UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE MATEMÁTICA, ESTATíSTICA E COMPUTAÇÃO CIENTíFICA

Códigos sobre Grafos que são Quocientes de Reticulados

Lívia Teresa Minami

Dissertação de Mestrado orientada pela Dr^{a}. Sueli Irene Rodrigues Costa

Códigos sobre Grafos que são Quocientes de Reticulados

Este exemplar corresponde à redação final da dissertação de mestrado devidamente corrigida e defendida por Lívia Teresa Minami e aprovada pela comissão julgadora.

Campinas, 03 de dezembro de 2004 .

_____
Sueli Irene Rodrigues Costa

Banca Examinadora:
1. Dr[a]. Sueli Irene Rodrigues Costa
2. Dr. Edson Agustini
3. Dr[a]. Claudina Izepe Rodrigues

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

Dissertação de Mestrado defendida por **Lívia Teresa Minami** e aprovada em **03** de **Dezembro** de **2004** pela Banca Examinadora constituída pelos professores:

Drª. Sueli Irene Rodrigues Costa

Dr. Edson Agustini

Drª. Claudina Izepe Rodrigues

Prefácio

Este trabalho aborda propriedades de grafos que são quocientes de reticulados e explora conexões destes com a teoria de códigos corretores de erros. Está organizado na seguinte forma: No primeiro capítulo são introduzidos conceitos e principais resultados de teoria de grafos a serem utilizados. O segundo capítulo contém uma breve introdução à teoria de códigos corretores de erros e finalmente no terceiro capítulo são analisadas propriedades de grafos que são quocientes de reticulados e suas relações com códigos em aspectos como rotulamentos e construção de códigos.

Abstract

Graphs which are quotients of lattices are studied in this dissertation and some of their connections to error correcting codes are explored. The text is organized as follows. In Chapter 1 the main concepts and results in Graph theory are introduced. Chapter 2 contains s brief introduction to error correcting codes theory and Chapter 3 is devoted to the study of properties of graphs which are quotient of lattices and their relations with codes in aspects like labelings and the construction of perfect codes.

Agradecimentos

Primeiramente à DEUS.

Agradeço à Prof[a] Dr[a]. Sueli Irene Rodrigues Costa pela paciência, aos meus pais (Celso e Tereza) pelo apoio , ao meu irmão Cal que acordou diversas noites para me buscar sem nem reclamar, ao Igor que me ajudou muito com os milhares de erros do WinEdt, ao meu noivo Fabiano por ter me incentivado nos momentos de desânimo e à sua família (D. Inês, Fer e Fran) que me acolheu todos os finais de semana.

Agradeço também à CAPES pela bolsa de mestrado.

Lívia Teresa Minami

03 de Dezembro de 2004

Sumário

Agradecimentos **v**

1 Uma Introdução à Teoria de Grafos **2**

1.1 Um pouco de História 2
1.2 Definições Iniciais 3
1.3 Principais Tipos de Grafos 4
1.4 Caminhos e Ciclos 5
1.5 Conexidade 6
1.6 Árvores e Florestas 6
1.7 Grafos regulares especiais 7
1.7.1 Grafos distância-regular 7
1.7.2 Grafos aresta regular e aresta co-regular 8
1.8 Álgebra Linear e Grafos 8
1.9 Planaridade 9
1.10 Outras superfícies 11
1.11 Grafos Eulerianos 14

2 Códigos Corretores de Erros **15**

2.1 Exemplos 15
2.2 Métrica de Hamming e Métrica de Lee 16
2.3 Anéis e corpos 18
2.4 Os Inteiros 22
2.5 Códigos Lineares 22
2.5.1 Definições iniciais 22
2.5.2 Matriz Geradora 24
2.5.3 Códigos Duais 25
2.5.4 Exemplos de Códigos Lineares 27
2.6 Decodificação 30

3 Grafos dados por Quocientes de Reticulados **33**
3.1 Reticulado, empacotamento e kissing number 33
3.1.1 O Problema do Empacotamento de Esferas 34
3.1.2 O Problema do Kissing Number 35
3.2 Grafos que são Quocientes de Reticulados (Grafos e Ladrilhamentos sobre Toros) 38
3.2.1 O Toro Planar 39
3.2.2 Grafos Regulares Sobre Toros Planares 39
3.2.3 Ladrilhamento 40
3.2.4 Perfil de Distâncias em $\Gamma^{\vec{u},\vec{v}}$ 43
3.2.5 Toro Gerado por $\vec{u}$ =(a,b) e $\vec{v}$ =(-b,a) 44
3.2.6 Códigos perfeitos 45
3.3 Gênero do Grafo $\mathbb{Z}_q^n$ 46
3.3.1 Gênero dos Grafos $\mathbb{Z}_q^2$ com a Métrica de Lee 46
3.3.2 Gênero dos Grafos $\mathbb{Z}_q^2$ com a Métrica de Hamming 47
3.3.3 Grafo $\mathbb{Z}_4^2$ 47
3.3.4 Gênero dos Grafos $\mathbb{Z}_2^n$ 47
3.4 Exemplos de Grafos distância-regulares 49
3.4.1 $\mathbb{Z}_4 \times \mathbb{Z}_4$ 49
3.4.2 $\Gamma_{\vec{u},\vec{v}}$ 49

Bibliografia **51**

Introdução

O objetivo deste trabalho foi o estudo de uma classe especial de grafos ligados a códigos corretores de erros. Através de propriedades e resultados da teoria de grafos procuramos analisar características importantes em exemplos de códigos.

Assim , discutimos alguns problemas envolvendo grafos e códigos com a perspectiva de, num trabalho futuro aprofundarmos o tema visando a construção de bons códigos associados a grafos através da análise de propriedades geométricas especiais.

No primeiro capítulo apresentamos uma introdução à teoria de grafos, contendo as principais definições, exemplos e resultados importantes. São abordados conceitos como grafos regulares e gênero topológico de um grafo que serão utilizados no decorrer do trabalho. Incluímos também no final a discussão do problema das pontes de Könisberg, o qual motivou o surgimento da teoria dos grafos.

O segundo capítulo é uma breve introdução à teoria dos códigos corretores de erros. A ênfase foi dada aos códigos lineares e códigos perfeitos incluindo exemplos clássicos como os códigos de Hamming e de Reed-Solomon. Apresentamos também os conceitos das métricas de Hamming e de Lee associadas a alfabetos q-ários.

O último capítulo é dedicado à analise de algumas relações entre códigos e uma classe especial de grafos: Os quocientes de reticulados utilizando principalmente a referência [9]. Estes grafos são associados a ladrilhamentos em toros planares. Introduzimos inicialmente conceitos fundamentais associados a reticulados, e passamos aos grafos quocientes destes discutindo propriedades como uniformidade, regularidade e gênero topológico e a conexão destas com a construção de códigos com características especiais como os códigos perfeitos e com rotulamento cíclico.

Capítulo 1

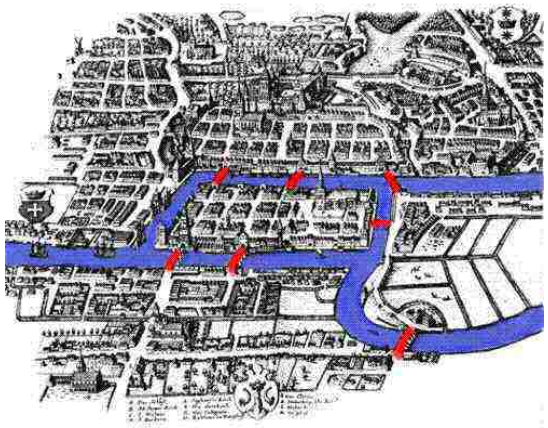
Uma Introdução à Teoria de Grafos

Este primeiro capítulo é dedicado a uma introdução à teoria de grafos. Nele, estaremos visando sempre atingir nosso objetivo de relacionar os grafos com empacotamento de esferas, códigos corretores de erros e reticulados. As principais referências para este capítulo são [3], [5], [6] e [7].

1.1 Um pouco de História

A Teoria de Grafos é relativamente recente na história da matemática . A primeira evidência do uso da teoria de grafos data de 1736 quando Euler utilizou-a para resolver o problema das "Pontes de Königsberg", enunciado abaixo.

Königsberg é uma cidade russa que é cortada pelo rio Pregel, dividindo a cidade em duas ilhas. Há uma ponte que as liga, uma ilha possui uma ponte ligando-a a cada uma das duas margens opostas e a outra, duas pontes ligando-a a cada uma das margens (veja figura abaixo). A pergunta é se seria possível realizar um passeio pelas ilhas passando uma única vez em cada uma das sete pontes e voltar para o ponto do início do passeio. Esse problema será discutido mais adiante, depois que introduzirmos a teoria.



Desde então os grafos têm sido utilizados em uma grande variedade de aplicações pois são capazes de modelar diversas situações reais em física, química, biologia, engenharia elétrica, entre outras.

1.2 Definições Iniciais

Um *grafo* G é um par (V, A) onde V é um conjunto de pontos chamados vértices e A o conjunto de segmentos que ligam dois dos elementos de V, denominados arestas. Denotamos por xy a aresta de G que liga os vértices x e y. Quando quisermos nos referir ao conjunto de vértices de G podemos usar a notação $V(G)$ e para o conjunto de arestas $A(G)$.

Dado um grafo G, chamamos de *ordem de* G, o número de vértices que ele possui e denotamos por $|G|$. Dizemos ainda que um vértice v é *incidente* a uma aresta e se $v \in e$. Se xy for uma aresta de G, então os vértices x e y são ditos *adjacentes ou vizinhos* (caso contrário são independentes). Este mesmo termo pode ser dado para arestas, ou seja, dizemos que duas arestas são adjacentes se possuem vértice comum.

Na teoria de grafos, dois grafos $G(V, A)$ e $G^{'}(V^{'}, A^{'})$ são chamados isomorfos se existir bijeção $\phi : V \to V^{'}$, tal que $xy \in A \Leftrightarrow \phi(x)\phi(y) \in A^{'}$. Neste caso denotamos por $G \simeq G^{'}$ e dizemos que ϕ é um *isomorfismo.* Se tivermos $G = G^{'}$, teremos que ϕ é um *automorfismo.* Uma função f tomando grafos como argumentos é chamada *grafo-invariante* se, dados grafos isomorfos G e H, $f(G) = f(H)$.

Proposição 1.1. *: $f : G \to G$ é uma isometria se, e somente se, f for um isomorfismo.*

Um desenho ou mergulho de um grafo G no $\mathbb{R}^n$ é um isomorfismo de G em $G^{'}$ onde $G^{'}$ é um grafo em $\mathbb{R}^n$. Neste caso, os vértices são pontos e as arestas são curvas ligando dois pontos.

Se $V^{'} \subseteq V$ e $A^{'} \subseteq A$, então dizemos que $G^{'}(V^{'}, A^{'})$ é um *subgrafo* de $G(V, A)$ e denotamos por $G^{'} \subseteq G$. Ainda, se $G^{'} \subseteq G$ e $G^{'}$ contém todas as arestas $xy \in A$, então $G^{'}$ é *subgrafo induzido* de G. Neste último caso dizemos que $V^{'}$ induz ou gera $G^{'}$ em G e denotamos por $G^{'} = G[V^{'}]$.

Se G e $G^{'}$ são disjuntos, denotamos por $G * G^{'}$ o grafo obtido de $G \cup G^{'}$ unindo todos os vértices de G a todos os vértices de $G^{'}$. Isto é, as arestas de $G * G^{'}$ são as arestas de G, as de $G^{'}$ e mais estas ligações.

O *complemento* de um grafo $G = (V, A)$ é $\overline{G} = (V, \overline{A})$ onde o conjunto das arestas $\overline{A} = [V]^2 \setminus A$, ou seja, são as arestas xy tal que x, y são vértices de V mas xy não pertence a A.

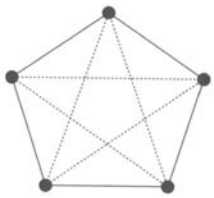
O *grau de um vértice* v é o número de arestas em v, ou seja, é o número de vértices vizinhos de v. Denotamos por $d(v)$ ou $d_G(v)$. Um vértice de grau zero é dito ser isolado.

O *grau mínimo* de um grafo G é dado por $\delta(G) := \min\{d(v)|v \in V\}$ e o *grau máximo* é dado por $\Delta(G) := \max\{d(v)|v \in V\}$.

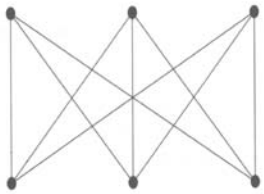
1.3 Principais Tipos de Grafos

Grafos Triviais: um grafo trivial é aquele de ordem 0 ou 1.

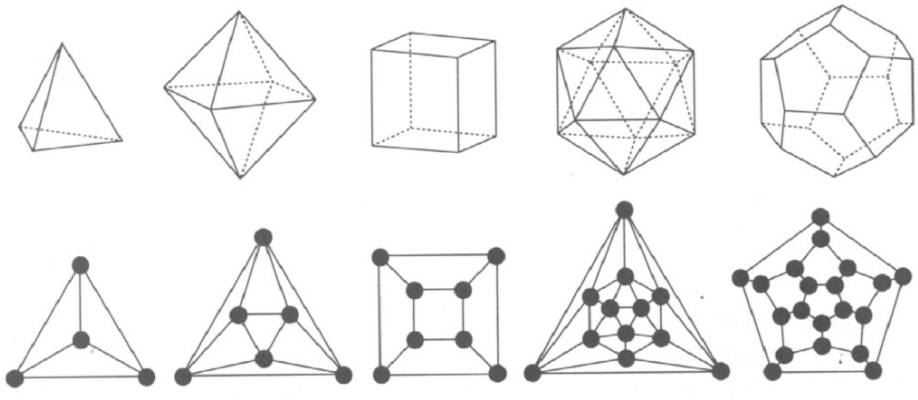
Grafos Completos: um grafo é completo se dados quaisquer dois de seus vértices, existe uma aresta que os liga, ou seja, dados quaisquer dois vértices, estes são adjacentes. Se este grafo possui k vértices, denotamos por K_k (abaixo temos o K_5).



Grafos Bipartidos: um grafo bipartido é aquele em que podemos escrever o conjunto de seus vértices como união disjunta de dois conjuntos A e B e ainda, cada aresta de G liga um vértice de A a um vértice de B. Se A possui m elementos e B possui n, denotamos este grafo bipartido por $K_{m,n}$ (temos o $K_{m,n}$).



Grafos Platônicos: estes são os grafos originados pelos sólidos regulares de Platão (tetraedro, hexaedro, octaedro, dodecaedro e icosaedro).



Grafos Regulares: um dado grafo é chamado regular se todos os seus vértices possuem o mesmo grau. Se este grau for k, dizemos que G é um grafo k-regular e k é a valência deste grafo. Existem vários tipos de grafos regulares e os mais importantes serão apresentados na seção 1.7.

1.4 Caminhos e Ciclos

Um caminho é um grafo não vazio $P(V, A)$ tal que $V = \{x_0, x_{1,...,}x_k\}$ e $A = \{x_0x_1, x_1x_2, ..., x_{k-1}x_k\}$ onde $x_i \neq x_j$ se $i \neq j$. O comprimento de um caminho é dado pelo número de arestas que ele possui. Denotamos este caminho de x_0 a x_k por $P = x_0x_1...x_k$.

Outras notações usadas:

$$Px_i = x_0...x_i$$
$$x_iP = x_i...x_k$$
$$x_iPx_j = x_i...x_j$$
$$P^o = x_1...x_{k-1}$$
$$Px_i^o = x_0...x_{i-1}$$
$$x_i^oP = x_{i+1}...x_k$$
$$x_i^oPx_j^o = x_{i+1}...x_{j-1}$$

Dado um caminho $P = x_0x_1...x_{k-1}$, com $k \geq 3$ e $x_i \neq x_j$, chamamos de *ciclo* o grafo $C = P \cup x_{k-1}x_0$ e denotamos por $x_0x_1...x_{k-1}x_0$.

O *comprimento de um ciclo* é o número de arestas que este possui. O comprimento mínimo de ciclos em G é chamado "Girth"e denotado por $g(G)$ e o comprimento máximo de ciclos em G é sua circunferência. Chamamos de corda a aresta que liga dois vértices de um ciclo, mas que não é uma aresta deste ciclo.

A *distância* $d_G(x, y)$ em G de dois vértices x e y é o comprimento do menor caminho ligando x e y. Observamos que $d_G : G \times G \to \mathbb{R}$ é de fato uma métrica em G, desde que o grafo seja conexo, isto é:

1) $d_G(x, y) = d_G(y, x)$

2) $d_G(x, y) \geq 0$ e $d_G(x, y) = 0 \Leftrightarrow x = y$

3) $d_G(x, y) + d_G(y, z) \geq d_G(x, z)$

A maior distância entre dois vértices quaisquer é o *diâmetro de* G que é denotado por $diam(G)$.

Proposição 1.2. *[3]: Todo grafo G contém um ciclo satisfazendo*

$$g(G) \leq 2\ diam(G) + 1$$

Um *vértice é central* em G se a maior distância entre ele e qualquer outro vértice é a menor possível. Esta distância é chamada de *raio de* G e denotado por $rad(G)$.

Proposição 1.3. *[3]:* $rad(G) \leq diam(G) \leq 2\ rad(G)$

Uma *caminhada* em um grafo G é uma sequência não vazia $v_0e_0v_1e_1...e_{k-1}v_k$ alternando vértices e arestas em G tal que, $e_i = \{v_i, v_{i+1}\}$, para todo $i < k$. Se os vértices são todos distintos, então temos um caminho em G.

1.5 Conexidade

Um grafo não vazio $G = (V, A)$ é dito *conexo* se quaisquer dois de seus vértices puderem ser ligados por um caminho em G. Um subgrafo conexo maximal de G é chamado componente conexa de G.

Se $B, C \subseteq V$ e $X \subseteq V \cup A$ são tais que todo caminho de B a C em G contém um vértice (ou uma aresta) de X, nós dizemos que X *separa os conjuntos* B *e* C *em* G. Mais geralmente, dizemos que X separa G se X separa dois vértices de $G\backslash X$ em G. Um vértice que separa dois outros vértices da mesma componente conexa é um *vértice de corte (cutvertex)* e uma aresta separando seus vértices finais é uma *ponte* (pontes não podem pertencer a ciclos). G é k*-conexo* se $|G| > k$ e $G - X$ é conexo, $\forall X \subseteq V$ com $|X| < k$, ou seja, não existem dois vértices de G que são separados por pelo menos k outros vértices. O maior inteiro k tal que G é k-conexo é a *conexidade* $\Bbbk(G)$ de G.

1.6 Árvores e Florestas

Floresta é um grafo que não possui nenhum ciclo. Uma floresta conexa é uma *árvore*. Os vértices de grau 1 em uma árvore são suas *folhas*.

Teorema 1.4. *[3]: As seguintes afirmações são equivalentes:*

(i) T *é uma árvore*

(ii) Quaisquer dois vértices de T *são ligados por um único caminho em* T

(iii) T *é minimalmente conexo, isto é,* T *é conexo mas* $T - e$ *é desconexo, para toda aresta* e *de* T.

(iv) T *é maximalmente acíclico, isto é,* T *não possui ciclo mas* $T + xy$ *possui, quaisquer que sejam dois vértices não adjacentes* x *e* y *de* T.

Corolário 1.5. *[3]: Um grafo conexo com* n *vértices é uma árvore se e somente se possui* $n - 1$ *arestas.*

Às vezes é conveniente considerar um vértice de uma árvore como especial. Tal vértice é chamado de raiz desta árvore. Uma árvore com uma raiz fixa é uma *árvore enraizada*.

Escolhendo uma raiz r em uma árvore T, impomos uma ordem parcial em $V(T)$ dada por: $x \leq y$ se x está entre r e y, ou seja, $x \in rTy$. Esta é a *ordem da árvore* em $V(T)$ associada a T e r.

Uma árvore enraizada T contida em um grafo G é chamada *normal* em G se os finais de todos os T-caminhos são comparáveis na ordem da árvore de T.

Proposição 1.6. *[3]: Todo grafo conexo G contém uma árvore normal T, com algum vértice específico como raíz e tal que T gera G.*

1.7 Grafos regulares especiais

1.7.1 Grafos distância-regular

Definição 1.7. *Um grafo conexo Γ de diâmetro d é chamado distância-regular se existem inteiros b_i, c_i, com $0 \leq i \leq d$, tal que para quaisquer dois vértices $\gamma,\delta \in \Gamma$ com $d(\gamma,\delta) = i$, existem precisamente c_i vizinhos de δ em $\Gamma_{i-1}(\gamma) = \{x \in \Gamma \ / \ d(\gamma,x) = i-1\}$ e b_i vizinhos de δ em $\Gamma_{i+1}(\gamma) = \{y \in \Gamma \ / \ d(\gamma,y) = i+1\}$. Em particular, Γ é regular de valência $k = b_0$.*

Como d é a distância máxima, não existe b_d e como não podemos ter pontos à distância -1, não existe c_0.

A sequência $\iota(\Gamma) := \{b_0, b_1, ..., b_{d-1}; c_1, c_2, ..., c_d\}$ é chamada de vetor intersecção (intersection array) de Γ.

Exemplo:

1. Polígonos

   Eles têm vetor intersecção $\{2, 1, ..., 1; 1, ...1, c_d\}$, onde $c_d = 2$ para os $2d-gonos$ e $c_d = 1$ para os $(2d+1)-gonos$.

2. Sólidos de Platão

   Seus vértices e arestas formam grafos distâncias-regulares com vetor intersecção $\{3; 1\}$ para o tetraedro, $\{4, 1; 1, 4\}$ para o octaedro, $\{3, 2, 1; 1, 2, 3\}$ para o cubo, $\{5, 2, 1; 1, 2, 5\}$ para o icosaedro e $\{3, 2, 1, 1, 1; 1, 1, 1, 2, 3\}$ para o dodecaedro.

□

1.7.2 Grafos aresta regular e aresta co-regular

Consideremos inicialmente, grafos regulares tendo uma ou mais das propriedades abaixo:

R_1) Quaisquer dois vértices adjacentes possuem precisamente $\lambda = \lambda(\Gamma)$ vértices vizinhos comuns.

R_2) Quaisquer dois vértices cuja distância entre eles é 2, possuem precisamente $\mu = \mu(\Gamma)$ vértices vizinhos comuns.

R_3) Quaisquer dois vértices não adjacentes possuem precisamente $\mu = \mu(\Gamma)$ vértices vizinhos comuns.

Um grafo regular com v vértices e valência k é chamado *aresta-regular* com parâmetros (v, k, λ) se R_1 acontece. *Amplamente regular* com parâmetros (v, k, λ, μ) se R_1 e R_2 acontecem. *Aresta co-regular* com parâmetros (v, k, μ) se R_3 acontece e *fortemente regular* com parâmetros (v, k, λ, μ) se R_1 e R_3 acontecem.

Observação 1.8. *Vamos agora citar algumas observações relacionadas às definições dadas acima.*

1. *Todo grafo distância regular é amplamente regular* ($\lambda = a_1, \mu = c_2$) *e é fortemente regular se possuir diâmetro no máximo* 2.

   Um grafo satisfazendo R_3 *(ou apenas* R_2*) com* $\mu = 0$ *é a união disjunta de pontos. Se* $\mu > 0$*, o grafo é conexo e tem diâmetro no máximo* 2.

2. *Para um grafo aresta-regular não completo temos* $\mu \leq k$*. Um grafo aresta co-regular com* $\mu = k$ *é um grafo multipartido completo* $K_{3\times t}$.

Chamamos um grafo aresta co-regular de *não trivial* se ele não é completo e $0 < \mu < k$.

1.8 Álgebra Linear e Grafos

Seja o grafo $G = (V, A)$ com $V = \{v_1, ..., v_n\}$ e $A = \{e_1, ..., e_m\}$. O *espaço dos vértices* $\nu(G)$ de G é o espaço vetorial sobre o corpo de 2 elementos $F_2 = \{0, 1\}$ de todas as funções $V \to F_2$. Temos que $\{\{v_1\}, ..., \{v_n\}\}$ é *base canônica* de $\nu(G)$ e portanto, $dim(\nu(G)) = n$.

Da mesma forma, as funções $A \to F_2$ formam o *espaço das arestas* $\varepsilon(G)$ de G, cujos elementos são subconjuntos de A. Como anteriormente, temos que $\{\{e_1\}, ..., \{e_m\}\}$ é *base canônica* de $\varepsilon(G)$ e então $dim\ (\varepsilon(G)) = m$.

Um conjunto é isomorfo ao das funções de B em $0, 1$ se, e somente se, cada subconjunto de arestas está identificado com um elemento de $\varepsilon(G)$.

Dados $F, F' \in \varepsilon(G)$ e seus coeficientes $\lambda_1, ..., \lambda_m$ e $\lambda_1', ..., \lambda_m'$ com respeito a base canônica, podemos definir o produto interno:

$$< F, F^{'} > \ := \ \lambda_1\lambda_1^{'} + ... + \lambda_m\lambda_m^{'} \in \digamma_2$$

e note que $< F, F^{'} > \ = \ 0 \Leftrightarrow F$ e $F^{'}$ possuem um número par de arestas em comum.

Dado um subespaço $\digamma$ de $\varepsilon(G)$, temos que:

$$\digamma^{\perp} \ := \ \{D \in \varepsilon(G) \ / \ < F, D > \ = \ 0, \forall \ F \in \digamma\}$$

que é ainda um subespaço de $\varepsilon(G)$. Ainda, temos que:

$$dim(\digamma) + dim(\digamma^{\perp}) = m$$

A *matriz incidência* $B = (b_{i,j})_{nxm}$ de um grafo $G = (V, A)$ com $V = \{v_1, ..., v_n\}$ e $A = \{e_1, ..., e_m\}$ é definida sobre $\digamma_2$ por:

$$b_{i,j} := 1 \text{ se } v_i \in e_j$$

$$b_{i,j} := 0 \text{ se } v_i \notin e_j$$

Sendo B^t a transposta de B, temos que B e B^t definem funções lineares $B : \varepsilon(G) \to \nu(G)$ e $B^t : \nu(G) \to \varepsilon(G)$ com respeito à base canônica.

A *matriz adjacência* $A = (a_{i,j})_{nxn}$ de G é definida por:

$$a_{i,j} = 1 \ se \ v_iv_j \in A$$

$$a_{i,j} = 0 \ se \ v_iv_j \notin A$$

Proposição 1.9. *[3]: Seja D a matriz diagonal $D = (d_{i,j})_{n\times n}$ com $d_{ii} = d(v_i)$ e $d_{ij} = 0$ se $i \neq j$. Temos que:*

$$BB^t = A + D$$

1.9 Planaridade

Um grafo é *planar* se pode ser desenhado no plano (mergulho) sem auto-interseção.

Uma face num grafo planar é um polígono homeomorfo a um disco cujo contorno é dado por uma curva fechada composta por arestas do grafo.

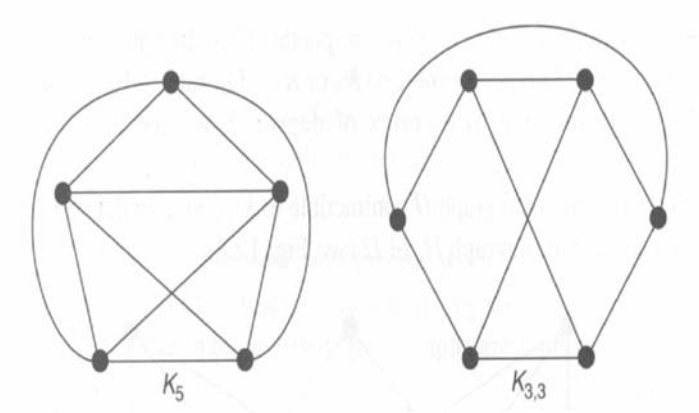
Dizemos que dois grafos são *homeomorfos* se ambos podem ser obtidos do mesmo grafo, inserindo novos vértices de grau dois.

Fórmula de Euler usando componentes conexas: $V - A + F = k + 1$, onde k é o número de componentes conexas do grafo de V vértices, A arestas e F faces.

Fórmula de Euler para grafos planares: seja G um grafo planar com V vértices, A arestas e F faces. Temos então que $V - A + F = 2$.

Teorema 1.10. *[6]: Seja F o número de faces de um grafo conexo planar $G = (V, A)$ e m a cardinalidade de A $(m > 1)$. Então $3F \leq 2m$.*

Mas nem todos os grafos são planares. Um exemplo é o $K5$ e o $K3,3$, pois como podemos ver na figura abaixo, toda representação deles no plano terá uma auto- interseção.



Corolário 1.11. *Os grafos $K3,3$ e $K5$ não são planares.*

Demonstração: Seja n o número de vértices de $K5$ e m seu número de arestas. A Fórmula de Euler nos diz que se $K5$ fosse planar, teríamos que

$$F = 2 - n + m = 2 - 5 + 5(5-1)/2 = 7$$

Mas 3 $F = 21$ e 2 $m = 20$, contradizendo o teorema anterior. Portanto, $K5$ não é planar.

Para provar que $K3,3$ não é planar, observemos que qualquer ciclo de $K3,3$ contém um número par (maior que 3) de arestas. Se denotarmos por Fi o número de faces com exatamente i arestas na fronteira, temos que

$$F1 + 2F2 + 3F3 + ... \leq 2m,$$

pois cada aresta é contabilizada duas vezes.

Como a fronteira de uma face numa realização planar de um grafo é constituída pelos arcos de um ciclo, temos que as faces de uma realização planar de $K3,3$ (se existisse) teriam pelo menos 4 arcos na fronteira e portanto,

$$4F = 4F4 + 4F6 + ... \leq 4F4 + 6F6 + \leq 2m.$$

Mas lembrando que o número de faces de $K3,3$ seria 5 caso fosse planar, temos que

$$20 = 4F \leq 2m = 18,$$

o que é uma contradição. Portanto, $K3,3$ não é planar. □

Pode-se notar que todo grafo que possui um subgrafo não planar é não planar. Portanto, temos que todo grafo que possui o $K5$ ou o $K3,3$ como subgrafo, é não planar.

Na verdade, existe um resultado mais forte, que é o Teorema de Kuratowski que nos possibilita verificar se um grafo é ou não planar exatamente a partir dos dois grafos não planares que vimos.

Teorema 1.12. *[6]: Um grafo é planar se, e somente se, não contém subgrafo homeomorfo a $K3,3$ ou $K5$.*

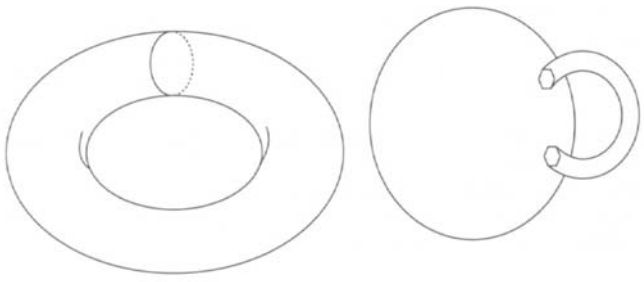
Dado um grafo G, definimos o *número de cruzamentos de* G, denotado por $cr(G)$ como o número mínimo de cruzamentos que podem ocorrer quando G é desenhado no plano, onde esses cruzamentos só podem ocorrer entre duas arestas.

Temos então que se G é planar, $cr(G) = 0$ e nos exemplos mostrados anteriormente, $cr(K3,3) = cr(K5) = 1$.

1.10 Outras superfícies

Até agora, vimos grafos desenhados no plano, o que é equivalente a serem desenhados na superfície esférica. A partir daqui, consideraremos grafos em outras superfícies como por exemplo, no toro.

Como é conhecido, o toro é uma superfície que pode ser vista como uma esfera que possui uma "alça", ou seja, topologicamente o toro é obtido de uma esfera retirando-se dois discos e colando-se um cilindro nestes bordos. Ao repetirmos esta operação g vezes, obtemos a superfície (uma esfera com g alças) que é conhecida como g-toro. Um teorema central de topologia das variedades bi-dimensionais é o que classifica as superfícies orientáveis compactas.



Teorema 1.13. *[10]: Toda superfície orientável compacta é homeomorfa a um g-toro.*

O *gênero(genus)* de uma superfície compacta orientável é g se ela for topologicamente homeomorfa à esfera com g "alças"(g-toro).

Portanto, o toro possui gênero 1 e a esfera, gênero 0. Uma superfície de gênero g (g-toro) pode ser construida a partir de uma identificação dos bordos de um polígono de $4g$ lados.

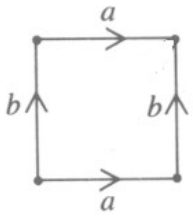
Um resultado central sobre a topologia dos grafos é o que se segue:

Teorema 1.14. *[10]: Todo grafo pode ser mergulhado sem auto-interseção sobre uma superfície de gênero g.*

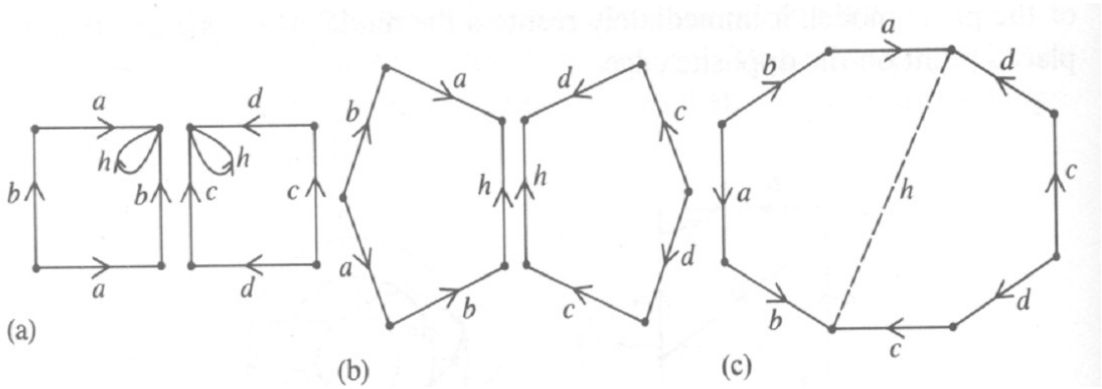
Um grafo possui gênero g se pode ser mergulhado sem auto-interseção em uma superfície de gênero g, mas não em uma superfície de gênero $g-1$, isto é, *gênero de um grafo* é o gênero da superfície mais simples na qual o grafo pode ser mergulhado sem auto-interseção.

Em geral, existe grande dificuldade em descobrirmos o gênero de um dado grafo:

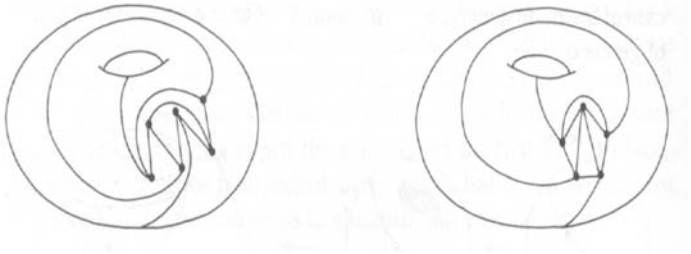
$g = 1 \Rightarrow 4g = 4 \Rightarrow$ o espaço de identificação é um polígono de 4 lados com a borda identificada.



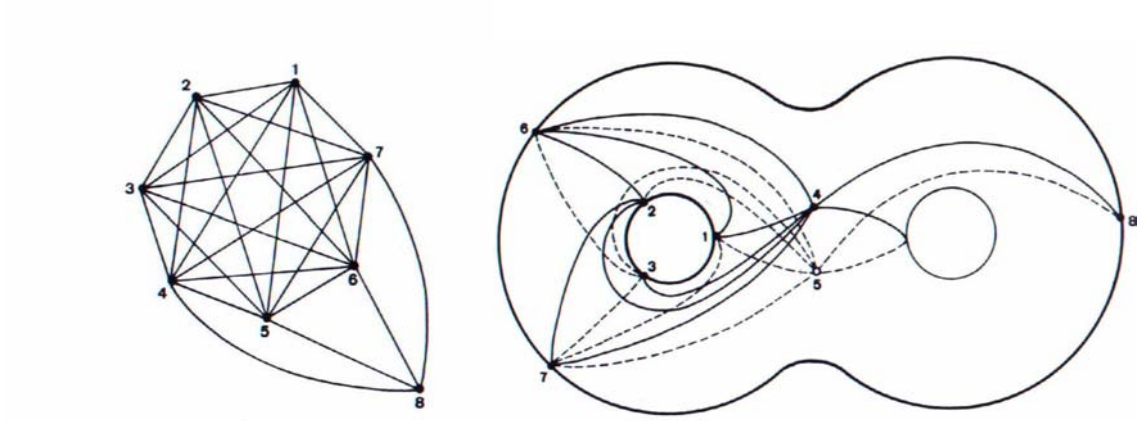
$g = 2 \Rightarrow 4g = 8 \Rightarrow$ o espaço de identificação é um polígono de 8 lados com a borda identificada.



O gênero de um grafo mede sua complexidade, uma vez que seu gênero aumenta conforme aumentamos sua complexidade. Grafos planares podem ser colocados numa esfera e se voltarmos novamente aos exemplos $K3,3$ e $K5$, veremos que ambos podem ser desenhados no toro sem auto-interseção e têm portanto gênero 1.



Para se ter uma idéia do grau de dificuldade que podemos encontrar, observe o grafo abaixo o qual produz certa dificuldade para se descobrir em qual superfície ele pode ser mergulhado sem auto interseção e logo a seguir, vemos que este grafo possui gênero 2.



Existem alguns resultados que podem nos ajudar a encontrar o gênero de um dado grafo e um deles, que na verdade não fornece o número exato mas sim um limitante é o que segue:

Teorema 1.15. *[6]: O gênero de um grafo G não ultrapassa seu número de cruzamentos, isto é, $g \leq cr(G)$.*

Teorema 1.16. *[6]: Para grafos de gênero g, temos que $V - A + F = 2 - 2g$.*

Seja Λ um grafo e V o número de vértices de Λ. Temos que se $V \geq 3$, o gênero g de Λ satisfaz a seguinte desigualdade:

$$g \leq \frac{(V-3)(V-4)}{12}$$

Teorema 1.17. *[6]: Seja Λ um grafo conexo, V seu número de vértices e A seu número de arestas. Temos então que se $V \geq 3$, então*

$$\frac{1}{6}A - \frac{1}{2}(V-2) \leq g \leq \frac{(V-3)(V-4)}{12}$$

1.11 Grafos Eulerianos

Concluimos este capítulo voltando ao problema que motivou a Teoria de Grafos, o Problema das Pontes de Königsberg. Um grafo conexo G é euleriano se existe uma trajetória fechada contendo todas as arestas de G. Note que cada aresta deve ser atravessada uma única vez. Um grafo não euleriano g é semi-euleriano se existe uma trajetória contendo todas as arestas de G.

Teorema 1.18. *[3]: Se G é um grafo em que cada um de seus vértices possui grau no mínimo 2, então G contém um ciclo.*

Incluimos a demonstração do teorema a seguir que é o que resolve o problema que deu origem à teoria de grafos.

Teorema 1.19. *[3]: Um grafo conexo G é euleriano se, e somente se, o grau de cada um dos vértices de G é par.*

Demonstração: $\Rightarrow$)Suponha que P é uma trajetória euleriana de G. Cada vez que P passa por um vértice de G, contribui com dois graus neste vértice e como cada aresta é percorrida uma única vez por P, cada vértice tem que ter grau par.

$\Leftarrow$)A prova é por indução no número de arestas de G.

Suponha que o grau de cada vértice é par. Desde que G é conexo, cada vértice tem grau no mínimo 2 e então, pelo teorema anterior, G contém um ciclo C.

Se C contém todas as arestas de G, a prova está completa.

Caso contrário, removemos de G as arestas de C obtendo um novo grafo H possivelmente desconexo com menos arestas que G e cada vértice deverá ter grau par. Pela hipótese de indução, cada componente de H possui no mínimo um vértice em comum com C, por conexidade, obtemos a trajetória euleriana de G e consequentemente, um vértice não isolado é alcançado por arestas de C, traçando a trajetória euleriana de um componente de H que contém este vértice, percorrendo as arestas de C até alcançarmos um vértice pertencente a outra componente de H.

Este processo termina quando retornarmos para o vértice inicial. □

Para solucionar o problema das ponte de Königsberg, Euler modelou-o como um grafo, identificando cada ponte com uma aresta e cada ilha e margem com um vértice. Daí, o problema ficou reduzido a verificar se seria possível encontrar uma trajetória sobre o grafo, que percorresse todas as arestas e vértices uma única vez, ou seja, verificar se este grafo é euleriano .

O problema das pontes de Königsberg é bem conhecido e se observarmos o teorema anterior, podemos ver que como nenhum vértice possui grau par, este grafo não é euleriano. Podemos então concluir que é impossível realizar tal passeio.

Capítulo 2

Códigos Corretores de Erros

Neste capítulo, estaremos interessados em introduzir a teoria sobre códigos corretores de erros, dando maior ênfase aos códigos lineares e aos códigos perfeitos. Para isso, a principal bibliografia será [1] e [8].

A teoria dos códigos corretores de erros foi fundada pelo matemático C. E. Shannon, em 1948. Inicialmente, os maiores interessados em Teoria dos Códigos foram os matemáticos que a desenvolveram consideravelmente nas décadas de 50 e 60. A partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria começou a interessar também aos engenheiros. Hoje em dia, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo a sua confiabilidade.

2.1 Exemplos

1. Seja A o conjunto formado pelas 23 letras do alfabeto da língua portuguesa, pelo espaço em branco, ç e pelas vogais acentuadas. Este conjunto será chamado alfabeto e cada palavra é um elemento de A^{27} onde 27 é o comprimento da palavra inconstitucionalissimamente, que é a mais longa de nosso vocabulário. Denotamos por P a língua portuguesa, como subconjunto próprio de A^{27}.

   Este código é capaz de detectar e corrigir erros pois se produzirmos a palavra cathorro, como não pertence a P, sabe-se que ocorreu um erro e então corrige-se pela palavra mais próxima (cachorro). Podemos observar ainda que não é muito eficiente pois existem palavras muito próximas em P, como por exemplo, rato, pato, gato e galo, dificultando detectar um erro.

2. Códigos com dígitos verificadores (dígitos de controle). Exemplos destes códigos são os usados em contas bancárias e CPF. Se é dado um CPF $x_1x_2...x_{10}x_{11}$, os chamados dígitos de controle são os dois últimos x_{10} e x_{11}, que possuem uma relação de

dependência com os nove primeiros números. Esta dependência é dada pelas seguintes fórmulas:

$$x_{10} = \left(\left(\sum_{i=1}^{9} i \cdot x_i \right) \bmod 11 \right) \bmod 10$$
$$x_{11} = \left(\left(\sum_{i=2}^{10} (i-1) \cdot x_i \right) \bmod 11 \right) \bmod 10$$

Esses dígitos servem para testar a autenticidade do CPF fornecido.

2.2 Métrica de Hamming e Métrica de Lee

Sejam $u = (u_1, ..., u_n),\ v = (v_1, ..., v_n) \in\ A^n$. A distância de Hamming de u e v é o número de coordenadas em que u e v diferem, ou seja,

$$d_h(u, v) = |\ \{i\ /\ u_i \neq v_i\ ,\ 1 \leq i \leq n\}\ |$$

Propriedades:

1) $d_h(u, v) \geq 0$
2) $d_h(u, v) = 0 \Leftrightarrow\ u = v$
3) $d_h(u, v) = d_h(v, u)$
4) $d_h(u, v) \leq d_h(u, w) + d_h(w, v)$

Por (1),(2),(3) e (4), temos que d_h é métrica. Podemos então chamá-la de Métrica de Hamming.

Sejam $a, b \in \mathbb{Z}_q^n$, onde $a = (a_1, ..., a_n)$ e $b = (b_1, ..., b_n)$. A métrica de Lee é definida sobre $\mathbb{Z}_q^n$ da seguinte forma:

$$d_L\,(a, b) = \sum_{i=1}^{n} \min\{|a_i - b_i|, |q - (a_i - b_i)|\}$$

Chamamos de Espaço de Lee o espaço sobre o $\mathbb{Z}_q^n$ com a métrica de Lee, ou seja $(\mathbb{Z}_q^n, d_L)$.

Sejam $a \in\ A^n$ e $t \in\ \mathbb{R}$. O *disco* $D(a, t)$ de centro a e raio t e a *esfera* $S(a, t)$ de mesmo centro e mesmo raio são dados por:

$$D(a, t) = \{u \in A^n\ /\ d(u, a) \leq t\}$$

$$S(a, t) = \{u \in A^n\ /\ d(u, a) = t\}$$

E temos ainda que:

$$|D(c,r)| = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

$$|S(a,i)| = \binom{n}{i} (q-1)^i$$

Dado um código C, para $u, v \in C$ temos que a *distância mínima* d de C é dada por $d = min\{\ d_h(u,v)\ /u \neq v\}$. Temos ainda que o número de palavras de um código será denotado por M e k definido da seguinte forma $k = \left\lfloor \frac{d-1}{2} \right\rfloor$. Os parâmetros n, M e d são os *parâmetros fundamentais* de um código e serão denotados por $[n, M, d]$.

Corolário 2.1. *[1]: Seja C um código com distância mínima d e c, $c^{'} \in C$ com $c \neq c^{'}$. Portanto, se $D(c,k) \cap D(c^{'},k) = \varnothing$, C corrige k erros e detecta $d-1$ erros.*

Dado um código C com distância mínima d e corrigindo k erros, ele será um *código perfeito* se $\cup_{c \in C} D(c,k) = A^n$.

Uma função $F : A^n \to A^n$ é uma *isometria* se $d_h(F(x), F(y)) = d_h(x,y)$ com $x,\ y \in A^n$.

Propriedades:

1) Toda isometria de A^n é bijeção;
2) A função identidade de A^n é uma isometria;
3) Se F é isometria, então F^{-1} também o é;
4) Se F e G são duas isometrias, então temos que $F\ o\ G$ também é isometria.

Dados dois códigos $C, C^{'} \in A^n$. Dizemos que estes *códigos são equivalentes* se existir isometria F de A^n tal que $F(C) = C^{'}$. Neste caso, denotaremos por $C \approx C^{'}$.

Propriedades:

1) $C \approx C$;
2) $C \approx C^{'} \Rightarrow C^{'} \approx C$;
3) Se $C \approx C^{'}$ e $C^{'} \approx C^{''} \Rightarrow C \approx C^{''}$.

Temos então que $\approx$ é uma relação de equivalência.

Proposição 2.2. *[1]: Se $C \approx C^{'}$, então os dois códigos possuem os mesmos parâmetros.*

Teorema 2.3. *[1]: Seja $F : A^n \to A^n$ uma isometria. Então existem permutações Π de $\{1, ..., n\}$ e bijeções f_i com $i = 1, ..., n$ tais que $F = T_\Pi o T^1_{f_1} o ... o T^n_{f_n}$ onde $T^i_f(a_1, ..., a_n) = (a_1, ..., f(a_i), ..., a_n)$ e $T_\Pi(a_1, ..., a_n) = (a_{\Pi(1)}, ..., a_{\Pi(n)})$.*

Corolário 2.4. *[1]: $C \approx C'$ se, e somente se, existem permutações Π de $\{1, ..., n\}$ e bijeções f_i com $i = 1, ..., n$ tais que $C' = \{(f_{\Pi(1)}(x_{\Pi(1)}), ..., f_{\Pi(n)}(x_{\Pi(n)})) \ \ /(x_1, ..., x_n) \in C\}$.*

Sejam C e C' códigos sobre A de comprimento n cujos elementos são letras. Então temos que $C \approx C'$ se e somente se um pode ser obtido do outro através de:

(i) substituição das letras numa dada posição fixa em todas as palavras do código por bijeção de A;

(ii) permutação das posições das letras em todas as palavras, mediante permutação fixa de $\{1, ..., n\}$.

2.3 Anéis e corpos

O conjunto A munido de duas operações (+ e .) é chamado de *anel* se:
(i) $\forall a, b, c \in A,\ (a + b) + c = a + (b + c)$
(ii) $\exists\ 0 \in A$ tal que $a + 0 = 0 + a = a,\ \forall a \in A$. Este elemento é chamado neutro de (+).
(iii) $\forall\ a \in A,\ \exists\ (-a) \in A$ tal que $a + (-a) = 0$
(iv) $\forall\ a, b \in A,\ a + b = b + a$
(v) $\forall\ a, b, c \in A,\ (ab)c = a(bc)$
(vi)$\forall\ a \in A,\ \exists\ 1 \in A$ tal que $a1 = 1a = a$. Este elemento é o neutro da operação (.)
(vii) $\forall\ a, b \in A,\ ab = ba$
(viii)$\forall\ a, b, c \in A,\ a(b + c) = ab + ac$

Propriedades:

1) $a \cdot 0 = 0,\ \forall a \in A$
2) Os elementos neutros das duas operações são únicos.

O anel A será um *domínio de integridade* se $\forall\ a, b \in A$, com $a \neq 0$ e $b \neq 0$, temos que $ab \neq 0$, isto é, se $ab = 0$ então $a = 0$ ou $b = 0$. Seja A um domínio de integridade, temos que A será um *corpo* se $\forall\ a \in A,\ a \neq 0,\ \exists\ b \in A$ tal que $ab = ba = 1$. Todo elemento a com esta propriedade é dito ser *invertível*.

Teorema 2.5. *[1]: Se A é corpo, então é domínio de integridade.*

Lei do Cancelamento: Seja A um domínio de integridade e $c \neq 0$. Então temos que $ac = bc \Rightarrow a = b$.

Dado um domínio de integridade A, denotamos o *corpo de frações* de A por $Q(A)$ e o definimos da seguinte forma:

$$Q(A) = \left\{ \frac{a}{b} \; com \; a, \; b \in A \; e \; b \neq 0 \right\}$$

onde $\frac{a}{b} \approx \frac{c}{d} \Leftrightarrow ad = bc$

Potenciação: Sejam A um anel, $a, b \in A$ e $m, n \in \mathbb{Z}$. Temos então as seguintes propriedades:

1) $na = -(-n)a = (-n)(-a) = -n(-a)$
2) $na = (n1)a$
3) $n(ma) = (nm)a$
4) $n(a \pm b) = na \pm nb$
5)$(n \pm m)a = na \pm ma$

Para $a \in A$ e $m, n \in \mathbb{N} \cup \{0\}$, temos que:

6) $(a^m)^n = a^{mn}$
7) $(ab)^n = a^n b^n$
8) $a^{n+m} = a^n a^m$

Teorema 2.6. *[1]: Seja A um corpo e M uma matriz cujos elementos pertencem a A. O conjunto de matrizes deste tipo serão denotadas por M_A. Temos então que M é invertível se, e somente se, $det(M) \neq 0$.*

Matriz de Vandermond

Seja A um anel e $a_1, ..., a_n \in A$. A *Matriz de Vandermond* $V(a_1, ..., a_n)$ é uma matriz $n \times n$ e será dada por:

$$V(a_1, ..., a_n) = \begin{pmatrix} 1 & a_1 & a_1^2 & . & a_1^{n-1} \\ 1 & a_2 & a_2^2 & . & a_2^{n-1} \\ . & . & . & . & . \\ 1 & a_n & a_n^2 & . & a_n^{n-1} \end{pmatrix}$$

Propriedades:

1) $det(V(a_1, ..., a_n)) = \Pi_{i=1}^{n-1} \; \Pi_{i=j+1}^{n-1}(a_i - a_j) = \Pi_{i>j}(a_i - a_j)$
2) Se A for um domínio de integridade, então $det(V(a_1, ..., a_n)) \neq 0 \Leftrightarrow a_i \neq a_j, i \neq j$.

Seja A um anel e $a, b \in A$. Temos que a *divide* b se $\exists \; c \in A$ tal que $b = ac$. Neste caso, escrevemos $a|b$.

Propriedades: Seja A um anel e $a, b, c, u, \lambda, \mu \in A$, onde u é invertível.

1) $u|a$
2) $a|0$
3) $a|a$
4) Se $a|u$, então a é invertível
5) Se $a|b$ e $b|c$, então $a|c$
6) Se $a|b$ e $a|c$, então $a|(\lambda b + \mu c)$

Seja A um anel e $a, b \in A$. Dizemos que a e b são *associados* se existe elemento invertível $u \in A$ tal que $a = ub$. Isso será denotado por $a \sim b$.

Propriedades:

1) $a \sim a$
2) $a \sim b \Rightarrow b \sim a$
3) Se $a \sim b$ e $b \sim c$, então $a \sim c$
Portanto, $\sim$ é uma relação de equivalência.
4) $u \sim 1 \Leftrightarrow u$ invertível
5) $a \sim b \Rightarrow a|b$ e $b|a$
6) $a|b \Leftrightarrow \forall\ c \sim a, \forall\ d \sim b$, temos que $c|d \Leftrightarrow \exists\ c' \sim a$ e $d' \sim b$, temos que $c'|d'$
7) Se A for um domínio de integridade, $a|b$ e $b|a$, então $a \sim b$

Seja A um anel e $a \in A$ um elemento não invertível. Dizemos que a é *irredutível* se os únicos divisores de a são seus associados e os invertíveis de A. Dado um anel A e $a \in A\backslash\{0\}$ com a não invertível, dizemos que a é *primo* se $\forall\ b, c \in A$ tal que $a|bc$ então $a|b$ ou $a|c$.

Teorema 2.7. *[1]: Seja A um domínio de integridade e $a \in A$. Se a é primo, então a é irredutível (a recíproca não é verdadeira).*

Sejam A um domínio de integridade, $a, b \in A$ não simultaneamente nulos e $d \in A$. Dizemos que d é o *máximo divisor comum (mdc)* de a e b se:

1) $d|a$
2) $d|b$
3) $\forall c \in A$, tal que $c|a$ e $c|b$, então $c|d$
Notação: $d = mdc(a, b)$

Propriedades:

1) Se $a' \sim a$ e $b' \sim b$, então $mdc(a,b) = mdc(a',b')$
2) Se $d = mdc(a,b)$, então $\forall\ d' \sim d,\ d' = mdc(a,b)$
3) Se $a = 0$ e $b \neq 0$ ou $a = b$, então $mdc(a,b) \sim b$

Seja A um anel e $a, b \in A$. Dizemos que a e b são *primos entre si* se os únicos divisores comuns de a e b são os invertíveis de A.

Dado o anel A e $a, b, m \in A$, temos que m será o *mínimo múltiplo comum (mmc)* de a e b se:

1) $a|m$
2) $b|m$
3) $\forall\ c \in A$, tal que $a|c$ e $b|c$, então $m|c$
Notação: $d = mmc(a,b)$

Seja A um anel e $a, b, m \in A$. Temos que a *é congruente a* b *módulo* m se $m|(a-b)$. Denotaremos por $a \equiv b\ mod\ m$.
Propriedades:

1) $a \equiv a\ mod\ m$
2) Se $a \equiv b\ mod\ m$, então $b \equiv a\ mod\ m$
3) Se $a \equiv b\ mod\ m$ e $b \equiv c\ mod\ m$, então $a \equiv c\ mod\ m$
4) Se $a \equiv a'\ mod\ m$ e $b \equiv b'\ mod\ m$, então $a + b \equiv a' + b'\ mod\ m$ e $ab \equiv a'b'\ mod\ m$
Portanto, $\equiv$ é uma relação de equivalência.

Seja A um anel e $a, m \in A$. A *classe residual de* a *módulo* m será dada por:

$$[a] = \{x \in A\ /\ x \equiv a\ mod\ m\} = \{a + m\lambda\ /\ \lambda \in A\}$$

Dizemos que a é o representante de $[a]$. Ainda temos que $mA = \{m\lambda\ /\ \lambda \in A\}$, ou seja, $[a] = a + mA$. Denotaremos o conjunto de todas as classes residuais em A módulo m por A_m.

Propriedades:

1) $[a] = [b] \Leftrightarrow m|(a-b)$, isto é, $(a-b) \in mA$
2) $[a] \cap [b] \neq \emptyset \Leftrightarrow [a] = [b]$
3) $A = \cup_{a \in A}[a]$
4) Se A for um domínio de integridade, então existe bijeção entre $[a]$ e mA.
5) $[a] + [b] = [a+b]$
6) $[a][b] = [ab]$

Teorema 2.8. *[1]: O conjunto A_m munido das operações (+) e (.) é um anel com elementos neutros 0 e 1 respectivamente.*

2.4 Os Inteiros

Estudaremos agora o conjunto $\mathbb{Z}$ dos números inteiros. Para este conjunto, temos que os únicos elementos invertíveis são ± 1 e ainda, que é um domínio de integridade. Os associados de $a \in A$ são $\pm a$.

Dado um anel A, temos que A será um anel ordenado se tiver uma relação de ordem satisfazendo as seguintes propriedades:

1) $\forall\ a \in A,\ a \leq a$
2) $\forall\ a, b, c \in A$, se $a \leq b$ e $b \leq c$, então $a \leq c$
3) Se $a \leq b$ e $b \leq a$, então $a = b$
4) $\forall\ a, b \in \mathbb{Z},\ a \leq b$ ou $b \leq a$
5) Se $a \leq b$, então $a + c \leq b + c$, $\forall\ a, b, c \in \mathbb{Z}$
6) Se $a \leq b$ e $0 \leq c$, então $ac \leq bc$

2.5 Códigos Lineares

2.5.1 Definições iniciais

Seja K um corpo finito com q elementos, o qual tomaremos como nosso *alfabeto*. Se $C \subset K^n$ é um código, dizemos que C é um *código linear* se for subespaço vetorial de K^n. Chamaremos então de k a *dimensão de C sobre K* e tomaremos como *base de C* o conjunto $\beta = \{v_1, ..., v_k\}$.

Para cada $x \in K^n$, definimos o *peso de x* como sendo $w(x) := |\ \{i\ /\ x_i \neq 0\}\ | = d(x, \mathbf{0})$. E peso de C como $w(C) := min\{w(x)\ /\ x \in C \backslash \{0\}\}$.

O peso de C coincide com a distância mínima do código pois $\forall\ x, y \in C$ com $x \neq y$ tem-se $z = x - y \in C\backslash\{0\}$ e $d(x, y) = w(z)$. Portanto, em termos de cálculo, é bem mais fácil achar a distância mínima de um código pois basta fazer $M - 1$ cálculos, onde M é o número de elementos do código linear.

Dado um código linear, ele pode ser representado de duas formas, como imagem e como núcleo de uma transformação linear.

1. $Im(T) = C$, $k \leq n$

$$T : K^k \to K^n$$

$$(x_1, ..., x_k) \mapsto x_1v_1 + ... + x_kv_k$$

Temos que esta transformação é linear e injetora pois:

$$ker(T) = \{(x_1, ..., x_k) \in K^k / T(x_1, ..., x_k) = \mathbf{0}\} = \{(x_1, ..., x_k) \in K^k / x_1v_1 + ... + x_kv_k = \mathbf{0}\}$$

mas como $v_1, ..., v_k$ são LI, temos então que

$$x_1 = ... = x_k = 0$$

ou seja,

$$ker(T) = \mathbf{0}.$$

Como $Im(T) = C$, temos que dado um código linear, podemos representá-lo como imagem de uma transformação linear injetora. Inversamente, temos que para cada transformação linear injetora, a imagem define um código linear.

2. $ker(H) = C$

Outra forma de se representar um código linear é através do núcleo de uma transformação. Seja C' o subespaço de dimensão n-k de K^n que é complementar de C, isto é, $C \oplus C' = K^n$. Defina então a seguinte transformação:

$$H : C \oplus C' \to K^{n-k} u \oplus v \mapsto v$$

e temos que $ker(H) = C$.

2.5.2 Matriz Geradora

A *matriz geradora* de C associada à base ordenada $\beta = \{v_1, ..., v_k\}$ será dada por

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$$

Se tomarmos a transformação $T: K^k \to K^n$ com $T(x) = xG$, temos que $Im(T) = C$ e portanto, podemos considerar K^k como sendo o código da fonte, C o código de canal e T uma codificação.

Exemplo: $K = \mathbb{F}_2$ e $T : \mathbb{F}_2^3 \to \mathbb{F}_2^5$ com $T(x) = xG$.

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Se quisermos codificar a palavra 101, basta aplicar T a x e teremos $T(x) = (101)G = (01010)$.

Agora, se quisermos decodificar a palavra 10101, teríamos que encontrar a palavra x tal que $T(x) = (10101)$ cuja solução é (100). Mas encontrar esta solução pode não ser tão fácil. □

Sabemos que uma base de um espaço vetorial pode ser obtida de outra através de operações do tipo:

- permutação de dois elementos da base;
- multiplicação de um elemento da base por um escalar não nulo;
- substituição de um vetor da base por ele mesmo somado com um múltiplo escalar de outro vetor da base;

Temos então que uma matriz geradora de um código pode ser obtida de outra através de:

- permutação de duas linhas;
- multiplicação de uma das linhas por um escalar não nulo;
- adição de um múltiplo escalar de uma linha a outra;

No exemplo anterior, note que se efetuarmos as operações acima à matriz G, obteremos uma matriz

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

e temos então que

$$xG' = (x_1x_2x_3x_2x_3)$$

onde $x = (x_1x_2x_3)$, que nos fornece de forma direta a palavra decodificada.

Diremos que a matriz geradora G de um código linear C está na forma padrão se $G = (Id_k|A)$ onde A é uma matriz $k \times (n-k)$.

2.5.3 Códigos Duais

Sejam $u = (u_1, ..., u_n)$ e $v = (v_1, ..., v_n)$ elementos de K^n, o produto interno de u e v é dado por $\langle u, v\rangle = u_1v_1 + ... + u_nv_n$.

Propriedades:

1. $\langle u, v\rangle = \langle v, u\rangle$
2. $\langle u + \lambda w, v\rangle = \langle u, v\rangle + \lambda\langle w, v\rangle$

Seja $C \subset K^n$ um código linear. Chamamos de *código dual de* C o conjunto $C^\perp = \{v \in K^n \ / \ \langle v, u\rangle = 0, \forall\ u \in C\}$.

Temos que $C^\perp$ é um subespaço vetorial de K^n e portanto, um código linear.

Teorema 2.9. *[1]:* $x \in C^\perp \Leftrightarrow Gx^t = 0$

Demonstração: $x \in C^\perp \Leftrightarrow \forall\ y \in C,\ \langle x, y\rangle = 0 \Leftrightarrow x$ é ortogonal a todos os elementos da base $\beta \Leftrightarrow Gx^t = 0$ □

Teorema 2.10. *[1]: Se G está na forma padrão, dim $C^\perp = n - k$ e $H = (-A^t \mid Id_{n-k})$ é matriz geradora de $C^\perp$.*

Demonstração: (i) $x \in C^\perp \Leftrightarrow Gx^t = 0 \Leftrightarrow (Id_k \mid A)x^t = 0 \Leftrightarrow \begin{pmatrix} x_1 \\ . \\ x_n \end{pmatrix} + A \begin{pmatrix} x_{k+1} \\ . \\ x_n \end{pmatrix} =$

$0 \Leftrightarrow \begin{pmatrix} x_1 \\ . \\ x_n \end{pmatrix} = -A \begin{pmatrix} x_{k+1} \\ . \\ x_n \end{pmatrix}$.

Temos então que $|C^\perp| = q^{n-k}$ e como $|C^\perp| = q^{\dim_K C^\perp}$, $dim_K C^\perp = n - k$.

(ii) As linhas de H são LI por causa do bloco Id_{n-k} e, portanto, geram um subespaço vetorial de dimensão $n - k$. Como as linhas de H são ortogonais às linhas de G, temos que

o espaço gerado pelas linhas de H está contido em $C^{\perp}$ e como esses dois subespaços têm a mesma dimensão, eles coincidem. portanto, H é matriz geradora de $C^{\perp}$. □

Teorema 2.11. *[1]:* $v \in C \Leftrightarrow Hv^t = 0$

De fato, $v \in C \Leftrightarrow v \in (C^{\perp})^{\perp} \Leftrightarrow Hv^t = 0$.

Esta matriz H é chamada matriz teste de paridade de C e o vetor Hv^t é chamado de síndrome de v, para $v \in K^n$.

A matriz H também é utilizada para obtermos um parâmetro para o peso de C da seguinte forma:

Observação 2.12. *1.* $w(C) \geq s$ *se, e somente se, quaisquer* $s-1$ *colunas de* H *são LI.*

2. $w(C) = s$ *se, e somente se, quaisquer* $s-1$ *colunas de* H *são LI e ainda, existem* s *colunas de* H *que são LD.*

Exemplo: Seja C um código sobre F_2 cuja matriz geradora é dada por

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

que está na forma padrão, o que possibilita encontrarmos facilmente a matriz teste de paridade

$$H = (A^t | Id_{n-k}) = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Temos então que dados os vetores (100111) e (010101), para sabermos se pertencem ou não ao código C, basta multiplicarmos pela matriz H, ou seja, $H(100111)^t = (000)$ e $H(010101)^t = (110)$ e temos então que (100111) pertence a C mas (010101) não. □

Cota de Singleton: Seja C um código linear com distância mínima d e $k = \left\lfloor \frac{d-1}{2} \right\rfloor$. Temos a seguinte desigualdade:

$$d \leq n - k + 1$$

Se valer a igualdade, o código é chamado de MDS(maximum distance separable).

2.5.4 Exemplos de Códigos Lineares

Incluimos aqui exemplos de códigos lineares sobre $F_2 = \mathbb{Z}_2$ bastante conhecidos e utilizados em aplicações.

1. CÓDIGO DE HAMMING:

   Um código de Hamming C de ordem m e dimensão k sobre $F_2 = \{0, 1\}$ é um código com matriz teste de paridade H_m de ordem $m \times n$ cujas colunas são os elementos de $F_2^m \backslash \{0\}$.

   Para $m = 3$, temos que uma matriz teste de paridade é dada por

$$H_3 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   Como F_2^m possui 2^m elementos, temos que $\mathbf{n = 2^m - 1}$ uma vez que estamos retirando o elemento $(0, ..., 0)$.

$$dim\ C^{\perp} = n - k = m \Rightarrow k = n - m \Rightarrow \mathbf{k = 2^m - 1 - m}$$

   Temos ainda que em F_2^m dois elementos são sempre LI e que conseguimos facilmente três elementos LD, isto é, duas colunas de H são sempre LI e existem três colunas LD e daí, $\mathbf{d = 3}$

   Teorema 2.13. *[1]: Todo código de Hamming é perfeito.*

   Demonstração: Seja $\hbar = [(d-1)/2] = 1$ a capacidade de correção de C.

   Dado $c \in F_2^n$, temos que $|D(c, 1)| = 1 + n!\ /\ (1!(n-1)!) = 1 + n$.

   Portanto, $|\cup_{c \in C} D(c, 1)| = [1 + n]2^k = [1 + 2^m - 1]2^{n-m} = 2^n$ e, consequentemente, $\cup_{c \in C} D(c, 1) = F_2^n$. □

   Observação 2.14. *Temos que o código de Hamming C é MDS $\Leftrightarrow m = 2$ pois temos que: C é MDS $\Leftrightarrow d = n - k + 1 \Leftrightarrow 3 = (2^m - 1) - 1 + 1 \Leftrightarrow 4 = 2^m \Leftrightarrow m = 2$.*

2. CÓDIGO DE REED-SOLOMON

   O *código de Reed-Solomon* é obtido através da imagem da transformação linear injetora:

$$T : K[X]_{k-1} \to K^n$$

$$P \mapsto (P(\alpha_1), ..., P(\alpha_n))$$

onde $K[X]_{k-1} = \{P \in K[X] \mid gr(P) \leq k-1\} \cup \{0\}$, $n \in \mathbb{N}$, $n \geq k$ e $\alpha_1, ..., \alpha_n \in K$.

T ser injetora se deve ao fato de que $kerT = \{P \in K[X]_{k-1} \ / \ P(\alpha_1) = ... = P(\alpha_n) = 0\}$. Supondo por absurdo que $kerT \neq \{0\}$, isto é, $\exists\ P \in K[X]_{k-1},\ P \neq \{0\}$ e tal que $P(\alpha_1) = ... = P(\alpha_n) = 0 \Rightarrow P$ possui n raízes distintas $\Rightarrow P$ tem grau $n \geq k$, o que é uma contradição.

Uma possibilidade para a matriz geradora G é dada por:

$$G = \begin{pmatrix} T(1) \\ T(X) \\ . \\ T(X^{k-1}) \end{pmatrix} = \begin{pmatrix} 1 & 1 & . & 1 \\ \alpha_1 & \alpha_2 & . & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & . & \alpha_n^2 \\ . & . & . & . \\ \alpha_1^{k-1} & \alpha_2^{k-1} & . & \alpha_n^{k-1} \end{pmatrix}_{k \times n}$$

Teorema 2.15. *[1]: Para os parâmetros de um código de Reed-Solomon, temos que* $\mathbf{d = n - k + 1}$*, ou seja, é MDS.*

Demonstração: Pela Cota de Singleton, temos que $d \leq n - k + 1$. Temos então que mostrar que $d \geq n - k + 1$.

Assim,

$$c \in C,\ c \neq \{0\} \Rightarrow \exists\ P \in K[X]_{k-1} \ / \ T(P) = c \tag{2.1}$$

$$\Rightarrow \exists\ P \in K[X]_{k-1} \ / \ (P(\alpha_1) = ... = P(\alpha_n)) = c \tag{2.2}$$

$$\Rightarrow w(c) = |\ \{i \in \{1, ..., n\} : P(\alpha_i) \neq 0\}\ | = n - |\ \{i \in \{1, ..., n\} : P(\alpha_i) = 0\}\ | \geq \tag{2.3}$$

$$n - gr(P)\ \geq n - (k-1) = n - k + 1 \tag{2.4}$$

$$\Rightarrow d\ \geq n - k + 1 \tag{2.5}$$

Portanto, $d = n - k + 1$. □

Exemplo: Considere $K = F_7$, $k = 4$, $n = 6$, $\alpha_1 = 3^0 = 1$, $\alpha_2 = 3^1 = 3$, $\alpha_3 = 3^2 = 2$, $\alpha_4 = 3^3 = 6$, $\alpha_5 = 3^4 = 4$ e $\alpha_6 = 3^5 = 5$.

Portanto, o código de Reed Solomon correspondente tem $d = n - k + 1 = 3$ e possui matriz geradora

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 3^0 & 3^1 & 3^2 & 3^3 & 3^4 & 3^5 \\ 3^0 & 3^2 & 3^4 & 3^6 & 3^8 & 3^{10} \\ 3^0 & 3^3 & 3^6 & 3^9 & 3^{12} & 3^{15} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{pmatrix}$$

□

3. CÓDIGO DE REED-MULLER DE 1^a ORDEM

O *código de Reed-Muller de 1^a ordem* será denotado por $R(1, m)$ e é definido como sendo o código gerado pela matriz

$$G = \begin{pmatrix} 1 & 1 \\ H_m & 0 \end{pmatrix}_{(m+1)\times 2^m}$$

onde H_m é a matriz teste de paridade de um código de Hamming.

Como a matriz geradora possui $m + 1$ linhas LI, temos que $\mathbf{k} = \mathbf{m} + \mathbf{1}$ e pelo número de colunas de G, $\mathbf{n} = \mathbf{2}^m$.

Teorema 2.16. *[1]: Para um código de Reed-Muller C, temos que* $\mathbf{d} = \mathbf{2}^{m-1}$.

Demonstração: (i) Seja $u \in C$ tal que $u = 1...1$. Temos então que $w(u) = n = 2^m$.

(ii) Seja $c \in C$, $c = v_{i_1} + ... + v_{i_r}$ tal que v_{i_j} são vetores linhas de G. Suponhamos então que nenhum desses vetores é igual a u.

Considere a matriz $B = \begin{pmatrix} v_{i_1} \\ . \\ v_{i_r} \end{pmatrix}$ que possui 2^r colunas distintas correspondentes aos vetores de F_2^r, cada uma repetida 2^{m-r} vezes. Portanto, a matriz possui metade das colunas de peso par e metade de peso ímpar $\Rightarrow$ c possui metade de suas coordenadas iguais a 1 e metade igual a 0 $\Rightarrow$ $w(c) = 2^m \ / \ 2 = 2^{m-1}$.

Por (i) e (ii), temos que os elementos de C possuem peso igual a 2^m ou igual a 2^{m-1} e portanto, $d = 2^{m-1}$. □

O código utilizado na nave Mariner 9 corresponde ao caso $m = 5$, ou seja, $R(1, 5)$ cujos parâmetros são $(32, 6, 16)$.

2.6 Decodificação

Para obtermos um algoritmo de decodificação para um código linear C com matriz teste de paridade H, temos primeiramente que definir um *vetor erro* e como sendo $e = r - c$, onde r é o vetor recebido e c o vetor transmitido.

Temos então que $w(e) = d(r, c) =$ número de erros cometidos e que e e r possuem a mesma síndrome uma vez que como $c \in C,\ He^t = H(r-c)^t = Hr^t - Hc^t = Hr^t$.

Teorema 2.17. *[1]: Se C possui capacidade de correção h, para $r \in K^n$ e $c \in C$ tal que $d(c, r) \leq h$, temos que $\exists!\ e,\ w(e) \leq h$ e cuja síndrome é igual a síndrome de r e tal que $e = r - c$.*

Demonstração: O nosso vetor e satisfaz as propriedades citadas no teorema por definição. Temos então que provar a unicidade.

Suponha que existem dois elementos de mesma síndrome $e = (\alpha_1, ..., \alpha_n)$ e $e' = (\alpha_1', ..., \alpha_n')$ tais que $w(e) \leq \hbar$ e $w(e') \leq \hbar$. Então, temos que $He^t = He'^t \Rightarrow \sum_{i=1}^n \alpha_i h^i = \sum_{i=1}^n \alpha_i' h^i \Rightarrow \sum_{i=1}^n (\alpha_i - \alpha_i')h^i = 0$, o que nos dá uma relação de dependência linear entre $2h(\leq d-1)$ colunas de H. Como quaiquer $d-1$ colunas de H são LI, temos que $\alpha_i - \alpha_i' = 0 \Rightarrow \alpha_i = \alpha_i' \Rightarrow e = e'$. □

Pelo teorema anterior, temos que para obtermos a decodificação, temos que descobrir quem é o vetor e pois neste caso, $c = r - e$. Mas como fazer isso?

1. Se $w(e) \leq 1$ e $d \geq 3$.

   (i) $He^t = 0 \Rightarrow Hr^t = 0 \Rightarrow r \in C \Rightarrow c = r$.

   (ii) $He^t \neq 0 \Rightarrow w(e) = 1 \Rightarrow$ e possui apenas uma coordenada não nula, isto é, $e = (0, ..., \alpha, ..., 0)$ com $\alpha \neq 0 \Rightarrow He^t = \alpha h^i$, onde h^i é a i-ésima coluna de $H \Rightarrow Hr^t = He^t = \alpha h^i$.

   Portanto, neste caso basta aplicar a matriz teste de paridade H ao vetor recebido e comparar com as colunas de H para descobrir quem é α e, consequentemente, quem é o vetor e.

   Exemplos: Considere o código com matriz teste de paridade

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

   Se o vetor recebido for $r = (10100)$, temos que $He^t = Hr^t = 010 = 1.h^4$ e daí $e = (00010)$ e finalmente $c = r - e = (10110)$. □

2. Caso Geral

   Seja $v \in K^n$ e C um código linear. Chamamos de *classe lateral de v segundo C* o conjunto $v + C = \{v + c \ / \ c \in C\}$ e dado um elemento de uma classe lateral, dizemos que ele é um elemento líder se for o de peso mínimo nesta classe.

Teorema 2.18. *[1]: Seja $u \in K^n$ com $w(u) \leq h$. Então u é o único elemento líder de sua classe.*

Demonstração: Suponha $u, v \in K^n$ tal que $w(u) \leq h$ e $w(v) \leq h \Rightarrow$ como $(u - v) \in C$, $w(u - v) \leq w(u) + w(v) \leq 2h \leq d - 1 \Rightarrow u - v = 0 \Rightarrow u = v$. □

Algoritmo:

i) Determine todos os elementos $u \in K^n \ / \ w(u) \leq h$;

ii) Calcule as síndromes destes elementos e coloque tudo em uma tabela;

iii) Calcule a síndrome da palavra recebida: $Hr^t = s^t$;

iv) Se s pertence à tabela e l é o líder desta classe, então troque r por $r - l$, isto é, $c = r - e = r - l$;

v) Se s não pertence à tabela, então foram cometidos mais de h erros.

Exemplos: Considere o código cujos parâmetros são $n = 6$ e $k = 3$ sobre F_2, cuja matriz teste de paridade é dada por

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Temos então que $d = 3$ e $\hbar = 1$. Calculando então os vetores de peso menor ou igual a 1 com as suas síndromes, obtemos a seguinte tabela:

líder	síndrome
000000	000
000001	101
000010	011
000100	110
001000	001
010000	010
100000	100

Se a palavra recebida for $r = (100011)$, $Hr^t = (010)^t$ e portanto, $e = (010000)$ e $c = r - e = (110011)$. Mas se $r = (111111)$, $Hr^t = (111)^t$ que não se encontra na tabela e

temos daí que ocorreu mais de um erro □

Capítulo 3

Grafos dados por Quocientes de Reticulados

Neste capítulo apresentamos algumas relações entre códigos e uma classe especial de grafos, os quocientes de reticulados, utilizando principalmente a referência [9]. Estes grafos são associados a ladrilhamentos em toros planares. Introduzimos inicialmente conceitos fundamentais associados a reticulados, e passamos aos grafos quocientes destes discutindo propriedades como uniformidade, regularidade, perfil de distâncias e gênero topológico e a conexão destas com a construção de códigos com características especiais como os códigos perfeitos e com rotulamento cíclico.

3.1 Reticulado, empacotamento e kissing number

Neste tópico estaremos interessados em introduzir o conceito de reticulado e analisar o problema do "empacotamento de esferas"e o problema do "kissing number". Para isso, usaremos a referência [4].

Um reticulado é um tipo especial de grafo, um grafo com a propriedade de que cada um de seus vértices pode ser escrito como combinação linear inteira de outros vértices do grafo. Formalmente definimos:

Definição 3.1. *Dados* $\alpha = \{v_1, ..., v_m\}$ *conjunto de vetores linearmente independentes de* $\mathbb{R}^n$*, definimos o reticulado* $\Lambda = \Lambda_\alpha$ *de base* α *por* $\Lambda = \{\sum_{i=1}^{m} m_i v_i \ ; \ m_i \in \mathbb{Z}\}$ *e denotamos por* $\Lambda = \Lambda_\alpha = < v_1, ..., v_m >$.

Um subreticulado $\Lambda' \subset \Lambda$ 'e um subconjunto de Λ que também é um reticulado.

De agora em diante, consideraremos os reticulados onde $m = n$, isto é, os que têm "dimensão n"em $\mathbb{R}^n$.

Definição 3.2. *Dado o reticulado* $\Lambda = \Lambda_\alpha,\ \alpha = \{v_1, ..., v_n\}$ *de* $\mathbb{R}^n$, *dizemos que*

$$F = \{v = \theta_1 v_1 + ... + \theta_n v_n,\ 0 \leq \theta_i \leq 1\}$$

é uma região fundamental de Λ_α.

A região de Voronoi de um ponto $v \in \Lambda_\alpha$ é definida como os pontos de $\mathbb{R}^n$ que estão mais próximos de v do que de qualquer outro ponto do reticulado (com a métrica usual).

É importante observar que, independente da base do reticulado e de sua região fundamental, o volume de uma região fundamental permanece o mesmo. Por sua vez as regiões de Voronoi são todas congruentes e possuem volume igual ao de uma região fundamental. O quadrado deste volume é chamado de determinante ou discriminante do reticulado e denotado por $det(\Lambda)$. Isto é, $(volume\ de\ uma\ região\ fundamental)^2 = det(\Lambda)$.

Sejam $v_1, ..., v_m$ os vetores que geram um reticulado. Se $v_1 = (v_{11}, v_{12}, ..., v_{1n})$, $v_2 = (v_{21}, v_{22}, ..., v_{2n})$,..., $v_m = (v_{m1}, v_{m2}, ..., v_{mn})$, com $m \geq n$, temos que a matriz geradora do reticulado é dada por:

$$M = \begin{bmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \dots & v_{mn} \end{bmatrix}$$

Se o reticulado tiver dimensão n, temos que $det(\Lambda) = (\det M)^2$.

Chamamos de matriz de Gram a matriz A obtida por $A = M.M^t$, onde M^t é a transposta de M. Por meio desta matriz podemos obter o determinante de reticulados de dimensão menor que n pois $det(\Lambda) = detA$. Geometricamente, temos que $\sqrt{detA}$ é o volume m-dimensional do "paralelotopo"gerado por $v_1, ..., v_m$ (equivalente m-dimensional de um paralelogramo).

Definição 3.3. *Seja* $x = (x_1, ..., x_n) \in \Lambda$, *onde* Λ *é um reticulado. A norma* $N(x)$ *de* x *é dada por :*

$$N(x) = x.x =< x, x >= \sum x_i^2$$

Chamamos de norma minimal d *de* Λ, *o quadrado da distância mínima entre dois vetores do reticulado, isto é,*

$$d = \min\{N(x - y) : x, y \in \Lambda,\ x \neq y\} = min\{N(x) : x \in \Lambda,\ x \neq 0\}$$

3.1.1 O Problema do Empacotamento de Esferas

O Problema do empacotamento de esferas consiste em saber como empacotar um determinado número de esferas idênticas juntas, de tal forma que a fração do espaço coberto por essas esferas seja o maior possível.

Este problema foi citado por Hilbert em 1900 como o décimo oitavo problema de uma lista de questões que tiveram destaque no desenvolvimento da ciência e têm sido um grande desafio para vários matemáticos. Quando os centros dessas circunferências formam um reticulado, os empacotamentos são chamados de empacotamentos reticulados. Daí, o problema se transforma na obtenção de reticulados de alta densidade e que sejam ao mesmo tempo, manipuláveis. Do que é até agora conhecido, em grande parte das dimensões, os empacotamentos esféricos mais densos são os empacotamentos reticulados. No plano, as esferas são circunferências e sabe-se que a maior densidade possível é obtida através do reticulado hexagonal, com uma densidade de aproximadamente $0,9069$. Já no $\mathbb{R}^3$, provou-se que a maior densidade é alcançada com o empacotamento no qual os centros das esferas formam um reticulado fcc (face centered cubis), no qual podemos obter uma densidade de aproximadamente 0,7405. Observamos que partindo de um reticulado, as esferas de um empacotamento nele centradas terão raio $\frac{\sqrt{d}}{2}$ onde d é a norma minimal.

Definição 3.4. *Dada uma região limitada $M \subset \mathbb{R}^n$ de volume V, definimos a densidade de um empacotamento de reticulado E em M como sendo:*

$$\Delta_{E,M} = \frac{m.v}{V}$$

onde v é o volume de cada uma das esferas de E e m é o número de esferas contidas em M.

A densidade de empacotamento de E é dada por $\lim_{V\to\infty} \Delta_{E,M}$.

Esta densidade nos mostra quão bom é o empacotamento, ou seja, quanto maior a densidade, melhor o empacotamento.

3.1.2 O Problema do Kissing Number

Se pensarmos no $\mathbb{R}^3$, temos que nos perguntar: qual é o número máximo de bolas de bilhar que podemos arranjar em torno de uma bola B de forma que todas elas toquem ou "beijem" B? Este número é o chamado "kissing number". Se pensarmos no $\mathbb{R}^n$, a pergunta permanece a mesma: se tivermos várias esferas idênticas, qual é o número máximo de esferas que posso colocar em torno de uma esfera, de forma que todas elas toquem esta esfera?

Este problema surgiu de uma discussão entre Isaac Newton e seu professor David Gregory em 1694 onde Newton dizia que a solução deste problema em $\mathbb{R}^3$ era 12 e seu professor acreditava ser 13.

Os resultados conhecidos para o "kissing number" de empacotamentos de reticulados nas diferentes dimensões são:

n	τ
1	2
2	6
3	12
8	240
24	196.560

Veremos agora alguns exemplos de reticulados e verificaremos em cada caso, qual é a base, o determinante, o kissing number e todos os outros valores que foram definidos anteriormente.

Exemplo:

1. Seja $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$ o conjunto dos inteiros. Temos então que $\mathbb{Z}^n = \{(x_1, x_2, ..., x_n) : x_i \in \mathbb{Z}, \text{ para todo } 1 \leq i \leq n\}$. O conjunto $\mathbb{Z}^n$ é um reticulado e é chamado de reticulado cúbico ou inteiro n-dimensional. Temos que $\mathbb{Z}^2$ é chamado de reticulado quadrado pois sua malha é quadrada. Sua matriz geradora é a identidade, uma vez que a base é $< (1, 0, 0, ..., 0), \ (0, 1, 0, ..., 0), ..., (0, ..., 0, 1) >$ e portanto, o determinante do reticulado é 1. A norma minimal também é igual a 1.

   O kissing number deste reticulado é $\tau = 2n$, os vetores minimais são $(0, ..., \pm 1, ..., 0)$ e a região de Voronoi é um cubo. Já a densidade de empacotamento é dada por $\Delta = V_n 2^{-n}$, onde V_n é o volume da esfera n-dimensional de raio 1.

   Se tivermos $n = 2$, temos que $\Delta = \frac{\pi}{4} = 0,785...$

   Se tivermos $n = 3$, temos que $\Delta = \frac{\pi}{6} = 0,524...$

   Se tivermos $n = 4$, temos que $\Delta = \frac{\pi^2}{32} = 0,308...$

2. Um outro exemplo de reticulado é $A_n = \{(x_0, x_1, ..., x_n) \in \mathbb{Z}^{n+1} : x_0 + x_1 + ... + x_n = 0\}$.

   Para este reticulado, temos que uma matriz geradora e a respectiva matriz de Gram são dadas por:

$$M = \begin{bmatrix} -1 & 1 & 0 & 0 & . & 0 & 0 \\ 0 & -1 & 1 & 0 & . & 0 & 0 \\ 0 & 0 & -1 & 1 & . & 0 & 0 \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & -1 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 2 & -1 & 0 & . & 0 & 0 \\ -1 & 2 & -1 & . & 0 & 0 \\ 0 & -1 & 2 & . & 0 & 0 \\ . & . & . & . & . & . \\ 0 & 0 & 0 & . & 2 & -1 \\ 0 & 0 & 0 & . & -1 & 2 \end{bmatrix}$$

Portanto, $(detA_n) = 2^{n+1}$. A norma minimal é igual a 2, os vetores minimais são permutações de $(1, -1, 0, ..., 0)$ e o kissing number é dado por $\tau = n(n+1)$.

Para $n = 1$, temos que $A_1 \cong \mathbb{Z}$.

3. Se no exemplo anterior tomarmos $n = 2$, obteremos um reticulado Λ equivalente ao chamado reticulado hexagonal, que recebe este nome pelo fato de sua região de Voronoi ser da forma de um hexágono.

   Uma base para o reticulado hexagonal é $< (1, 0), \left(\frac{-1}{2}, \frac{\sqrt{3}}{2}\right) >$ e para tal, temos que a matriz geradora e a matriz de Gram são:

$$M = \begin{bmatrix} 1 & 0 \\ \frac{-1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

$$A = \begin{bmatrix} 1 & \frac{-1}{2} \\ \frac{-1}{2} & 1 \end{bmatrix}$$

   Temos então que $det(\Lambda) = \frac{3}{4}$, a norma minimal é igual a 1, os vetores minimais são $(\pm 1, 0)$ e $\left(\pm\frac{1}{2}, \pm\frac{\sqrt{3}}{2}\right)$, a densidade de empacotamento é $\Delta = \frac{\pi}{\sqrt{12}} = 0,9069...$ e $\tau = 6$.

4. Temos também o reticulado fcc (face centered cubic lattice) que é equivalente ao A_3. Este reticulado pode ser visto na forma piramidal ao empilharmos laranjas e é definido como $fcc = \{(x, y, z) \in \mathbb{Z}^3 : x + y + z \text{ é par}\}$.

   Para este reticulado temos :

$$M = \begin{bmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

$$A = \begin{bmatrix} 2 & 0 & -1 \\ 0 & 2 & -1 \\ -1 & -1 & 2 \end{bmatrix}$$

   Ainda temos que $det(fcc) = 4$, a norma minimal é 2, os vetores minimais são permutações de $(\pm 1, \pm 1, 0)$, a região de Voronoi é o chamado "dodecaedro rômbico", $\Delta = \frac{\pi}{\sqrt{18}} = 0,7405...$ e $\tau = 12$.

□

3.2 Grafos que são Quocientes de Reticulados (Grafos e Ladrilhamentos sobre Toros)

Neste tópico estaremos relacionando os grafos e os reticulados através da função quociente e para isso estaremos utilizando as referências [9] e [14].

Definição 3.5. *Um grupo topológico é um grupo G cujo conjunto subjacente está munido de uma topologia compatível com o produto no grupo, no sentido em que:*

1. *o produto $G \times G \longrightarrow G$ é uma aplicação contínua, quando se considera $G \times G$ com a topologia produto e*
2. *a inversão $i : G \longrightarrow G$ com $i(g) = g^{-1}$ é contínua.*

Dado um grupo G e um subgrupo H de G, uma classe lateral à esquerda de H é um conjunto $gH = \overline{g}$ para $g \in G$, onde $gH = \{gh : h \in H\}$.

O conjunto de todas as classes laterais à esquerda de H é chamado de família de classes laterais à esquerda de G módulo H e denotado por $\frac{G}{H}$.

Como é conhecido, $\frac{G}{H}$ tem uma estrutura de grupo quando H é subgrupo normal e esta é induzida naturalmente pela operação de G definida por $\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2}$. Neste caso, temos também que a função quociente

$$\begin{aligned} q : G &\to \tfrac{G}{H} \\ g &\mapsto \overline{g} \end{aligned}$$

é um morfismo de grupos.

Além disso, se G for um grupo topológico, consideramos em $\frac{G}{H}$ a topologia induzida por esta aplicação quociente. No caso de G ser um espaço métrico, a métrica em $\frac{G}{H}$ será dada por :

$$d(\overline{g_1}, \overline{g_2}) = min\{d(g_1, g_2);\ g_1, g_2 \in gH\}$$

Num reticulado Λ de dimensão n em $\mathbb{R}^n$, temos naturalmente uma estrutura de anel induzida por $\mathbb{Z}^n$ e portanto, um grupo aditivo abeliano a ele associado. Dado um subreticulado $\Lambda' \subset \Lambda$, o quociente $\frac{\Lambda}{\Lambda'}$ terá, portanto, estrutura de grupo e poderá ser identificado com um grafo num toro planar n-dimensional como veremos.

3.2.1 O Toro Planar

Estamos agora interessados em estudar o chamado toro planar, que, no caso bi-dimensional pode ser descrito como um retângulo com as bordas devidamente identificadas.

Consideraremos agora o espaço n-dimensional $\mathbb{R}^n$ com a métrica euclidiana usual.

Uma isometria $\Psi : \mathbb{R}^n \to \mathbb{R}^n$ é uma aplicação que preserva distâncias. As isometrias de $\mathbb{R}^n$ são dadas por transformações lineares ortogonais ou composição dessas com translações.

Algumas superfícies podem ser representadas como quociente de $\mathbb{R}^2$ por um grupo de isometrias Γ, ou seja, superfícies que podem ser vistas como $\frac{\mathbb{R}^2}{\Gamma}$, as quais chamamos de superfícies quociente. Este é o caso dos toros planares n-dimensionais onde Γ é o subgrupo de isometrias gerado por um conjunto de n translações dadas por vetores linearmente independentes.

Definição 3.6. *O toro planar bidimensional é definido por :*

$$\begin{aligned} \Gamma. : \mathbb{R}^2 &\to \tfrac{\mathbb{R}^2}{\Gamma_{\vec{u},\vec{v}}} = T^{\vec{u},\vec{v}} \\ (x,y) &\mapsto \overline{(x,y)} \end{aligned}$$

onde $\Gamma_{\vec{u},\vec{v}}$ é o grupo gerado pelas translações de $\vec{u}$ e de $\vec{v}$, ou seja,

$$\overline{(x,y)} = \{(a,b) \in \mathbb{R}^2;\ (a,b) = (x,y) + m\vec{u} + n\vec{v}\}$$

3.2.2 Grafos Regulares Sobre Toros Planares

Definição 3.7. *Sejam $\vec{u}$, $\vec{v} \in \mathbb{R}^2$ vetores linearmente independentes, $G_{\vec{u},\vec{v}} =< T_{\vec{u}}, T_{\vec{v}} >$ o grupo gerado pelas translações de $\vec{u}$ e $\vec{v}$ e $T_{\vec{u},\vec{v}} = \frac{\mathbb{R}^2}{G_{\vec{u},\vec{v}}}$ o toro planar. Temos que se $\Lambda_{\vec{u},\vec{v}} = \{m\vec{u} + n\vec{v} : m, n \in \mathbb{Z}\}$ é o reticulado gerado por $\vec{u}$ e $\vec{v}$, temos então que os pontos sobre o toro são classes de equivalência de pontos de $\mathbb{R}^2$ pela relação de equivalência dada por $A' \approx A \Leftrightarrow A - A \in \Lambda_{\vec{u},\vec{v}}$.*

O cilindro pode ser realizado no $\mathbb{R}^3$, mas o toro planar pode ser mapeado isometricamente apenas em $\mathbb{R}^n$ para $n \geq 4$.

Veremos a seguir alguns exemplos de realização de toros no $\mathbb{R}^4$.

Exemplo:

1. $\vec{u} = (r, 0)$ e $\vec{v} = (0, s)$

$$\varphi : \mathbb{R}^2 \to \mathbb{R}^4 \tag{3.1}$$

$$(x,y) \mapsto \left(\frac{r}{2\pi}\left(\cos\frac{2\pi x}{r}, sen\frac{2\pi x}{r}\right), \frac{s}{2\pi}\left(\cos\frac{2\pi y}{s}, sen\frac{2\pi y}{s}\right)\right) \tag{3.2}$$

(a)$\varphi(x,y) = \varphi(\tilde{x},\tilde{y})$ se, e somente se, $(x,y) \approx (\tilde{x},\tilde{y})$, isto é, $(x,y) - (\tilde{x},\tilde{y}) = m\vec{u} + n\vec{v}$, com $m, n \in \mathbb{Z}^2$

(b) $\varphi(\mathbb{R}^2) = ([r,0] \times [0,s])$

(c) φ identifica os lados opostos do retângulo gerado por $\vec{u}$ e $\vec{v}$

Por (a),(b) e (c), temos que o toro planar se realiza através da função φ, ou seja, φ induz uma correspondência injetora entre $T_{\vec{u},\vec{v}} = \frac{\mathbb{R}^2}{G_{\vec{u},\vec{v}}}$ e a superfície $\varphi(\mathbb{R}^2) = ([r,0] \times [0,s])$ em $\mathbb{R}^4$. Esta correspondência é, na verdade, uma isometria, isto é, a função preserva distância quando consideramos a distância geodésica em $\varphi(\mathbb{R}^2)$.

2. $\vec{u} = (a,b)$ e $\vec{v} = t(-b,a)$, $t \in \mathbb{R}$

$$\Phi : \mathbb{R}^2 \to \mathbb{R}^4 \tag{3.3}$$

$$(x,y) \mapsto \varphi(R_\alpha(x,y)) \tag{3.4}$$

onde R_α é a rotação de um ângulo α, e α é o ângulo entre $\vec{u}$ e $\vec{e_1} = (1,0)$, ou seja,

$$R_\alpha(x,y) = \frac{1}{||\vec{u}||}\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix}$$

Novamente, temos que $\Phi(\mathbb{R}^2) \subset \mathbb{R}^4$ e Φ é uma isometria local. Portanto, $T_{\vec{u},\vec{v}} \equiv \Phi(\mathbb{R}^2)$ já que Φ faz as identificações do toro.

Se tivermos $t = 1$, $T_{\vec{u},\vec{v}}$ é gerado por um quadrado e temos que:

$\Phi(x,y) = \frac{\sqrt{a^2+b^2}}{2\pi}\left(\cos\frac{2\pi(xa+yb)}{a^2+b^2}, sen\frac{2\pi(xa+yb)}{a^2+b^2}, \cos\frac{2\pi(ya-xb)}{a^2+b^2}, sen\frac{2\pi(ya-xb)}{a^2+b^2}\right)$

□

3.2.3 Ladrilhamento

Definição 3.8. *Seja G um grupo discreto de isometrias de um espaço métrico M. Um subconjunto π de M é chamado de região fundamental associada a G se, e somente se,*

(i) $\cup_{g\in G} g\pi = M$

(ii) $\overset{o}{\pi} \cap g\overset{o}{\pi} \neq \varnothing$ *se, e somente se,* $g = 1$, *onde* $\overset{o}{\pi}$ *é o maior conjunto aberto contido em* π

(iii) $\overset{o}{\pi} \neq \varnothing$

Uma cobertura de M dada por cópias de π sob a ação de G é chamado ladrilhamento de M associado a G ou um G-ladrilhamento.

O lema abaixo nos fornece uma condição suficiente para induzir um ladrilhamento em um espaço quociente.

Lema 3.9. *[9]: Seja G um grupo discreto de isometrias de M, $G' \subset G$ um subgrupo normal e π uma região fundamental de G em M. Sob essas condições, um $G-$ladrilhamento de M induz um $\frac{G}{G'}$-ladrilhamento de um espaço quociente $\frac{M}{G'}$, com região fundamental $\Psi(\pi)$, onde $\Psi : M \to \frac{M}{G'}$ é uma função que leva cada elemento de M na sua classe de equivalência, chamada de função quociente.*

Assumiremos a partir de agora $M = \mathbb{R}^2$, com ladrilhamento dado por grupos de translações.

No próximo lema iremos determinar condições sob as quais um ladrilhamento de $\mathbb{R}^2$ induz outro no toro $T_{\vec{u},\vec{v}}$. Este é o primeiro passo para caracterizar o ladrilhamento no toro planar por quadrados unitários.

Lema 3.10. *[9]: Sejam $\alpha = \{\vec{v_1}, \vec{v_2}\}$ e $\beta = \{\vec{w_1}, \vec{w_2}\}$ duas bases de $\mathbb{R}^2$, G_α e G_β os grupos de translação associados e um ladrilhamento regular com região fundamental π, $\mathbb{R}^2 = \cup_{g \in G_\alpha} g\pi$. Existe um ladrilhamento no toro planar $T_\beta = \frac{\mathbb{R}^2}{G_\beta}$ que é induzido pelo grupo de translações $G_\alpha \Leftrightarrow G_\beta$ é subgrupo de G_α, isto é, os vetores de β são combinações inteiras dos vetores de α.*

Teorema 3.11. *[9]: Sejam $\vec{u} = (a, b)$ e $\vec{v} = (c, d)$ vetores de $\mathbb{R}^2$, linearmente independentes, $T_{\vec{u},\vec{v}}$ o toro associado. Temos então que:*

(a) O reticulado canônico $\mathbb{Z}^2 \subset \mathbb{R}^2$ induz por Ψ um grafo regular $\Gamma^{\vec{u},\vec{v}}$ e um ladrilhamento por quadrados unitários no toro planar $T_{\vec{u},\vec{v}}$ se, e somente se, $\vec{u}$ e $\vec{v}$ possuem coordenadas inteiras.

Neste caso:

(b) $\Psi(\mathbb{Z}^2)$ são os vértices de $\Gamma^{\vec{u},\vec{v}}$.

(c) $\Psi(\{m\} \times [n, n+1])$ são as arestas.

(d) $\Psi([i, i+1] \times [j, j+1])$, $i, j \in \mathbb{Z}$ são as faces quadradas.

(e) O número de vértices V e o número de faces F de $\Gamma^{\vec{u},\vec{v}}$ são iguais a $|det[\vec{u}, \vec{v}]| = |ad - bc|$.

Demonstração: Os itens (a), (b), (c) e (d) são deduzidos do Lema 3.9 aplicado ao reticulado canônico $\mathbb{Z}^2$ associado ao grupo discreto de isometrias $G_\alpha =< T_{\vec{e_1}}, T_{\vec{e_2}} >$, $\vec{e_1} = (1, 0)$ e $\vec{e_2} = (0, 1)$, a região fundamental Π em $\mathbb{R}^2$ e $G_\beta =< T_{\vec{u}}, T_{\vec{v}} >$ subgrupo de G_α. O item (e) segue da relação de Euler para grafos em superfícies $V - A + F = 2 - 2g$, onde V é o número de vértices, A o número de arestas, F o número de faces e g é o gênero da superfície. No caso do toro, $g = 1$ e portanto, $V + F = A$. Cada face tem 4 arestas, mas cada aresta pertence a duas faces. Então, $A = \frac{4F}{2} = 2F$, e como $V + F = A$, temos que $V = 2F - F = F$. Desde que a área do paralelogramo gerado por $\vec{u}$ e $\vec{v}$ é dado por $|det[\vec{u}, \vec{v}]| = |ad - bc|$, e cada face tem área unitária, temos que $F = V = |ad - bc|$, concluindo a demonstração. □

A distância do grafo d_Γ em $\Gamma^{\vec{u},\vec{v}}$ de um vértice a outro é definida como o número mínimo de arestas conectando estes dois vértices, isto é, para $\overline{(m_1, n_1)}$ e $\overline{(m_2, n_2)}$ vértices do grafo,

temos:

$$d_\Gamma\left(\overline{(m_1,n_1)},\overline{(m_2,n_2)}\right) = \min\{|m_1-m_2|+|n_1-n_2|\}$$

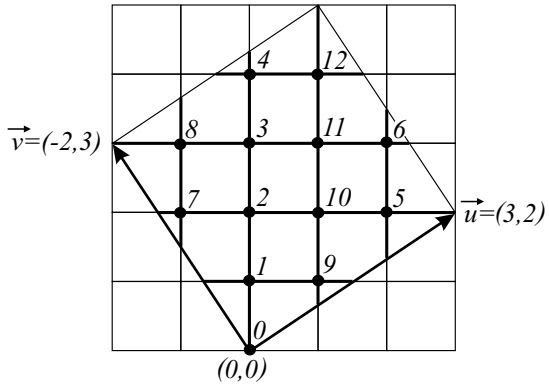
onde

$$(m_1,n_1)\in\overline{(m_1,n_1)} \text{ e } (m_2,n_2)\in\overline{(m_2,n_2)}.$$

Exemplo:

1. $\vec{u} = (3,2)$ e $\vec{v} = (-2,3)$. Como $(-2)^2 + 3^2 = 4+9 = 13$, teremos então um ladrilhamento do toro planar dado por 13 quadrados. Neste caso, os segmentos verticais do grafo são conectados quando identificamos os lados opostos.

   Se começarmos por qualquer um dos vértices e formos para o norte, todos eles serão atingidos e teremos portanto um grupo cíclico de isometrias $\mathbb{Z}_{13}$, agindo no grafo regular $\Gamma^{\vec{u},\vec{v}}$. Este grupo produz um rotulamento cíclico.



2. $\vec{u} = (m,0)$ e $\vec{v} = (0,m)$

   Neste caso, o ladrilhamento por quadrados é paralelo ao quadrado que gera o toro planar e cada segmento vertical gera um ciclo com m vértices. Daí, $\Gamma^{\vec{u},\vec{v}}$ é naturalmente rotulado por $\mathbb{Z}_m^2$, que é gerado por translações unitárias verticais e horizontais.

3. $\vec{u} = (a,b)$ e $\vec{v} = (c,d)$

   (i) $mdc(a,c) = 1$

   Neste caso temos que a imagem de qualquer reta vertical $x = k$, $k \in \mathbb{Z}$ através da função quociente é uma curva simples fechada C no toro planar, que contém todos os M vértices de $\Gamma^{\vec{u},\vec{v}}$, onde $M = |ad-bc|$. O rotulamento por $\mathbb{Z}_M$ é feito ciclicamente nesta curva da seguinte forma:

   - Primeiramente escolhe-se um vértice qualquer 0 de $\Gamma^{\vec{u},\vec{v}}$;

- Em seguida, rotula-se em direção ao norte até chegar à borda do paralelogramo fundamental

- Colar a borda e continuar do ponto equivalente

- Continuar rotulando em direção ao norte

- Repetir este processo até que todos os pontos de C estejam rotulados.

(ii) $mdc(b,d) = 1$

O rotulamento é feito da mesma forma, mas agora para retas horizontais

(iii) $mdc(a,c) = m \neq 1$

Neste caso, um rotulamento indo ao norte em retas verticais alcançará apenas $\frac{M}{m}$ vértices de $\Gamma^{\vec{u},\vec{v}}$.

(iv) $mdc(b,d) = n \neq 1$

Neste caso, o resultado é análogo ao anterior.

□

Desta discussão, destacamos o resultado a seguir que é formalizado em [9].

Proposição 3.12. *Sejam $\vec{u} = (a,b)$ e $\vec{v} = (c,d)$. Se $mdc\,(a,c) = 1$ ou $mdc(b,d) = 1$, então o grupo $\frac{\mathbb{Z}^2}{G_{\vec{u},\vec{v}}}$ é cíclico.*

3.2.4 Perfil de Distâncias em $\Gamma^{\vec{u},\vec{v}}$

Sejam $\vec{u} = (a,b)$ e $\vec{v} = (c,d)$ tal que $mdc(a,c) = 1$ e $mdc(b,d) = 1$. Como neste caso podemos rotular $\Gamma^{\vec{u},\vec{v}}$ por um grupo cíclico $\mathbb{Z}_M$, $M = |ad - bc|$, determinar o perfil de distância em $\Gamma^{\vec{u},\vec{v}}$ é o mesmo que procurar qual a métrica d_Γ em $\mathbb{Z}_M$ que translada a distância do grafo de $\Gamma^{\vec{u},\vec{v}}$ no toro planar. O grupo $\mathbb{Z}_M$ é induzido por translações no plano euclidiano que são isometrias no toro planar.

Teorema 3.13. *[9]: Sejam $\vec{u} = (a,b)$ e $\vec{v} = (c,d)$ tal que $mdc(a,c) = 1$. Então, $\Gamma^{\vec{u},\vec{v}}$ é rotulado por $\mathbb{Z}_M$, $M = |ad - bc|$ e para d_Γ, a métrica em $\mathbb{Z}_M$ que translada a distância do grafo em $\Gamma^{\vec{u},\vec{v}}$, temos que os 4 vizinhos à distância 1 de $\rho(0)$ são $\rho(1), \rho(M-1), \rho(M-s)$ e $\rho(s)$, onde s é o menor inteiro positivo tal que $ma + nc = 1$ e $mb + nd = s$ com $m, n \in \mathbb{Z}$.*

Demonstração: A primeira parte da afirmação é dada pela Proposição 3.12. Os vizinhos de $\overline{0}$ no grafo são $\overline{1}$, $\overline{M-1}$, $\overline{s}$ e $\overline{M-s}$, onde $(0,s) \approx (-1,0)$. Para todo s' tal que $(0,s') \approx (-1,0)$, temos que $(1,s') = m(a,b) + n(c,d)$ com $m,\ n \in \mathbb{Z}$, ou seja, $1 = ma + nc$ e $s' = mb + nd$. Esta primeira equação sempre tem solução, desde que $mdc(a,c) = 1$. Uma

solução m, n pode ser determinada pelo Algoritmo de Euclides. Desta forma, obtemos a segunda equação. Podemos verificar que toda solução s' difere de outra por múltiplos de M. Como o rotulamento ρ é definido em $0, 1, ..., M-1$, estamos interessados na menor solução positiva s. Esta solução é o resto da divisão de s' por M. □

3.2.5 Toro Gerado por $\vec{u}$ =(a,b) e $\vec{v}$ =(-b,a)

Se tivermos um toro gerado por quadrados, ou seja, $\Gamma^{\vec{u},\vec{v}}$ com $\vec{u} = (a, b)$ e $\vec{v} = (-b, a)$, $a, b \in \mathbb{Z}$, $\Gamma^{\vec{u},\vec{v}}$ é um grafo que gera uma constelação de sinais dada pelos $a^2 + b^2$ vértices.

Exemplos:

1. $\vec{u} = (m+1, m)$ e $\vec{v} = (-m, m+1)$

   Os representantes de $\Gamma^{\vec{u},\vec{v}}$ mais próximos da origem compõem a bola de raio m (na métrica do grafo).

   - Para cada vértice de $\Gamma^{\vec{u},\vec{v}}$, existem $4k$ vértices à distância k deste vértice, $0 \leq k < m$, isto é, a bola de raio k é completa em $\Gamma^{\vec{u},\vec{v}}$ com esta métrica.

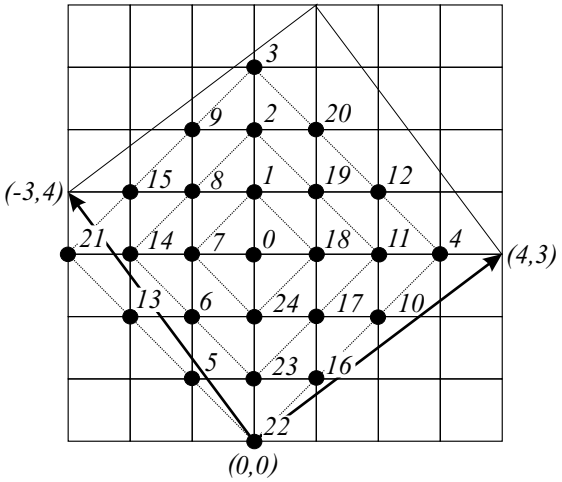
   - Grupo cíclico de rotulamento: $\mathbb{Z}_{(m+1)^2+m^2}$

   - Vizinhos de $\overline{0}$: $\overline{1}$, $\overline{2m+1}$, $\overline{2m(m+1)}$, $\overline{2m^2}$

2. $\vec{u} = (4, 3)$ e $\vec{v} = (-3, 4)$

   $m = 3 \Rightarrow (m+1)^2 + m^2 = 4^2 + 3^2 = 16 + 9 = 25$

   Portanto, o grupo cíclico de rotulamento será $\mathbb{Z}_{25}$.



3. $\vec{u} = (m, 1)$ e $\vec{v} = (-1, m)$

- Grupo cíclico de rotulamento: Z_{m^2+1}

- O diâmetro será igual a m se m^2+1 for ímpar e igual a $m-1$ se for par

- Vizinhos de $\overline{0}$: $\overline{1}$, $\overline{m}$, $\overline{m^2}$, $\overline{m^2-m}$

3.2.6 Códigos perfeitos

Seja Γ um grafo cujo conjunto de vértices é X e diâmetro d. Um código neste grafo é um subconjunto não vazio C de X.

Definimos a bola fechada de raio r e centro $x \in \Gamma$ da seguinte forma:

$$B_r(x) = \{y \in \Gamma : d(x,y) \leq r\}$$

A distância mínima em C é dada por:

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

Se a cardinalidade de C $|C| = 1$, $\delta(C) = 2d+1$

Se $\delta(C) \geq 2e+1$, temos que C é um código corretor de e erros.

Podemos também calcular a distância de um vértice $x \in X$ ao código C, ou seja,

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

O raio de cobertura de um código é o menor número t tal que bolas de raio t centradas em pontos de C cobrem todo X. Este número t é dado por:

$$t(C) := \max\{d(x,C) : x \in X\}$$

Temos a seguinte relação:

$$\delta(C) \leq 2.t(C) + 1$$

Se as bolas de raio $t(C)$ em torno de pontos de C formarem uma partição de X, temos que ocorrerá a igualdade, ou seja, $\delta(C) = 2.t(C)+1$. Neste caso, dizemos que C é um *código perfeito que corrige t erros.*

Seja Γ um grafo associado a um ladrilhamento regular em $\mathbb{R}^2$ por um grupo reticulado Λ de posto 2, e P o polígono de Voronoi. Se existe ladrilhamento de $\mathbb{R}^2$ por P através de um grupo reticulado Λ' e se Λ'' é um grupo reticulado de posto 2, $\Lambda'' \subset \Lambda' \subset \Lambda$, então Λ' induz um código perfeito corretor de k erros em um toro planar $\frac{\mathbb{R}^2}{\Lambda''}$ com grupo de rotulamento $\frac{\Lambda'}{\Lambda''}$.

Proposição 3.14. *[9]: Seja Γ um grafo associado ao ladrilhamento por quadrados de $\mathbb{R}^2$ por $\mathbb{Z}^2$. Seja $\vec{w_1} = (k+1, k)$, $\vec{w_2} = (-k, k+1)$, $k \in \mathbb{N}$ e seja $\Lambda_{\vec{u},\vec{v}}$ o reticulado gerado por $\vec{u} = a_1\vec{w_1} + b_1\vec{w_2}$ e $\vec{v} = c_1\vec{w_1} + d_1\vec{w_2}$, $a_1, b_1, c_1, d_1 \in \mathbb{Z}$. Então, se $mdc(b_1, d_1) = 1$ (ou $mdc(a_1, c_1) = 1$), $C = \{j\vec{w_1} : j = 0, ..., M\}$ é um código k-perfeito de ordem $M = \left| det \begin{bmatrix} a_1 & c_1 \\ b_1 & d_1 \end{bmatrix} \right|$ em $\Gamma^{\vec{u},\vec{v}}$.*

Se na proposição anterior consideramos $a_1 = d_1 = k-1$ e $b_1 = -c_1 = -k$, teremos $u = ((k+1)^2 + k^2), 0)$ e $v = (0, (k+1)^2 + k^2)$ o que permite escrever o resultado a seguir:

Corolário 3.15. *Para $q = (k+1)^2 + k^2$,$C = \{j(k+1, k); j = 0, 1, ...q-1\}$ é um código perfeito no espaço $\mathbb{Z}_q^2$ com a métrica de Lee e tem rotulamento cíclico por $\mathbb{Z}_q$*

Exemplos:

1. $C = \{j(4, 3); \}; 0 \leq j \leq 4\}$ é um código perfeito no espaço de Lee $\mathbb{Z}_{25}^2$.

2. $C = \{j(3, 2); \}; 0 \leq j \leq 4\}$ é um código perfeito no espaço de Lee $\mathbb{Z}_{13}^2$. Temos ainda que , neste caso, como $\mathbb{Z}_{13}$ é um corpo , podemos falar em linearidade e C é um código linear em $\mathbb{Z}_{13}^2$ que pode ser rotulado ciclicamente e tem por matriz de paridade :

$$\begin{pmatrix} -\overline{2} & \overline{3} \end{pmatrix} = \begin{pmatrix} \overline{11} & \overline{3} \end{pmatrix} \tag{3.5}$$

3.3 Gênero do Grafo $\mathbb{Z}_q^n$

Estaremos apresentando alguns problemas sobre o gênero de grafos do tipo $\mathbb{Z}_q^n$ e para isso, utilizaremos a referência [11].

3.3.1 Gênero dos Grafos $\mathbb{Z}_q^2$ com a Métrica de Lee

Teorema 3.16. *[11]: Dado um grafo $\mathbb{Z}_q^2$, temos que para $q \leq 3$ as métricas de Lee e de Hamming coincidem.*

Demonstração: Sejam $(\overline{a_1}, \overline{a_2}), (\overline{b_1}, \overline{b_2}) \in \mathbb{Z}_3^2$, com $0 \leq a_i \leq 2$ e $0 \leq b_i \leq 2$. Temos então que: $d_L((\overline{a_1}, \overline{a_2}), (\overline{b_1}, \overline{b_2})) = \sum min|a_i - b_i|, 3 - |a_i - b_i|$. Mas se $a_i, b_i \in \mathbb{Z}_3$, temos que o termo da direita será igual a zero se, e somente se, $a_i = b_i$. Portanto, neste caso, a métrica de Lee coincide com a métrica de Hamming. □

A partir de $q = 4$, as duas métricas são diferentes. Vamos então pensar no problema do gênero de $\mathbb{Z}_q^2$ utilizando a métrica de Lee.

Na métrica de Lee, o problema fica bem simples pois qualquer que seja $q \geq 3$, o grafo obtido pode ser mergulhado sem auto intersecção na superf ície de um toro gerando um ladrilhamento, ou seja, para todo q temos que o grafo obtido possui gênero 1 (para $q = 2$, $\mathbb{Z}_2^2$ possui gênero zero).

3.3.2 Gênero dos Grafos $\mathbb{Z}_q^2$ com a Métrica de Hamming

Assumiremos agora o problema anterior com a métrica de Hamming, o que aumenta bastante o grau de dificuldade uma vez que o número de vizinhos de um dado ponto aumenta.

Para $q = 3$, como a métrica de Hamming coincide com a métrica de Lee, temos que o grafo obtido possui gênero 1. Agora, para o caso $q = 4$, apresentamos uma conjectura e um limitante na próxima seção.

3.3.3 Grafo $\mathbb{Z}_4^2$

Este caso se complica pois não sabemos, caso haja ladrilhamento, qual o formato das faces e nem se este grafo é face-regular. Sabemos apenas que o número de vértices $V = 16$ e que o número de arestas $A = 48$.

Suponhamos então que o grafo obtido seja face-regular, ou seja, que possua F faces com q lados cada uma. Temos então que o número de arestas

$$A = \frac{F.q}{2}$$

e portanto para $q = 4$,

$$48 = \frac{F.4}{2} \Rightarrow F = 24$$

Da característica de Euler temos que:

$$V - A + F = 16 - 48 + 24 = -8$$

E então conseguimos encontrar o gênero do grafo da seguinte forma:

$$V - A + F = -8 = 2 - 2g \Rightarrow g = 5$$

Se o grafo não for face-regular, podemos apenas aplicar o Teorema 1.17. Como $A = 48$ e $V = 16$, então:

$$1 \leq g \leq 13$$

Para o caso em que o grafo não é face-regular, uma conjectura é de que $g = 5$, ou seja, de que o gênero do grafo coincida com o gênero no caso em que o grafo é face-regular.

3.3.4 Gênero dos Grafos $\mathbb{Z}_2^n$

Neste tópico estaremos interessados em encontrar o gênero de alguns casos particulares de $\mathbb{Z}_2^n$ e, por fim, generalizar para todo n.

1. Para $n = 2$, temos os quatro vértices de um quadrado e então,

$$V = 4 = 2^2,\ A = 4 = \frac{2^2.2}{2} \text{ e } F = \frac{2.2^2}{4} = 2.$$

Portanto, a característica de Euler é $V - A + F = 4 - 4 + 2 = 2$ e daí

$$2 - 2g = V - A + F = 2$$

Temos então que o gênero g deste grafo é:

$$g = 0$$

2. Para $n = 3$, temos vértices de um cubo.

$$V = 8 = 2^3,\ A = \frac{2^3.3}{2} = 12 \text{ e } F = \frac{2}{4}.\frac{2^3.3}{2} = 6.$$

Então,

$$2 - 2g = V - A + F = 8 - 12 + 6 = 2 \Rightarrow g = 0$$

3. Para $n = 4$,

$$V = 16 = 2^4,\ A = \frac{2^4.4}{2} = 32 \text{ e } F = \frac{2}{4}.\frac{2^4.4}{2} = 16.$$

Portanto,

$$2 - 2g = V - A + F = 16 - 32 + 16 = 0 \Rightarrow g = 1$$

4. Dado o grafo Z_2^n temos que, para $n \geq 4$,

(i) O número de vértices V de $\mathbb{Z}_2^n$ é:

$$V = 2^n$$

(ii) O número de arestas A é:

$$A = \frac{V.n}{2} = \frac{2^n.n}{2} = 2^{n-1}n$$

(iii) O número de faces F é:

$$F = \frac{2A}{4} = \frac{2^n.n}{4}$$

Temos então que a característica de Euler para Z_2^n é dada por:

$$V - A + F = 2^n(\frac{4-n}{4})$$

E finalmente, o gênero g de Z_2^n é:

$$g = 1 - 2^{n-1} + n.2^{n-3} = 1 + 2^{n-3}(n-4)$$

Observação 3.17. *Para encontrarmos o número de arestas, temos que multiplicar a equação* $4(ii)$ *por* n *pois é exatamente o grau de cada um dos vértices do grafo e dividir por* 2 *pelo fato de cada arestas ser contada duas vezes. No caso das faces, multiplicamos por* 2 *pois cada aresta pertence a duas faces e dividimos por* 4 *pois cada face é composta por* 4 *arestas. Para encontrarmos a característica de Euler e o gênero deste grafo, foram utilizados os resultados do capítulo 1.*

3.4 Exemplos de Grafos distância-regulares

Analisaremos a definição de grafos que são distância regular em dois exemplos já comentados anteriormente: o $\mathbb{Z}_4 \times \mathbb{Z}_4$ e o grafo $\Gamma_{\overrightarrow{u},\overrightarrow{v}}$ com $\overrightarrow{u} = (3,2)$ e $\overrightarrow{v} = (-2,3)$.

3.4.1 $\mathbb{Z}_4 \times \mathbb{Z}_4$

Neste caso, temos diâmetro $d = 4$ e portanto, $i = 0, 1, 2, 3, 4$. Vamos então analisar cada caso, lembrando que basta analisar um par de pontos em cada caso pois dados dois pontos a uma distância d, existe uma isometria (com a métrica de Lee) a quaisquer outros dois pontos a uma distância d.

1. $i = 0$. Neste caso, $\gamma = \delta$ e portanto, $b_0 = 4$.

2. $i = 1$. Se tomarmos γ e δ vizinhos, temos que $b_1 = 3$ já que dentre os vizinhos de δ, 3 estão à distância $i + 1 = 2$ de γ. E temos que $c_1 = 1$, uma vez que o próprio γ é o vizinho de δ à distância 0 de γ.

3. $i = 2$. Da mesma forma, analisamos dois pontos γ e δ à distância 2 e temos que $b_2 = 2$ e $c_2 = 2$.

4. $i = 3$. Neste caso, $b_3 = 1$ e $c_3 = 3$.

5. $i = 4$. Finalmente, temos que $c_4 = 4$.

Portanto, o vetor intersecção de $\mathbb{Z}_4 \times \mathbb{Z}_4$ é dado por $(b_0, ..., b_3; c_1, ..., c_4) = (4, 3, 2, 1; 1, 2, 3, 4)$. Temos então que este grafo é aresta regular de valência $k = 4$ e portanto, pela Observação 1.7.2.1, este grafo é amplamente regular, mas não fortemente regular.

3.4.2 $\Gamma_{\vec{u},\vec{v}}$

Neste exemplo temos diâmetro $d = 2$ e portanto, $i = 0, 1, 2$.

1. $i = 0$. Neste caso, como $\delta = \gamma$, $b_0 = 4$.

2. $i = 1$. Para γ e δ vizinhos, temos que $b_1 = 3$ e $c_1 = 1$.

3. $i = 2$. Para γ e δ à distância 2, $c_2 = 2$.

Portanto, o vetor intersecção deste grafo é $(b_0, b_1; c_1, c_2) = (4, 3; 1, 2)$, finalizando este exemplo.

Referências Bibliográficas

[1] HEFEZ, A. e VILLELA, M.L.T.; *Códigos Corretores de Erros*; IMPA, 2002;

[2] STILLWELL, J. ; *Geometry of Surfaces*; Springer-Verlag, cap. 2, 1992;

[3] DIESTEL, R.; *Graph Theory* ; Second edition, Springer, 2000;

[4] CONWAY, J.H. e SLOANE, N.J.A.; *Sphere Packings, Lattices and Groups*; Springer, 1988;

[5] CAMERON, P.J. e van LINT, J.H.; *Designs,Graphs,Codes and their Links*; Cambridge University Press, 1991;

[6] TRUDEAU, R.J.; *Introduction to Graph Theory*; Dover Publications, New York, 1993;

[7] BROWER, A.E. e NEUMAIER, A.; *Distance-Regular Graphs*; Springer-Verlag, New York, 1989;

[8] GONÇALVES, A.; *Introdução à Álgebra*; Projeto Euclides, 2001.

[9] COSTA, S.I.R. , MUNIZ, M. , AGUSTINI, E. e PALAZZO, R.; Graphs, Tesselations and Perfect Codes on Flat Tori; *IEEE-Transactions on Informations Theory*; vol 50, pp $2363 - 2377$, Oct 2004;

[10] MAUNDER, C. R. F.; *Algebraic Topology*; Van Nostrand Reinhold Company, London, 1970;

[11] MUNIZ, M. e COSTA, S.I.R.; Labelings of Lee and Hamming Spaces; *Discrete Mathematics* $260(2003)119 - 136$

[12] RICE, B. F. e WILD, C. O.; Error Correcting Codes 1; *UMAP-Modules and Monographs in Undergraduate Mathematics and its Applications*, Módulo 346;

[13] WILSON, R. J.; *Graph Theory*; Prentice Hall, fourth edition, 1996;

[14] McCARTY, G.; *Topology - an introduction with applications to topological groups*; Dover Publications, New York, 1988;