JOÃO ANTONIO CAMARGO NETO

Códigos Geométricos de Goppa Aprimorados

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2022

JOÃO ANTONIO CAMARGO NETO

Códigos Geométricos de Goppa Aprimorados

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Alonso Sepúlveda Castellanos.

UBERLÂNDIA - MG
2022

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

C172 Camargo Neto, João Antônio, 1998-
2022 Códigos Geométricos de Goppa Aprimorados [recurso eletrônico] / João Antônio Camargo Neto. - 2022.

Orientador: Alonso Sepúlveda Castellanos.
Dissertação (Mestrado) - Universidade Federal de Uberlândia, Pós-graduação em Matemática.
Modo de acesso: Internet.
Disponível em: http://doi.org/10.14393/ufu.di.2022.215
Inclui bibliografia.

1. Matemática. I. Castellanos, Alonso Sepúlveda,1980-, (Orient.). II. Universidade Federal de Uberlândia. Pós-graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Coordenação do Programa de Pós-Graduação em Matemática
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 160 - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4209/4154 - www.posgrad.famat.ufu.br - pgmat@famat.ufu.br

ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Matemática				
Defesa de:	Dissertação de Mestrado Acadêmico, 101, PPMAT				
Data:	30 de maio de 2022	Hora de início:	15:30	Hora de encerramento:	17:30
Matrícula do Discente:	12012MAT005				
Nome do Discente:	João Antônio Camargo Neto				
Título do Trabalho:	Códigos Geométricos de Goppa Aprimorados				
Área de concentração:	Matemática				
Linha de pesquisa:	Geometria Algébrica				
Projeto de Pesquisa de vinculação:	Semigrupo de Weierstrass em pontos e pesos generalizados de Hamming sobre curvas tipo Kummer				

Reuniu-se na Sala 1F-119 (Sala Multiuso da Faculdade de Matemática), Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-graduação em Matemática, assim composta: Professores Doutores: Luciane Quoos Conte - IM/UFRJ; Victor Gonzalo Lopez Neumann - FAMAT/UFU e Alonso Sepúlveda Castellanos - FAMAT/UFU, orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Alonso Sepúlveda Castellanos, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao Discente a palavra para a exposição do seu trabalho. A duração da apresentação do Discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

Aprovado.

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Alonso Sepulveda Castellanos**, **Professor(a) do Magistério Superior**, em 30/05/2022, às 17:07, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 30/05/2022, às 17:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Luciane Quoos Conte**, **Usuário Externo**, em 31/05/2022, às 09:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3553172** e o código CRC **722D2163**.

Referência: Processo nº 23117.029331/2022-33 SEI nº 3553172

"Agrada-te do Senhor e, Ele satisfará os desejos do teu coração."
(Salmo 37:4)

Agradecimentos

Agradeço primeiramente Àquele que é o centro de tudo e que fez com que todas as coisas contribuíssem para o meu bem, ao ponto de hoje, concluir este trabalho, Deus esteve presente em cada passo desta etapa, e somente por Ele cheguei aqui.

Agradeço àquela que se tornou minha esposa no decorrer deste processo, Nathália me deu suporte, correu por mim e por ela para que eu pudesse me dedicar a esta fase, sua presença me motiva a ser melhor e todas as minhas conquistas, são dela também. A amo mais todos os dias.

Agradeço àqueles que estão comigo desde o meu primeiro passo, literalmente. Meus pais fizeram por mim e continuam fazendo coisas que talvez nunca conseguirei retribuir. Eles fazem parte não somente da minha vida, mas também de quem eu sou. Com eles divido todas as coisas e hoje tenho a alegria de dividir uma conquista. Saibam que os amo e irei honrá-los até o fim.

Ao meu orientador Prof. Dr. Alonso Sepúlveda Castellanos dedico um agradecimento especial, foram longos anos tendo-o como mentor não somente acadêmico mas também pessoal. Agradeço sua sensibilidade em me ouvir, me cobrando na mesma intensidade que me motivou. O admiro e me inspiro em quem você é. Hoje tenho alegria em chamá-lo de amigo.

Agradeço aos meus amigos e colegas que estiveram ao meu lado, nos dias difíceis, eles me ajudaram a seguir em frente.

CAMARGO NETO, J. A. *Códigos Geométricos de Goppa Aprimorados.* 2022. (# pág) p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Neste trabalho estudamos uma melhoria para a construção dos Códigos Geométricos de Goppa (códigos AG), propondo uma construção menos complexa de uma família de códigos lineares que chamaremos de Códigos Geométricos de Goppa Aprimorados (GGA-códigos). Para isto, abordamos primeiramente, a teoria básica de códigos corretores de erros e retomamos rapidamente a construção usual dos chamados códigos AG. Depois, apresentamos uma construção dos GGA-códigos e então, através dela, utilizamos a curva de Klein para construir exemplos. Em seguida apresentamos a construção de GGA-códigos sobre a curva quase-Hermitiana que é definida por meio da curva Hermitiana, assim mostramos que uma família de GGA-códigos quase-Hermitianos excedem a cota de Garcia-Stichtenoth.

Palavras-chave: Geometria Algébrica, Teoria de Códigos Corretores de Erros, Códigos Geométricos de Goppa.

CAMARGO NETO, J. A. *Improved Geometric Goppa Codes* 2022. (# pages) p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

In this work we study an improvement for the construction of Geometric Goppa Codes (AG codes), proposing a less complex construction of a family of linear codes that we will call Improved Geometric Goppa Codes (GGA-códigos). To initially approach the basic theory of error codes and quickly resume the usual construction of so called AG codes. Then we present a construction of the GGA-códigos and then through it, we use Klein curve to build examples. Next, we present the construction of GGA-códigos on the Hermitian-like curve which is defined by means of the Hermitian curve, and then we show that a family of Hermitian-like GGA-códigos exceeded the Garcia-Stichtenoth bound.

Keywords: Algebraic Geometry, Error Correcting Code Theory, Algebraic Geometric Goppa Codes.

Introdução

João Antonio Camargo Neto
Uberlândia-MG, 30 de Maio de 2022.

A teoria dos códigos corretores de erros é um campo de pesquisa muito ativo atualmente em diversas áreas do conhecimento: matemática, computação, engenharia elétrica, estatística e entre outras. Na transmissão de dados na vida real, às vezes ocorrem problemas como interferências eletromagnéticas ou erros humanos (por exemplo, erros de digitação) que chamamos de ruído e que fazem com que a mensagem recebida seja diferente daquela que foi enviada. O objetivo da teoria de códigos corretores de erros é desenvolver métodos que permitam detectar e corrigir estes erros.

A teoria de códigos corretores de erros lineares sobre curvas algébricas (códigos algébricos geométricos (códigos AG)) passou a ser desenvolvida desde o trabalho de Goppa e Tsfasman e Vladut e Zink em 1981-1982.

Para a construção dos códigos AG, são utilizados divisores das curvas algébricas que são construídos por meio dos pontos racionais (ou lugares de grau 1) da curva. Dessa forma, é importante que a curva possua uma grande quantidade de pontos racionais para que os códigos construídos apresentem parâmetros como dimensão e distância mínima satisfatórios.

Os códigos algébricos geométricos (AG códigos), introduzidos por Goppa, são construídos escolhendo um conjunto de pontos de uma curva algébrica e o espaço de funções racionais desta curva. Os AG códigos possuem bons parâmetros. Porém, não existe um procedimento de baixa complexidade para sua construção.

Neste trabalho, apresentaremos o método para construção dos Códigos Geométricos de Goppa Aprimorados (GGA-códigos), que serão baseadas nos pontos racionais de curvas, como a curva de Klein e a curva quase-Hermitiana. Para isso, introduziremos alguns tipos de sequências monomiais, chamadas sequências bem-comportadas e quase-bem-comportadas. A distância mínima nos códigos de Goppa aprimorados podem ser facilmente determinadas, e, para distâncias específicas, códigos com maior comprimento podem ser construídos.

Os GGA-códigos possuem grande potencial de substituir os códigos de Reed-Solomon em várias aplicações, como sistemas de comunicações, tecnologia de discos compactos, sistema de memórias de alta velocidade para computadores, entre outras, por sua menor complexidade de construção e também de decodificação.

No capítulo 1, abordamos a teoria inicial dos códigos corretores de erros, definindo importantes conceitos que permearão os nossos resultados no decorrer do trabalho. Também iremos enunciar e mostrar alguns resultados chaves no desenvolvimento da teoria.

No capítulo 2, mostramos a construção usual dos códigos geométricos de Goppa, apresentando exemplos de sua construção.

O capítulo 3, é destinado a apresentação da construção dos códigos geométricos de Goppa aprimorados, mostrando importantes resultados que serão utilizados no decorrer do trabalho.

No capitulo 4, utilizamos a curva de Klein para aplicar a construção vista no capítulo 3, fazendo uma comparação entre diferentes formas de utilizar o mesmo método de construção.

No capítulo 5, apresentamos a curva quase-Hermitiana e são definidos novos conceitos para otimizar os códigos geométricos de Goppa aprimorados, melhorando seus parâmetros. Neste capítulo, mostramos um importante resultado de códigos que excedem a cota de Garcia-Stichtenoth.

Capítulo 1

Códigos Corretores de Erros

Os códigos corretores de erros participam do nosso cotidiano de diferentes formas, como, por exemplo, quando assistimos programas de TV, falamos ao telefone, ouvimos um CD ou navegamos pela internet. Nestas situações estamos utilizando informações digitalizadas [7].

Um código corretor de erros é, em essência, um modo organizado de acrescentar algum dado adicional a cada informação que se queira transmitir ou armazenar, que permita ao recuperar a informação, detectar e corrigir erros.

A Teoria de Códigos Corretores de Erros foi fundada pelo matemático Claude Elwood Shannon, matemático estadunidense conhecido como pai da teoria da informação, que publicou um trabalho intitulado *A Mathematical Theory of Communication* em 1948, no qual abordava qual a melhor forma de se codificar a informação que um emissor queira transmitir para um receptor.

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.

1.1 Código do Robô

Vejamos um exemplo, o qual chamaremos de código do Robô, para ilustrar os princípios desta teoria. Suponha que tenhamos um robô que se move sobre um tabuleiro quadriculado, de modo que, ao darmos um dos comandos (Leste, Oeste, Norte e Sul), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando. Podemos codificar os comandos, como elementos de $\{0,1\} \times \{0,1\}$, da seguinte forma:

$$\begin{array}{rcl} Leste & \mapsto & 00 \\ Oeste & \mapsto & 01 \\ Norte & \mapsto & 10 \\ Sul & \mapsto & 11 \end{array}$$

A coluna da direita é chamada *código da fonte*. Agora, suponhamos que os pares ordenados devem ser transmitidos por rádio e que o sinal sofra uma interferência no caminho, em decorrência deste ruído na informação, a mensagem 00 pode ser recebida como 01. Com isso, o robô ao invés de ir para o Leste, iria para o Oeste. Para que isso não aconteça, introduzimos redundâncias nas palavras recodificando-as, para que seja possível identificar e corrigir os erros.

Podemos recodificar nosso código da seguinte forma:

$$\begin{array}{ccccc} Leste & \mapsto & 00 & \mapsto & 00000 \\ Oeste & \mapsto & 01 & \mapsto & 01011 \\ Norte & \mapsto & 10 & \mapsto & 10110 \\ Sul & \mapsto & 11 & \mapsto & 11101 \end{array}$$

Veja que nesta recodificação, as duas primeiras posições reproduzem o código da fonte e os três números introduzidos são as redundâncias. Este novo código será chamado de **Código de canal**.

Suponha que se tenha introduzido um erro ao transmitirmos, por exemplo, a palavra 10110, de modo que a mensagem recebida seja 11110. Comparando essa mensagem com as palavras do código, notamos que não lhe pertence e, portanto, detectamos erros. A palavra do código mais próxima da palavra introduzida (a que tem menos coordenadas distintas) é 10110, que é precisamente a palavra transmitida.

O nosso estudo consiste, então, em transformar o código da fonte em um código de canal, sendo possível a detecção e correção de forma mais eficiente.

1.2 Métrica de Hamming

Seja A um conjunto finito, o qual chamaremos de Alfabeto. O número de elementos de A será denotado por $|A| = q$. Um código corretor de erros é um subconjunto próprio qualquer de $A^n = \{(x_1, x_2, \ldots, x_n) : x_i \in A; i = 1, 2, \ldots, n\}$, para $n \in \mathbb{N}$. Até agora utilizamos a noção intuitiva de proximidade entre palavras, porém vamos definir uma forma de medir essa distância.

Definição 1.1. *Dados dois elementos $u, v \in A^n$, a distância de Hamming entre u e v é definida como*

$$d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|.$$

Para exemplificar esta definição, considere $A = \{0, 1\}$ e $n = 4$:

$$d(0010, 1111) = 3,$$

$$d(1010, 0101) = 4,$$

$$d(1001, 1101) = 1.$$

Proposição 1.1. *Dados $u, v, w \in A^n$, valem as seguintes propriedades:*

i) Positividade: $d(u, v) \geq 0$, valendo a igualdade se, e somente se, $u = v$.

ii) Simetria: $d(u, v) = d(v, u)$.

iii) Desigualdade Triangular: $d(u, v) \leq d(u, w) + d(w, v)$.

Demonstração. *i) Temos por definição que $d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$, logo, temos que a distância será a quantidade de elementos deste conjunto, desta forma $d(u, v) \geq 0$.*

ii) Quando calculamos a distância de Hamming, comparamos coordenada a coordenada das palavras, dessa forma, independe a ordem que comparamos a i-ésima coordenada das palavras, ou seja, os conjuntos $d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$ e $d(v, u) = |\{i; v_i \neq u_i, 1 \leq i \leq n\}|$ são equivalentes.

iii) A contribuição das i-ésimas coordenadas de u e v para $d(u,v)$ é igual a 0 se $u_i = v_i$, e igual a 1 se $u_i \neq v_i$. No caso em que a contribuição é zero, certamente a contribuição das i-ésimas coordenadas de $d(u,v)$ é menor igual a das i-ésimas coordenadas de $d(u,w) + d(w,v)$ (= 0, 1 ou 2).

No outro caso, temos que $u_i \neq v_i$ e, portanto, não podemos ter $u_i = w_i$ e $w_i = v_i$. Consequentemente, a contribuição das i-ésimas coordenadas a $d(u,v) + d(w,v)$ é maior ou igual a 1, que é a contribuição das i-ésimas coordenadas de $d(u,v)$.

A Proposição 1 nos garante que a distância de Hamming, como definimos é uma métrica.

Dado um elemento $a \in A^n$ e um número real $t \geq 0$, definimos o disco e a esfera de centro a e raio t como sendo, respectivamente, os conjuntos

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

Os conjuntos acima são finitos pois A^n é finito. O próximo lema nos fornecerá as suas cardinalidades. Iremos a partir daqui utilizar a notação usual de números combinatórios:

$$\begin{pmatrix} n \\ i \end{pmatrix} = \frac{n!}{i!(n-i)!}.$$

Lema 1.1. *Para todo $a \in A^n$ e todo número natural $r > 0$, temos que*

$$|D(a,r)| = \sum_{i=0}^{r} \begin{pmatrix} n \\ i \end{pmatrix} (q-1)^i.$$

Demonstração. *Primeiramente, mostremos que*

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

$S(a,i)$ é o conjunto de n-uplas que diferem de a em exatamente i posições. Podemos escolher $\binom{n}{i}$ formas as posições nas quais um elemento de $S(a,i)$ difere de a. A seguir, em cada uma dessas coordenadas, temos $(q-1)$ escolhas dentre os elementos do conjunto A, já que só não podemos escolher o elemento, nessa posição, do elemento a. Pelo princípio multiplicativos, obtemos o resultado acima.

O resultado segue, observando que $S(a,i) \cap S(a,j) = \emptyset$ se $i \neq j$, e que

$$\bigcup_{i=0}^{r} S(a,i) = D(a,r).$$

Note que a cardinalidade de $D(a,r)$ depende apenas de n, q e r.

Definição 1.2. *Seja C um código de A^n. A distância mínima de C é o número*

$$d = min\{d(u,v); u,v \in C, u \neq v\}.$$

Por exemplo no código do robô, tínhamos $d = 3$.

Para calcularmos d, precisaríamos calcular $\begin{pmatrix} M \\ 2 \end{pmatrix}$ distâncias, onde M é o número de palavras do código, o que tem um alto custo computacional. Veremos a seguir uma forma de calcular d, com baixo custo computacional, quando utilizamos uma estrutura algébrica adicional.

Dado um código C de A^n com distância miníma d, define-se $\kappa = \left[\frac{d-1}{2} \right]$, onde $[t]$ representa a parte inteira de $t \in \mathbb{R}$.

Lema 1.2. *Seja C um código com distância mínima d. Se c e $c^{'}$ são palavras distintas de C então*

$$D(c,\kappa) \cap D(c^{'},\kappa) = \emptyset.$$

Demonstração. *De fato, se $x \in C$ pertencesse a $D(c,\kappa) \cap D(c^{'},\kappa)$, teríamos $d(x,c) \leq \kappa$ e $d(x,c^{'}) \leq \kappa$. Como $d(x,c) = d(c,x)$ pela desigualdade triangular temos que $d(c,c^{'}) \leq d(c,x) + d(x,c^{'}) \leq 2k$. Agora para $j,l \in \mathbb{Z}_{+}$ temos pelo algoritmo de euclides que existem $q,r \in \mathbb{Z}$ tais que $j = lq + r$, onde $0 \leq r < l$, o que implica que $l\left[\frac{j}{l}\right] = j - r$ e daí segue que,*

$$d(c,c^{'}) \leq d(c,x) + d(x,c^{'}) \leq 2\kappa \leq d - 1,$$

absurdo pois $d(c,c^{'}) \geq d$.

A importância da distância mínima d de um código se dá pelo teorema a seguir.

Teorema 1.1. *Seja C um código de A^n com distância mínima d. Então C pode corrigir até $\kappa = \left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Demonstração. *Se ao transmitirmos uma palavra c do código cometermos t erros, com $t \leq \kappa$, recebendo a palavra r, então $d(r,c) = t \leq \kappa$; enquanto que, pelo Lema anterior, a distância de r a qualquer outra palavra do código é maior que κ. Isso determina c univocamente a partir de r. Por outro lado, dada uma palavra do código, podemos nela introduzir até $d-1$ erros sem encontrar outra palavra do código, e assim, a detecção do erro será possível.*

Por exemplo no código do robô como $d = 3$, é possível corrigir até $\kappa = \left[\frac{3-1}{2}\right] = 1$ erros e detectar até $d - 1 = 4 - 1 = 3$ erros.

Podemos concluir que um código terá maior capacidade de detecção e correção de erros quanto maior a sua distância mínima, portanto é fundamental que calculemos d e que exista uma cota inferior para este parâmetro do código. É isto que iremos determinar a seguir.

Definição 1.3. *Seja $C \subset A^n$ um código com distância mínima d e seja $\kappa = \left[\frac{d-1}{2}\right]$. O código C será dito perfeito se*

$$\bigcup_{c \in C} D(c,\kappa) = A^n.$$

Um código C sobre um alfabeto A possui três parâmetros fundamentais $[n,k,d]$, que são respectivamente, o seu comprimento, o número de elementos (veremos que em códigos lineares representa a dimensão do código) e sua distância mínima.

1.3 Códigos Lineares

A classe de códigos mais utilizada na prática é conhecida como códigos lineares, à qual iremos abordar no decorrer do trabalho.

Denotaremos por $\mathbb{F}_q$ um corpo finito com q elementos tomado como alfabeto. Temos, portanto, para cada $n \in \mathbb{N}$, existe um $\mathbb{F}_q$-espaço vetorial $\mathbb{F}_q^n = \{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{F}_q, i = 1, 2, \ldots, n\}$ de dimensão n.

Sejam $u, v \in \mathbb{F}_q^n$ e $k \in \mathbb{F}_q$, onde $u = (u_1, u_2, \ldots, u_n)$ e $v = (v_1, v_2, \ldots, v_n)$. As operações definidas em $\mathbb{F}_q^n$ serão:

- **Soma:**

$$u + v = (u_1, u_2, \ldots, u_n) + (v_1, v_2, \ldots, v_n) = (u_1 + v_1, u_2 + v_2, \ldots, u_n + v_n).$$

Onde a soma de $u_i + v_i \in \mathbb{F}_q$, para $i = 1, 2, \ldots, n$ é a soma em $\mathbb{F}_q$.

- **Multiplicação por escalar:**

$$k \cdot u = k \cdot (u_1, u_2, \ldots, u_n) = (k \cdot u_1, k \cdot u_2, \ldots, k \cdot u_n)$$

Note que $u_i \in \mathbb{F}_q; i = 1, 2, \ldots, n$, dessa forma a operação $k \cdot u_i \in \mathbb{F}_q$ é o produto usual de $\mathbb{F}_q$.

Definição 1.4. *Todo subespaço $C \subset \mathbb{F}_q^n$ será chamado código linear sobre $\mathbb{F}_q$.*

Sabemos que a imagem de uma transformação linear é um subespaço vetorial, portanto, podemos representar os códigos por meio de uma transformação linear injetora, veja um exemplo a seguir.

O código robô é um código linear, considerando o alfabeto $A = \mathbb{F}_2$, conhecido como corpo de Galois, e o código robô é subespaço vetorial de $\mathbb{F}_2^5$. A transformação linear que gera o código robô é

$$\begin{array}{rccc} T: & \mathbb{F}_2^2 & \to & \mathbb{F}_2^5 \\ & (x_1, x_2) & \mapsto & (x_1, x_2, x_1, x_1 + x_2, x_2) \end{array}$$

De fato, veja que:

$$\begin{array}{l} T(0,0) = (0,0,0,0,0) \\ T(0,1) = (0,1,0,1,1) \\ T(1,0) = (1,0,1,1,0) \\ T(1,1) = (1,1,1,0,1) \end{array}$$

Todo código linear é por definição um espaço vetorial de dimensão finita. Portanto seja k a dimensão do código C e seja $(v_1, v_2, \ldots, v_k)$ uma de suas bases, portanto, todo $c \in C$, pode ser escrito como

$$c = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k,$$

onde $\lambda_i \in \mathbb{F}_q, i = 1, \ldots, k$. Segue daí que o número de palavras do código será $M = |C| = q^k$. E consequentemente,

$$\boxed{dim_{\mathbb{F}_q} C = k = log_q q^k = log_q M.}$$

Definição 1.5. *Seja $x \in \mathbb{F}_q^n$, dizemos que o peso de x é*

$$\omega(x) = |\{i; x_i \neq 0)\}|.$$

Uma definição equivalente é $\omega(x) = d(x, 0)$.

Definição 1.6. *O peso de um código linear C é*

$$\omega(C) = min\{\omega(x); x \in C \backslash \{0\}\}.$$

Proposição 1.2. *Seja $C \subset \mathbb{F}_q^n$ um código linear com distância mínima d. Temos que*

i) $\forall x, y \in \mathbb{F}_q^n$, $d(x, y) = \omega(x - y)$.

ii) $d = \omega(C)$.

Demonstração. *i) Por definição temos que $\forall u, v \in \mathbb{F}_q^n$, $d(u, v) = |\{i; u_i \neq v_i, 1 \leq i \leq n\}|$ e, $\forall u, v \in \mathbb{F}_q^n$ temos que, $\omega(u - v) = |\{i; u_i - v_i \neq 0, 1 \leq i \leq n\}|$, porém, podemos reescrever $u_i - v_i \neq 0$ como $u_i \neq v_i$, tornando assim os dois conjuntos iguais, logo, $\forall u, v \in \mathbb{F}_q^n$, $d(u, v) = \omega(u - v)$.*

ii) Para todo par de elementos $x, y \in C$, com $x \neq y$, tem-se que $z = x - y \in C\backslash\{0\}$ e $d(x, y) = \omega(z)$, logo a distância mínima será o menor peso de um elemento z assim construído do código.

Veremos agora um resultado que possibilita relacionar os parâmetros de um (n, k, d)-código e então enuciaremos uma cota chamada *Cota de Singleton.*

Teorema 1.2. *Seja $C \subset \mathbb{F}_q$ um $[n, k, d]$-código, com M elementos. Temos que*

$$M \leq q^{n-d+1}.$$

Demonstração. *Seja $C \subset \mathbb{F}_q$ o código com os parâmetros dados e considere a projeção*

$$\begin{array}{rccc} Pr & : & \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ & & (x_1, \ldots, x_n) & \mapsto & (x_d, x_{d+1}, \ldots, x_n). \end{array}$$

A restrição de Pr a C é injetora, pois se $Pr(x) = Pr(y)$ para $x, y \in C$, então $d(x, y) \leq d-1$, e pela definição de distância isto pode acontecer apenas se $d(x, y) = 0$, e assim temos que $x = y$. Portanto, temos que $Pr(C)$ é um subconjunto de $\mathbb{F}_q^{n-d+1}$ com M elementos, daí segue que $M \leq q^{n-d+1}$. □

Corolário 1.1. ***Cota de Singleton***
Os parâmetros $[n, k, d]$ de um código linear satisfazem à desigualdade

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

Demonstração. *Basta observar que em um código linear , $M = q^k$, assim*

$$q^k \leq q^{n-d+1} \Rightarrow d \leq n - k + 1.$$

1.4 Matriz Geradora de um Código

Considere $\mathbb{F}_q$ o corpo finito com q elementos e $C \subset \mathbb{F}_q^n$ um código linear. Chamaremos de *parâmetros do código linear* C à terna de inteiros $[n, k, d]$ onde k é a dimensão de C sobre $\mathbb{F}_q$ e d representa a distância mínima de C, que é também igual ao peso de $\omega(C)$ do código C. Note que o número de elementos M de C é igual a q^k.

Seja $\beta = \{v_1, v_2, \ldots, v_k\}$ uma base ordenada de C e considere a matriz G, cujas linhas são os vetores $v_i = (v_{i1}, \ldots, v_{in})$, $i = 1, \ldots, k$, isto é:

$$G = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}.$$

A matriz G é chamada de *matriz geradora* de C associada a base β.

Considere a transformação linear definida por:

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array}.$$

Se $x = (x_1, \ldots, x_k)$, temos que

$$T(x) = xG = x_1 v_1 + \cdots + x_k v_k.$$

Logo $T(\mathbb{F}_q^k) = C$. Podemos, então, considerar $\mathbb{F}_q^k$ como sendo o código da fonte, C o código de canal e a transformação T, uma codificação.

Note que a matriz G depende da escolha da base, dessa forma não é univocamente determinada por C.

Podemos também considerar o processo inverso e construir códigos a partir de matrizes geradoras. Para isso, basta tomar uma matriz cujas linhas são linearmente independentes e definir um código como sendo a imagem da transformação linear:

$$\begin{array}{rccc} T: & \mathbb{F}_q^k & \to & \mathbb{F}_q^n \\ & x & \mapsto & xG \end{array}.$$

Definição 1.7. *Diremos que uma matriz geradora G de um código $C \subseteq F_q^n$ está na forma padrão se tivermos*

$$G = (Id_k|A),$$

onde Id_k é a matriz identidade $k \times k$ e A uma matriz $k \times (n-k)$.

O teorema a seguir nos garante a existência da matriz na forma padrão de qualquer matriz geradora de um código C, e podemos obtê-la por meio de operações elementares e permutação de colunas.

Teorema 1.3. *Dado um código C, existe um código equivalente C' com matriz geradora na forma padrão.*

Demonstração. *A demonstração pode ser vista em [7] nas páginas 92-93.*

1.5 Código Dual

Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ elementos de $\mathbb{F}_q^n$, define-se o produto de u e v como sendo:

$$\langle u, v\rangle = u_1v_1 + \cdots + u_nv_n.$$

Essa operação possui as propriedades usuais de um produto interno, ou seja, é simétrica

$$\langle u, v\rangle = \langle v, u\rangle$$

e bilinear

$$\begin{gathered} \langle u + \lambda w, v\rangle = \langle u, v\rangle + \lambda\langle w, v\rangle \\ \langle u, v + \lambda w\rangle = \langle u, v\rangle + \lambda\langle w, v\rangle \\ \langle \lambda u, v\rangle = \langle u, \lambda v\rangle = \lambda\langle u, v\rangle \end{gathered}$$

para todo $\lambda \in \mathbb{F}_q$.

Seja $C \subset \mathbb{F}_q^n$ um código linear, define-se o conjunto:

$$C^\perp = \{v \in \mathbb{F}_q^n; \langle u, v\rangle = 0, \forall u \in C\}.$$

Lema 1.3. *Se $C \subset \mathbb{F}_q^n$ é um código linear, com matriz geradora G, então*

i) $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$.

ii) $x \in C^\perp \Leftrightarrow Gx^t = 0$.

Demonstração. *i) Considere $u, v \in C^\perp$ e $\lambda \in \mathbb{F}_q$. Temos que para todo $x \in C$*

$$\langle u + \lambda v, x\rangle = \langle u, x\rangle + \lambda\langle v, x\rangle = 0$$

e portanto, $u + \lambda v \in C^\perp$, provando que $C^\perp$ é um subespaço vetorial de $\mathbb{F}_q^n$.

ii) $x \in C^\perp \Leftrightarrow x$ é ortogonal a todos os elementos de $C \Leftrightarrow x$ é ortogonal a todos os elementos de uma base de C, o que é equivalente a dizer que $Gx^t = 0$ pois as linhas de G são uma base de C.

O subespaço vetorial $C^\perp$ de $\mathbb{F}_q^n$, ortogonal a C, é também um código linear que será chamado **código dual** de C.

Capítulo 2

Códigos Algébricos Geométricos de Goppa

Os códigos algébricos geométricos, que chamaremos de códigos AG, foram introduzidos por Valerii Denisovich Goppa em seu livro *Geometry and codes* publicado em 1988. Esta classe de códigos é muitas vezes chamada de códigos de Goppa. Como uma motivação para a construção desses códigos, primeiro consideramos os códigos de Reed-Solomon sobre o corpo finito $\mathbb{F}_q$, onde q é uma potência de um primo. Essa importante classe de códigos é bem conhecida na teoria dos códigos. Os códigos algébricos geométricos são uma generalização natural do Código de Reed-Solomon.

Maiores detalhes sobre a construção dos códigos AG podem ser vistas em [10].

2.1 Corpos de Funções Algébricas

Nesta seção, apresentaremos as definições e resultados básicos da teoria de Funções Algébricas, necessárias para a construção dos códigos algébricos geométricos de Goppa [11].

Iremos denotar por K um corpo finito qualquer.

2.1.1 Lugares

Definição 2.1. *Um corpo de funções F/K de uma variável sobre K é uma extensão $F \supseteq K$, tal que, F é uma extensão finita de $K(x)$ para algum elemento $x \in F$, onde x é transcendente em K [10].*

Exemplo 2.1. *O exemplo mais simples de corpo de funções é o corpo de funções racionais. F/K é chamado de racional se $F = K(x)$ para algum $x \in F$ transcende sobre K. Cada elemento $z \neq 0 \in K(x)$ possui uma representação única*

$$z = a \prod_i p_i(x)^{n_i},$$

onde $a \neq 0 \in K$, os polinômios $p_i(x) \in K[x]$ são mônicos, distintos dois a dois, irredutíveis e $n_i \in \mathbb{Z}$.

Definição 2.2. *Um anel de valorização do corpo de funções F/K é um anel $O \subset F$ que satisfaz as seguintes propriedades*

i) $K \subsetneq O \subsetneq F$.

ii) $\forall z \in F$, $z \in O$ *ou* $z^{-1} \in O$.

Proposição 2.1. *Seja O um anel de valorização do corpo de funções F/K. Então:*

i) O tem um único ideal maximal $P = O/O^*$, onde

$$O^* = \{x \in O | \exists z \in O \text{ onde } x.z = 1\}.$$

ii) Para $x \in F$, não nulo, temos: $x \in P \Leftrightarrow x^{-1} \in O$.

iii) Para $\bar{K}$ o corpo de constantes de F/K, temos $\bar{K} \subseteq O$ e $\bar{K} \cap P = \{0\}$.

Demonstração. *i) Primeiro seja $x \in P$ e $z \in O$, se $zx \in O^* \Rightarrow \exists w \in O$ onde $zxw = 1 \Rightarrow x(zw) = 1 \Rightarrow x \in O^*$.*

Agora sejam $x, y \in P$. Considere $\frac{x}{y} \in F$, então $\frac{x}{y} \in O$ ou $\frac{y}{x} \in O$.

Se $\frac{x}{y} \in O \Rightarrow 1 + \frac{x}{y} \in O \Rightarrow x + y = y(1 + \frac{x}{y}) \in P$. Se $\frac{y}{x} \in O$ é análogo.

Portanto $x + y \in P$ onde temos que P é um ideal.

Mostremos agora que P é maximal.

Seja J um ideal onde $P \subsetneq J \subseteq O$. Tome $x \in J/P$. Então $x \in O^*$, pois $P = O \backslash O^*$, assim $xx^{-1} \in J$, pois J é um ideal. Logo $1 \in J \Rightarrow O \subset J \Rightarrow J = O$. Portanto P é maximal.

P é o único ideal maximal de O. De fato, seja J ideal maximal de O. Se J não contém unidades de O, então $J \subseteq P \Rightarrow J = P$, pois J é maximal. Agora se J possui uma unidade, então $J = O$.

Portanto P é o único ideal maximal próprio de O.

ii) $x \in P \Leftrightarrow x \in O/O^* \Leftrightarrow x \notin O^* \Leftrightarrow x^{-1} \notin O^*$.

iii) Seja $z \in \bar{K}$. Suponha que $z \notin O$. Então $z^{-1} \in O$ pois O é um anel de valorização. Como z^{-1} é algébrico sobre K, existem elementos $a_1, \ldots, a_r \in K$ com $a_r(z^{-1})^r + \cdots + a_1 z^{-1} + 1 = 0$, consequentemente $z^{-1}(a_r(z^{-1})^{r-1} + \cdots + a_1) = -1$. Portanto $z = -(a_r(z^{-1})^{r-1} + \cdots + a_1 \in K[z^{-1}] \subseteq O$ então $z \in O$. Temos uma contradição pois assumimos que $z \notin O$. Mostramos assim que $\bar{K} \subseteq O$. A intersecção $\bar{K} \cap P = \{0\}$ é trivial.

Definição 2.3. *1. Um lugar P de um corpo de funções F/K é o ideal maximal de algum anel de valorização O de F/K. Todo $t \in P$ tal que $P = tO$ é chamado de um elemento primo de P (outras notações são parâmetro local ou variável uniforme).*

2. $\mathbb{P}_F = \{P; P \text{ é um lugar de } F/K\}$.

Definição 2.4. *Uma valorização discreta de F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:*

i) $v(x) = \infty \Leftrightarrow x = 0$.

ii) $v(xy) = v(x) + v(y), \forall x, y \in F$.

iii) $v(x + y) \geq min\{v(x), v(y)\}, \forall x, y \in F$.

iv) $\exists z \in F$, tal que , $v(z) = 1$.

v) $v(a) = 0, \forall a \in K$ não nulo.

Definição 2.5. *Para todo lugar $P \in \mathbb{P}_F$ associamos uma função $v_p : F \to \mathbb{Z} \cup \{\emptyset\}$. Escolha t um elemento primo de P. Então para todo $z \in F$ não nulo, temos uma única representação $z = t^n u$ com $u \in O^*$ e $n \in \mathbb{Z}$. Defina $v_P(z) = n$ e $v_P(0) = \infty$.*

2.1.2 Divisores

Definição 2.6. *O grupo de divisores de F/K é definido como o grupo abeliano livre que é gerado pelos lugares de F/K, denotado por $Div(F)$. Os elementos de $Div(F)$ são chamados divisores de F/K. Ou seja, um divisor é uma soma*

$$D = \sum_{P \in \mathbb{P}_F} n_P P$$

com $n_P \in \mathbb{Z}$, quase todos nulos.

Definição 2.7. *O suporte de D é definido como*

$$supp(D) = \{P \in \mathbb{P}_F | n_p \neq 0\}.$$

Podemos também escrever o divisor como

$$D = \sum_{P \in S} n_P P,$$

onde $S \subseteq \mathbb{P}_F$ é finito com $supp(D) \subseteq S$.

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ é chamado **divisor primo**. Considere $D = \sum n_P P$ e $D' = \sum n'_P P$ a soma de divisores é definida como

$$D + D' = \sum (n_P + n'_P) P$$

O elemento neutro do grupo de divisores $Div(F)$ é o divisor $0 = \sum_{P \in \mathbb{P}_F} r_P P$, onde $r_p = 0, \forall P \in \mathbb{P}_F$.

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P \in \mathbb{P}_F} n_P P \in Div(F)$, definimos $v_Q(D) = n_Q$. Assim $supp(D) = \{P \in \mathbb{P}_F | v_P(D) \neq 0\}$ e $D = \sum_{P \in \mathbb{P}_F} v_P(D) P$.

Com isso definimos uma ordem parcial para os divisores de F:

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2), \forall P \in \mathbb{P}_F.$$

Definição 2.8. *O grau de um divisor é definido por $gr(D) = \sum_{P \in \mathbb{P}_F} v_P(D) gr(P)$.*

Definição 2.9. *Um divisor $D \geq 0$ é chamado positivo ou* ***efetivo****.*

Definição 2.10. *Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se, e somente se, $v_P(z) > 0$. P é um polo de z se, e somente se, $v_P(z) < 0$. Se $v_P(z) = m > 0$ P é dito um zero de z de ordem m. Se $v_P(z) = -m < 0$, P é dito polo de z de ordem m.*

Um elemento $x \in F$ não nulo tem somente uma quantidade finita de zeros e pólos em $\mathbb{P}_F$. Assim podemos definir:

Definição 2.11. *Sejam $x \neq 0 \in F$ e Z (respectivamente N) o conjunto de zeros(respectivamente pólos) de x em $\mathbb{P}_F$. Definimos*

$$(x)_0 = \sum_{P \in Z} v_P(x) P, \text{ o divisor de zeros de } x.$$

$$(x)_\infty = \sum_{P \in N} (-v_P(x)) P, \text{ o divisor de pólos de } x.$$

$$(x) = (x)_0 - (x)_\infty \text{ o divisor principal de } x.$$

Veja que $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$.

Definição 2.12. *O conjunto dos divisores* $Princ(F) = \{(x) \mid 0 \neq x \in F\}$ *é chamado de conjunto de divisores principais de* F/K.

Note que $(xy) = (x) + (y), \forall x, y \in F$ não nulos, temos então que $Princ(F)$ é subgrupo de $Div(F)$.

Dois divisores $D, D' \in Div(F)$ são chamados de *divisores equivalentes* se $D = D' + (x)$, para algum $(x) \in Princ(F)$.

Definição 2.13. *Para um divisor* $A \in Div(F)$, *definimos o espaço de Riemann-Roch associado a* A *por:*

$$\mathcal{L}(A) = \{x \in F | (x) \geq -A\} \cup \{0\}.$$

Podemos interpretar essa definição analogamente como o conjunto de $(x) \in F$, tal que, $(x) + A$ é efetivo.

A partir daqui enunciaremos alguns resultados para o desenvolvimento da teoria, porém omitiremos algumas demonstrações, que podem ser encontradas em [10].

Lema 2.1. *Sejam* $A, B \in Div(F)$ *com* $A \leq B$. *Então* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e* $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq gr(B) - gr(A)$.

Proposição 2.2. *Para cada divisor* $A \in Div(F)$, $\mathcal{L}(A)$ *é um espaço vetorial de dimensão finita sobre* K.

Definição 2.14. *Seja* $A \in Div(F)$, *o inteiro* $l(A) = dim(\mathcal{L}(A))$ *é chamado de dimensão do divisor* A.

Teorema 2.1. *Todo divisor principal tem grau zero. Mais precisamente: seja* $x \in F/K$ *e* $(x)_0$, *respectivamente* $(x)_\infty$, *o divisor de zeros, respectivamente o divisor de polos de* x. *Então:* $gr(x)_0 = gr(x)_\infty = [F : K(x)]$.

Definição 2.15. *O gênero* g *de* F/K *é definido por*

$$g = max\{gr(A) - l(A) + 1; A \in Div(F)\}.$$

2.1.3 Teorema de Riemann-Roch

Nesta seção, F/K denota um corpo de funções algébricas de gênero g. Mais detalhes podem ser vistos em [8].

Definição 2.16. *Para* $A \in Div(F)$, *o inteiro*

$$i(A) = l(A) - gr(A) + g - 1$$

é chamado ***índice de especialidade*** *de* A.

O teorema de Riemann nos diz que $i(A)$ é um inteiro não negativo e que $i(A) = 0$ para $gr(A)$ suficientemente grande.

Definição 2.17. *Um adele de* F/K *é uma aplicação* $\alpha : \mathbb{P}_F \to F$, $P \mapsto \alpha_P$, *tal que* $\alpha_P \in O_P$ *para quase todo* $P \in \mathbb{P}_\mathbb{F}$.

Consideramos um adele como um elemento do produto direto $\prod_{P \in \mathbb{P}_\mathbb{F}} F$ e portanto usamos a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_\mathbb{F}}$, ou ainda, $\alpha = (\alpha_P)$.

O conjunto $\mathcal{A}_F = \{\alpha; \alpha$ é um adele de $F/K\}$ é chamado de espaço adele de F/K. Este conjunto é considerado um espaço vetorial sobre K. O adele principal de um elemento $x \in F$ é o adele cuja totalidade das componentes são iguais a x, o qual faz sentido, pois x tem no máximo finitos polos.

A definição de adele principal nos fornece um mapeamento $F \mapsto \mathcal{A}_F$, e a função valorização v_p de F/K é naturalmente extendida para $\mathcal{A}_F$ por $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a P-componente do adele α. Por definição, temos $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$.

Definição 2.18. *Para $A \in Div(F)$ definimos:*

$$\mathcal{A}_F(A) = \{\alpha \in \mathcal{A}_F; v_P(\alpha) \geq -v_P(A), \forall P \in \mathbb{P}_F$$

o K-espaço de $\mathcal{A}_F$.

Teorema 2.2. *Para cada $A \in Div(F)$, o índice de especialidades de A é dado por:*

$$i(A) = dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

Demonstração. Ver em [11, Pags. 35-36]. □

Corolário 2.1.

$$g = dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)).$$

Demonstração.

$$dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F)) = i(0) = l(0) - gr(0) + g - 1 = g$$

isto porque $l(0) = 1$ e $gr(0) = 0$. □

Podemos então escrever:

$$l(A) = gr(A) + 1 - g + dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

2.2 Códigos AG

Vamos primeiramente construir o Reed-Solomon generalizado, através de uma aplicação linear, sobre um corpo finito $\mathbb{F}_q$.

Sejam $n = q - 1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^*$, isto é, $\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^n = 1\}$. Para um inteiro k com $1 \leq k \leq n$ considere o espaço vetorial k-dimensional

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[X] | gr(f) \leq k - 1\}$$

e a aplicação avaliação, $ev : \mathcal{L}_k \to \mathbb{F}_q^n$, definida como

$$ev(f) = (f(\beta), f(\beta^2), \ldots, f(\beta^n)) \in \mathbb{F}_q^n.$$

Note que esta aplicação é $\mathbb{F}_q$-linear, isto é, que $ev(f + g) = ev(f) + ev(g)$ onde $f, g \in \mathbb{F}_q[X]$ e que $ev(\alpha f) = \alpha ev(f)$ com $\alpha \in \mathbb{F}_q$. A primeira igualdade acontece pelo fato de que em $\mathbb{F}_q[X]$ vale $(f + g)(x) = f(x) + g(x)$, portanto, basta que separemos termo a termo e reorganizemos obtendo $ev(f) + ev(g)$, já a segunda igualdade ocorre pelo fato de $(\alpha f)(x) = \alpha f(x)$, portanto colocando α em evidência concluímos que valem as duas igualdades e portanto a aplicação ev é, de fato, $\mathbb{F}_q$-linear.

Além disso a aplicação é também injetiva, isto porque um polinômio não nulo $f \in \mathbb{F}_q[X]$ de grau $< n$ possui menos que n raízes distintas. Com isso garantimos que a aplicação ev define um $[n, k]$-código

$$C_k = \{(f(\beta), f(\beta^2), \ldots, f(\beta^n)) | f \in \mathcal{L}_k\}.$$

Este código é um código de Reed-Solomon (código RS). O peso das palavras $0 \neq c = ev(f) \in C_k$ é dado por

$$\begin{aligned} \omega(c) &= n - |\{i \in \{1, \ldots, n\}; f(\beta^i) = 0\}| \\ &\geq n - gr(f) \geq n - (k - 1). \end{aligned}$$

Portanto a distância mínima d de C_k satisfaz $d \geq n + 1 - k$, por outro lado, a cota de Singleton nos garante que $d \leq n + 1 - k$ portanto $d = n + 1 - k$, sendo dessa forma um código MDS sobre $\mathbb{F}_q$.

Para introduzirmos a noção de códigos algébricos geométricos, fixaremos as seguintes notações:

- $F/\mathbb{F}_q$ é um corpo de funções algébricas de gênero g.
- $P_1, P_2, \ldots, P_n$ são lugares distintos dois a dois de $F/\mathbb{F}_q$ de grau 1.
- $D = P_1 + P_2 + \cdots + P_n$.
- G é um divisor de $F/\mathbb{F}_q$, tal que, $\text{supp}G \cap \text{supp}D = \emptyset$.

Definição 2.19. *Um código algébrico geométrico (ou código AG) $C_{\mathcal{L}}(D, G)$ associado aos divisores D e G é definido por*

$$C_{\mathcal{L}}(D, G) = \{(f(P_1), \ldots, f(P_n)) | f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Note que esta definição faz sentido, pois para $f \in \mathcal{L}(G)$ temos $v_{P_i}(f) \geq 0$ $(i = 1, \ldots, n)$, pois supp $G \cap$ supp $D = \emptyset$. A classe residual $f(P_i)$ de f módulo P_i é um elemento do corpo da classe residual de P_i. Como $gr(P_i) = 1$, esse corpo de classes residuais é $\mathbb{F}_q$, portanto $f(P_i) \in \mathbb{F}_q$.

Assim como no exemplo inicial, consideremos a aplicação avaliação $\mathbf{ev}_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ dada por

$$ev_D(x) = (x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n.$$

Esta aplicação é $\mathbb{F}_q$-linear, analogamente ao que fizemos no caso do código de Reed-Solomon e, $C_{\mathcal{L}}(D, G)$ é a imagem de $\mathcal{L}(G)$ sob esta aplicação. Veja que a construção do código de Reed-Solomon generalizado é um caso particular desta definição, escolhendo apropriadamente o corpo de funções e os divisores. O teorema a seguir nos mostrará porque estes códigos são interessantes, pois podemos calcular seus parâmetros através do Teorema de Riemann-Roch e, além disso, conseguimos obter uma cota inferior para a distância mínima.

Teorema 2.3. *$C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código com parâmetros*

$$k = l(G) - l(G - D) \text{ e } d \geq n - gr(G).$$

Demonstração. *A aplicação avaliação é linear e sobrejetiva de $\mathcal{L}(G)$ para $C_{\mathcal{L}}(D, G)$ com núcleo*

$$Nuc(ev_D) = \{f \in \mathcal{L}(G) | v_{P_i}(f) > 0 \text{ para } i = 1, \ldots, n\} = \mathcal{L}(G - D).$$

Segue do teorema do núcleo e da imagem que $k = dim C_{\mathcal{L}}(D, G) = dim \mathcal{L}(G) - dim \mathcal{L}(G-D) = l(G) - l(G-D)$. A afirmação sobre a distância mínima d faz sentido somente se considerarmos $C_{\mathcal{L}}(D, G) \neq 0$, portanto assumiremos isto. Tome um elemento $f \in \mathcal{L}(G)$ com $\omega(ev_D(f)) = d$. Então exatos $n - d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ no suporte de D são zeros de f, então

$$f \neq 0 \in \mathcal{L}(G - (P_{i_1}, \ldots, P_{i_{n-d}})).$$

Concluímos então que

$$0 \leq gr(G - (P_{i_1}, \ldots, P_{i_{n-d}})) = gr(G) - n + d$$

Portanto $d \geq n - gr(G)$.

Corolário 2.2. *Suponha que o $gr(G) < n$. Então a aplicação avaliação $ev_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D, G)$ é injetora, e temos:*

i) $C_{\mathcal{L}}(D, G)$ é um $[n, k, d]$-código com

$$d \leq n - gr(G) \text{ e } k = l(G) \geq gr(G) + 1 - g$$

. Portanto

$$k + d \geq n + 1 - g.$$

ii) Se $2g-2 < gr(G) < n$ *então* $k = gr(G) + 1 - g$.

iii) Se $\{f_1, f_2, \ldots, f_n\}$ *é uma base de* $\mathcal{L}(G)$ *então a matriz*

$$M = \begin{pmatrix} f_1(P_1) & f_1(P_2) & \ldots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \ldots & f_2(P_n) \\ \ldots & \ldots & \ddots & \ldots \\ f_n(P_1) & f_n(P_2) & \ldots & f_n(P_n) \end{pmatrix}$$

é uma matriz geradora do código $C_{\mathcal{L}}(D, G)$.

Demonstração. *A demonstração pode ser vista na página 50 em [10].*

2.3 Códigos AG sobre a curva Hermitiana

Nesta seção, iremos mostrar uma construção de códigos algébricos geométricos sobre a curva Hermitiana. Esta classe de códigos são exemplos interessantes de códigos AG, porque a curva Hermitiana é uma curva maximal, e este tipo de curva tem se mostrado fundamental para a obtenção de códigos AG com bons parâmetros, para maiores detalhes ver [10].

Primeiramente, vamos relembrar algumas propriedades do corpo de funções $\mathcal{H}$ da curva Hermitiana. $\mathcal{H}$ é o corpo de funções sobre $\mathbb{F}_{q^2}$ e pode ser representado por

$$\mathcal{H} = \mathbb{F}_{q^2}(x, y)$$

com equação afim dada por

$$y^q + y = x^{q+1}$$

O gênero de $\mathcal{H}$ é $g = q(q-1)/2$, e $\mathcal{H}$ tem $N = 1 + q^3$ lugares de grau um, sendo eles:

1. O único polo comum Q_∞ de x e y.
2. Os pares $(\alpha, \beta) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$, com isso há um único lugar $P_{\alpha,\beta} \in \mathbb{P}_H$ tal que $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.
3. $v_{Q_\infty}(x) = -(q)$ e $v_{Q_\infty}(y) = -(q+1)$.

Observe que para todo $\alpha \in \mathbb{F}_{q^2}$, existem q elementos distintos $\beta \in \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$, este número é a fibra da função traço. Portanto o número de lugares $P_{\alpha,\beta}$ é q^3.

Definição 2.20. *Para* $r \in \mathbb{Z}$ *definimos o código*

$$C_r = C_{\mathcal{L}}(D, rQ_\infty),$$

onde

$$D = \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta}$$

é a soma de todos os lugares de grau um (exceto Q_∞*) do corpo de funções Hermitiano* $\mathcal{H}/\mathbb{F}_{q^2}$*. Os códigos* C_r *são chamados códigos Hermitianos.*

Os códigos Hermitianos possuem comprimento $n = q^3$ sobre o corpo $\mathbb{F}_{q^2}$. Para $r \leq s$ nós temos, claramente, que $C_r \subseteq C_s$. Primeiramente vejamos alguns casos triviais. Para $r < 0$, $\mathcal{L}(rQ_\infty) = 0$ e consequentemente $C_r = 0$. Para $r > q^3 + q^2 - q - 2 = q^3 + (2g-2)$, o teorema 4.2 e o teorema de Riemann-Roch nos garante que

$$\begin{aligned} dim\ C_r &= l(rQ_\infty) - l(rQ_\infty - D) \\ &= (r + 1 - g) - (r - q^3 + 1 - g) = q^3 = n. \end{aligned}$$

Dessa forma, nos resta estudar o caso onde $0 \leq r \leq q^3 + q^2 - q - 2$.

Proposição 2.3. *O código dual de C_r é*

$$C_r^{\perp} = C_{q^3+q^2-q-2-r}.$$

Portanto C_r é auto-ortogonal se $2r \leq q^3+q^2-q-2$, e C_r é auto-dual para $r = (q^3+q^2-q-2)/2$.

Demonstração. *Ver em [?, Pag. 294].*

Agora vamos determinar os parâmetros de C_r. Consideremos o conjunto I dos polos de Q_∞, isto é:

$$I = \{n \geq 0 | z \in \mathcal{H}; (z)_\infty = nQ_\infty\}.$$

Para $s \geq 0$ defina

$$I(s) = \{n \in I | n \leq s\}.$$

Então $|I(s)| = l(sQ_\infty)$, e pelo teorema de Riemann-Roch

$$|I(s)| = s + 1 - q(q-1)/2$$

para $s \geq 2g - 1 = q(q-1) - 1$.

Podemos ainda descrever $I(s)$ da seguinte forma:

$$I(s) = \{n \leq s | n = iq + j(q+1) \text{ com } i \geq 0 \text{ e } 0 \leq j \leq q-1\}.$$

Portanto,

$$|I(s)| = |\{(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0 | j \leq q-1 \text{ e } iq + j(q+1) \leq s\}|.$$

Proposição 2.4. *Suponha que $0 \leq r \leq q^3 + q^2 - q - 2$. Então segue que:*

i) A dimensão de C_r é dada por

$$dim\ C_r = \begin{cases} |I(r)| & para \quad 0 \leq r < q^3 \\ q^3 - |I(s)| & para \quad q^3 \leq r \leq q^3 + q^2 - q - 2 \end{cases}$$

onde $s = q^3 + q^2 - q - 2 - r$ e $I(r) = \{n \in I | n \leq r\}$.

ii) Para $q^2 - q - 2 < r < q^3$, temos que

$$dim\ C_r = r + 1 - q(q-1)/2.$$

iii) A distância mínima d de C_r, satisfaz

$$d \geq q^3 - r$$

Demonstração. *i) Para $0 \leq r < q^3$ o corolário 4.3 nos garante que*

$$dim C_r = dim \mathcal{L}(rQ_\infty) = |I(r)|.$$

Para $q^3 \leq r \leq q^3+q^2-q-2$, temos que $s = q^3+q^2-q-2$. Então $0 \leq s \leq q^2-q-2 < q^3$. Pela proposição 4.8, obtemos:

$$dim C_r = q^3 - dim C_s = q^3 - |I(s)|.$$

ii) Para $q^2 - q - 2 = 2g - 2 < r < q^3$*, pelo corolário 4.3, temos*

$$dim C_r = r + 1 - g = r + 1 - q(q-1)/2.$$

iii) A desigualdade $d \geq q^3 - r$ *segue do teorema 4.3.*

Exemplo 2.2. *Vamos construir a matriz geradora do código Hermitiano, sobre* $\mathbb{F}_{3^2}$ *e, tomaremos* $r = 10$*. Primeiramente vamos construir a extensão* $\mathbb{F}_9$*, para isso considere o polinômio* $x^2 + x + 2 \in \mathbb{F}_3$ *irredutível, seja* α *a raíz deste polinômio, os elementos de* $\mathbb{F}_9$ *serão portanto,*

$$\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$$

Para calcularmos os pontos do corpo que pertencem a curva Hermitiana, considere o seguinte quadro com a norma e o traço de cada elemento.

Elemento	Traço	Norma
0	0	0
1	1	2
2	1	1
α	2	1
$\alpha+1$	1	0
$\alpha+2$	2	2
2α	2	2
$2\alpha+1$	2	1
$2\alpha+2$	1	0

A curva hermitiana é definida por

$$y^q + y = x^{q+1}$$

. Portanto queremos $(x, y) \in \mathbb{F}_{3^2}^2$ *tal que* $y^q + y = x^{q+1}$*, isto é equivalente a encontrarmos elementos cujos traço e norma são iguais.*

Dessa forma os pontos da curva são:

$$\begin{aligned}\mathcal{H} \;=\; & \{(0,0);(0,\alpha+1);(0,2\alpha+2);(1,2);(1,\alpha);(1,2\alpha+1);(2,2);(2,2\alpha+1);(2,\alpha);\\ & (\alpha,1);(\alpha,\alpha+2);(\alpha,2\alpha);(\alpha+1,2);(\alpha+1\alpha);(\alpha+1,2\alpha+1);(\alpha+2,1);(\alpha+2,\alpha+2);\\ & (\alpha+2,2\alpha);(2\alpha,1);(2\alpha,\alpha+2);(2\alpha,2\alpha);(2\alpha+1,1);(2\alpha+1,\alpha+2);(2\alpha+1,2\alpha);\\ & (2\alpha+2,2);(2\alpha+2,\alpha);(2\alpha+2,2\alpha+1)\} \cup \{P_\infty = (0:1:0)\}\end{aligned}$$

Devemos agora calcular o espaço de Riemann-Roch:

$$\mathcal{L}(10P_\infty) = \{f \in \mathbb{F}_q(X,Y) : (f) + 10Q_\infty \geq 0\}$$

Utilizando as propriedades da valorização, obtemos o seguinte conjunto:

$$\mathcal{L}(10P_\infty) = \{1, x, y, x^2, y^2, xy, x^3, x^2y\}$$

Então, basta que apliquemos os pontos da curva nas funções encontradas. Considere o conjunto $\mathcal{H}$ *como um conjunto ordenado dos pontos da curva:*

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & \dots & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & \dots & 2\alpha+1 & 2\alpha+1 & 2\alpha+2 & 2\alpha+2 & 2\alpha+2 \\ 0 & \alpha+1 & 2\alpha+2 & 2 & \alpha & \dots & \alpha+2 & 2\alpha & 2 & \alpha & 2\alpha+1 \\ 0 & 0 & 0 & 1 & 1 & \dots & 2\alpha+2 & 2\alpha+2 & 2 & 2 & 2 \\ 0 & \alpha+1 & 2\alpha+2 & 2 & \alpha & \dots & \alpha+2 & 2\alpha & 2 & \alpha & 2\alpha+1 \\ 0 & 0 & 0 & 2 & \alpha & \dots & \alpha+1 & 1 & \alpha+1 & \alpha+2 & \alpha \\ 0 & 0 & 0 & 1 & 1 & \dots & \alpha & \alpha & \alpha+1 & \alpha+1 & \alpha+1 \\ 0 & 0 & 0 & 2 & \alpha & \dots & 2\alpha & 2\alpha+1 & 1 & 2\alpha & \alpha+2 \end{pmatrix}$$

A matriz G é a Matriz Geradora do código Hermitiano sobre o corpo $\mathbb{F}_{3^2}$ com $r = 10$. Podemos também explicitar um intervalo para a distância mínima do código construído acima através das seguintes desigualdades vistas anteriormente:

$$\begin{array}{rcl} d & \leq & n - gr(G) \\ d & \geq & q^3 - r. \end{array}$$

Como $n = 27$, $gr(G) = q + 1 = 4$, $q^3 = 3^3 = 27$ e $r = 10$, temos:

$$17 \leq d \leq 23.$$

Capítulo 3

Códigos Geométricos de Goppa Aprimorados

Neste capítulo estudamos as construções feitas nos artigos [2], [1] e [3].

3.1 Construção

Seja $\mathbb{F}_q$ o corpo finito com $q = p^r$ elementos, onde $r \in \mathbb{Z}$ com $r \geq 1$ e p é um primo. Sejam também $\mathbb{F}_q^m$ o m-espaço dimensional afim sobre $\mathbb{F}_q$ e seus pontos racionais são escritos na forma $(x_m, x_{m-1}, \ldots, x_2, x_1)$,com $x_k \in \mathbb{F}_q$, para $k = 1, \ldots, m$. Seja $S := \{f_1, f_2, \ldots, f_t\}$ um conjunto de polinômios irredutíveis de m variáveis sobre $\mathbb{F}_q$. Seja $LS := \{P_1, P_2, \ldots, P_n\}$, o conjunto das raízes dos polinômios de S, LS é chamado *conjunto de localização*. Dado um conjunto de localização LS, cada monômio ou polinômio f é associado à uma n-upla $(f(P_1), f(P_2), \ldots, f(P_n))$, este vetor é chamado de vetor de valorização de f em LS. Iremos utilizar os termos monômios ou polinômios para nos referirmos ao seu vetor de valorização correspondente. O monômio $f.g$ e o polinômio $f + g$ são associados aos vetores de valorização, respectivamente:

$$(f(P_1) \cdot g(P_1), f(P_2) \cdot g(P_2), \ldots, f(P_n) \cdot g(P_n)),$$

$$(f(P_1) + g(P_1), f(P_2) + g(P_2), \ldots, f(P_n) + g(P_n)).$$

Dizemos que um monômio $g = x_m^{i_m} \ldots x_1^{i_1}$ é não-degenerado se $i_j < q$, para todo $j = 1, \ldots, m$, caso contrário, dizemos que ele é um monômio degenerado [3].

Definiremos o peso de um monômio baseado apenas no conjunto de localização LS. Cada variável x_μ será associado a um inteiro $w(x_\mu)$, o qual será chamado *peso* de x_μ. Definimos

$$w(x_m^{i_m} \ldots x_1^{i_1}) = \sum_{\mu=1}^{m} i_\mu w(x_\mu).$$

Claro que $w(1) = 0$.

Os pesos $w(x_\mu)$ para $1 \leq \mu \leq m$ devem ser consistentes, isto é, para cada equação contendo todos os pontos de LS, devem haver ao menos dois monômios com o mesmo peso maximal.

Exemplo 3.1. *Considere a curva $x_2^3 x_1 + x_1^3 + x_2 = 0$, se $w(x_2) = 2$ e $w(x_1) = 3$, então esta equação possui dois monômios com o mesmo peso maximal:*

$$w(x_2^3 x_1) = 9 = w(x_1^3).$$

Portanto os pesos são consistentes.

Exemplo 3.2. *Considere a curva dada pela equação* $x_3^2 + x_2^2 + x_1^8 + x_2^2 x_3 = 0$ *e defina os pesos* $w(x_3) = 4$, $w(x_2) = 2$ *e* $w(x_1) = 1$. *Veja que*

$$w(x_3^2) = w(x_1^8) = w(x_2^2 x_3) = 8.$$

Dessa forma os pesos são consistentes.

Podemos resumir as condições para que os pesos sejam consistentes da seguinte forma: Suponha que todos os pontos de LS satisfaçam a equação abaixo

$$\sum_{s=1}^{h} \sum_{\nu=1}^{\lambda_s} a_{s,\nu} g_{s,\nu} = 0,$$

onde $a_{s,\nu} \in \mathbb{F}_q$, $g_{s,\nu+1}$ é um fator de $g_{s,\nu}$ e

$$g_{s,\nu} = \prod_{\mu=1}^{m} x_\mu^{i_{s,\nu,\mu}}.$$

Então, entre os seguintes pesos

$$\sum_{\mu=1}^{m} i_{1,1,\mu} w(x_\mu), \sum_{\mu=1}^{m} i_{2,1,\mu} w(x_\mu), \ldots, \sum_{\mu=1}^{m} i_{h,1,\mu} w(x_\mu)$$

existem pelo menos dois termos com o mesmo valor maximal.

Os exemplos a seguir ilustram as definições acima.

Exemplo 3.3. *Considere a equação*

$$x^3 + x^2 + x + x^2 y^4 + xy^2 + y^4 + y^3 + y = 0$$

sobre $\mathbb{F}_4$.

Nesta equação, os termos x^2 *e* x *são fatores de* x^3, *além disso,* xy^2, y^3, y, y^4 *são fatores de* x^2y^4. *Portanto existem dois termos,* x^3 *e* x^2y^4 *com o mesmo peso maximal. Temos então que,* $3w(x) = 2w(x) + 4w(y)$. *Resolvendo a equação para* $w(x)$ *e* $w(y)$, *encontramos* $w(x) = 4$ *e* $w(y) = 1$ *satisfazendo as condições vistas acima.*

Exemplo 3.4. *Considere as seguintes equações*

$$\begin{cases} x_3^3 + x_2^2 + x_2 &= 0 \\ x_2^3 + x_1^2 + x_1 &= 0. \end{cases}$$

Entre os polinômios da primeira equação, devemos ter ao menos dois que possuam o mesmo peso maximal. Então $3w(x_3)$ *e* $2w(x_2)$ *devem ser iguais, logo,* $3w(x_3) = 2w(x_2)$. *De forma análoga, da segunda equação devemos ter que* $3w(x_2) = 2w(x_1)$.

Das equações acima, concluimos que $w(x_1) = 9$, $w(x_2) = 6$ *e* $w(x_3) = 4$, *satisfazendo as condições necessárias acima, para termos pesos consistentes.*

A seguir definimos uma ordem lexicográfica de monômios, referida como a ordem total de monômios.

Definição 3.1. *Considere os monômios* $x_m^{i_m} \ldots x_1^{i_1}$, $x_m^{j_m} \ldots x_1^{j_1}$.

Dizemos que $x_m^{i_m} \ldots x_1^{i_1} <_t x_m^{j_m} \ldots x_1^{j_1}$ *se:*

i) $w(x_m^{i_m} \ldots x_1^{i_1}) < w(x_m^{j_m} \ldots x_1^{j_1})$ *ou*

ii) $w(x_m^{i_m} \ldots, x_1^{i_1}) = w(x_m^{j_m} \ldots x_1^{j_1}), i_\mu = j_\mu$ *para* $1 \leq \mu \leq \nu - 1$ *e* $i_\nu < j_\nu$

Exemplo 3.5. *Considere os mônomios* $x_3^3 x_2 x_1^2$ *e* $x_2^3 x_1^2$ *nas variáveis* x_1, x_2 *e* x_3. *Sejam* $w(x_3) = 2$, $w(x_2) = 3$ *e* $w(x_1) = 4$. *Note que*

$$w(x_3^3 x_2 x_1^2) = w(x_2^3 x_1^2) = 17, i_2 < j_2$$

Então $x_3^3 x_2 x_1^2 <_t x_2^3 x_1^2$.

Dado um conjunto S, seja $H = \{h_1, h_2, \ldots, h_n\}$ a sequência de todos os monômios não-degenerados, linearmente independentes módulo S, ordenados com a ordem total.

Exemplo 3.6. *Considere a curva dada pela equação* $y^3 + x^2 + x = 0$ *sobre* $\mathbb{F}_4$ *e defina* $w(x) = 3$ *e* $w(y) = 2$. *Note que* $x^3 \notin H$, *pois* $x^3 = y^3 x + x^2$, *onde* $y^3 x <_t x^3$ *e* $x^2 <_t x^3$, *portanto* x^3 *é linearmente dependente módulo* S.

Definimos o conjunto

$$W = \{w(h_1), w(h_2), \ldots, w(h_n)\},$$

onde $w(h_i) \leq w(h_{i+1})$.

Denotamos $h_{i,j}$ o monômio não-degenerado produto de h_i por h_j, utilizando a relação $x_\mu^q = x_\mu$, ou seja, $h_{i,j} := h_i \cdot h_j$.

O lema a seguir nos permite calcular o peso de $h_{i,j}$.

Lema 3.1. *Sejam* $h_i = x_m^{i_m} \ldots x_1^{i_1}$ *e* $h_j = x_m^{j_m} \ldots x_1^{j_1}$. *Então*

$$w(h_{i,j}) = w(h_i) + w(h_j) - (q-1) \sum w(x_\mu),$$

onde o somatório é feito por todos os μ, *tal que,* $i_\mu + j_\mu \geq q$.

Demonstração. *Sejam* $h_i = x_m^{i_m}, \ldots, x_1^{i_1}$ *e* $h_j = x_m^{j_m}, \ldots, x_1^{j_1}$, *então*

$$\begin{aligned} h_{i,j} &= (x_m^{i_m}, \ldots, x_1^{i_1}).(x_m^{j_m}, \ldots, x_1^{j_1}) \\ &= (x_m^{i_m + j_m}, \ldots, x_1^{i_1 + j_1}). \end{aligned}$$

Se $i_\mu + j_\mu < q$ *então* $w(x_\mu^{i_\mu + j_\mu}) = (i_\mu + j_\mu) w(x_\mu) = i_\mu w(x_\mu) + j_\mu w(x_\mu)$.
Se $i_\mu + j_\mu \geq q$, *então temos que* $i_\mu + j_\mu - q > 0$, *portanto podemos escrever*

$$\begin{aligned} x_\mu^{i_\mu + j_\mu} &= x_\mu^{i_\mu + j_\mu + q - q} \\ &= x_\mu^q x_\mu^{i_\mu + j_\mu - q} \\ &= x_\mu x_\mu^{i_\mu + j_\mu - q}. \end{aligned}$$

Assim temos que

$$\begin{aligned} w(x_\mu^{i_\mu + j_\mu}) &= w(x_\mu x_\mu^{i_\mu + j_\mu - q}) \\ &= w(x_\mu) + w(x_\mu^{i_\mu + j_\mu - q}) \\ &= w(x_\mu^{i_\mu + j_\mu}) + w(x_\mu^{-q}) + w(x_\mu) \\ &= (i_\mu + j_\mu) w(x_\mu) - q w(x_\mu) + w(x_\mu) \\ &= i_\mu w(x_\mu) + j_\mu w(x_\mu) - (q-1) w(x_\mu). \end{aligned}$$

Portanto, $w(h_{i,j}) = w(h_i) + w(h_j) - (q-1) \sum w(x_\mu)$ *onde o somatório é feito por todos os* μ, *tal que,* $i_\mu + j_\mu \geq q$.

Exemplo 3.7. *Considere dois monômios linearmente independentes* $h_i = x_2^5 x_1^2$ *e* $h_j = x_2^4 x_1^3$ *sobre* $\mathbb{F}_8$. *Neste caso* $i_2 + j_2 = 9 > 8 = q$. *Além disso*

$$h_i \cdot h_j = x_2^5 x_1^2 \times x_2^4 x_1^3 = x_2^9 x_1^5 = x_2^2 x_1^5 := h_{i,j}.$$

Então,

$$w(h_{i,j}) = w(x_2^2 x_1^5) = 2w(x_2) + 5w(x_1).$$

Por outro lado,

$$\begin{aligned} w(h_i) + w(h_j) &= 5w(x_2) + 2w(x_1) + 4w(x_2) + 3w(x_1) \\ &= 9w(x_2) + 5w(x_1). \end{aligned}$$

Dessas duas expressões acima, observe que

$$w(h_{i,j}) = w(h_i) + w(h_j) - 7w(x_2)$$

como visto no Lema 3.1.

Seja $L(\underline{r})$ o espaço linear sobre $\mathbb{F}_q$ gerado pelos r primeiros monômios de H. Pela construção de h_{r+1} segue que

$$h_{r+1} \in L(\underline{r+1}) - L(\underline{r}).$$

Se um monômio $h \in L(\underline{r+1}) - L(\underline{r})$ e $w(h) = w(h_{r+1})$, dizemos que os monômios h e h_{r+1} são consistentes e denotamos $h \sim h_{r+1}$.

Considere as variáveis u, v, i, j, tais que $1 \leq u \leq i$, $1 \leq v \leq j$ e $u + v < i + j$.

Essas condições podem ser representadas de forma simplificada por $(u, v) < (i, j)$.

Definição 3.2. *Seja* $h_{i,j}$ *um monômio tal que*

$$w(h_i) + w(h_j) \leq W_m := w(h_n)$$

e $h_{i,j} \sim h_{r+1}$. *Se para todo* $(u, v) < (i, j)$ *e* $r' < r + 1$, *temos que*

$$h_{u,v} \in L(\underline{r'}) - L(\underline{r' - 1}),$$

então $h_{i,j}$ *é chamado termo bem-comportado de* H *ou também chamado termo bem-comportado consistente com* h_{r+1}.

Mostraremos a seguir que o número de termos bem-comportados consistentes com h_{r+1} é um parâmetro muito importante. O conceito introduzido aqui, ajuda a gerar mais termos bem-comportados para a construção de sequências com tais monômios.

Definição 3.3. *Seja* H *uma sequência de* **n** *monômios linearmente independentes. Se para cada monômio* $h_{i,j}$, *tal que*

$$w(h_i) + w(h_j) \leq W_m := w(h_n)$$

tivermos

$$h_{i,j} \in L(\underline{r+1}) - L(\underline{r}).$$

E $h_{r+1} <_t h_{i,j}$ *ou* $w(h_{r+1}) = w(h_{i,j})$, *então* H *é chamada sequência bem comportada do conjunto de localização LS.*

Estaremos interessados apenas em sequências bem-comportadas.

Teorema 3.1. *Seja* H *uma sequência de* n *monômios linearmente independentes ordenados com a ordem total, então* H *é uma sequência bem-comportada.*

Demonstração. *Seja $h_{i,j}$ um monômio tal que*

$$w(h_i) + w(h_j) \leq W_m := w(h_n)$$

e

$$h_{i,j} \in L(\underline{r+1}) - L(\underline{r}).$$

Primeiramente temos que $h_{i,j} \in H^{'}$. Temos também que $h_{i,j}$ é linearmente dependente aos seus monômios prévios ou $h_{i,j} = h_{r+1}$, pois $h_{i,j} \in L(\underline{r+1}) - L(\underline{r})$.

Se $h_{i,j} = h_{r+1}$ então $w(h_{i,j}) = w(h_{r+1})$, por outro lado, se $h_{i,j}$ for linearmente dependente aos seus monômios prévios, pela ordem definida em $H^{'}$ e pelo fato de $h_{i,j}$ ser linearmente dependente a h_{r+1} (pois está em $L(\underline{r+1}) - L(\underline{r})$) temos que $h_{r+1} <_t h_{i,j}$.

O exemplo abaixo ilustrará as definições dadas acima.

Exemplo 3.8. *Seja LS as raízes da seguinte superfície em um espaço tridimensional afim:*

$$x_3 + x_2x_1 = 0 \quad \textit{sobre} \quad \mathbb{F}_4.$$

Defina $w(x_3) = 2$ e $w(x_2) = w(x_1) = 1$. Construindo H e W como definidos acima, temos os seguintes conjuntos

$$H = \{1, x_2, x_1, x_3, x_2^2, x_1^2, x_3x_2, x_2^3, x_3x_1, x_1^3, x_3^2, x_3x_2^2, x_3x_1^2, x_3^2x_2, x_3^2x_1, x_3^3\}$$

$$W = \{0, 1, 1, 2, 2, 2, 3, 3, 3, 3, 4, 4, 4, 5, 5, 6\}.$$

Considere a seguinte representação matricial, onde em cada coordenada (i, j) estarão os elementos $h_{i,j} = h_i \cdot h_j$. Cada monômio $h_{i,j}$ será representado por um vetor (abc) que denotam $x_3^a x_2^b x_1^c$.

(000)	(010)	(001)	(100)	(020)	(002)	(110)	(030)	...
(010)	(020)	(011)	(110)	(030)	(012)	...		
(001)	(011)	(002)	(101)	(021)	...			
(100)	(110)	(101)	(200)	...				
(020)	(030)	(021)	...					
(002)	(012)	...						
(110)	...							

Note que pela equação da superfície temos que

$$h_{2,3} = (011) = h_4, h_{2,2} = (020) = h_5$$

e como $(2, 2) < (2, 3)$, segue pela Definição 3.2, que o monômio $h_{2,3}$ não é um termo bem-comportado. É fácil ver que a sequência H está definida com a ordem total, e seus monômios são linearmente independentes, então pelo Teorema 3.1, H é uma sequência bem-comportada. Além disso, note que $h_{2,3} = (011) = h_4$ e pela ordem total, temos que $h_4 <_t h_{2,3}$.

Dada uma sequência H bem-comportada construída sobre um conjunto LS, podemos definir um código linear da seguinte forma.

Sejam as matrizes,

$$H_r := \begin{bmatrix} \overrightarrow{h_1} \\ \overrightarrow{h_2} \\ \vdots \\ \overrightarrow{h_r} \end{bmatrix} \quad e \quad H_r^* := \begin{bmatrix} H_r \\ \overrightarrow{h_{v_1}} \\ \vdots \\ \overrightarrow{h_{v_l}} \end{bmatrix}$$

onde $\overrightarrow{h_i} = (h_i(P_1), h_i(P_2), \ldots, h_i(P_n))$, para $1 \leq i \leq r$ e $r+1 < v_1 < \cdots < v_l$. Temos que H_r^* será a matriz teste de paridade de um código $C_r \subset \mathbb{F}_{q^n}$, estes códigos serão chamados Códigos Geométricos de Goppa Aprimorados (GGA-códigos). Note que se $l = 0$, temos que $H_r = H_r^*$ será a matriz teste de paridade do código Geométrico de Goppa usual.

Iremos a partir de agora descrever um método simples para determinar a distância mínima de um código linear definido por H_r^*.

Definição 3.4. *Seja* $\mathbf{r}$ *um vetor recebido,* $\mathbf{c}$ *uma palavra de* C_r *e* $\mathbf{e}$ *o vetor erro. Temos então que* $\mathbf{r} = \mathbf{c} + \mathbf{e}$. *Defina as seguintes síndromes:*

$$s_i = \overrightarrow{h_i} \cdot \mathbf{r}^t \qquad e \qquad S_{i,j} = \overrightarrow{h_{i,j}} \cdot \mathbf{r}^t.$$

Pela definição de C_r, temos

$$s_i = \overrightarrow{h_i} \cdot \mathbf{e}^t, \qquad para\ i = 1, 2, \ldots, r, v_1, \ldots, v_l$$

e

$$S_{i,j} = \overrightarrow{h_{i,j}} \cdot \mathbf{e}^t, \qquad se\ h_{i,j} \in L(\underline{r}, v_1, \ldots, v_l).$$

Dizemos que s_i para $i = 1, 2, \ldots, r$ e $S_{i,j}$ para $h_{i,j} \in L(\underline{r})$ são *síndromes primitivas conhecidas*. Além disso, s_i para $i = v_1, \ldots, v_l$ e $S_{i,j}$ para $h_{i,j} \in L(\underline{r}, v_1, \ldots, v_l)$ e $h_{i,j} \notin L(\underline{r})$ são chamadas *síndromes suplementares conhecidas*.

Quando $e = \vec{0}$, as síndromes conhecidas são iguais a 0. Qualquer outra síndrome é chamada *síndrome desconhecida*.

Como $h'_{r+1} \notin L(\underline{r})$ e $h'_{r+1} \in L(\underline{r+1})$, isto é, h_{r+1} e h'_{r+1} são consistentes, temos que s_{r+1} e $s'_{r+1} := h'_{r+1} \cdot \mathbf{r}^t$ também são consistentes, ou seja, s'_{r+1} é uma síndrome consistente de s_{r+1} ou somente *síndrome consistente*. Podemos escrever s'_{r+1} da seguinte forma:

$$s'_{r+1} = \sum_{i=1}^{r+1} a_i s_i,$$

onde $a_{r+1} \neq 0$.

Com estas definições temos o seguinte Lema.

Lema 3.2. *Se* $s_i = 0$ *para* $1 \leq i \leq r+1$, *então* $s'_{r+1} = 0$. *Se* $s_i = 0$ *para* $1 \leq i \leq r$, *e* $s_{r+1} \neq 0$, *então* $s'_{r+1} \neq 0$.

Demonstração. *O resultado segue diretamente da Definição de* s'_{r+1}.

Para obtermos resultados importantes sobre os códigos que iremos construir, serão necessárias algumas definições adicionais.

Definição 3.5. *Seja*

$$W_{n\times n} = (w_{i,j}),$$

onde $w_{1,v} = w_{v,1} = w(h_v)$ *e* $w_{i,j} = w_{i,1} + w_{1,j}$. *Sejam também,*

$$H_{n\times n} = (h_{i,j})_{n\times n},$$

e

$$S_{n\times n} = (S_{i,j})_{n\times n} \quad e \quad S^{\overline{r+1}} = (S_{i,j})_{1\leq i\leq r+1, 1\leq j\leq r+1}.$$

Definição 3.6. *Definimos* $N(h_r) = N_r$ *como o número de* $h_{i,j}$ *bem-comportados, consistentes com* h_r.

Segue da definição de H, o seguinte resultado:

Lema 3.3. *Em $H_{n\times n}$, se $h_{i,j} \sim h_r$ e $h_{i,j}$ é bem comportado, então para todo $(u,v) < (i,j)$, temos que $h_{u,v} \in L(\underline{r})$.*

Demonstração. *A demonstração segue das Definições 3.2 e 3.5.*

Com isto, veremos os resultados a respeito da distância mínima dos códigos que iremos construir.

Teorema 3.2. *Seja* **r** *igual a palavra do código $c := (c_1, c_2, \ldots, c_n)$. Se $s_{r+1} \neq 0$, então*

$$w(c) \geq N_{r+1}.$$

Demonstração. *Temos que*

$$S^{\overline{(r+1)}} = \begin{pmatrix} S_{1,1} & S_{1,2} & \ldots & S_{1,r+1} \\ S_{2,1} & S_{2,2} & \ldots & S_{2,r+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{r+1,1} & S_{r+1,2} & \ldots & S_{r+1,r+1} \end{pmatrix} = \begin{pmatrix} h_{1,1}\cdot c^t & h_{1,2}\cdot c^t & \ldots & h_{1,r+1}\cdot c^t \\ h_{2,1}\cdot c^t & h_{2,2}\cdot c^t & \ldots & h_{2,r+1}\cdot c^t \\ \vdots & \vdots & \ddots & \vdots \\ h_{r+1,1}\cdot c^t & h_{r+1,2}\cdot c^t & \ldots & h_{r+1,r+1}\cdot c^t \end{pmatrix}.$$

Como $H_r^* \cdot c^t = \vec{0}$, então $s_i = 0$ para todo $1 \leq i \leq r$ e $i = v_1, \ldots, v_l$. Por hipótese temos que $s_{r+1} \neq 0$, dessa forma, pelo Lema 3.2, $s'_{r+1} \neq 0$. Portanto existem N_{r+1} polinômios consistentes e bem comportados com s_{r+1} não nulos e suas síndromes consistentes nas coordenadas (i,j), com $w_{i,j} = w(h_{r+1})$.

Pelo Lema 3.3, para todo $(u,v) < (i,j)$, temos que $h_{u,v} \in L(\underline{r})$, isto é, $S_{u,v} = 0$. Dessa forma, $posto(S^{\overline{(r+1)}}) \geq N_{r+1}$.

Podemos decompor a matriz $S^{\overline{(r+1)}} = XYX^t$, onde X e Y são as matrizes abaixo:

$$X = \begin{bmatrix} h_1(P_1) & h_1(P_2) & \ldots & h_1(P_n) \\ h_2(P_1) & h_2(P_2) & \ldots & h_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ h_r(P_1) & h_r(P_2) & \ldots & h_r(P_n) \\ h_{r+1}(P_1) & h_{r+1}(P_2) & \ldots & h_{r+1}(P_n) \end{bmatrix} \qquad Y = \begin{bmatrix} c_1 & 0 & \ldots & 0 \\ 0 & c_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & c_n \end{bmatrix}.$$

Dessa forma, como $posto(S^{\overline{(r+1)}}) = posto(XYX^t) = min\{posto(X), posto(Y), posto(X^t\}$, então $posto(Y) \geq N_{r+1}$, e assim, $w(c) \geq N_{r+1}$.

Como $H_r^* \cdot c^t = \vec{0}$, então $s_i = 0$ para todo $1 \leq i \leq r$ e $i = v_1, \ldots, v_l$. Por hipótese temos que $s_{r+1} \neq 0$, dessa forma, pelo Lema 3.2, $s'_{r+1} \neq 0$. Portanto existem N_{r+1} polinômios consistentes e bem comportados com s_{r+1} não nulos e suas síndromes consistentes nas coordenadas (i,j), com $w_{i,j} = w(h_{r+1})$.

Pelo Lema visto anteriormente, para todo $(u,v) < (i,j)$, temos que $h_{u,v} \in L(\underline{r})$, isto é, $S_{u,v} = 0$. Dessa forma, $posto(S^{\overline{(r+1)}}) \geq N_{r+1}$.

Segue portanto, um importante resultado que irá nos dar uma cota inferior para a distância mínima dos GGA-códigos.

Teorema 3.3. *Seja H_r^* a matriz teste de paridade de um código linear C_r. Se $N_v \geq N_{r+1}$ para $r < v \leq n$ e $v \neq v_1, v_2, \ldots, v_l$ então C_r tem distância mínima maior igual a N_{r+1}.*

Demonstração. *Seja $c \in C_r$ uma palavra não nula, se $s_{r+1} \neq 0$, então pelo Teorema 3.2 temos que $w(c) \geq N_{r+1}$. Se $s_{r+1} = 0$ então existe um valor minimal p, onde $r \leq p < n$, tal que $s_u = 0$ para $1 \leq u \leq p$ e $s_{p+1} \neq 0$. Dessa forma, c é uma palavra dos códigos $C_{r+1}, \ldots, C_p$. Portanto, como $s_{p+1} \neq 0$ e $N_v \geq N_{r+1}$ para $r < v \leq n$ e $v \neq v_1, \ldots, v_l$, segue pelo Teorema 3.2, que $w(c) \geq N_v \geq N_{r+1}$. Portanto a distância mínima de C_r é maior igual a N_{r+1}.*

Se $l = 0$ podemos escrever o Teorema 3.3 da seguinte forma:

Teorema 3.4. *Seja $H_r^* = H_r$ a matriz teste de paridade de um código linear C_r. Então a distância mínima d_r^* de C_r é maior igual a $min\{N_v | r < v \leq n\}$.*

Usando este resultado temos uma cota inferior para a distância mínima de códigos geométricos sem a utilização do Teorema de Riemann-Roch. Veremos nos exemplos a seguir que em alguns casos as cotas inferiores obtidas pelos resultados mostrados até aqui, são melhores que as obtidas por meio do Teorema de Riemann-Roch aplicado nos códigos AG.

Veremos então a construção dos códigos geométricos de Goppa aprimorados, baseados em sequências bem comportadas de monômios.

Construção 3.1. *Dada uma distância mínima d, seja $\{1, 2, \ldots, r, v_1, \ldots, v_l\}$ um subconjunto de $\{1, 2, \ldots, n\}$, tal que*

1) Para $0 \leq k < r$, $N_k < d$ e $N_{r+1} \geq d$;

2) Para $r + 1 < h \leq n$, se $N_h < d$, então $h \in \{v_1, \ldots, v_l\}$.

Este código terá parâmetros $[n, n-r-l, \geq d]$ e será chamado Código Geométrico de Goppa Aprimorado (GGA-código).

3.2 GGA-códigos sobre a curva de Klein

Seja a familia de curvas definida sobre $\mathbb{F}_q$ dada por

$$x^a y^c + y^{b+c} + f(x, y) = 0 \tag{3.1}$$

onde $mdc(a, b) = 1$ e $gr(f(x, y)) < min(a, b)$.

Pelo Teorema de Riemann-Roch, a distância mínima d de um AG código é dado por $d \geq r - g + 1$, onde g é o gênero da curva. Em [1] vemos que o gênero desta família de curvas é dado por $g = \frac{1}{2}(a-1)(b-1) + (a+1)c$.

Para que tenhamos pesos consistentes, considerando a equação acima, observe que $w(x^a y^c) = w(y^{b+c})$, com isso, temos que

$$\begin{gathered} w(x^a y^c) = w(y^{b+c}) \\ w(x^a) + w(y^c) = w(y^{b+c}) \\ aw(x) + cw(y) = bw(y) + cw(y) \\ aw(x) = bw(y) \end{gathered}$$

como $mdc(a, b) = 1$, devemos tomar $w(x) = b$ e $w(y) = a$.

Pelo feito acima,podemos construir GGA-códigos sobre curvas com equação 3.1, mas nesta seção estudaremos um caso particular, que é a curva de Klein, definida sobre $\mathbb{F}_8$ pela equação:

$$x^3 y + y^3 + x = 0.$$

Note que o gênero da curva de Klein é 3. Devemos tomar $w(x) = 2$ e $w(y) = 3$. Defina primeiramente $x = x_1$ e $y = x_2$. Logo a equação da curva sobre $\mathbb{F}_8$ será:

$$x_1^3x_2 + x_2^3 + x_1 = 0. \tag{3.2}$$

Devemos agora construir a sequência H ordenada usando a ordem total. Primeiramente sabemos que todos os monômios da forma $y^{i_2}x^{i_1}$ (ou então $x_2^{i_2}x_1^{i_1}$), $i_1 \geq 8$ e $i_2 \geq 8$ não estarão em H, pois são monômios degenerados. Além disso, devemos verificar, utilizando a equação da curva, quais monômios são linearmente dependentes a outros, construindo assim a sequência H.

Note que,

$$\begin{array}{ccc} x_2x_1^3 = x_2^3 + x_1; & x_2^6x_1 = x_1^3 + x_2^2; & x_2^6x_1^2 = x_1^4 + x_2^2x_1 \\ x_2^5x_1 = x_1^5 + x_2^2x_1^2 + x_2; & x_2^5x_1^2 = x_1^6 + x_2^4; & x_2^7 = x_1^7. \end{array}$$

Obtemos então que a sequência H é dada por,

$$H = \{1, x_1, x_2, x_1^2, x_2x_1, x_2^2, x_1^3, x_2x_1^2, x_2^2x_1, x_1^4, x_2^3, x_2^2x_1^2, x_1^5, x_2^3x_1, x_2^4, x_1^6, x_2^3x_1^2, x_2^4x_1, x_1^7, x_2^5, x_2^4x_1^2, x_2^6\},$$

e assim, $|H| = 22$. Devemos agora calcular os pesos dos monômios de H para construirmos a sequência de pesos W, que será dada por:

$$W = \{0, 2, 3, 4, 5, 6, 6, 7, 8, 8, 9, 10, 10, 11, 12, 12, 14, 14, 15, 16, 18\}.$$

E por fim, construímos a sequência N, formada pelo número de monômios consistentes $h_{i,j}$ a cada monômio $h_r \in H$. Para isso iremos utilizar a matriz síndrome, que será composta por entradas da forma i_2i_1, onde $x_2^{i_2}x_1^{i_1}$, assim o monômio $x_2^4x_1$ será representado por 41 ou então $h_{1,2} = h_1\dot{h}_2 = x_1x_2$ será representado por 11.

Vejamos então. a representação de uma parte da matriz síndrome:

00	01	10	02	11	20	03	12	21	04	30	22	05	31	40	06	32
01	02	11	03	12	21	04	13	22	05	31	23	06	32	41	07	...
10	11	20	12	21	30	13	22	31	14	40	32	15	41	50	...	
02	03	12	04	13	22	05	14	23	06	32	24	07	33	...		
11	12	21	13	22	31	14	23	32	15	41	33	16	...			
20	21	30	22	31	40	23	32	41	24	50	42	...				
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	...					

Para calcularmos $N(h_r)$ através da matriz síndrome, devemos considerar todo elemento (u, v) da matriz, tal que, $1 \leq u, v \leq r$ que possuí o mesmo peso de h_r e que seja bem-comportado.

Calculemos portanto $N_5 = N(h_5)$, devemos então olhar para a sub-matriz:

00	01	10	02	11
01	02	11	03	12
10	11	20	12	21
02	03	12	04	13
11	12	21	13	22

Neste caso, $N_5 = 4$, pois existem 4 $h_{i,j}$ consistentes com h_5, sendo eles $h_{5,1}, h_{1,5}, h_{3,2}$ e $h_{2,3}$. Realizando este cálculo para todos os monômios de H, temos a seguinte sequência N:

$$N = \{1, 2, 2, 3, 4, 3, 4, 6, 6, 5, 8, 9, 6, 10, 11, 7, 12, 13, 8, 14, 15, 17\}.$$

Após construirmos a sequência N, podemos utilizar a Construção 3.1 para obtermos a matriz teste de paridade H_r do código linear C_r.

Suponha que queiramos construir um GGA-código com parâmetros $n = 22$ e $d = 3$ sobre $\mathbb{F}_8$. Logo, temos que $N_1, N_2, N_3 < 3$, $N_4 = 3$ e $N_k \geq 3$ para todo $4 < k \leq n$. Dessa forma temos que $H_3^* = (1, x, y)^T$ é a matriz que define um GGA-código com parâmetros $[22, 19, 3]$. Para obtermos um AG código com o mesmo comprimento e a mesma distância mínima, utilizando como divisores $G = 10(1:0:0)+10(0:0:1)$ e D os outros pontos da curva de Klein homogeinizada, seus parâmetros seriam $[22, 18, 3]$. Observamos que a dimensão é menor e, portanto, teríamos menos palavras no código, fazendo com que o resultado obtido pela Construção 3.1 melhore a construção usual para a distância mínima 3 e comprimento 22.

Para construirmos um GGA-código com parâmetros $n = 22$ e $d = 6$ sobre $\mathbb{F}_8$, observe que teríamos $N_1, N_2 \ldots, N_7 < 6$, $N_8 = N_9 = 6$ e $N_{10} < 6$ e todos os outros valores de N_k são maiores que 6, portanto, temos $r = 7$, $l = 1$ e $v_l = 10$. Dessa forma, temos que $H_7^* = (1, x, y, x^2, xy, y^2, x^3, |x^4)^T$ é a matriz que define um GGA-código com parâmetros $[22, 14, 6]$. Para obtermos um AG código com o mesmo comprimento e a mesma distância mínima, utilizando como divisores $G = 8(1:0:0) + 8(0:0:1)$ e D os outros pontos da curva de Klein homogeinizada, teríamos que seus parâmetros seriam $[22, 15, 6]$, portanto, percebemos que, ao aumentar a distância mínima, neste exemplo, o resultado da construção usual não é igualado.

Escolhendo $n = 22$ e $d = 12$, teríamos que $N_1, N_2, \ldots, N_{16} < 12$, $N_{17} = N_{18} = 12$ e $N_{19} < 12$ e todos os outros valores da sequência N são maiores ou iguais a 12, dessa forma, $r = 16$, $l = 1$ e $v_l = 19$. Assim, $H_{16}^* = (1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, x^4, y^3, x^2y^2, x^5, xy^3, y^4, x^6, x^7)^T$ é a matriz que define um GGA-código com parâmetros $[22, 5, 12]$. Para obtermos um AG código com o mesmo comprimento e a mesma distância mínima, utilizando como divisores $G = 5(1:0:0) + 5(0:0:1)$ e D os outros pontos da curva de Klein homogeinizada teríamos que seus parâmetros seriam $[22, 8, 12]$. Dessa forma, a construção usual, neste contexto se mostra melhor, porém, veremos que é possível aperfeiçoar os parâmetros dos GGA-códigos, utilizando ainda a Construção 3.1.

Observe que, em alguns casos, especialmente para $r < 2g$ os GGA-códigos são melhores em termos de parâmetros relativos, que os códigos usuais de Goppa.

Vejamos agora que, ao definir as variáveis de forma diferente, obtemos outros códigos, podendo melhorar algum parâmetro, utilizando a mesma curva e a Construção 3.1.

Exemplo 3.9. *Considere a curva de Klein definida pela equação*

$$x^3y + y^3 + x = 0$$

sobre $\mathbb{F}_8$*, com os pesos definidos anteriormente,* $w(x) = 2$ *e* $w(y) = 3$*. Agora considere* $x = x_2$ *e* $y = x_1$*. Reescrevemos a equação acima da seguinte forma*

$$x_2^3x_1 + x_1^3 + x_2 = 0.$$

Assim como fizemos anteriormente, devemos construir a sequência H*, para isso, analogamente todos os monômios da forma* $x^{i_2}y^{i_1}$*, com* $i_1 \geq 8$ *e* $i_2 \geq 8$ *não estarão em* H*, pois são monômios degenerados. Além disso, veja que* $x_2^7x_1 = x_1^7 + x_2x_1^4$*, dessa forma o monômio* $x_2^7x_1$ *não estará em* H*, pois não será linearmente independente. E dessa forma não estarão em* H *todos os monômios degenerados ou linearmente dependentes.*

Com isso a sequência H *será dada por:*

$$\begin{aligned} H \;=\; & \{1, x_2, x_1, x_2^2, x_2x_1, x_2^3, x_1^2, x_2^2x_1, x_2^4, x_1^4, x_2x_1^2, x_2^3x_1, x_2^5, x_2^2x_1^2, x_2^4x_1, x_2^6, x_2^3x_1^2, x_2^5x_1, x_2^7, x_2^4x_1^2 \\ & x_2^6x_1, x_2^6x_1^2\} \end{aligned}$$

dessa forma, $|H| = 22$*. As sequências* W *e* N *serão respectivamente:*

$$\begin{aligned} W &= \{0,2,3,4,5,6,6,7,8,8,9,10,10,11,12,12,13,14,14,15,16,18\} \\ N &= \{1,2,2,3,4,4,3,6,5,6,8,6,9,10,7,12,12,8,15,14,18,21\}. \end{aligned}$$

Observe que a sequência N obtida neste exemplo é diferente da sequência obtida anteriormente, apenas mudando as variáveis.

Suponha que queiramos construir um código geométrico de Goppa aprimorado, com $n = 22$ e $d = 3$ sobre $\mathbb{F}_8$. Usando a Construção 3.1 e a sequência N obtida acima, temos que $r = 3$ e $l = 0$, isto porque, $N_1, N_2, N_3 < 3$, $N_4 = 3$ e $N_t \geq 3$, para $4 < t \leq n$. Temos então que,

$$H_3^* = (1, x, y)^T$$

e esta matriz teste de paridade define um $[22, 19, 3]$ GGA-código.

Suponha que queiramos construir, desta vez, um código geométrico de Goppa aprimorado, com $n = 22$ e $d = 6$ sobre $\mathbb{F}_8$. Usando a Construção 3.1 e a sequência N obtida acima, temos que $r = 7$, $l = 1$ e $v_1 = 9$, isto porque, $N_1, N_2, \ldots, N_7 < 6$, $N_8 = 6$, $N_9 < 6$ e $N_t \geq 6$, para $9 < t \leq n$. Temos então que,

$$H_7^* = (1, x, y, x^2, xy^2, x, y^2, x^4)^T$$

e esta matriz teste de paridade define um $[22, 14, 6]$ GGA-código.

Vejamos mais um exemplo, onde construiremos de forma diferente a sequência H, onde poderemos ver que existem diversas técnicas possíveis para se construir uma sequência bem-comportada de monômios.

Exemplo 3.10. *Considere a curva de Klein de equação 3.2. Para construirmos a sequência H^* iremos considerar os monômios na forma $y^{i_2}x^{i_1}$ não-degenrados e também os monômios tal que $i_1 < 2i_2$. Note que se $i_2 \neq 0$ então $i_1 \geq 3$, e $x_2^{i_2+2}x_1^{i_1-3} <_t x^{i_2}x_1^{i_1}$. Portanto $x_2^{i_2}x_1^{i_1}$ não estarão em H pois são iguais a $x_2^{i_2+2}x_1^{i_1-3} + x_2^{i_2-1}x_1^{i_1-2}$. No entanto, se $i_2 = 0$, todos os monômios contendo o termo $x_1^{i_1}$, tal que, $i_1 \neq 0$, não estarão em H^*.*

Com isso teremos a seguinte sequência H^* bem-comportada sobre LS:

$$\begin{aligned} H^* = \{&1, x_2, x_2x_1, x_2^2, x_2x_1^2, x_2^2x_1, x_2^3, x_2^2x_1^2, x_2^3x_1, x_2^4, x_2^3x_1^2, x_2^4x_1, x_2^5, x_2^4x_1^2, x_2^5x_1, x_2^6, x_2^5x_1^2, x_2^6x_1, \\ &x_2^7, x_2^6x_1^2, x_2^7x_1, x_2^7x_1^2\}. \end{aligned}$$

Portanto, $|H^*| = 22$.

Da sequência acima obtemos W^* e N^*.

$$\begin{aligned} W^* &= \{0,3,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,25\} \\ N^* &= \{1,2,2,3,2,4,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19\}. \end{aligned}$$

Suponha que queiramos construir um GGA-código com $n = 22$ e $d = 3$ sobre $\mathbb{F}_8$. Observe que teremos $r = 3$, $l = 1$ e $v_1 = 5$, isto porque, $N_1, N_2, N_3 < 3$, $N_4 = 3$, $N_5 < 3$ e $N_j \geq 4$, para $5 < j \leq n$. Portanto, temos que $H_3^* = (1, y, xy, x^2y)^T$ e esta matriz define um $(22, 18, 3)$ GGA-código.

Suponha que queiramos construir, desta vez, um código geométrico de Goppa aprimorado, com $n = 22$ e $d = 6$ sobre $\mathbb{F}_8$. Usando a Construção 3.1 e a sequência N obtida acima, temos que $r = 8$ e $l = 0$, isto porque, $N_1, N_2, \ldots, N_8 < 6$, $N_9 = 6$ e $N_t \geq 6$, para $9 < t \leq n$. Temos então que,

$$H_8^* = (1, y, xy, y^2, x^2y, xy^2, y^3, x^2y^2)^T$$

e esta matriz define um $(22, 14, 6)$ GGA-código.

Suponha que queiramos construir um GGA-código com $n = 22$ e $d = 12$ sobre $\mathbb{F}_8$. Observe que teremos $r = 14$, isto porque, , $N_1, N_2, N_3, \ldots, N_{14} < 12$ e $N_j \geq 12$, para $15 < j \leq n$. Portanto temos que $H_{12}^* = (1, y, xy, y^2, x^2y, xy^2, y^3, x^2y^2, xy^3, y^4, x^2y^3, xy^4, y^5, x^2y^4)^T$ e esta matriz define um $(22, 18, 12)$ GGA-código.

Podemos comparar os resultados obtidos nos exemplos construidos, para verificarmos que, por meio de uma construção mais simples, igualamos e até melhoramos os resultados dos AG-códigos, surgindo questionamentos a respeito de quando se torna mais eficaz utilizá-lo. Observe o seguinte quadro comparativo:

Método	(d = 3)	(d=6)	(d=6)
Exemplo 1	(22,19,3)	(22,14,6)	(22,5,12)
Exemplo 2	(22,19,3)	(22,14,6)	(22,6,12)
Exemplo 3	(22,18,3)	(22,14,6)	(22,8,12)

Estes resultados nos mostram que, a construção dos GGA-códigos nos gera códigos com melhores parâmetros que os AG-códigos para algumas distâncias mínimas, porém, ao aumentarmos esta distância, não vemos um resultado eficiente. Desta problemática surge o questionamento de se há maneiras de melhorar a construção utilizada até aqui dos GGA-códigos, afim de obter uma sequência ótima de H, sendo, assim, possível a construção de uma classe de códigos com bons parâmetros assintóticos.

O que iremos fazer a seguir é, utilizar outra curva, conhecida como *Curva quase-Hermitiana*, para obter uma melhoria na construção dada até aqui, sobre um corpo finito especifico, mostrando que, com estes procedimentos, obteremos códigos que excedem a cota de Garcia-Stichtenoth, além de possibilitar a construção de códigos com ótimos parâmetros, dado certas dimensões e comprimentos.

Capítulo 4

GGA-códigos sobre a curva quase-Hermitiana

A curva Hermitiana sobre $\mathbb{F}_{q^2}$ é definida pela equação

$$X^{q+1} = Y^q + Y. \tag{4.1}$$

Esta curva possui q^3 pontos racionais afins e para cada $X \in \mathbb{F}_{q^2}$, existem q valores distintos para $Y \in \mathbb{F}_{q^2}$, tal que, (X, Y) é um ponto racional da equação acima.

Exemplo 4.1. *Para $q = 2$, considere a curva Hermitiana sobre $\mathbb{F}_4$, dada por:$X^3 = Y^2 + Y$ onde $q = 2$. Esta curva possui 8 pontos racionais afins, sendo eles*

$$\{(0,0), (0,1), (1,\alpha), (1,\alpha^2), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,\alpha^2)\}$$

onde α é um elemento primitivo de $\mathbb{F}_4$.

Para obtermos a curva quase-Hermitiana, faremos uma pequena mudança. Para $X \neq 0$, seja $x = X$ e $y = Y/X$. Dessa forma, $Y = yX$ e substituindo em 4.1, temos:

$$\begin{aligned} X^{q+1} &= Y^q + Y \\ x^{q+1} &= (yX)^q + yX \\ x^{q+1} &= y^q x^q + yx \end{aligned}$$

Como $X \neq 0$, podemos escrever a equação da seguinte forma

$$x^q = y^q x^{q-1} + y. \tag{4.2}$$

A equação acima define a curva quase-Hermitiana sobre $\mathbb{F}_{q^2}$. Para cada $x \neq 0$, existem q $y \neq 0$, tal que, (x, y) são raízes de 4.2. Dessa forma, temos $(q^2 - 1)q$ pontos racionais afins, quando $x \neq 0$. Se $y = 0$, então $(0, 0)$ é um ponto racional afim de 4.2. Portanto 4.2 possui $n = (q^2 - 1)q + 1$ pontos racionais afins.

Exemplo 4.2. *Para $q = 2$, considere a curva quase-Hermitiana sobre $\mathbb{F}_4$ dada por:*

$$x^2 = y^2 x + y.$$

Esta curva possui 7 pontos racionais afins, sendo eles

$$(x, y) \quad = \quad (0,0), (1,\alpha), (1,\alpha^2), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,\alpha), (\alpha^2,\alpha^2).$$

Exemplo 4.3. *Para $q = 3$, considere a curva quase-Hermitiana sobre $\mathbb{F}_9$ dada por:*

$$x^3 = y^3x^2 + y.$$

Esta curva possui 25 pontos racionais afins, sendo eles:

$$\{(0,0), (\beta^i, \beta^i), (\beta^i, \beta^{i+5}), (\beta^i, \beta^{i+7})\}$$

para $i = 0, 2, 4, 6$. E

$$\{(\beta^i, \beta^i), (\beta^i, \beta^{i+1}), (\beta^i, \beta^{i+3})\}$$

para $i = 1, 3, 5, 7$. Onde β é um elemento primitivo de $\mathbb{F}_9$.

Para analizarmos o comportamento assintótico dos códigos, o número de pontos racionais afins deve ser o maior possível, então, para isso, podemos extender as curvas para o m-espaço dimensional afim, dessa forma, a curva quase-Hermitiana seria representada por um sistema de equações, da seguinte forma:

$$\begin{cases} x_1^q &= x_2^q x_1^{q-1} + x_2 \\ x_2^q &= x_3^q x_2^{q-1} + x_3 \\ \vdots & \vdots \\ x_{m-1}^q &= x_m^q x_{m-1}^{q-1} + x_m \end{cases} \tag{4.3}$$

sobre $\mathbb{F}_{q^2}$. Observe que para cada x_i existem q x_{i+1}, tal que, $(\dots, x_{i+1}, x_i, \dots)$ são pontos racionais afins de 4.3, além disso, $(0, 0, \dots, 0)$ também é uma raíz. O número de pontos racionais afins deste sistema de equações é portanto$n = (q^2 - 1))q^{m-1} + 1$.

Exemplo 4.4. *Considere a curva quase-Hermitiana no espaço m-dimensional afim sobre $\mathbb{F}_4$:*

$$\begin{cases} x_1^2 &= x_2^2 x_1 + x_2 \\ x_2^2 &= x_3^2 x_2 + x_3 \\ \vdots & \vdots \\ x_{m-1}^2 &= x_m^2 x_{m-1} + x_m \end{cases} \tag{4.4}$$

o número de pontos racionais afins desta curva é $n = 3 \cdot 2^{m-1} + 1$.

Exemplo 4.5. *Considere a curva quase-Hermitiana no espaço m-dimensional afim sobre $\mathbb{F}_9$:*

$$\begin{cases} x_1^3 &= x_2^3 x_1^2 + x_2 \\ x_2^3 &= x_3^3 x_2^2 + x_3 \\ \vdots & \vdots \\ x_{m-1}^3 &= x_m^3 x_{m-1}^2 + x_m \end{cases}$$

o número de pontos racionais afins desta curva é $n = 8 \cdot 3^{m-1} + 1$.

O gênero da curva quase-Hermitiana foi calculado por Garcia e Stichtenoth [4] e é dado por

$$g_m = \begin{cases} q^m + q^{m-1} - q^{\frac{m-1}{2}} - 2q^{\frac{m-1}{2}+1} & \text{se m é ímpar;} \\ q^m + q^{m-1} - \frac{1}{2}q^{\frac{m}{2}+1} - \frac{3}{2}q^{\frac{m}{2}} - q^{\frac{m-2}{2}} + 1 & \text{se m é par.} \end{cases}$$

Seja $d = r - g_m + 1$, este valor é chamado cota de Garcia-Stichtenoth para distância mínima.

Utilizaremos a curva quase-Hermitiana ao invés da curva Hermitiana, pois ela possui um gênero grande comparado ao número de pontos racionais afins da curva e, sabemos que a distância mínima, do ponto de vista algébrico geométrico, pode ser calculado utilizando a expressão $r - g - 1$ fazendo com que a quase-Hermitiana seja mais interessante que a curva Hermitiana [9].

Exemplo 4.6. *Considere a curva Hermitiana sobre* $\mathbb{F}_4$*, vista no Exemplo 4.1, dada pela equação* $X^3 = Y^2 + Y$*. Vimos que esta curva possui 8 pontos racionais afins. Note que devemos tomar* $w(X) = 2$ *e* $w(Y) = 3$ *para que os pesos sejam consistentes. Temos então a seguinte sequência* H*:*

$$H = \{00, 10, 01, 20, 11, 02, 21, 03\}$$

onde ab denota X^aY^b*. Da equação da curva, dada acima, em* $\mathbb{F}_4$ *temos* $X^4 + XY^2 + XY = 0$*. Como* $X^4 = X$*, temos também que* $XY^2 = X + XY$*, dessa forma* 12 *é combinação linear de* 10 *e* 11*, por este motivo* 12 *não pertence a* H*. A sequência de pesos* W *é dada por:*

$$W = \{0, 2, 3, 4, 5, 6, 7, 9\}.$$

Para esta sequência H *temos a seguinte matriz síndrome:*

00	10	01	20	11	02	21	03
10	20	11	30	21	12	21	...
01	11	02	21	12	03	...	
20	30	21	40	31	...		
11	21	12	31	...			
02	12	03	...				
21	31	...					
03	...						

Na matriz acima, temos que $31 \sim 03$*, pois,* $X^3Y = Y^3 + XY$*, observe que* $w(X^3Y) = w(Y^3) = 9$ *e portanto a consistência é verificada. Temos também que* $12 \sim 11$*,* $30 \sim 02$ *e* $40 \sim 10$*. Podemos ver dessa forma, que todos os termos da sequência são bem-comportados e assim* H *é uma sequência bem-comportada. Podemos também calcular a sequência* N *utilizando a matriz síndrome, efetuando os cálculos obtemos a seguinte sequência:*

$$N = \{1, 2, 2, 3, 4, 5, 6, 8\}.$$

Sendo assim, com base na construção dada, se escolhermos os 4 primeiros monômios da sequência H *para formar a matriz teste de paridade, isto é, se escolhermos* $r = 4$ *então o código definido por tal matriz teste de paridade terá distância mínima igual a* 4*, isto porque,* $N_k \geq 4$ *para* $k > 4$*. Os parâmetros do código serão, portanto,* $[8, 4, 4]$*, parâmetro igual ao obtido pela construção usual do código de Goppa, utilizando os divisores* $G = 4(0 : 1 : 0)$ *e* D *como todos os outros pontos da curva Hermitiana homogeinizada.*

Exemplo 4.7. *Considere a curva quase-Hermitiana sobre* $\mathbb{F}_4$*, vista no Exemplo 4.2, dada pela equação* $x^2 = y^2x + y$*. . Esta curva possui* 7 *pontos racionais e definimos* $w(x) = 2$ *e* $w(y) = 1$*. Podemos construir a seguinte sequência de monômios lineramente independentes:*

$$H = \{00, 10, 01, 11, 02, 12, 03\},$$

onde ab denotam y^ax^b*. Calculando os pesos dos monômios acima, obtemos a seguinte sequência* $W = 0, 1, 2, 3, 4, 5, 6$*. Com isso obtemos a seguinte matriz síndrome:*

00	10	01	11	02	12	03
10	20	11	21	12	22	...
01	11	02	12	03	...	
11	21	12	22	...		
02	12	03	...			
12	22	...				
03	...					

A equação da curva é dada por $x^2 = y^2x + y$*, assim temos que* $x^2y = y^3x + y^2$ *ou então, como estamos em* $\mathbb{F}_4$ *podemos escrever* $x^2y + y^3x + y^2 = 0$*. Note que* y^3x *e* x *possuem o mesmo vetor de avaliação, portanto* $y^2 = x^2y + x$*, assim* $y^2 \sim x^2y$*, isto é,* $20 \sim 12$*. Mas note que* $w(y) + w(y) = 2 < 5 = w(x^2y)$*, isto é,* 20 *não é um termo bem-comportado e portanto* H *não é uma sequência bem-comportada.*

Agora temos que $22 = 03 + 11$*, assim,* $22 \sim 03$*; E também* $21 = 02 + 10$*, assim,* $21 \sim 02$*. Dessa forma, os outros termos são todos bem-comportados. Se escolhermos*

$$\widehat{H} = \{00, 01, 11, 02, 12, 03, 13\}$$

teremos $\widehat{W} = \{0, 2, 3, 4, 5, 6, 7\}$ *e portanto a seguinte matriz síndrome:*

00	01	11	02	12	03	13
10	02	12	03	13	...	
11	12	22	13	...		
02	03	13	...			
12	13	...				
03	...					
13	...					

Considerando as consistências vistas acima, podemos ver que a sequência é bem-comportada, pois possui todos os seus termos bem-comportados. Podemos ainda calcular a sequência

$$\widehat{N} = \{1, 2, 2, 3, 4, 5, 6\}.$$

Veja que a construção acima nos garante um código de distância mínima no máximo 6, o qual teria como parâmetros $(8, 2, 6)$, o qual também iguala ao parâmetro obtido pela construção usual, utilizando os divisores $G = 4(0 : 1 : 0)$ e D como todos os outros pontos da curva Hermitiana homogeinizada. Podemos nos perguntar, portanto, se há uma forma diferente de se realizar a escolha dos monômios que compõe a sequência H, para que tenhamos uma nova sequência N onde a distância mínima será melhorada. Veremos a seguir, portanto, uma forma de aprimorarmos a construção dos GGA-códigos vista até aqui.

4.1 Melhoria da distância mínima dos GGA-códigos sobre a curva quase-Hermitiana

Podemos perceber que os parâmetros obtidos pelas sequências bem-comportadas, muitas vezes, não são tão bons, isto porque, são colocadas condições fortes em sua construção. Veremos agora uma forma de melhorarmos estes parâmetros enfraquecendo as condições de construção das sequências vistas até aqui.

Primeiramente, temos que ao estimar cada N_r relacionada a uma sequência H, que não precisa ser bem-comportada, ou seja, ser bem-comportada é uma condição suficiente, mas não necessária no cálculo de N. Em uma sequência bem-comportada cada termo $h_{s,t}$ é bem-comportado e portanto $w(h_{s,t}) = w(h_k)$ ou $w(h_{s,t}) > w(h_k)$, onde $h_{s,t} = h_k + \sum_\mu h_\mu$ e $w(h_\mu) < w(h_k)$. Esta condição nos garante que ao calcularmos N_{r+1}, para todo (i, j) tal que $h_{i,j} \in L(r+1)$ e $w(h_{i,j}) = w(h_{r+1})$, teremos que $s_{i,j} \neq 0$ enquanto $s_{u,v} = 0$ para todo $(u, v) < (i, j)$.

Podemos no entanto atingir este mesmo objetivo, desde que, $w(h_k) < w(h_{r+1})$, mesmo que, $w(h_k)$ seja maior que $w(h_{s,t})$. Assim definimos uma sequência *quase bem-comportada* para r, da seguinte forma.

Definição 4.1. *Seja* $H = \{h_1, \ldots, h_r, \ldots, h_{\widehat{r}}, \ldots, h_n\}$ *uma sequência de monômios não-degenerados e linearmente independentes, ela será chamada sequência quase bem-comportada para* r*, se*

$$w(h_1) < w(h_2) < \cdots < w(h_r) < \cdots < w(h_{\widehat{r}}) < \cdots < w(h_n) = W_{max},$$

e para cada $\widehat{r} > r$, *se* h_i *e* h_j *satisfizer* $w(h_i) + w(h_j) \leq w(h_{\widehat{r}})$, $h_{i,j}$ *é um termo bem-comportado ou* $w(h_k) \leq w(h_{\widehat{r}})$.

Dessa forma, tendo mais liberdade ao construir a sequência H, conseguiremos aumentar a cota inferior da distância mínima. Vejamos o exemplo a seguir, que mostra a vantagem de utilizar uma sequência quase bem-comportada, ao invés de uma sequência bem-comportada.

Exemplo 4.8. *Considere a curva quase-Hermitiana sobre* $\mathbb{F}_4$ *vista no Exemplo 4.2. Vimos no Exemplo 4.7 que a sequência* $H = \{00, 10, 01, 11, 02, 12, 03\}$, *não é bem-comportada. Porém note que* H *é uma sequência quase bem-comportada, isto porque sabemos que apenas* $20 \sim 12$ *não é um termo bem-comportado, mas* $w(12) < w(03)$, *portanto pela definição acima,* H *é uma sequência quase bem-comportada para* $r = 6$.

Calculando a sequência N *com base em* H, *vemos que* $N(03) = N_7 = 7$, *isto é, o código definido pelos 6 primeiros monômios de* H *terá distância mínima no mínimo 7, o que é uma melhoria relativa ao código construído utilizando a sequência bem-comportada* $\widehat{H}$, *o qual vimos que, o código definido pelos seus 6 primeiros elementos teria como cota inferior para sua distância mínima 6. Com isso notamos a vantagem que teremos ao utilizar sequências quase bem-comportadas.*

A segunda melhoria que iremos propor é baseada em propriedades algébricas da curva que estamos utizando para construção dos códigos. Na curva quase-Hermitiana, alguns monômios aparentemente diferentes, com pesos distintos, podem possuir um mesmo vetor de avaliação. Por exemplo, considere os códigos Quase-Hermitianos sobre $\mathbb{F}_{q^2}$. Se $a_m, \ldots, a_{i+1}, a_{i-1}, \ldots, a_1$ não são todos nulos, então $x_m^{a_m} \ldots x_i^{q^2-1} \ldots x_1^{a_1}$ e $x_m^{a_m} \ldots x_i^0 \ldots x_1^{a_1}$ são dois vetores de avaliação iguais, porém, com pesos diferentes. Portanto, se substituirmos um monômios por outro com mesmo vetor de avaliação, teremos uma sequência H distinta, onde ela será bem-comportada ou quase bem-comportada. Propomos, dessa forma, uma reorganização da sequência H, onde a cota inferior, estabelecida para distância mínima, baseada na sequência N será sempre aprimorada, pelo fato de podermos controlar as substituições, fazendo com que o número de $h_{i,j}$ consistentes com h_r seja sempre maior que o obtido previamente, aprimorando a cota inferior da distância mínima dos códigos que serão construidos.

A construção dos GGA-códigos, faz com que a sequência N, composta pelos $N(h_r)$ determine os parâmetros do código, portanto construindo-a de uma forma otimizada, teremos códigos com melhores parâmetros. Para melhorarmos, portanto, a sequência N, precisamos calcular $N_{\hat{r}}$ para $r < \hat{r} \leq n$ e escolhermos o menor deles, pois ele será uma cota inferior para o peso das palavras do código. Quando utilizamos $N_{\hat{r}}$ para determinar uma cota inferior para o peso de uma palavra do código, nós assuminos que $s_{\hat{r}}(c) \neq 0$, porém $s_i(c) = 0$ para $i < \hat{r}$. Para otimizarmos $N_{\hat{r}}$ podemos substituir, deletar ou reorganizar os monômios na sequência H antes de $h_{\hat{r}}$ e manter h_j ordenado para $\hat{r} < j \leq n$, de forma, que teremos duas sequências quase-bem-comportadas para $\hat{r}$, chamaremos de $SL_{\hat{r}}$ e $SC_{\hat{r}}$. Então a primeira linha e primeira coluna da nova matriz síndrome $S_{\hat{r}}$ correspondem a $SL_{\hat{r}}$ e $SC_{\hat{r}}$, respectivamente. Poderemos então calcular $N_{\hat{r}}$ pela matriz síndrome $\widehat{S}_{\hat{r}}$.

Observe que o número $N_{\hat{r}}$ será otimizado, pois podemos controlar a seleção das sequências $SL_{\hat{r}}$ e $SC_{\hat{r}}$, tal que, o número de $h_{i,j}$ consistentes com $h_{\hat{r}}$ aumente, ou seja, podemos escolher as sequências de forma a gerar elementos consistentes com $h_{\hat{r}}$ em mais coordenadas da matriz síndrome. Assim, a terceira melhoria que iremos propor será que a escolha das sequências $SL_{\hat{r}}$ e $SC_{\hat{r}}$ para diferentes $\hat{r}$ serão independentes uma das outras. Combinando essas melhorias, conseguimos uma melhor estimativa para a distância mínima, e podemos construir um exemplo que apresenta bons parâmetros.

Exemplo 4.9. *Considere a curva quase-Hermitiana no 4-espaço dimensional afim sobre* $\mathbb{F}_4$*:*

$$\begin{cases} x_1^2 + x_2^2 x_1 + x_2 &= 0 \\ x_2^2 + x_3^2 x_2 + x_3 &= 0 \\ x_3^2 + x_4^2 x_3 + x_4 &= 0. \end{cases}$$

Temos que $w(x_4) = 1$*,* $w(x_3) = 2$*,* $w(x_2) = 4$*,* $w(x_1) = 8$*. Usando a técnica de substituição, conseguimos encontrar a seguinte sequência bem-comportada:*

$$\begin{aligned} H \;=\; \{&0000, 0001, 0011, 0002, 0102, 0012, 1012, 0112, 1112, 0003, 1003, 0103, 1103, \\ &0013, 1013, 0113, 1113, 1004, 0104, 1104, 1014, 0114, 1114, 1005, 1105\}, \end{aligned}$$

onde abcd denota $x_4^a x_3^b x_2^c x_1^d$*. A sequência de pesos* W *correspondente será:*

$$W = \{0, 8, 12, 16, 18, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 33, 34, 35, 37, 38, 39, 41, 43\}$$

e $W_{max} = 43$*. Iremos calcular a sequência* N*, neste exemplo, sem a utilização da matriz síndrome, descrevendo um método para o cálculo de forma mais automatizada e simples. Sabemos que* N_{h_r} *é o número de* $h_{i,j} = h_i \cdot h_j$*, tal que,* $h_r \sim h_{i,j}$ *e portanto, para que isso aconteça temos que* $w(h_{i,j}) = w(h_r)$*. Portanto, conseguiremos calcular* N_{h_r} *observando exclusivamente a sequência* W*. Escreva a sequência* $W = \{\phi_1, \phi_2, \ldots, \phi_n\}$*, veja que* N_{h_r} *será a quantidade de* $\phi_i + \phi_j = w(h_r)$*, portanto basta que eu encontre quantas são essas combinações, o que é facilmente feito em um software. Utilizando o software* ***MatLab*** *com o seguinte código:*

```
clear all
close all

W = [0,8,12,16,18,20,21,22,23,24,25,26,27,28,29,30,31,33,34, 35, 37, 38, 39,41,43];

N = zeros(length(W));

for r = 1:length(W)
for i = 1:length(W)
    for j = 1:length(W)
        if W(i)+W(j) == W(r)
           N(r) = N(r)+ 1;
        else
           continue
        end
    end
    end
end

for i = 1:length(W)
    L(i) = N(i,1);
end
```

Figura 4.1: Programa para calcular a sequência N.

Obtemos a sequência N*, que será:*

$$N = \{1, 2, 2, 3, 2, 4, 2, 2, 2, 5, 2, 4, 2, 6, 4, 6, 4, 6, 8, 6, 8, 10, 10, 12, 14\}.$$

Para esta sequência bem-comportada, o gênero é $g = 15$ *que é igual ao número de gaps de pesos. Seja* C *o código definido pela matriz teste de paridade formado pelos 23 primeiros monômios de* H*. Usando o teorema de Riemann-Roch, a distância mínima de* C *é no mínimo* $23 - 15 + 1 = 9$*. Usando* N *como uma cota, a distância mínima de* C *será no mínimo* 12*.*

Se utilizarmos as técnicas enunciadas anteriormente para encontrar o maior N_{24} *e* N_{25} *possível, então teremos uma cota inferior ainda maior para a distância mínima do código que*

pode ser construído utilizando a sequência H. Por exemplo, para o monômio 1005*, construímos as seguintes sequências:*

$$\begin{aligned} SL_{24} &= \{0000, 0001, 0101, 1101, 0011, 0002, 0102, 0012, 1012, 1112, 1003, 1013, 1113, 1005, \dots\} \\ SC_{24} &= \{0000, 0101, 0011, 0002, 0102, 0012, 1012, 1112, 1003, 1013, 0113, 1113, 1004, 1005, \dots\}. \end{aligned}$$

Observe que as sequências são construídas reorganizando e substituindo monômios na sequência H, de tal forma que, se denotarmos $SL_{24} = \{p_1, p_2, \dots, p_r = 1005, \dots\}$ e $SC_{24} = \{k_1, k_2, \dots, k_r = 1005, \dots\}$, temos que $w(p_1) + w(p_r) = w(1005)$, $w(p_2) + w(p_{r-1}) = w(1005)$, $w(p_3) + w(p_{r-2}) = w(1005)$ e assim sucessivamente, portanto, temos que, pelo menos, todos os elementos da diagonal secundária da matriz síndrome serão consistentes com h_{24} e portanto o número N_{24} será otimizado.

A matriz síndrome $\widehat{S}_{24}$ será dada por:

0000	0101	0011	0002	0102	0012	1012	1112	1003	1013	0113	1113	1004	1005	...
0001	0102	0012	0003	0103	0013	1013	1113	1004	1014	0114	1114	1005	...	
0101	0202	0112	0103	0203	0113	1113	1213	1004	1114	0214	1214	...		
1101	1202	1112	1103	1203	1113	2113	2213	2004	2114	1214	...			
0011	0112	0022	0013	0113	0023	1023	1123	1014	1024	...				
0002	0103	0013	0004	0104	0014	1014	1114	1005	...					
0102	0203	0113	0104	0204	0114	1114	1214	...						
0012	0113	0023	0014	0114	0024	1024	...							
1012	1113	1023	1014	1114	1024	...								
1112	1213	1123	1114	1214	...									
1003	1104	1014	1005	...										
1013	1114	1024	...											
1113	1214	...												
1005	...													
...														

Por esta matriz, encontramos um novo $N_{24} = 14$, conseguimos portanto melhorar a cota inferior para a distância mínima. Podemos fazer o mesmo processo para o monômio $1105 = N_{25}$*. Teremos as seguintes sequências:*

$$\begin{aligned} SL_{25} &= \{0000, 0001, 0011, 0111, 1111, 0002, 1002, 0102, 0012, 1012, 0112, 1112, 1003, 1103, 0013, 1013, 1113, 1104, 1105, \dots\} \\ SC_{25} &= \{0000, 0001, 0011, 0111, 1111, 0002, 0102, 0012, 1012, 0112, 1112, 1003, 0103, 1103, 0013, 1013, 1113, 1104, 1105, \dots\}. \end{aligned}$$

Com estas sequências encontramos $N_{25} = 19$. Segue que este código terá distância mínima no mínimo 14*, e assim melhoramos a cota inferior.*

4.2 Códigos quase-Hermitianos sobre $\mathbb{F}_4$

Veremos agora GGA-códigos quase-Hermitianos sobre $\mathbb{F}_4$, que melhoram a cota de Garcia-Stichtenoth, mas para isso, veremos alguns resultados envolvendo esta curva.

Sabemos que a curva quase-Hermitiana possui $3 \cdot 2^{m-1} + 1$ pontos racionais. Considere agora, α um elemento primitivo de $\mathbb{F}_4$, onde $\alpha^2 + \alpha + 1 = 0$. Então os pontos da curva quase-Hermitiana serão $(0, 0, \dots, 0)$ e $(r_1, r_2, \dots, r_m)$ onde para cada $r_i = 1$, temos que $r_{i+1} = \alpha, \alpha^2$, isto porque (r_i, r_{i+1}) são pontos racionais da curva quase-Hermitiana, a qual vimos no Exemplo 4.1; Para cada $r_i = \alpha$, temos que $r_{i+1} = 1, \alpha$; Para cada $r_i = \alpha^2$ temos que $r_{i+1} = 1, \alpha^2$. E pela equação da curva quase-Hermitiana sabemos que $r_1 = 1, \alpha, \alpha^2$.

Denotaremos por $a_m a_{m-1} \dots a_1$ o monômio $x_m^{a_m} x_{m-1}^{a_{m-1}} \dots x_1^{a_1}$ e definimos o peso de cada variável como sendo

$$w(x_i) = 2^{m-i}.$$

Pela equação da curva quase-Hermitiana, temos que

$$\cdots 21 \cdots = \cdots 02 \cdots + \cdots 10 \cdots \tag{4.5}$$

e podemos escrever de forma mais geral que

$$\cdots (i+2)(j+1) \cdots = \cdots i(j+2) \cdots + \cdots (i+1)j \cdots . \tag{4.6}$$

Somente o ponto $(0, 0, \dots, 0)$ possui elementos nulos. Por outro lado, como $x_i^3 = 1$ para todo $x_i \neq 0$, pois são elementos de $\mathbb{F}_4$ temos que:

$$a_m \cdots a_i \cdots a_1 = a_m \cdots (a_i + 3) \cdots a_1 \tag{4.7}$$

para $a_m a_{m-1} \cdots a_1 \neq 0 \cdots 0 \cdots 0$. Vejamos um exemplo que ilustra essas transformações:

Exemplo 4.10. *Para $m = 5$, considere os monômios* 00103, 20031, 00104, 20034, 0004. *Pelas igualdades vistas acima, teremos a seguintes igualdades:* $00103 = 00100$, $20031 = 20001$, $00104 = 00101$, $20034 = 20001$, $0004 = 0001$. *Porém* $0003 \neq 0000$.

Também temos que utilizando as Equações 4.5, 4.6 e 4.7 acima e a equação da curva 4.4, teremos as seguintes reduções monomiais

$$\dots 22 \cdots = \dots 00 \cdots + \dots 11 \dots \tag{4.8}$$

e

$$\dots 20 \cdots = \dots 12 \cdots + \dots 01 \dots . \tag{4.9}$$

A partir de agora, estaremos interessados nos monômios $a_m a_{m-1} \dots a_1$, em que $a_i \in 0, 1$ para $2 \leq i \leq m$ e $a_1 \geq 0$, estes monômios serão chamados de monômios padrões.

Lema 4.1. *O produto de quaisquer dois monômios padrões $a_m a_{m-1} \dots a_1$ e $b_m b_{m-1} \dots b_1$ pode ser escrito de forma única como uma combinação linear de monômios padrões $c_m^{\mu} \dots c_1^{\mu}$ utilizando as reduções acima.*

Exemplo 4.11. *Seja* $10111 \cdot 10104 = 20215$. *Pela Equação 4.9 temos que* $20215 = 12215 + 01215$. *Usando a Equação 4.8 para o primeiro termo da soma, temos que* $20215 = 12215 + 01215 = 10015 + 11115 + 01215$. *Agora pela Equação 4.6 para o último termo teremos que* $20215 = 12215 + 01215 = 10015 + 11115 + 01215 = 10015 + 11115 + 01105 + 01025$. *E por fim, utilizando novamente a Equação 4.6 para o último termo da soma, teremos que* $20215 = 12215 + 01215 = 10015 + 11115 + 01215 = 10015 + 11115 + 01105 + 01025 = 10015 + 11115 + 01105 + 01006 + 01014$.

Comparando este resultado com [6] e [5], vemos que encontramos uma nova abordagem para a construção de códigos Quase-Hermitianos mais eficientes sobre $\mathbb{F}_4$.

Iremos construir um algoritmo para determinar termos bem-comportados com h_r. Para isso iremos selecionar pares de monômios padrões, onde o produto entre eles resulte em monômios bem-comportados com h_r.

A seguir, mostraremos 3 lemas que nos ajudarão a construir esses monômios bem-comportados.

Lema 4.2. *Seja $1 \cdots 1$ uma sequência de k $1's$ consecutivos. Então,* $21 \cdots 15 \sim 10 \cdots 15$.

Demonstração. *Usaremos indução para demonstrar este resultado. Quando* $k = 1$*, temos que* $215 = 025 + 105 = 006 + 014 + 105$*. Como* $006 = 003$*, então* $215 = 003 + 104 + 105$*. Note que* $w(105) > w(003)$ *e* $w(105) > w(014)$*. Portanto* $215 \sim 015$*. Assuma agora que o lema é válido para* k *e considere o caso* $k+1$*. Pela equivalência 4.5 temos então que* $211\cdots15 = 101\cdots15 + 021\cdots15$*. Usando a hipótese de indução segue que* $021\cdots15 \sim 010\cdots15$*, mas por outro lado, note que* $w(010\cdots15) < w(101\cdots15)$*, logo* $211\cdots15 \sim 101\cdots15$*.*

□

Lema 4.3. *Sejam* $a_m\cdots a_{p+1}$ *elementos arbitrários e* $\cdots1$ *uma sequência de* $k-1$ $1's$ *consecutivos. Temos então a seguinte consistência:*

$$a_m\cdots a_{p+1}01\cdots15 \sim a_m\cdots a_{p+1}20\cdots15.$$

Esta consistência é equivalente a $01\cdots15 \sim 20\cdots15$*.*

Demonstração. *Utilizaremos novamente a indução para mostrar este resultado. Para* $k = 1$*, temos que* $015 = 205 + 125 = 205 + 106 + 114$ *e como* $006 = 003$ *segue que* $015 \sim 205$*. Assuma que o lema é válido para* k*. Considere agora o caso* $k+1$*. Teremos que* $011\cdots15 = 201\cdots15 + 121\cdots15$*. Usando o lema anterior, o segundo termo da soma é consistente com* $110\cdots15$*. Como* $w(110\cdots15) < w(201\cdots15)$*, temos que* $011\cdots15 \sim 210\cdots15$ *e portanto o lema é válido para* $k+1$*.*

Lema 4.4. $\cdots011\cdots12\cdots \sim \cdots201\cdots12\cdots$

Demonstração. *Usaremos a igualdade* $20 = 01 + 22$ *repetidamente e ao final, usaremos também que* $22 = 11 + 00$*, dessa forma temos que*

$$\begin{aligned}
\cdots201\cdots12\cdots &= \cdots011\cdots12\cdots + \cdots121\cdots12\cdots \\
&= \cdots011\cdots12\cdots + \cdots110\cdots12\cdots + \cdots102\cdots12\cdots \\
&= \cdots011\cdots12\cdots + \cdots110\cdots12\cdots + \cdots + \cdots101\cdots22\cdots \\
&= \cdots011\cdots12\cdots + \cdots110\cdots12\cdots + \cdots + \cdots101\cdots11\cdots + \cdots101\cdots00\cdots
\end{aligned}$$

Entre os termos que aparecem do lado direito da igualdade, $\cdots110\cdots12\cdots$ *possui o maior peso e este é igual ao peso de* $\cdots201\cdots12\cdots$*. Sendo assim,* $\cdots011\cdots12\cdots \sim \cdots201\cdots12\cdots$ *e a prova está completa.*

Usando os Lemas 4.2, 4.3, 4.4, encontramos os seguintes termos bem-comportados para h_r.

Teorema 4.1. *Sejam* $a_m, \ldots, a_p \in \{0, 1\}$*. Então,*

$$\begin{aligned}
a_m\cdots a_p00\cdots011\cdots12a_q\cdots a_25 &\sim a_m\cdots a_p00\cdots201\cdots12a_q\cdots a_25 \\
&\sim a_m\cdots a_p002\cdots101\cdots12a_q\cdots a_25 \\
&\sim a_m\cdots a_p021\cdots101\cdots12a_q\cdots a_25 \\
&\sim a_m\cdots a_p21\cdots101\cdots12a_q\cdots a_25
\end{aligned}$$

Demonstração. *O Teorema segue diretamente das consistências demonstradas nos Lemas acima, além disso, utilizamos repetidas vezes o fato que* $01 = 20$ *e* $02 = 21$*, pela propriedade 4.6, resultantes da equação da curva.*

□

Exemplo 4.12. *O Teorema 4.1 nos garante as seguintes consistências:*

$$0011000115 \sim 0011002015 \sim 0011021015 \sim 0011211015 \sim 0201211015 \sim 2101211015.$$

Agora consideremos o problema de como encontrar sequências de linha e de coluna, de forma a serem sequências quase bem-comportadas com h_r, sendo h_r um monômio padrão com $a_2 = 1$ e $a_1 = 5$. Primeiramente, construiremos uma fórmula para construção de tais sequências linha e coluna, depois provaremos que de fato são quase bem-comportadas com h_r.

Exemplo 4.13. *Pelos resultados acima, temos que* $11015 \sim 11205$. *Para o monômio* 11205*, selecionamos para a sequência linha e coluna de* H *os monômios da forma* $**10@$*, onde* $* \in \{0, 1\}$ *e* $@ \in \{0, 2, 3, 5\}$. *Então* 00000 *e* 11015 *estarão na sequência linha e coluna, e* 11012 *e* 00003 *não estarão na sequências construidas. Para este exemplo a sequência linha será:*

$$\{00000, 00102, 10102, 01102, 11102, 00103, 10103, 01103, 11103, 11015\}$$

e a sequência coluna será:

$$\{00000, 00102, 10102, 01102, 11102, 00103, 10103, 01103, 11103, 11015\}.$$

Estas sequências formam a seguinte matriz síndrome:

00000	00102	10102	01102	11102	00103	10103	01103	11103	11015
00102	00204	10204	01204	11204	00205	10205	01205	11205	
10102	10204	20204	11204	21204	10205	20205	11205		
01102	01204	11204	02204	12204	01205	11205			
11102	11204	21204	12204	22204	11205				
00103	00205	10205	01205	11205					
10103	10205	20205	11205						
01103	01205	11205							
11103	11205								
11015									

Exemplo 4.14. *Temos que* $001110015 \sim 001110205 \sim 001112105 \sim 020112105 \sim 210112105$. *Estaremos interessados apenas em* 001112105*,* 020112105 *e* 210112105*. Teremos então a seguinte escolha para as sequências linha e coluna:*

	001112105	$\sim$	020112105	$\sim$	210112105
Linha	$00***110@$		$010**110@$		$110**110@$
Coluna	$00***100@$		$010**100@$		$100**100@$
♯	16		8		8

Os termos 000000000*,* 001110015 *são adicionadas nas sequências, respectivamente. Obtemos portanto as sequências linha e coluna com tamanho* $16 + 8 + 8 + 2 = 34$. *Portanto, temos que* $N(001110015) \geq 34$.

Mostraremos a seguir como encontrar as sequências quase bem-comportadas, que chamamos de sequência linha e sequência coluna. Uma vez que as sequências são selecionadas, nós podemos calcular o tamanho das sequências linha e coluna, o que nos dará uma cota inferior de $N(h_r)$.

Para cada h_r, com $a_2a_1 = 15$, podemos dividir o monômio $a_m \dots a_3 15$ em partições, que chamaremos de $\mathcal{L}_\mu$ e $\mathcal{K}_\mu$, cujos tamanhos representaremos por l_μ e k_μ, respectivamente, para $\mu = 1, 2, \dots, p$. Teremos que $\mathcal{L}_\mu$ conterá $1's$ consecutivos enquanto $\mathcal{K}_\mu$ conterá $0's$ consecutivos. O índice μ crescerá da direita para a esquerda e k_p deverá ser 0 enquanto k_μ será maior igual a 1 para $\mu \neq p$ e $l_\mu \geq 1$ para todo μ.

Exemplo 4.15. *Considere o seguinte monômio padrão*

$$11100001100010011115.$$

Temos que $p = 4$*;* $L_1 = 1111$*;* $K_1 = 00$*;* $L_2 = 1$*;* $K_2 = 000$*;* $L_3 = 11$*;* $K_3 = 0000$*;* $L_4 = 111$*;* $K_4 = \emptyset$*; e* $l_1 = 4$*;* $k_1 = 2$*;* $l_2 = 1$*;* $k_2 = 3$*;* $l_3 = 2$*;* $k_3 = 4$*;* $l_4 = 3$*;* $k_4 = 0$.

Seja h_r o monômio padrão do exemplo visto no exemplo acima. Seja $h^{'}$ o monômio obtido, através das seguintes mudanças: para cada $\mu \neq p$

i) $\mathcal{L}_\mu$ é transformado em $\mathcal{L}_\mu^{'}$ trocando o 1 mais a esquerda por 0.

2) $\mathcal{K}_\mu$ é transformado em $\mathcal{K}_\mu^{'}$ trocando o 0 mais a esquerda por 2 e todos os outros $0's$ devem ser trocados por 1.

Assim, pelos teoremas mostrados anteriormente, sabemos que $h_r \sim h^{'}$. Então temos que

$$h^{'} = 00\cdots011\cdots5 \sim 00\cdots201\cdots5 \sim \cdots \sim 21\cdots101\cdots5.$$

Estes monômios serão chamados *monômios úteis de* h_r. Por exemplo, considere o monômio $h_r = 11100001100010011115$, então, o monômio 11121110121102101115 é o único monômio útil de h_r. Agora, se considerarmos $h_r = 001110000011000100111115$, teremos os seguintes monômios úteis:

$$001112111010121102101115 \sim 020112111010121102101115 \sim 210112111010121102101115.$$

Definição 4.2. *Um monômio na forma* $c_m\cdots c_25$ *onde* $c_i \in \{0,1,2\}$ *para* $i = 2,\ldots,m$, *é chamado monômio quase-padrão.*

Considere um monômio quase-padrão $c_m\cdots c_j\cdots 5$. Se $\cdots c_jc_{j-1}\cdots c_i2\cdots$, onde $c_s = 1$ para $s = i, i+1,\ldots,j$, então a j-ésima posição é chamada *posição dupla*. Se $\cdots c_jc_{j-1}\cdots c_i0\cdots$, onde $c_s = 1$ para $s = i, i+1,\ldots,j$, então a j-ésima posição é chamada *posição simples*. Se $c_j = 0, 2$, então a j-ésima posição é chamada *posição zero* ou *posição dois*, respectivamente. Com estas notações, podemos construir a seguinte regra:

Definição 4.3. ***Algoritmo de Seleção*** *: Para cada monômio útil de* h_r, *os monômios da sequência linha serão escolhidos da seguinte forma: nas posições duplas coloramemos* $*$*; nas posições simples colocaremos* 1*; Nas posições 0 e 2 colocaremos 0 ou 1; na primeira posição estará um* @. *Já para a sequência coluna, faremos da seguinte forma: nas posições duplas colocaremos* $*$*; nas posições simples colocaremos* 0*; nas posições 0 ou 2 colocaremos 1 ou 0; na primeira posição colocaremos* @.

Vejamos um exemplo para entendermos melhor as definições acima.

Exemplo 4.16. *Considere* $h_r = 001110000011000100111115$, *vimos acima que seus monômios úteis são 001112111010121102101115, 020112111010121102101115 e 210112111010121102101115. Portanto selecionamos os monômios das sequências linha e coluna da seguinte forma:*

001112111010121102101115	020112111010121102101115	210112111010121102101115
$00***11110*1110110***@$	$010**11110*1110110***@$	$110**11110*1110110***@$
$00***10000*1000100***@$	$010**10000*1000100***@$	$100**10000*1000100***@$

Teorema 4.2. *Dado um monômio* h_r, *com* $a_2a_1 = 15$, *o tamanho* $N^*(h_r)$ *da linha e coluna obtida pela regra de seleção acima é dado por:*

$$N^*(h_r) = 2(2^{\sum_{\mu=1}^{p}(l_\mu-1)}(k_p+2)) + 2. \tag{4.10}$$

Demonstração. *O resultado segue do algoritmo dado para a obtenção das sequências linha e coluna.* □

Exemplo 4.17. *Se tivermos* $p = 2$, $\mathcal{L}_1 = 1$, $\mathcal{K}_1 = 0$, $\mathcal{L}_2 = 11$, $\mathcal{K}_2 = \emptyset$ *e* $l_1 = 1$, $k_1 = 1$, $l_2 = 2$, $k_2 = 0$, *pelo teorema acima, temos que:*

$$N^*(11015) = 2(2^{(1-1)+(2-1)}(0+2)) + 2 = 10.$$

Exemplo 4.18. *Se tivermos* $p = 2$, $\mathcal{L}_1 = 1$, $\mathcal{K}_1 = 0$, $\mathcal{L}_2 = 11$, $\mathcal{K}_2 = \emptyset$ *e* $l_1 = 1$, $k_1 = 1$, $l_2 = 2$, $k_2 = 0$, *pelo teorema acima, temos que:*

$$N^*(11015) = 2(2^{(1-1)+(2-1)}(0+2)) + 2 = 10.$$

Exemplo 4.19. *Pelo teorema acima, temos que:*

$$N^*(111000011000010011115) = 2(2^{(4-1)+(1-1)+(2-1)+(3-1)}(0+2)) + 2 = 258.$$

Agora iremos demonstrar o teorema principal desta seção.

Teorema 4.3. *As sequência linha e coluna, obtidas pelo algoritmo 4.3 são sequências quase-bem-comportadas para* h_r.

Demonstração. *Sejam* $r_m \cdots r_1$ *e* $c_m \cdots c_1$ *monômios das sequências linha e coluna, respectivamente, diferentes de* h_1 *e* h_r *e* $w(r_m \cdots r_1) + w(c_m \cdots c_1) \leq w(h_r)$. *Seja* $p_m \cdots p_1 = r_m \cdots r_1 + c_m \cdots c_1$, *onde* $p_i = r_i + c_i$, *para* $m \geq i \geq 1$. *Seja também,* $m - k_p \geq i$, *se a* i*-ésima posição é uma posição 0 ou 2, então* $p_i = 0$ *ou* 2, *respectivamente; se é uma posição simples, então* $p_i = 1$*; se é uma posição dupla, então* $p_i = 0, 1$ *ou* 2. *Nas últimas posições de* k_p, *denotamos por* $p_m \cdots p_{m-k_p+1}$, *se* $p_\mu = 2$, *então* $p_{\mu-1} = \cdots = p_{m-k_p+1} = 1$. *Portanto este produto é consistente com* h_p, *dessa forma,* $w(h_p) \leq w(h_r)$. *Isto completa a prova do teorema.*

□

4.3 Códigos que excedem a cota de Garcia-Stichtenoth

Nesta seção estaremos interessados nos monômios padrões $t_m \cdots t_{l+1}01 \cdots 15$, onde $l > 2$. Iremos encontrar uma cota inferior para $N(t_m \cdots t_{l+1}01 \cdots 15)$.

Pelo algoritmo visto anteriormente, sabemos que $t_m \cdots t_{l+1}01 \cdots 15$ e $t_m \cdots t_{l+1}20 \cdots 15$ são monômios quase-padrões equivalentes. Selecionamos os seguintes monômios para a sequência linha

$$\begin{gathered} 00 \cdots 00 \\ t_m \cdots t_{l+1}0a_{l-1} \cdots a_2a_1 \\ t_m \cdots t_{l+1}10a'_{l-2} \cdots a'_2a'_1 \\ t_m \cdots t_{l+1}01 \cdots 15 \end{gathered}$$

e para sequência coluna, os seguintes monômios

$$\begin{gathered} 00 \cdots 00 \\ 0 \cdots 0b_{l-1} \cdots b_2b_1 \\ 0 \cdots 10b'_{l-2} \cdots b'_2b'_1 \\ t_m \ldots t_{p+1}01 \cdots 15 \end{gathered}$$

onde $a_i + b_i = a'_i + b'_i = 1$, para $2 \leq i \leq l-2$, $a_{l-1} + b_{l-1} = 1$, $a_1 + b_1 = a'_1 + b'_1 = 5$, $a_1, a'_1, b_1, b'_1 \in \{2, 3\}$ e $a_i, b_i, a'_i, b'_i \in \{0, 1\}$. Assim, cada linha e coluna possui $2^l + 2^{l-1}$ termos. A matriz

síndrome é uma sequência quase-bem-comportada, pois selecionamos os monômios utilizando o algoritmo 4.3 O número de termos bem-comportados consistentes com $t_m \cdots t_{l+1}01 \cdots 15$ é igual portanto a $2^l + 2^{l-1}$. Portanto segue diretamente do Teorema 4.2 o seguinte resultado.

Corolário 4.1.

$$N(t_m \cdots t_{l+1}01 \cdots 15) \geq 2^l + 2^{l-1} + 2.$$

Exemplo 4.20. *Considere o monômio* 10115. *Neste caso,* $m = 5$, $l = 3$. *Temos que* 10115 *e* 12015 *são monômios quase-padrões equivalentes. As sequências linha e coluna serão dadas por:*

$$\begin{aligned} SL &= \{00000, 10002, 11002, 10102, 10012, 11012, 10112, 10003, 11003, 10103, 10013, 11013, 10113, 10115\} \\ SC &= \{00000, 00002, 01002, 00102, 01012, 00112, 00003, 01003, 00103, 00013, 01013, 00113, 10115, 10115\}. \end{aligned}$$

Teremos portanto a seguinte matriz síndrome:

00000	00002	01002	00102	01012	00112	00003	01003	00103	00013	01013	00113	10115	10115
10002	10004	11004	10104	10014	10014	10114	10005	11005	10105	10015	11015	10115	
11002	11004	12004	11104	11014	11014	11114	11005	12005	11105	11015	12015		
10102	10104	11104	10204	10114	10114	10214	10105	11105	10205	10115			
10012	10014	11014	10114	10024	11024	10124	10015	11015	10115				
11012	11014	12014	11114	11024	10124	11124	11015	12015					
10112	10114	11114	10214	10124	10015	10224	10115						
10003	10005	11005	10105	10015	11015	10115							
11003	11005	12005	11105	11015	10115								
10103	10105	11105	10205	10115									
10013	10015	11015	10115										
11013	11015	12015											
10113	10115												
10115													

Temos portanto, pelo corolário acima, $2^l + 2^{l-1} + 2 = 14$ *termos bem-comportados consistentes com* 10115.

Se escolhermos todos os monômios exceto $t_m \cdots t_{l+1}t_l1 \cdots 15$ para compor a matriz teste de paridade, então esta matriz definirá um (n, k, d)-código quase-Hermitiano sobre $\mathbb{F}_4$, onde $n = 3\dot{2}^{m-1} + 1$, $k = 2^{m-l+1}$, e $d \geq 2^l + 2^{l-1} + 2$. Considere o caso especial, onde $l = \frac{m}{2}$, para algum m par. Então,

$$k + d \geq 2^{\frac{m}{2}+1} + 2^{\frac{m}{2}} + 2^{\frac{m}{2}-1} + 2 = 3 \cdot 2^{\frac{m}{2}} + 2^{\frac{m}{2}-1} + 2. \tag{4.11}$$

Por outro lado, para $q = 2$ o gênero é dado por:

$$g_m = \begin{cases} 2^m + 2^{m-1} + 2^{\frac{m+1}{2}} - 2^{\frac{m+1}{2}} + 1 & \text{se m é ímpar;} \\ 2^m + 2^{m-1} + 2^{\frac{m}{2}-1} - 2^{\frac{m+2}{2}} + 1 & \text{se m é par.} \end{cases} \tag{4.12}$$

Temos portanto que

$$n - g_m = \begin{cases} 2^{\frac{m+1}{2}+1} + 1 & \text{se m é ímpar} \\ 3 \cdot 2^{\frac{m}{2}} + 1 & \text{se m é par.} \end{cases} \tag{4.13}$$

Quando m é par, se construirmos o AG-código com parâmetros (n, k, d^*), então, pelo teorema de Riemann-Roch, temos que $d^* = n - k - g_m + 1$, isto é, $d^* + k - 1 \geq n - g_m$. Comparando 4.11 com 4.13, temos que

$$d + k - 1 > d^* + k - 1.$$

Estes códigos excedem a cota de Garcia-Stichtenoth.

Este caso é apenas um caso especial, utilizando o Teorema 3.2, podemos construir muitos códigos que superam a cota de Garcia-Stichtenoth.

Referências Bibliográficas

[1] FENG, G. L., RAO, Thammavarapu R. N., *A Simple Approach for Construction of Algebraic-Geometric Codes from Affine Plane Curves* , in IEEE Transaction On Information Theory, vol. 40, n. 4, p. 1003-1012, 1994. https://doi.org/10.1159/000239294

[2] FENG, G. L., KOLLURU, Mahadev S., RAO, Thammavarapu R. N.,*Construction of Improved Geometric Goppa Codes from Klein Curves and Klein-like Curves*, AAECC 10, p. 433–464, 2000. https://doi.org/10.1007/s002009900018

[3] FENG, G. L., RAO, Thammavarapu R. N., *Improved Geometric Goppa Codes Part 1: Basic Theory*, in IEEE Transaction On Information Theory, vol. 41, n. 6, p. 1678-1693, 1995. https://doi.org/10.1159/000239294

[4] GARCIA, Arnaldo, STICHTENOTH, Henning.*A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, in Invent Math 121, p. 211–222, 1995. https://doi.org/10.1007/BF01884295

[5] GOPPA, Valery D.,*Codes associated with divisors*, Problemy Peredachi Informatasii, vol. 13, p.33-39, 1977.

[6] GOPPA, Valery D., *Rational representation of codes and (L,g)-codes*, Problemy Peredachi Informatsii, vol. 7, p. 223-229, 1971.

[7] HEFEZ, Abramo e VILLELA, Maria Lucia T., *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, 2008.

[8] HODOLT, Tom, LINT, Jacobous V., PELLIKAAN, Ruud, *Algebraic Geometry Codes*, in Handbook of Coding Theory, vol. 1, p. 871-961, Elsevier, Amsterdam, 1998.

[9] PEELLINKAAN, Ruud, *On the existence of order functions*, in Journal of Statistical Planning and Inference, vol. 94, n. 2, p. 287-301, 2001. https://doi.org/10.1016/S0378-3758(00)00260-3

[10] STICHTENOTH, Henning, *Algebraic Function Fields and Codes*, Springer, 2º Edição, p. 1-65, 2009. https://doi.org/10.1007/978-3-540-76878-4

[11] VICENTIM, Steve da Silva, *Curvas algébricas sobre corpos finitos*, Dissertação (Mestrado em Matemática) - Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2012. https://doi:10.11606/D.55.2012.tde-19072012-112150.