, a_0 \text{ é inteiro ímpar positivo}\}$, é uma árvore infinita $(p+1)$ -regular.

Defina-se agora o subgrupo normal $\Lambda(2q)$ de $\Lambda(2)$ por

$$\Lambda(2q) = \{[\alpha] \in \Lambda(2) : 2q \mid a_j, j = 1, 2, 3\}$$

e considere-se o grafo de Cayley $X^{p,q} = X_2(H', S)$ que tem como grupo $H' = \Lambda(2)/\Lambda(2q)$ e S como conjunto simétrico. Prova-se que $X^{p,q}$ é grafo de Ramanujan.

De seguida, por forma a ser utilizado nos próximos capítulos, constrói-se $X^{p,q}$ com base no grupo $PGL_2(\mathbb{Z}_q)$.

Proposição 3.8 [17] *Seja*

$$\begin{aligned} \varphi : \Lambda(2) &\rightarrow PGL_2(\mathbb{Z}_q) \\ [\alpha] &\mapsto \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix}, \end{aligned}$$

então

$$Im \varphi = \begin{cases} PGL_2(\mathbb{Z}_q) & \text{se } \left(\frac{p}{q}\right) = -1 \\ PSL_2(\mathbb{Z}_q) & \text{se } \left(\frac{p}{q}\right) = 1. \end{cases}$$

Demonstração.

A demonstração desta proposição sai do âmbito desta dissertação, recorrendo-se nomeadamente à teoria das séries singulares de Hardy e Littlewood e à teoria das equações quadráticas diofantinas. Para uma melhor compreensão aconselha-se a consulta de [17].

□

Assim, pelo Teorema 2.5, uma vez que $Nuc \varphi = \Lambda(2q)$ tem-se que:

$$\begin{cases} \Lambda(2)/\Lambda(2q) \cong PGL_2(\mathbb{Z}_q) & \text{se } \left(\frac{p}{q}\right) = -1 \\ \Lambda(2)/\Lambda(2q) \cong PSL_2(\mathbb{Z}_q) & \text{se } \left(\frac{p}{q}\right) = 1. \end{cases}$$

Conclui-se por isso que, através de φ , se faz corresponder cada gerador de $S = \{\alpha_1, \dots, \bar{\alpha}_s\}$ a uma matriz de $PGL_2(\mathbb{Z}_q)$ cujo determinante é p , logo o grafo $X^{p,q}$ pode ser identificado com $\Lambda(2)/\Lambda(2q)$.

Teorema 3.9 $X^{p,q}$ é um grafo de Ramanujan.

Demonstração. Para a demonstração de que $X^{p,q}$, pela forma como é construído, é um grafo de Ramanujan recorre-se a conceitos e resultados que ultrapassam o âmbito desta dissertação, nomeadamente na Teoria da Medida, na ação de grupos de isometrias e em séries de Eisenstein. Para a compreensão (da complexidade) desta demonstração aconselha-se a consulta de [17]. \square

Depois da construção LPS, procuram-se agora estabelecer resultados para a cintura destes grafos, no caso de serem bipartidos (ver [5]).

3.4 Cintura de grafos de Ramanujan bipartidos

Tal como referido no primeiro capítulo, foram vários os autores que apresentaram minorantes, majorantes e resultados exatos para a cintura dos grafos de Ramanujan que serão apresentados nesta secção. Comece-se por apresentar algumas definições (ver [14]) e resultados acerca de $\Lambda(2q)$ por forma a culminar na apresentação desses valores para a cintura.

Definição 3.10 Seja G um grafo e sejam $v_1, v_2 \in V(G)$. Diz-se que G é *vértice-transitivo* se existe um automorfismo $\eta : V(G) \rightarrow V(G)$ tal que $\eta(v_1) = v_2$, isto é o grupo de automorfismos de G atua transitivamente sobre $V(G)$.

Considerem-se, no que se segue nesta secção, dois primos distintos $p, q \equiv 1 \pmod{4}$ tais que $q^2 > p$.

Sendo $X^{p,q}$ um grafo de Cayley, e por consequência vértice-transitivo (ver [4]), a sua cintura é a distância mínima entre um vértice etiquetado com uma matriz identidade e um vértice etiquetado com um elemento não trivial de $\Lambda(2q)$ na árvore infinita em $\Lambda(2)$. Daqui por diante dir-se-á que um elemento de $\Lambda(2)$ está no nível r se está à distância r da identidade na árvore em $\Lambda(2)$. Na presença de um grafo bipartido, esta distância é necessariamente par.

Lema 3.11 [5] Se $[b] \in \Lambda(2q)$ está no nível $2r$, para $r > 0$, então

$$b = b_0 + 2q(b_1i + b_2j + b_3k) \in L(\mathbb{Z})$$

pode ser escolhido tal que:

$$b_0 = \pm (p^r - mq^2),$$

onde $m > 0$ é par.

Demonstração. Se existe b tal que:

$$\begin{aligned} p^{2r} &= N(b) \\ &= b_0^2 + 4q^2b_1^2 + 4q^2b_2^2 + 4q^2b_3^2 \end{aligned}$$

então

$$b_0^2 \equiv p^{2r} \pmod{q^2}.$$

Como $(\mathbb{Z}_{q^2})^*$ é cíclico então é possível extrair a raiz quadrada, logo:

$$b_0 \equiv \pm p^r \pmod{q^2}.$$

Como $r > 0$, conclui-se que a congruência tem soluções para além das triviais $b_0 = \pm p^r$. Além disso, tem-se que:

$$\begin{aligned} b_0^2 &= p^{2r} - 4q^2b_1^2 - 4q^2b_2^2 - 4q^2b_3^2 \\ &< p^{2r}. \end{aligned}$$

Finalmente, uma vez que $|b_0| < p^r$ e que b_0 é ímpar tem-se o pretendido.

□

Antes do próximo lema, que auxilia na determinação de um majorante para a cintura de $X^{p,q}$, veja-se um conceito essencial para este (ver [5]) e também o Teorema de Legendre que caracteriza quais inteiros podem ser escritos como soma de três quadrados.

Definição 3.12 Seja n inteiro positivo. Diz-se que n é *good* se não existem α e β inteiros não negativos tais que $n = 4^\alpha(8\beta + 7)$.

Teorema 3.13 [5] (Teorema de Legendre) *Seja n inteiro positivo. Então n é good se e só se n pode ser escrito como soma de três quadrados.*

Lema 3.14 [5] *Seja $b = b_0 + b_1i + b_2j + b_3k \in L(\mathbb{Z})$. Existe uma classe de equivalência $[b] \in \Lambda(2q)$ no nível $2r$ com $b_0 = p^r - mq^2$ (onde m é par e positivo) se e só se $2mp^r - m^2q^2$ é good.*

Demonstração. Se existe $[b] \in \Lambda(2q)$ no nível $2r$ com $b_0 = p^r - mq^2$ então, pelo Lema (3.11), pode escrever-se

$$p^{2r} = (p^r - mq^2)^2 + 4q^2 (b_1^2 + b_2^2 + b_3^2).$$

Equivalentemente, tem-se que,

$$2mp^r - m^2q^2 = (2b_1)^2 + (2b_2)^2 + (2b_3)^2.$$

Assim, pelo Teorema 3.13, $2mp^r - m^2q^2$ é good, tal como se pretendia.

Já no que diz respeito à implicação contrária, comece-se por notar que, como m é par, então

$$2mp^r - m^2q^2 \equiv 0 \pmod{4}.$$

Como $2mp^r - m^2q^2$ é good então, pelo Teorema 3.13, tem-se que $2mp^r - m^2q^2$ pode ser escrito como soma de três quadrados pares:

$$2mp^r - m^2q^2 = (2b_1)^2 + (2b_2)^2 + (2b_3)^2.$$

Assim, tem-se que:

$$p^{2r} = (p^r - mq^2)^2 + (2qb_1)^2 + (2qb_2)^2 + (2qb_3)^2.$$

Conclui-se por isso que se $b = (p^r - mq^2) + 2qb_1i + 2qb_2j + 2qb_3k$ então $[b] \in \Lambda(2q)$ está no nível $2r$, o que completa a demonstração.

□

Exemplo 3.15 Recorde-se a condição necessária $q^2 > p$. Esta condição permite rejeitar grafos cuja cintura seja 2, ou seja, grafos que contenham arestas paralelas. Tal condição impõe-se para evitar a hipótese de que $r = 1$, isto é, evita-se que exista $[b] \in \Lambda(2q)$ no nível 2.

Para $m = 2$ e $r = 1$ tem-se $2mp^r - m^2q^2 = 4(p - q^2)$. Se $4(p - q^2) < 0$ então não é good. Além disso,

$$4(p - q^2) < 0 \Leftrightarrow p < q^2.$$

Conclui-se que, para $m = 2$ e $r = 1$, se $p < q^2$ então $4(p - q^2)$ não é good, isto é, não existe $[b] \in \Lambda(2q)$ no nível 2.

Considerem-se $p = 37$ e $q = 5$. Pode escrever-se 37 como soma de quatro quadrados, recorrendo aos valores:

$$(1, \pm 6, 0, 0), (1, 0, \pm 6, 0), (1, 0, 0, \pm 6), (5, \pm 2, \pm 2, \pm 2),$$

$$(1, \pm 2, \pm 4, \pm 4), (1, \pm 4, \pm 2, \pm 4) \text{ e } (1, \pm 4, \pm 4, \pm 2)$$

Para $m = 2$ e $r = 1$ tem-se $4p - 4q^2 = 4 \cdot 12 = 4 \cdot (2^2 + 2^2 + 2^2)$ é good. Assim, existe $[b] \in \Lambda(2q)$ tal que $b_0 = p - 2q^2 = -13$, onde $b = b_0 + 4qi + 4qj + 4qk$. Note-se que $|-13| < 37$.

Assim, a partir de $(5, \pm 2, \pm 2, \pm 2)$, tem-se que

$$\begin{aligned} b &= (-1) \cdot (5 - 2i - 2j - 2k)^2 \\ &= -1(13 - 20i - 20j - 20k) \\ &= -13 + 20i + 20j + 20k \end{aligned}$$

e

$$\begin{aligned} N(b) &= (-1)^2 \cdot 37^2 \\ &= 1369 \end{aligned}$$

Note-se que, em $\Lambda(2)/\Lambda(2q)$, o quaternião $5 - 2i - 2j - 2k$ é igual ao seu inverso. Partindo da identidade, chega-se ao quaternião $5 - 2i - 2j - 2k$ e depois regressa-se à identidade pela mesma aresta. Havendo repetição de, pelo menos, uma aresta não existe circuito o que implica a impossibilidade da medição da cintura do grafo. Assim, tal como referido em [5] e [29], exige-se que $q^2 > p$.

Teorema 3.16 [5] *Sejam p e q primos tais que $p, q \equiv 1 \pmod{4}$ e $\left(\frac{p}{q}\right) = -1$ então:*

$$4 \log_p q - \log_p 4 \leq g(X^{p,q}) < 4 \log_p q + \log_p 4 + 2.$$

Demonstração. Comece-se por provar que pelo menos um dos inteiros da forma $2mp^r - m^2q^2$, para $m = 2$ ou $m = 4$, é good, estando assegurado que ambos são positivos. Suponha-se que para o caso em que $m = 2$ o inteiro não é good, ou seja, o inteiro $4(p^r - q^2)$ não é good, e que, por consequência $p^r - q^2$ não é good. Assim, para alguns α e β inteiros não negativos, pode escrever-se:

$$p^r - q^2 = 4^\alpha(8\beta + 7).$$

Para $m = 4$ obtém-se um inteiro da forma $8p^r - 16q^2$, onde:

$$\begin{aligned} 8p^r - 16q^2 &= 8(p^r - q^2) - 8q^2 \\ &= 8(4^\alpha(8\beta + 7) - q^2). \end{aligned}$$

Como $p, q \equiv 1 \pmod{4}$ então $p^r, q^2 \equiv 1 \pmod{4}$, logo $\alpha \geq 1$. Conclui-se que $4^\alpha(8\beta + 7) - q^2$ é ímpar e que, por consequência, $8p^r - 16q^2$ é good.

Seja r_0 o menor inteiro r para o qual $p^r > 2q^2$ e note-se que, assim sendo, tanto $4(p^r - q^2)$ como $8p^r - 16q^2$ são positivos. Então:

$$p^{r_0-1} < 2q^2. \tag{3.9}$$

Por (3.9) tem-se que:

$$\begin{aligned} (r_0 - 1) \log_p p &< \log_p (2q^2) \\ r_0 - 1 &< \log_p 2 + 2 \log_p q \\ r_0 &< 2 \log_p q + \log_p 2 + 1. \end{aligned}$$

Finalmente, pelo que foi verificado anteriormente, existe $[b] \in \Lambda(2q)$ no nível $2r_0$ o que implica

$$g(X^{p,q}) \leq 2r_0 < 4 \log_p q + \log_p 4 + 2,$$

ficando determinado um majorante para a cintura destes grafos, caso sejam bipartidos.

Por forma a determinar um minorante da cintura, comece-se por enunciar dois conceitos essenciais para essa determinação (ver [8] e [11])

Definição 3.17 Dados um grafo G e $V' \subseteq V(G)$, com $V' \neq \emptyset$, designa-se por *subgrafo* de G *induzido* por V' e denota-se por $\langle V' \rangle_G$, o subgrafo de G cujo conjunto de vértices é V' e o conjunto de arestas é composto por todas as arestas de G cujos extremos pertencem a V' .

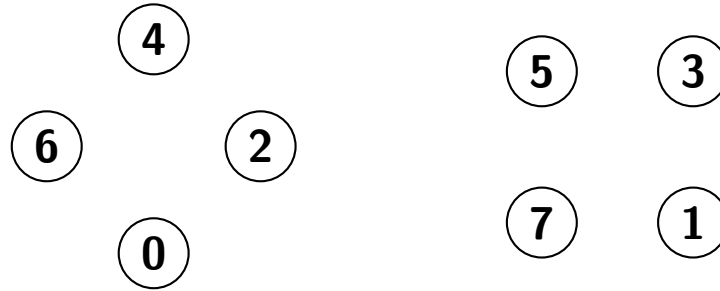
Definição 3.18 Seja G um grafo e sejam $V_1, V_2 \subseteq V(G)$ tais que $\langle V_1 \rangle_G$ e $\langle V_2 \rangle_G$ são isomorfos. G diz-se um grafo *homogéneo* se existe um automorfismo de G definido de V_1 para V_2 .

É relevante neste trabalho o facto de que todo o grafo de Cayley é homogéneo. Explicite-se então que o grafo de Cayley considerado no Exemplo 3.3 o verifica.

Exemplo 3.19 Considere-se o grafo de Cayley $X(H, S)$ do Exemplo 3.3 (onde $H = \mathbb{Z}_8$ e $S = \{3, -3\}$) e considere-se também a partição dos seus vértices em

$$V(X(H, S)) = V_1 \cup V_2, \text{ onde } V_1 = \{0, 2, 4, 6\} \text{ e } V_2 = \{1, 3, 5, 7\}.$$

Representam-se de seguida os subgrafos induzidos de $X(H, S)$, $\langle V_1 \rangle_{X(H, S)}$ (à esquerda) e $\langle V_2 \rangle_{X(H, S)}$ (à direita), sendo que $\langle V_1 \rangle_{X(H, S)}$ e $\langle V_2 \rangle_{X(H, S)}$ são claramente isomorfos.



Considere-se o automorfismo

$$\begin{aligned} \eta : V_1 &\rightarrow V_2 \\ i &\mapsto i + 1, \end{aligned}$$

para $i \in \{0, 2, 4, 6\}$ tal que se $uv \in E(\langle V_1 \rangle_{X(H, S)})$ então $\eta(u)\eta(v) \in E(\langle V_2 \rangle_{X(H, S)})$. Tal condição verifica-se trivialmente pois nenhum dos subgrafos induzidos possui arestas. Conclui-se assim que $X(H, S)$ é um grafo homogéneo.

Depois de vistos estes conceitos, determine-se o minorante apresentado (ver [17]).

Como $X^{p,q}$ é um grafo de Cayley então é homogéneo. Assim, pode dizer-se que um dos circuitos de menor comprimento é o circuito que tem como vértices inicial e final a identidade. Na árvore $\Lambda(2)$ esse comprimento corresponde ao número de fatores em

S do menor elemento não trivial de $\Lambda(2q)$. Se $\rho \in \Lambda(2q)$ não é uma unidade e possui t fatores em S então existe um quaternião $\tilde{\rho} \in \Lambda'(2)$ tal que

$$\tilde{\rho} = \beta_1 \beta_2 \dots \beta_t, \text{ onde } \beta_j \in S, j \in \{1, \dots, t\}.$$

Tem-se assim que:

$$N(\tilde{\rho}) = p^t \text{ e } \tilde{\rho} = a_0 + 2qa_1i + 2qa_2j + 2qa_3k, a_t \in \mathbb{Z}, t \in \{0, 1, 2, 3\}.$$

Como ρ não é uma unidade então pelo menos um de entre a_1, a_2 e a_3 é não nulo.

Assim, pode escrever-se

$$p^t = a_0^2 + 4q^2a_1^2 + 4q^2a_2^2 + 4q^2a_3^2. \quad (3.10)$$

Estando a estudar a cintura no caso do grafo bipartido, ou seja $\left(\frac{p}{q}\right) = -1$, e como da equação (3.10) se tem que

$$a_0^2 \equiv p^t \pmod{q^2},$$

então $\left(\frac{p}{q}\right) = 1$ logo $t > 0$ é par, isto é, existe $r \in \mathbb{N}$ tal que $t = 2r$.

Assim a equação (3.10) tem as soluções triviais $a_0 = \pm p^r$. De facto, a congruência

$$x_0^2 \equiv p^t \pmod{q^2} \quad (3.11)$$

admite apenas

$$x_0 \equiv \pm p^r \pmod{q^2} \quad (3.12)$$

como soluções já que $(\mathbb{Z}_{q^2})^*$ é cíclico.

Suponha-se que (3.10) admite soluções não triviais onde se verifica

$$p^t < \frac{q^4}{4}. \quad (3.13)$$

Assim, $p^r < \frac{q^2}{2}$, logo, por (3.12), qualquer solução x_0 da congruência (4.1) diferente de $\pm p^r$ satisfará:

$$|x_0| \geq \frac{q^2}{2}$$

e portanto $x_0^2 \geq \frac{q^4}{4}$.

Da equação (3.10) tem-se que $p^t > \frac{q^4}{4}$ contradizendo a equação (3.13).

Assim $p^t \geq \frac{q^4}{4}$, logo:

$$\begin{aligned}
p^t &\geq \frac{q^4}{4} \\
t &\geq \log_p(q^4) - \log_p 4 \\
t &\geq 4\log_p q - \log_p 4,
\end{aligned}$$

o que completa a prova.

□

Como consequência do teorema anterior surge o colorário seguinte.

Corolário 3.20 *Sejam p e q primos tais que $p \geq 17$, $p, q \equiv 1 \pmod{4}$, $\left(\frac{p}{q}\right) = -1$ e $\left\lceil \log_p \left(\frac{q^4}{4}\right) \right\rceil$ ímpar (positivo). Então $g(X^{p,q}) = \left\lceil \log_p \left(\frac{q^4}{4}\right) \right\rceil + 1$, onde $\lceil x \rceil$ denota o menor inteiro maior ou igual ao número real x .*

Demonstração. Do Teorema 3.16 tem-se que, se $\left(\frac{p}{q}\right) = -1$ então:

$$4\log_p q - \log_p 4 \leq g(X^{p,q}) < 4\log_p q + \log_p 4 + 2.$$

A amplitude deste intervalo é $2 + \log_p 16$.

Começando por observar que $4\log_p q - \log_p 4 = \log_p \left(\frac{q^4}{4}\right)$, suponha-se que $\left\lceil \log_p \left(\frac{q^4}{4}\right) \right\rceil$ é ímpar positivo, isto é, existe $k \in \mathbb{N}$ tal que $\left\lceil \log_p \left(\frac{q^4}{4}\right) \right\rceil = 2k + 1$.

Como $\left(\frac{p}{q}\right) = -1$ então $X^{p,q}$ é bipartido e, por consequência, a sua cintura é par, não podendo por isso ser $2k + 1$ nem $2k + 3$.

Como, para $p \geq 17$, se tem que $2 + \log_p 16 < 2 + 1 = 3$ e é garantida a existência e unicidade do valor da cintura do grafo, logo

$$\begin{aligned}
g(X^{p,q}) &= 2k + 2 \\
&= \left\lceil \log_p \left(\frac{q^4}{4}\right) \right\rceil + 1.
\end{aligned}$$

□

Além deste caso particular pode ir-se mais longe e obter um outro corolário que relaciona a cintura de qualquer grafo de Ramanujan bipartido com a sua ordem, apresentando-se também um resultado exato para a cintura de qualquer grafo de Ramanujan bipartido.

Corolário 3.21 [5] *Sejam $p, q \equiv 1 \pmod{4}$ primos tais que $\left(\frac{p}{q}\right) = -1$. Então verifica-se que*

$$\lim_{q \rightarrow +\infty} \frac{\log_p q (q^2 - 1)}{g(X^{p,q})} = \frac{3}{4}.$$

Seja $x(p, q) = \lceil \log_p(q^2) \rceil$. Se $p^{x(p,q)} - q^2$ é good então $g(X^{p,q}) = 2x(p, q)$. Caso contrário $g(X^{p,q}) = 2\lceil \log_p(q^2) + \log_p 2 \rceil$, onde $\lceil x \rceil$ denota o menor inteiro maior ou igual ao número real x (ver [5]).

Depois deste capítulo, onde são introduzidos os grafos de Ramanujan e algumas das suas características relacionadas com o seu espectro e com a sua cintura, apresenta-se no próximo capítulo uma aplicação destes grafos aos códigos LDPC.

Capítulo 4

Aplicação à Teoria dos Códigos

Neste quarto capítulo, depois de introduzidos alguns conceitos relevantes da Teoria dos Códigos (ver [6] e [18]), são construídos e exemplificados códigos LDPC, partindo (da construção LPS) de grafos de Ramanujan. Além disso, na sua última secção, apresentam-se alguns conceitos, resultados e exemplos de possíveis deteções e correções de erros.

Seja \mathbb{F}_q um corpo finito e \mathbb{F}_q^n o espaço vetorial de todos os n -uplos (em \mathbb{F}_q). Diz-se que $C(n, m)$ é um *código linear* sobre \mathbb{F}_q se $C(n, m)$ é um subespaço vetorial de \mathbb{F}_q^n , com m elementos. Sendo $q, k \in \mathbb{N}$ tais que $m = q^k$ então $C(n, m)$ diz-se um código $[n, k]$.

Diz-se que um vetor $(f_1, \dots, f_n) \in \mathbb{F}_q^n$, que pode ser escrito como $f_1 \dots f_n$, é uma *palavra de código* se $(f_1, \dots, f_n) \in C(n, m)$.

Daqui por diante denota-se um código linear por C e consideram-se os códigos lineares designados por códigos LDPC (*Low-density Parity-check Codes*), ou seja, códigos gerados por matrizes esparsas.

Uma vez que C é um subespaço vetorial de dimensão k de \mathbb{F}_q^n então C é o conjunto de todas as combinações lineares de k vetores linearmente independentes com n entradas, isto é, existe uma base $B_C = \{c_1, \dots, c_k\}$ tal que qualquer palavra de código pode ser escrita como combinação linear dos vetores de B_C , podendo por isso um código linear, e em particular, um código LDPC ser representado matricialmente (ver [6]) através da sua matriz geradora ou da sua matriz de paridade (ver [18]).

Definição 4.1 Sejam $k, n \in \mathbb{N}$, com $k < n$. A uma matriz G de dimensão $k \times n$ e de característica completa tal que $C = \{xG : x \in \mathbb{F}_q^k\}$ é um código LDPC chama-se de *matriz geradora* de C . Alternativamente, C pode ser definido a partir de uma matriz H de dimensão $(n - k) \times n$ e de característica completa tal que $C = \{y \in \mathbb{F}_q^n : Hy^T = 0\}$, onde H se designa por *matriz de paridade* de C .

Nota 4.2 Da definição de matriz de paridade tem-se que cada linha desta matriz indica uma restrição para as palavras de código.

Dada uma matriz geradora G , qualquer vetor $v \in \mathbb{F}^k$ pode ser codificado numa palavra de código $c \in \mathbb{F}^n$, contendo k símbolos de informação e $n - k$ símbolos redundantes. Define-se a *razão* r de um código LDPC de dimensão k por $r := \frac{k}{n}$, podendo-se, por isso, afirmar que quanto maior a razão de um código maior será a quantidade de informação relativamente à sua redundância.

Depois de apresentadas algumas definições da Teoria dos Códigos prossegue-se este texto, na próxima secção, com a construção e exemplificação de códigos LDPC.

4.1 Construção de um código LDPC

Nesta secção, depois de visitados alguns conceitos da Teoria dos Códigos, pretende-se, como já referido, construir e exemplificar códigos LDPC (ver [26]) recorrendo também a resultados de capítulos anteriores.

Comece-se, para isso, por recordar que, pelo já enunciado Teorema 2.13, a equação $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$, com a_0 ímpar e a_1, a_2 e a_3 pares e com $p \equiv 1 \pmod{4}$ primo tem exactamente $p + 1$ soluções. A cada uma dessas soluções é associada uma matriz da forma

$$A = \begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix} \pmod{q}, \quad (4.1)$$

onde $i^2 \equiv -1 \pmod{q}$.

Denotando por S' o conjunto formado por estas $p + 1$ matrizes, construa-se um grafo, G_c , (d_1, d_2) -biregular, onde $d_1 = \frac{p+1}{2}$ e $d_2 = p + 1$, da seguinte forma:

Considerem-se todos os $q^3 - q$ vértices de $X^{p,q}$ bipartido e considere-se daqui por diante, em toda a construção do código LDPC e no exemplo que lhe segue, que o símbolo \times representa o produto de matrizes.

Comecem-se por dispor numa coluna L os vértices cuja etiquetação (uma matriz) seja um elemento de $PSL_2(\mathbb{F}_q)$. De seguida faça-se uma cópia de L a qual, daqui por diante, se denotará por L' .

Considerando que $L_j \in (L \cup L')$ e que $M_k^{\pm 1} \in S'$, onde $j \in \{1, \dots, q^3 - q\}$ e $k \in \{1, \dots, \frac{p+1}{2}\}$ disponham-se todos os elementos da forma $R_i = L_j \times M_k^{\pm 1}$ numa coluna, onde $i \in \{1, \dots, \frac{q^3 - q}{2}\}$. Esta coluna designar-se-á, daqui por diante por R . Um vértice R_i pertence a R se a matriz a ele associado pertence a $PGL_2(\mathbb{F}_q)$ e não pertence a $PSL_2(\mathbb{F}_q)$.

Assim, por simplicidade de linguagem, diz-se que um vértice de G_c é da esquerda ($L \cup L'$) se o determinante da matriz a ele associado é resíduo quadrático mod q e diz-se que um vértice de G_c é da direita (R) se o determinante da matriz a ele associado é não resíduo quadrático mod q .

Já no que toca às arestas, começa-se por determinar i tal que $i^2 \equiv -1 \pmod{q}$ e aplicar módulo q a todas as entradas das matrizes de S' , obtendo-se:

$$S' = \{M_1^{\pm 1}, M_2^{\pm 1}, \dots, M_{\frac{p+1}{2}}^{\pm 1}\},$$

onde as $p + 1$ matrizes de S' são da forma de (4.1) e onde M_k^{-1} denota a matriz inversa de M_k , $k \in \{1, \dots, \frac{p+1}{2}\}$.

Assim, no que toca às arestas, diz-se que $e \in E(G_c)$ se existem $L_j \in L \cup L'$ e $M_k^{\pm 1} \in S'$ tais que $e = L_j(L_j \times M_k^{\pm 1}) = (L_j \times M_k^{\pm 1})L_j$.

Tendo G_c construído, diz-se que a sua matriz de adjacência é a matriz de paridade do código LDPC que é por ele originado, sendo que como anteriormente referido, cada linha desta corresponde a uma restrição para as palavras de código. Veja-se um exemplo.

Exemplo 4.3 Considere-se $X^{p,q}$ um grafo de Ramanujan onde $p = 5$ e $q = 17$. Este grafo é regular pois é grafo de Ramanujan e é bipartido pois 5 é não resíduo quadrático de 17. Assim $X^{p,q}$ é um grafo (3, 6)-biregular.

Comece-se por observar que $i = 4$ é solução da congruência $i^2 \equiv -1 \pmod{17}$ e a

equação

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = 5,$$

que tem $p + 1 = 6$ soluções com a_0 ímpar e a_1, a_2, a_3 pares, sendo elas

$$(1, \pm 2, 0, 0), (1, 0, \pm 2, 0) \text{ e } (1, 0, 0, \pm 2).$$

A cada uma das soluções é associada uma matriz da forma:

$$M = \begin{bmatrix} a_0 + 4a_1 & a_2 + 4a_3 \\ -a_2 + 4a_3 & a_0 - 4a_1 \end{bmatrix} \pmod{17}, \text{ obtendo-se as 6 matrizes:}$$

$$M_1^{\pm 1} = \begin{bmatrix} 1 \pm 8 & 0 \\ 0 & 1 \mp 8 \end{bmatrix}, M_2^{\pm 1} = \begin{bmatrix} 1 & \pm 2 \\ \mp 2 & 1 \end{bmatrix} \text{ e } M_3^{\pm 1} = \begin{bmatrix} 1 & \pm 8 \\ \mp 8 & 1 \end{bmatrix}.$$

Comecem-se por dispor numa coluna L os vértices cuja a sua etiquetação (uma matriz) seja um elemento de $PSL_2(\mathbb{Z}_{17})$. De seguida faça-se um cópia de L a qual se denominará por L' .

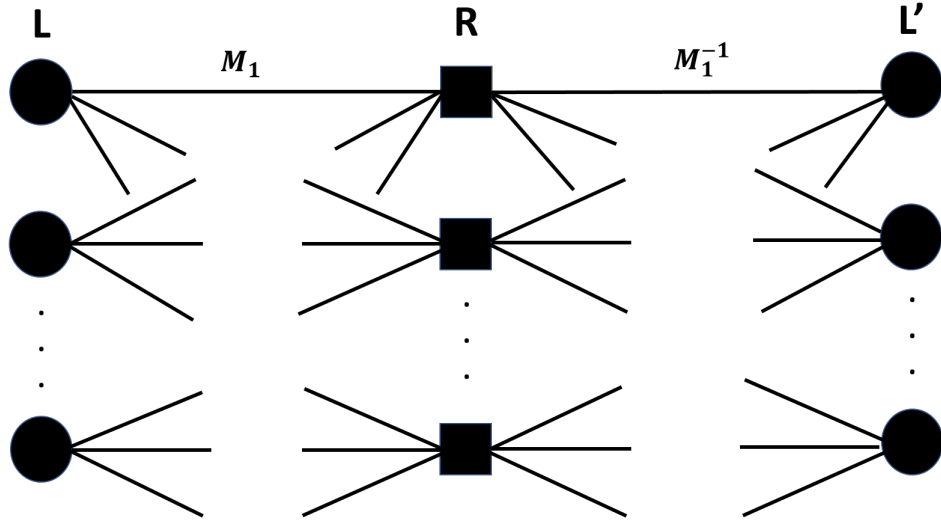
Considerando que $L_j \in PSL_2(\mathbb{Z}_{17})$ e que $M \in S' = \{M_1^{\pm 1}, M_2^{\pm 1}, M_3^{\pm 1}\}$ disponham-se os elementos da forma $R_i = L_j \times M_k^{\pm 1}$ numa coluna, a qual se designará por R , ou seja, R tem todas as matrizes que pertencem a $PGL_2(\mathbb{Z}_{17})$ e que não pertencem a $PSL_2(\mathbb{Z}_{17})$.

Assim, diz-se por simplicidade de linguagem, que um vértice de G_c é da esquerda ($L \cup L'$) se o determinante da matriz a ele associado é resíduo quadrático $\pmod{17}$ e que um vértice de G_c é da direita (R) se o determinante da matriz a ele associado é não resíduo quadrático $\pmod{17}$.

No que toca às arestas, diz-se que $e \in E(G_c)$ se existem $L_j \in (L \cup L')$ e $M_k^{\pm 1} \in S'$ tais que $e = L_j(L_j \times M_k^{\pm 1}) = (L_j \times M_k^{\pm 1})L_j$.

Tendo G_c construído diz-se que a matriz de paridade do código LDPC que se procura construir é a matriz de adjacência de G_c , sendo que cada linha desta corresponde a uma restrição para as palavras de código. Obtemos assim, o seguinte grafo:

Identifica-se, etiquetando cada um dos $17(17^2 - 1) = 4896$ vértices de $L \cup L'$ com uma matriz de $PSL_2(\mathbb{Z}_{17})$, onde $|L| = |L'| = 2448$. Cada um dos 2448 vértices de R é etiquetado com uma matriz da forma $R_i = L_j \times M_k^{\pm 1}$, $i, j \in \{1, \dots, 2448\}$, $k \in \{1, \dots, 3\}$,



com $L_j \in PSL_2(\mathbb{Z}_{17})$ e $M_k^{\pm 1} \in S'$ obtendo-se a matriz de paridade H do código LDPC associado, com 2448 linhas e 6 colunas, onde $H = (h_{ij})$. Assim, $h_{ij} = 1$ se o vértice $R_i \in R$ e o vértice $L_j \in (L \cup L')$ estão unidos por uma aresta e $h_{ij} = 0$, caso contrário.

Para $n = 4896$ tem-se que o código apresenta $\frac{n}{2} = 2448$ restrições para as palavras de um código de razão $\frac{1}{2}$.

Depois de finalizada esta secção com a exemplificação de um código LDPC é possível avançar para a última secção deste quarto capítulo, por forma a apresentar possibilidades de deteção e correção de erros numa mensagem.

4.2 Deteção e correção de erros

Depois de obtidas as palavras de código de um código LDPC interessa agora perceber como e em que circunstâncias é possível detetar e corrigir erros de uma mensagem, recorrendo a um código deste tipo.

Comece-se por apresentar alguns conceitos (ver [6]).

Definição 4.4 Sejam $x = (x_1, \dots, x_n)$ e $y = (y_1, \dots, y_n)$ duas palavras de código em \mathbb{F}_q^n . Define-se a *distância de Hamming* entre as palavras de código x e y por:

$$d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|.$$

Seja C um código LDPC que contém pelo menos duas palavras. Define-se d a *distância*

mínima de C por:

$$d = d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

Assim, passa a dizer-se que C é um código $[n, k, d]$.

Depois de definidos os conceitos de distância de Hamming e de distância mínima num código, avança-se agora para dois métodos exemplificados que permitem eventuais deteções e correções de erros de uma mensagem.

Teorema 4.5 [18] *Um código C com distância mínima d corrige $\lfloor \frac{1}{2}(d-1) \rfloor$ erros, onde $\lfloor x \rfloor$ denota o maior inteiro menor ou igual ao número real x . Se d é par então C corrige $\frac{d-1}{2}$ erros e deteta $\frac{d}{2}$ erros.*

Exemplo 4.6 Considere-se o código binário linear $C = \{000000, 010010, 001100, 011110\}$, onde, por exemplo, $B_C = \{010010, 001100\}$, isto é qualquer palavra do código C pode ser escrita como combinação linear dos elementos de B_C . Como

$$d(000000, 010010) = 2, d(000000, 001100) = 2, d(000000, 011110) = 4,$$

$$d(010010, 001100) = 4, d(010010, 011110) = 2, d(001100, 011110) = 2.$$

então $d = d(C) = 2$ e $\lfloor \frac{1}{2}(2-1) \rfloor = 0$, logo C não corrige qualquer erro. Como $d = 2$ é par então C deteta 1 erro.

Seja C um código LDPC e seja s inteiro positivo. Diz-se que C deteta s erros se e só se, quando ocorrem s erros ou menos, a palavra obtida não pertence ao código C . Diz-se também que C corrige s erros se e só se o método de descodificação por distância mínima corrige s , ou menos, erros sendo este método o seguinte: depois de recebida a palavra $y \in \mathbb{F}_q^n$, procura-se $x' \in C$ tal que

$$d(x', y) = \min\{d(x, y) : x \in C\},$$

ou seja, y é descodificada pela palavra de código à qual se encontra a uma menor distância.

Exemplo 4.7 Considere-se o código binário linear $C = \{00000, 11100, 00111, 11011\}$ e suponha-se que a palavra recebida é $y = 00101$. Como

$$d(00101, 00000) = 2, d(00101, 11100) = 3, d(00101, 00111) = 1 \text{ e } d(00101, 11011) = 4$$

então, usando o método de decodificação por distância mínima, decodifica-se a palavra 00101 pela palavra de código 00111.

Depois de estudada uma aplicação dos grafos de Ramanujan à Teoria dos Códigos, com recurso à construção de um código LDPC, que por sua vez permitem eventualmente a deteção e a correção de erros, veja-se agora uma aplicação destes à Criptografia.

Capítulo 5

Aplicação à Criptografia

Neste capítulo, tal como já referido, começam-se por definir alguns conceitos essenciais para a construção de funções de síntese a partir de grafos expansores e de grafos de Ramanujan em particular. Finalmente, com base num grafo expensor é construída e exemplificada uma função de síntese resistente a colisões, construindo-se também uma função de síntese com base num grafo de Ramanujan.

5.1 Função de síntese

Nesta primeira secção define-se função de síntese e também a colisão entre duas mensagens de forma a que seja possível nas duas secções seguintes explicitar a minimização de probabilidade de colisão e também a construção de funções de síntese, recorrendo a grafos expansores e por último, em particular, a grafos de Ramanujan.

Em Criptografia, entende-se por *função de Hash criptográfica*, ou simplesmente por *função de síntese* ou *dispersão*, uma função f com domínio X , cujos elementos se designam por mensagens, e com contradomínio Y , cujos elementos se designam por sínteses, que verifica as seguintes condições:

1. Dada uma mensagem $x \in X$ é fácil determinar $f(x)$, isto é, se x tem comprimento n então a complexidade do cálculo de $f(x)$ é $O(n^k)$, para algum k positivo.
2. f é determinista, isto é, uma mesma mensagem resulta sempre na mesma síntese.
3. Uma pequena alteração de uma dada mensagem deve implicar uma grande

alteração na síntese, de tal forma que seja difícil obter a mensagem original a partir dessa síntese.

4. É computacionalmente impraticável a obtenção de uma mensagem a partir da sua síntese, isto é, é impraticável em tempo útil encontrar uma mensagem x a partir de $f(x)$, sendo que qualquer método de pesquisa conhecido não admite qualquer resultado em tempo útil.

Uma das condições para que uma função de síntese seja considerada útil na proteção de dados é que seja resistente a colisões (ver [1]).

Definição 5.1 Seja $f : X \rightarrow Y$ uma função de síntese. Se existem mensagens x_1 e $x_2 \in X$ diferentes tais que $f(x_1) = f(x_2)$ diz-se que x_1 e x_2 constituem uma *colisão*.

Embora seja computacionalmente impraticável a descoberta de duas mensagens diferentes que tenham a mesma síntese, é possível a existência de colisões. Neste sentido estuda-se, na próxima secção, como devem ser distribuídas as mensagens de forma a que a probabilidade de colisão seja mínima.

5.2 Minimização da probabilidade de colisão

Nesta secção apresenta-se a forma de minimização da probabilidade de colisões. Começa-se por entender que qualquer grafo de Ramanujan é um (bom) grafo expensor tendo por isso uma cintura grande, sendo que se entende que o grafo possui uma cintura grande no sentido em que apenas tem ciclos com grande comprimento. Esta propriedade é fundamental para assegurar que se obtém uma função de síntese com uma baixa probabilidade de colisões. Apresentem-se então os conceitos de grafo expensor e de grafo bom expensor (ver [2]).

Definição 5.2 Seja G um grafo bipartido e seja $X \subseteq V(G)$. Designa-se por *vizinhança de X* , e denota-se por $N_G(X)$ o conjunto formado pelos vértices de G que são vizinhos de pelo menos um vértice de X , isto é:

$$N_G(X) = \{v \in V(G) : vx \in E(G), \text{ para algum } x \in X\}.$$

Considere-se que existe uma partição de $V(G)$ em dois seus subconjuntos V_1 e V_2 tal que $|V_1| = |V_2| = m$ e que o grau máximo de um vértice de $V(G)$ é d . Diz-se que G é

(m, d, c) -expansor se qualquer subconjunto de vértices X , onde $|X| = j \leq \frac{m}{2}$, verifica:

$$|N_G(X)| \geq \left(1 + c \left(1 - \frac{j}{m}\right)\right) j.$$

Definição 5.3 Seja G um grafo (k, k) -biregular e considere-se uma partição de $V(G)$ em dois seus subconjuntos V_1 e V_2 tal que $|V_1| = |V_2| = m$. Seja λ o segundo menor valor próprio de G . Nestas condições diz-se que G é um grafo (m, k, c) bom expansor, onde

$$c = \frac{2k\lambda - \lambda^2}{k^2}.$$

Se G é um grafo de Ramanujan bipartido então G é um bom grafo expansor. De facto, considerando $G = X^{p,q}$ um grafo $(p+1)$ -regular com a partição dos seus vértices em $V(G) = V_1 \cup V_2$, onde $|V_1| = |V_2| = \frac{q^3-q}{2}$ e onde λ é o segundo menor valor próprio de G então G é $\left(\frac{q^3-q}{2}, p+1, c\right)$ bom expansor, onde:

$$c = \frac{2(p+1)\lambda - \lambda^2}{(p+1)^2}.$$

A resistência a colisões pode ser avaliada pela cintura do grafo de Ramanujan a partir do qual se constrói a função de síntese sendo que descobrir uma colisão é equivalente a encontrar ciclos no grafo tendo-se que quanto maior é a cintura menor é a probabilidade de colisão. Interessa por isso, com recurso a alguns conceitos da Teoria das Probabilidades, determinar a forma como devem ser distribuídas as mensagens como objetos da função de síntese de modo a minimizar a probabilidade de colisão.

Um *processo estocástico* Ω é uma sequência temporal de variáveis aleatórias que representa a evolução de um sistema com n estados e pode ser descrito pelo vetor de estados (X_1, \dots, X_n) , onde $X_t, t \in \{1, \dots, n\}$ é o estado no qual o sistema se encontra no instante t . Um processo estocástico designa-se por *cadeia de Markov* se a transição de um estado do sistema para outro estado do mesmo sistema depende apenas do estado atual no qual o sistema se encontra, isto é, (ver [24]):

$$P(X_{n+1} = x_{n+1} | X_0 = x_0, X_1 = x_1, \dots, X_n = x_n) = P(X_{n+1} = x_{n+1} | X_n = x_n).$$

A distribuição de probabilidade para um sistema se encontrar num determinado estado i pode escrever-se como um conjunto de números reais não negativos tais que a sua

soma seja igual a 1 e pode representar-se por um vetor $p_t = (p_1, p_2, \dots, p_n)$ tal que $p_i = P(X_t = i)$ é a probabilidade do sistema se encontrar no estado i no instante t .

Diz-se que uma distribuição de probabilidade é uniforme se, em qualquer instante, o sistema pode encontrar-se em qualquer um dos estados com igual probabilidade. Represente-se esse vetor de probabilidades, cuja soma das componentes é 1, por:

$$u_p = \left(\frac{1}{n}, \dots, \frac{1}{n} \right).$$

Considere-se que cada uma das possíveis sínteses (de uma função de síntese) é representada por um dos estados com um sistema que possui uma determinada distribuição de probabilidade a si associada. Então a distribuição de probabilidade uniforme minimiza a probabilidade de colisão. De facto, supondo que $p_t = (p_1, p_2, \dots, p_n)$, tem-se que dadas duas mensagens a probabilidade das suas sínteses coincidirem num determinado estado j no instante t é dado por p_j^2 , uma vez que esses acontecimentos são independentes. Assim, considerando todos os estados, a probabilidade total de colisão é dada por:

$$\sum_{i=1}^n p_i^2$$

Pela desigualdade de Cauchy-Schwarz tem-se

$$\begin{aligned} n \sum_{i=1}^n p_i^2 &\geq \left(\sum_{i=1}^n p_i \right)^2 \\ n \sum_{i=1}^n p_i^2 &\geq 1^2 \\ \sum_{i=1}^n p_i^2 &\geq \frac{1}{n}, \end{aligned}$$

o que prova que a distribuição uniforme minimiza a probabilidade de colisão.

Por forma a obter uma função de síntese f com um melhor desempenho interessa também que f seja, além de resistente a colisões, resistente à descoberta de uma pré-imagem e resistente à descoberta de uma segunda pré-imagem (ver [25]).

Definição 5.4 Entende-se que uma função de síntese f é resistente à descoberta de uma *pré-imagem* se, dado $f(m)$, é computacionalmente impraticável a descoberta de

uma mensagem m' tal que $f(m) = f(m')$, onde m é desconhecida. Uma função de síntese f diz-se resistente à descoberta de uma *segunda pré-imagem* se, dada uma mensagem m , é computacionalmente impraticável a descoberta de uma mensagem m' tal que $m' \neq m$ e $f(m') = f(m)$.

Depois de vistos estes conceitos fundamentais da Criptografia, tendo em conta a definição de grafo expensor e o facto de que os grafos de Ramanujan bipartidos são bons expansores, é possível agora avançar para a construção das funções de síntese a partir destes.

5.3 Construção de uma função de síntese resistente a colisões

Por forma a construir funções de síntese (ver [25]), além do referido no final na secção anterior, recorre-se também a conceitos elementares da Teoria dos Grafos, enunciados no segundo capítulo.

Seja G um grafo expensor k -regular e considere-se a aresta artificial, a qual se designa por *aresta inicial* $e_0 = v_{-1}v_0 \in E(G)$, onde v_{-1} é um vértice artificial e v_0 é o vértice inicial de um passeio. Por forma a evitar qualquer passagem consecutiva por uma mesma aresta nesse passeio determinado pela função de síntese, defina-se, para a construção desta, $\theta : (V(G) \times V(G)) \times \{1, \dots, k-1\} \rightarrow V(G)$, uma função de ordenação de vizinhança, isto é, para qualquer aresta $e = v_tv_{t+1}$ tem-se que:

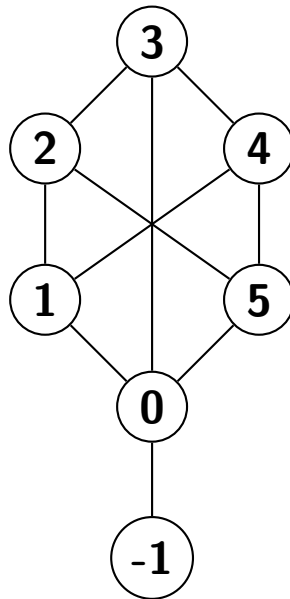
$$\{\theta(v_t, v_{t+1}, i) : i \in \{1, \dots, k-1\}\} \cup \{v_t\}$$

é o conjunto de todos os vértices vizinhos de v_{t+1} .

Dada uma mensagem m , começa-se por escrever m na base $k-1$, ou seja, escreve-se $m = m_1 \dots m_\mu$, onde $m_i \in \{1, \dots, k-1\}$. De seguida, com $i = 0$ até $i = \mu-1$, calcula-se de forma recursiva $v_{i+1} := \theta(u_i, v_i, m_i)$ retornando no final v_μ . Obtém-se um passeio em G no qual os seus sucessivos vértices são v_1, \dots, v_μ . O valor da função de síntese f , alcançado pelo passeio, é dado por v_μ .

Para uma melhor compreensão da construção desta função, veja-se um exemplo.

Exemplo 5.5 Considere-se um grafo $(3, 3)$ -biregular ao qual se acrescenta um vértice e uma aresta artificiais -1 e $-1\ 0$, respetivamente:



Considere-se uma função de síntese f e a mensagem $m = 121221$. Para $k = 3$ e $\mu = 6$ estabelece-se a função de ordenação da vizinhança θ tal que:

$$\theta(u_i, v_i, 1) = \min_{v_j \neq u_i} \{v_j : v_j \in N(u_i)\} \text{ e } \theta(u_i, v_i, 2) = \max_{v_j \neq u_i} \{v_j : v_j \in N(u_i)\}$$

Assim, e fazendo $u_i = v_{i-1}$, começando um passeio P no vértice $u_1 = -1$, tem-se que $v_1 = 0$ e percorre-se $e_1 = -1\ 0$. Como o primeiro dígito de m é 1, não podendo regressar a $u_1 = -1$, pela forma como está construída a função de ordenação, escolhe-se o vértice $v_2 = 1$ e percorre-se a aresta $e_2 = 01$ passando-se a ter $P = u_1 e_1 v_1 e_2 v_2$, onde obviamente $u_2 = v_1$ na próxima iteração, e assim sucessivamente. Logo, representando por (u_i, v_i) os vértices extremos de cada aresta em cada interação e representando por \rightarrow a passagem de uma aresta para outra aresta de acordo com o dígito seguinte de m , tem-se que P pode ser descrito por:

$$(-1, 0) \rightarrow (0, 1) \rightarrow (1, 4) \rightarrow (4, 3) \rightarrow (3, 2) \rightarrow (2, 5) \rightarrow (5, 0)$$

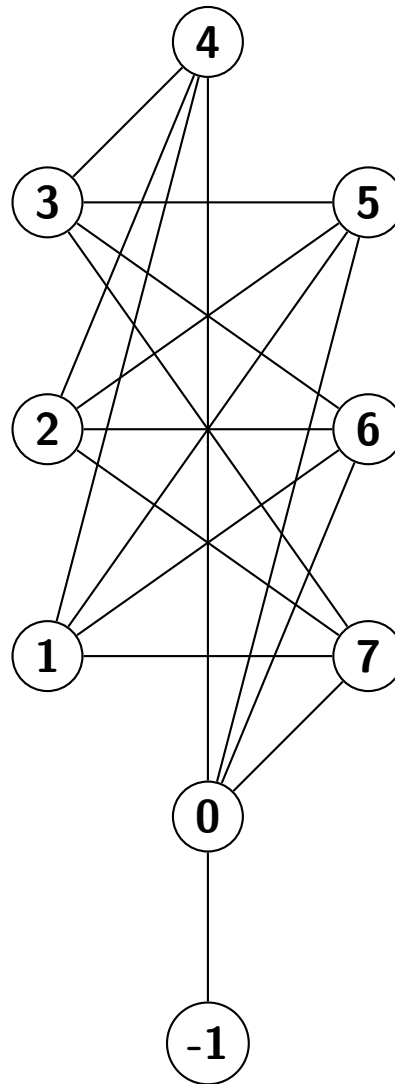
Assim o valor da função de síntese de m é dado por $v_6 = f(m) = 0$.

A função de ordenação utilizada neste exemplo é funcional na medida em que a mensagem m está escrita na base 2. De modo geral, para encriptar uma mensagem

escrita numa qualquer base deve recorrer-se a outra função de ordenação de vizinhança. Considere-se um grafo k -regular ao qual se acrescenta um vértice e uma aresta artificiais -1 e -1 0 respetivamente. Como o grafo considerado é k -regular a base na qual se encontra escrita m é $k - 1$. Considere-se uma função de síntese f e $m = m_1 \dots m_\mu$, onde $m_i \in \{1, \dots, k - 1\}, \forall i \in \{1, \dots, \mu\}$. Assim, estabelece-se a função de ordenação de vizinhança θ onde:

$$\theta(u_i, v_i, i) \text{ é o } m_i\text{-ésimo menor } v_j \text{ tal que } v_j \neq u_i.$$

Exemplo 5.6 Considere-se um grafo $(4, 4)$ -biregular ao qual se acrescenta um vértice e uma aresta artificiais -1 e -1 0, respetivamente:



Como o grafo é $(4, 4)$ -biregular então a base na qual se encontra escrita m é 3. Considere-se uma função de síntese f e $m = 1321213$, onde $m_i \in \{1, 2, 3\}, \forall i \in \{1, \dots, 7\}$.

Recordando que a função de ordenação de vizinhança é

$$\theta(u_i, v_i, i) \text{ é o } m_i\text{-ésimo menor } v_j \text{ tal que } v_j \neq u_i,$$

inicia-se um passeio P no vértice $u_1 = -1$, tem-se que $v_1 = 0$ e percorre-se a aresta $e_1 = -1 \ 0$. Pela forma como está definida θ , à semelhança do exemplo anterior, é possível continuar o passeio P :

$$(-1, 0) \rightarrow (0, 4) \rightarrow (4, 3) \rightarrow (3, 6) \rightarrow (6, 0) \rightarrow (0, 5) \rightarrow (5, 1) \rightarrow (1, 7).$$

Assim, o valor da função de síntese de m é dado por $v_7 = f(m) = 7$.

Já no caso de um grafo de Ramanujan (ver [27]), considere-se um grupo finito $\langle H, * \rangle$ e um conjunto simétrico S tal que $S \subseteq H$ e defina-se $a := |S| - 1$. Escolha-se uma função π definida por: $\pi : \{0, \dots, a - 1\} \times S \rightarrow S$ tal que, para todo o $h \in H$, os conjuntos $\pi(\{0, 1, \dots, a - 1\} \times \{h\})$ e $S \setminus \{h^{-1}\}$ são iguais.

Começa-se por converter uma mensagem m num número $x_0x_1\dots x_r$ na base a . Defina-se a sequência $(h_i)_{0 \leq i \leq r}$ de forma iterativa tal que $h_i = \pi(x_i, h_{i-1})$, onde h_{-1} é algum elemento fixo de S . A síntese correspondente a m é $hh_0h_1\dots h_r \in S$, onde h é um elemento fixo de H .

Capítulo 6

Conclusão

Nas últimas décadas, a teoria dos grafos, e em particular o estudo dos grafos de Ramanujan, ganhou grande destaque na matemática já que se alimenta de diversos ramos desta, nomeadamente da álgebra, da teoria dos números e da combinatória. Um dos objetivos desta dissertação foi a caracterização dos grafos de Ramanujan, apresentando construções destes últimos assim como a sua ligação, partindo por um lado do conjunto dos inteiros de Lipschitz e por outro do grupo $PGL_2(\mathbb{F}_q)$. Finalmente, são estudadas algumas aplicações desta família de grafos, designadamente à teoria dos códigos e à criptografia.

Deste modo, depois do primeiro capítulo, onde se apresenta o estado da arte e onde se introduz a temática em estudo, o segundo capítulo deste trabalho é dedicado à apresentação de conceitos e resultados preliminares fundamentais que tiveram como objetivo o estudo e uma construção da família dos grafos de Ramanujan assim como algumas aplicações destes, nomeadamente a construção de códigos LDPC e de funções de síntese.

No terceiro capítulo estudou-se uma propriedade espectral da família dos grafos regulares e definiram-se grafos de Ramanujan, tendo também sido apresentadas construções. Neste capítulo foram ainda apresentados um minorante, um majorante e valores exatos da cintura destes grafos.

De seguida, no quarto capítulo, procurou-se dar a conhecer uma aplicação dos grafos de Ramanujan à teoria dos códigos. No contacto por meio de conversações virtuais podem ocorrer erros aquando do envio de uma mensagem. Assim, interessa detetar e,

se possível, corrigir eventuais erros através do que foi designado nesta dissertação por código (LDPC). Tendo por base os grafos de Ramanujan, foram definidos, construídos e exemplificados estes códigos e foram também apresentadas formas de deteção e correção de erros.

No quinto capítulo, depois da apresentação de (bons) grafos expansores, apresenta-se uma aplicação dos grafos de Ramanujan à criptografia, nomeadamente a construção de funções de síntese a partir destes, que podem ter como objetivo, por exemplo, a proteção de uma conta bancária ou a simples proteção de dados pessoais. Neste capítulo foram expostas as construções de duas funções de síntese, uma com base num grafo expensor e outra partindo de um grafo de Ramanujan.

Bibliografia

- [1] P. Almeida, D. Napp *Criptografia e Segurança*, Publindústria, 2007.
- [2] N. Alon, *Eigenvalues and expanders*, Combinatorica 6 (2) (1986) 83-96, 1986.
- [3] A. S. Asratian, C. J. Casselgren, *On interval edge colorings of (α, β) -biregular bipartite graphs*, Discrete Mathematics, Volume 307, Issue 15, 1951-1956, 2007.
- [4] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1974.
- [5] N. L. Biggs, A. G. Boshier, *Note on the girth of Ramanujan Graphs*, Journal of Combinatorial Theory, Series B 49, 190-194 (1990), 1990.
- [6] R. E. Blahut *Theory and Practice of Error Control Codes*, Addison-Wesley Publishing Company, 1983.
- [7] R. C. Brigham, R. D. Dutton, *Bounds on Graph Spectra*, Journal of Combinatorial Theory, Series B 37, 228-234 (1984), 1984.
- [8] D. M. Cardoso, J. Szymański, M. Rostami, *Matemática Discreta*, Escolar Editora, 2009.
- [9] G. Davidoff, P. Sarnak, A. Valette, *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, Cambridge University Press, 2003.
- [10] S. S. Dragomir, *Some Trace Inequalities for Operators in Hilbert Spaces*, Kragujevac Journal of Mathematics Vol. 41 (1), 33–55 (2017), 2017.
- [11] H. Enomoto, *Combinatorially Homogeneous Graphs*, Journal of Combinatorial Theory, Series B 30, 215-223 (1981), 1981.

- [12] T. W. Hungerford, *Algebra*, Springer, 1974.
- [13] A. Krebs, O. Verbitsky, *Universal covers, color refinement, and two-variable counting logic: Lower bounds for the depth*, 2014.
- [14] K. Kutnar, D. Marusic *Recent Trends and Future Directions in Vertex-Transitive Graphs*, ARS Mathematica Contemporanea 1 (2008) 112–125, 2008.
- [15] M. Lipschitz, *Recherches sur la transformation par des substitutions réelles d’une somme de deux ou de trois carrés en elle-même*, Journal de Mathématiques Pures et Appliquées, 2 373–439 (1886), 1886.
- [16] A. Lubotzky, *Expander Graphs in Pure and Applied Mathematics*, Bulletin of the American Mathematical Society 49 (1), 113-162, 2012.
- [17] A. Lubotzky, R. Phillips, P. Sarnak *Ramanujan Graphs*, Combinatorica 8 (3), 261-277 (1988), 1988.
- [18] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.
- [19] G. Margulis, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica, 2 (1), 71-78 (1982), 1982.
- [20] G. Margulis, *Explicit group- theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators*, Problems Inform. Transmission, 24 (1), 39-46, 1988.
- [21] A. Mowshowitz, *The Characteristic Polynomial of a Graph*, Journal of Combinatorial Theory, 12 (B), 177-193 (1972), 1972.
- [22] M. B. Nathanson, *Elementary Methods in Number Theory*, Springer, 2000.
- [23] E. D. Nering, *Linear Algebra and Matrix Theory*, John Wiley & Sons, Inc., 1970.
- [24] E. Pardoux, *Markov Processes and Applications*, John Wiley & Sons, Ltd, 2008.
- [25] C. Petit, *On graph-based cryptographic hash functions*, Université Catholique de Louvain, 2009.

- [26] J. Rosenthal, P. O. Vontobel, *Constructions of LDPC Codes using Ramanujan Graphs and Ideas from Margulis*, 2000.
- [27] N. Smart, *Advances in Cryptology - EUROCRYPT 2008*, Springer, 2008.
- [28] H. Täubig, J. Weihmann, *Matrix power inequalities and the number of walks in graphs*, Discrete Applied Mathematics 176, 122-129 (2014), 2014.
- [29] P. O. Vontobel, *Algebraic Coding for Iterative Decoding*, Swiss Federal Institute of Technology, 2003.
- [30] H. Zhang, S. Liu, W. Li, *A Note on the Permanental Roots of Bipartite Graphs*, Discussiones Mathematicae Graph Theory 34, 49–56 (2014), 2014.
- [31] X. Zhu, *Circular Colouring and Graph Homomorphism*, Bulletin of the Australian Mathematical Society, Vol. 59, 83-97 (1999), 1999.
- [32] D. Cvetkovic, M. Doob, H. Sachs, *Spectra of Graphs, Theory and Applications*, VEB Deutscher Verlag der Wissenschaften, Berlin (D.D.R.), 1979.