Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Tese de Doutorado

Codificação de certos códigos de Goppa geométricos utilizando a teoria de Bases de Gröbner e códigos sobre a curva Norma-Traço

por

Guilherme Chaud Tizziotti

Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Fernando Eduardo Torres Orihuela

Este trabalho contou com apoio financeiro do CNPq e da CAPES.

Codificação de certos códigos de Goppa geométricos utilizando a teoria de Bases de Gröbner e códigos sobre a curva Norma-Traço

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Guilherme Chaud Tizziotti** e aprovada pela comissão julgadora.

Campinas, 03 de junho de 2008.

Prof. Dr. Fernando E. Torres Orihuela

Banca examinadora:

Prof. Dr. Fernando E. Torres Orihuela.

Prof. Dr. Paulo Roberto Brumatti.

Profª. Drª. Sueli Irene Rodrigus Costa.

Prof. Dr. Cicero Carvalho.

Profª. Drª. Miriam del Milagro Abdon.

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

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues

Tizziotti, Guilherme Chaud

T546c Codificação de certos códigos de Goppa geométricos utilizando a teoria de bases de Gröbner e códigos sobre a curva Norma-Traço / Guilherme Chaud Tizziotti -- Campinas, [S.P. :s.n.], 2008.

Orientador : Fernando Eduardo Torres Orihuela

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos de Goppa. 2. Bases de Gröbner. 3. Weierstrass, Pontos de. I. Torres Orihuela, Fernando Eduardo. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: Encoding geometric Goppa codes via Gröbner basis and codes on Norm-Trace curves

Palavras-chave em inglês (Keywords): 1. Goppa codes. 2. Gröbner basis. 3. Weierstrass points.

Área de concentração: Álgebra, Geometria Algébrica

Titulação: Doutor em Matemática

Banca examinadora:

Prof. Dr. Fernando Eduardo Torres Orihuela (IMECC-UNICAMP)
Prof. Dr. Paulo Roberto Brumatti (IMECC-UNICAMP)
Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)
Prof. Dr. Cícero Carvalho (UFU)
Profa. Dra. Miriam del Milagro Abdon (UFF)

Data da defesa: 03/06/2008

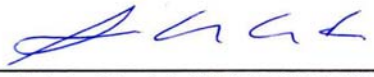
Programa de pós-graduação: Doutorado em Matemática

Tese de Doutorado defendida em 03 de junho de 2008 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA

Prof. (a). Dr (a). PAULO ROBERTO BRUMATTI



Prof. (a). Dr (a). SUELI IRENE RODRIGUES COSTA

Prof. (a). Dr (a). ~~MIRIAM~~ DEL MILAGRO ABDON

Prof. (a). Dr (a). CÍCERO FERNANDES DE CARVALHO

Agradecimentos

Agradeço:

Primeiramente ao meu amigo e orientador Fernando Torres por todos ensinamentos e dedicação.

À UNICAMP e a todos do IMECC pela oportunidade, em especial aos professores da Álgebra.

À CAPES e CNPq pela ajuda financeira.

Aos meus pais e irmãos por todo o apoio.

À Catarine, amor da minha vida, pelo companheirismo e apoio.

À toda minha família, avós, tios e primos.

Aos meus amigos, em especial a meu companheiro Ednei.

À Universidad de Valladolid pela forma com que me recebeu e por todas as oportunidades, agradeço ao professor Antônio Campillo em nome de todos.

Ao professor Carlos Munuera pelos ensinamentos e atenção que a mim foram dados.

Agradeço a Deus por colocar todas estas pessoas em minha vida, pelas oportunidades e por tudo que Ele sempre fez por mim.

Abstract

We extend results of Heegard, Little and Saints concerning the Gröbner basis algorithm for one-point Hermitian codes. We work with two-point and n-point Hermitian codes and codes arising from the Norm-Trace curve. We also determine the Weierstrass semigroup at a certain pair of rational points in such curves and uses these computations to improve the lower bound on the minimum distance of two-point algebraic geometry codes arising from them.

Resumo

Estendemos resultados de Heegard, Little e Saints relacionados a bases de Gröbner para códigos Hermitianos pontuais. Trabalhamos com códigos Hermitianos bipontuais e n-pontuais, e com códigos sobre a curva Norma-Traço. Além disso, determinamos o semigrupo de Weierstrass de um certo par de pontos racionais sobre a curva Norma-Traço e com esse semigrupo conseguimos melhorar a cota da distância mínima de códigos construídos sobre tais curvas.

SUMÁRIO

Introdução

Seja $\mathcal{X}_m$ a curva Hermitiana dada pela equação $y^m + y = x^{m+1}$ sobre $\mathbb{F}_{m^2}$, onde m é potência de um número primo. Sejam P_∞ o único ponto no infinito e D a soma dos outros m^3 pontos $\mathbb{F}_{m^2}$-racionais de $\mathcal{X}_m$. Utilizando um automorfismo do código de Goppa geométrico $C = C_L(D, aP_\infty)$, com $a \in \mathbb{N}$, de ordem $m^2 - 1$ (ver 1.0.5) e aproveitando uma estrutura de módulo para C sobre $\mathbb{F}_{m^2}[t]$, J. Little, H. Saints e C. Heegard definiram, em [14], diagrama de raízes para tal código, o qual fornece uma base de Gröbner para o submódulo $\overline{C}$ de $\mathbb{F}_{m^2}[t]$ associado a C (ver final da seção 1.0.2). Tal base de Gröbner será de muita importância para a utilização de um algorítmo de codificação, dado no final da seção 1.0.4, também feito por J. Little et al., mas em [13].

Os resultados obtidos por Little, Saints e Heegard serão vistos no capítulo 1 juntamente com uma introdução sobre codificação que nos motivou a fazer este trabalho.

Começamos a apresentar nossos resultados nos capítulos 2 e 3, que têm como resultados principais o Teorema 2.041, a Proposição 2.0.48 e o Teorema 3.1.6. Nestes capítulos faremos a construção de um diagrama de raízes para códigos Hermitianos bipontuais $C(D, aP_\infty + bP_0)$ e n-pontuais. Para conseguirmos construir tal diagrama utilizamos um automorfismo de ordem $m + 1$ (dado em 2.1 no início do capítulo 2) que possui a característica de fixar a coordenada y em cada uma de suas órbitas. O fato que nos motivou a fazer este estudo é o de que, geralmente, códigos bipontuais possuem melhores parâmetros relativos que os pontuais.

Para a segunda parte deste trabalho estudamos curvas $\mathcal{X}_{q,r}$ sobre $\mathbb{F}_{q^r}$ com a seguinte equação no plano: $x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y^q + y$, onde q é potência de um número

primo e $r \geq 2$ é um inteiro. Tais curvas, chamadas de Norma-Traço, são maximais, possuem um único ponto no infinito $P_\infty = (0 : 1 : 0)$ e podem ser vistas como uma generalização das curvas Hermitianas. No capítulo 4, utilizando um automorfismo η, mostramos que os resultados obtidos por Littles et al. para curvas Hermitianas podem ser obtidos para as curvas Norma-Traço.

Por fim, no capítulo 5 veremos como construir o semigrupo de Weierstrass em um e dois pontos racionais de $\mathcal{X}_{q,r}$ (seção 5.3), e, utilizando tais semigrupos, veremos que códigos de Goppa geométricos bipontuais sobre $\mathcal{X}_{q,r}$ possuem melhores parâmetros quando comparados aos pontuais sobre a mesma (Teorema 5.4.5).

CAPÍTULO 1

Preliminares e Motivação do trabalho

Neste primeiro capítulo, que está dividido em cinco partes, veremos alguns dos fatos que nos motivaram a realizar este trabalho. Começaremos com uma introdução sobre códigos corretores de erros e seu processo de codificação, e encerraremos com os trabalhos de Little, Saints e Heegard sobre codificação de códigos de Goppa geométricos e construção de algoritmo para bases de Gröbner.

Antes de começarmos vejamos algumas notações que serão usadas no decorrer deste trabalho.

$\mathbb{F}_q$ denotará um corpo finito com q elementos, onde q é uma potência de um número primo. Denotaremos por $F/\mathbb{F}_q$, ou simplesmente F, um corpo de funções algébricas sobre $\mathbb{F}_q$.

$\mathcal{X}$ denotará uma curva suave, projetiva e irredultível sobre $\mathbb{F}_q$, e $\mathbb{F}_q(\mathcal{X})$ será o corpo de funções racionais de $\mathcal{X}$ definidas sobre $\mathbb{F}_q$.

$\mathcal{X}_m$ denotará a curva Hermitiana definida sobre $\mathbb{F}_{m^2}$ pela equação afim $x^{m+1} = y^m + y$, onde m também será potência de um número primo.

A definição a seguir será constantemente citada em todo o trabalho.

Definição 1.0.1. Chama-se de *lugar racional* um lugar de $F/\mathbb{F}_q$ que tem grau um. Equivalentemente, um *ponto racional* de $\mathcal{X}$ é um ponto P de $\mathcal{X}$ cujas coordenadas estão em $\mathbb{F}_q$.

1.0.1 Códigos Corretores de Erros

O que vamos ver nesta seção é um exemplo de como a linguagem matemática pode ser aplicada para descrever certas questões do nosso cotidiano. Uma destas aplicações é a codificação sobre a qual começaremos a falar a partir de agora.

Quando queremos transmitir uma informação (mensagem) através de um canal de comunicação (que pode ser uma linha telefônica, um CD, internet, etc.) podemos ter alguns problemas para realizá-la. Tal canal de comunicação pode provocar erros (por exemplo um ruído) em nossa informação inicial. Assim, precisamos de algum mecanismo que permita detectar tais erros e, se possível, corrigi-los para recuperarmos nossa informação inicial. Para resolver este problema foram criados os "códigos corretores de erros", que possuem a seguinte definição.

Definição 1.0.2. Sejam $\mathcal{A}$ um conjunto finito e $n \in \mathbb{N}$. Um *código* (corretor de erros) é um subconjunto $C \subseteq \mathcal{A}^n$.

Chamaremos $\mathcal{A}$ de *alfabeto*, os elementos de C de *palavras* e n será o *comprimento* (ou longitude) de C.

Exemplo 1.0.3. Um simples exemplo desses códigos é a língua portuguesa, onde $\mathcal{A}$ é composto pelas letras do nosso alfabeto e C é formado por todas as palavras da nossa língua.

Observamos que se transmitimos, através de um canal, a palavra "ALFABETO", e recebemos, por exemplo, "ALFABETR", logo vemos que se produziu algum erro, já que "ALFABETR"não pertence a C. Mais ainda, neste caso não é tão difícil de corrigí-lo, pois não existem outras palavras parecidas a "ALFABETR"a não ser a palavra "ALFABETO".

Agora, e se transmitimos a palavra "RATO"e recebemos "RAHO"? Neste caso vemos que há um erro, mas já não podemos corrigi-lo, pois poderíamos ter emitido "RAIO", ou "RARO", que também são palavras muito parecidas a "RAHO". Poderíamos também ter recebido "PATO"ou "TATO", e nem seguer detectaríamos o erro.

De uma forma mais geral, suponhamos que enviamos uma palavra $c \in C$, de um código C qualquer, e recebemos um vetor $c' \in \mathcal{A}^n$. Se $c' \notin C$, podemos garantir que houve erro, mas se $c' \in C$, então não podemos estar seguros de que houve ou não algum erro.

Mas se o código C está bem contruído, suas palavras serão muito diferentes umas das outras e, assim, será mais difícil que uma palavra se transforme em outra com os erros produzidos pelo canal.

Uma maneira de medir a diferença entre duas palavras, ou vetores de $\mathcal{A}^n$, é a distância de Hamming.

Definição 1.0.4. Dados $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{A}^n$, chamamos de *distância de Hamming* entre $\mathbf{x}$ e $\mathbf{y}$, denotada por $d(x, y)$, o número de coordenadas distintas entre $\mathbf{x}$ e $\mathbf{y}$, ou seja,

$$d(x, y) = \sharp\{i \ ; \ x_i \neq y_i \ ; \ 1 \leq i \leq n\}.$$

Com esta definição podemos dar o conceito de distância mínima que é de muita importância no estudo dos códigos.

Definição 1.0.5. A *distância mínima* de um código C é dada por

$$d = d_C = min\{d(x, y) \ ; \ x, y \in C \text{ e } x \neq y\}.$$

Com tal definição temos o seguinte resultado.

Teorema 1.0.6. *Um código C com distância mínima d pode detectar até $d - 1$ erros.*

Agora, vejamos quando e como podemos corrigir esses erros.

Um método natural para corrigir os erros de uma informação é o chamado "método do vizinho mais próximo"que consiste no seguinte: se recebemos a palavra x, a associamos com a palavra $c \in C$ que satisfaz a condição $d(x, c) < d(x, c')$, para qualquer $c' \in C$, com $c' \neq c$.

Logo vemos que tal método possui um problema, podem existir duas ou até mais palavras $c \in C$ que satisfazem tal condição e, assim, não podemos corrigir os erros (vimos este fato no exemplo da língua portuguesa quando recebemos a palavra RAHO). Por outro lado, utilizando esse método podemos quantificar a capacidade de correção do código C. É o que veremos no resultado a seguir.

Teorema 1.0.7. *Um código C com distância mínima d pode corrigir, aplicando o médoto do vizinho mais próximo, até $\lfloor \frac{d-1}{2} \rfloor$ erros.*

Observamos que dado $n \in \mathbb{R}$, o símbolo $\lfloor n \rfloor$ representa o maior inteiro que é menor ou igual a n.

Voltando ao exemplo da língua portuguesa, vemos que uma maneira de diminuir os possíveis erros que não podem ser corrigidos é utilizar uma codificação baseada nas iniciais.

Por exemplo, codificar a palavra "RATO"como Rapaz-Alegria-Total-Ópera. Este método foi muito utilizado em meados do século passado, e até mesmo nos dias de hoje, por exemplo, quando vamos passar uma informação pelo telefone e dizemos B de "Bola", ou D de "Dado".

Tal codificação diminui o problema dos erros, mas por outro lado pode se tornar impraticável quando temos uma mensagem de tamanho maior.

De um modo geral a codificação dos códigos corretores de erros não são muito eficientes, mesmo para serem realizadas computacionalmente, já que são feitas através de tabelas.

O exemplo a seguir, é mais um exemplo destes códigos que encontramos em nosso dia-a-dia.

Exemplo 1.0.8. Código de barras 2/5: Tal código, que é visto nos produtos de um supermercado, é um símbolo gráfico que permite armazenar informação através de uma alternância de barras e espaços em branco de duas espessuras distintas, uma representando o 1 e outra o zero.

Para armazenar um certo número n em um código de barras primeiramente temos que reescrever n de forma binária. Para isso utizamos a seguinte tabela

0=00110	5=10100
1=10001	6=01100
2=01001	7=00011
3=11000	8=10010
4=00101	9=01010

Observe que a cifra se codifica com cinco *bits*: dois 1 e três 0, daí o nome 2/5. Neste caso o alfabeto é $\mathbb{F}_2 = \{0, 1\}$ e o código $C = \{00110, \ldots, 01010\} \subseteq \mathbb{F}_2^5$.

Assim, se queremos representar o número $n = 45$ em um código de barras, escrevemos 45 na sua forma binária, que é 0010110100, e representamos os 0 e 1 com suas respectivas barras, deixando sempre um espaço em branco entre cada uma delas.

Com o objetivo de melhorar o processo de codificação se começou a construir códigos com estruturas algébricas que produzem esta melhora. Assim, surgiram, e continuam surgindo, muitos tipos de códigos, como por exemplo: os códigos lineares, cujo processo de codificação é feito através de uma matriz geradora, os códigos cíclicos, com codificação baseada em divisões polinomiais, e, por fim, os códigos algébricos geométricos, que podem possuir uma

estrutura de módulos com a qual se produz um eficiente algoritmo de codificação utilizando bases de Gröbner.

Citamos estes códigos, pois os veremos mais detalhadamente nas próximas seções.

1.0.2 Códigos Lineares e Automorfismos

Seja $\mathbb{F}_q$ um corpo finito com q elementos. Se o alfabeto $\mathcal{A}$ é $\mathbb{F}_q$ e $C \subseteq \mathbb{F}_q^n$ é um subespaço linear, então dizemos que C é um *código linear* (sobre $\mathbb{F}_q$). Denotaremos por $dimC$ a dimensão (como $\mathbb{F}_q$-subespaço vetorial) de C e d será sua distância mínima. Lembramos que n é o comprimento de C.

Um código com parâmetros $[n, k, d]$, ou $[n, k, d]$-código, é um código de comprimento n, dimensão k e distância mínima d.

Seja C um código linear com parâmetros $[n, k, d]$ sobre um corpo finito $\mathbb{F}_q$. Como $dimC = k$ e C é um subespaço vetorial de $\mathbb{F}_q^n$, C pode ser interpretado como imagem de uma aplicação linear injetiva $\alpha : \mathbb{F}_q^k \to C \subseteq \mathbb{F}_q^n$. A matriz M, de ordem $k \times n$, que é a transposta da matriz de tal aplicação é chamada de matriz geradora do $[n, k, d]$-código C e as linhas dessa matriz formam uma base de C.

Usando a matriz M obtemos o seguinte algoritmo de codificação para C: dado $\mathbf{w} \in \mathbb{F}_q^k$, multiplicamos o vetor linha $\mathbf{w} = (w_1, \ldots, w_k)$ por M. Logo, temos $w.M = c$, onde c é um vetor linha em $\mathbb{F}_q^n$ e $c \in C$.

Este algoritmo pode não ser tão eficiente, pois a quantidade de informações necessárias para realizá-lo, que são as entradas de M, pode ser muito grande, tornando esse algoritmo menos eficaz.

Então, procuramos códigos com alguma estrutura algébrica extra que nos permita realizar uma codificação mais eficiente que o da matriz geradora. Um tipo de código que possui uma estrutura algébrica para isso são os códigos cíclicos.

Definição 1.0.9. Um código $C \subseteq \mathbb{F}_q^n$ sobre $\mathbb{F}_q$ é *cíclico* se satisfaz a seguinte condição: se $(c_1, \ldots, c_n) \in C$, então $(c_n, c_1, \ldots, c_{n-1}) \in C$.

Em outras palavras, se σ é a permutação de $\{1, \ldots, n\}$ dada por $\sigma(n) = 1$ e $\sigma(i) = i + 1$, para $i = 1, 2, \ldots, n - 1$, então C é cíclico se $(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)}) \in C$, para todo $c \in C$.

Denotaremos $\sigma(c) = (c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)})$, para $c \in C$.

O resultado (visto em [8] Teorema 1 seção 6.3) que nos dá uma estrutura algébrica extra para um código cíclico é o seguinte.

Teorema 1.0.10. *Seja C um código linear sobre $\mathbb{F}_q$ de comprimento n e dimensão k. Então C é cíclico se, e somente se, C pode ser visto (identificado) como um ideal do anel $\dfrac{\mathbb{F}_q[t]}{\langle t^n-1\rangle}$, que é um anel principal.*

Isto significa que se C é cíclico, existe $g(x) = \overline{g(x)} \in \frac{\mathbb{F}_q[x]}{\langle x^n-1\rangle}$, de grau $r = n-k$, que divide x^n-1, tal que C pode ser associado a $\langle g(x)\rangle$ (ideal gerado por $g(x)$). Sendo $g(x) = x^r + a_{r-1}x^{r-1} + \ldots + a_1x + a_0$ temos a seguinte sistemática de codificação:

Dado $\overrightarrow{w} = (w_1, w_2, \ldots, w_k) \in \mathbb{F}_q^k$, construímos o polinômio $w(x) = w_1x^{n-1} + w_2x^{n-2} + \ldots + w_kx^{n-k}$. Dividimos $w(x)$ pelo polinômio gerador $g(x)$ e, assim, $w(x) = q(x).g(x) + r(x)$, onde o grau de $r(x)$ é menor que $n-k$. Logo $w(x) - r(x) = q(x).g(x) \in \langle g(x)\rangle$ e, portanto pode-se associar $w(x) - r(x)$, através de seus coeficientes, a uma palavra de C. Note que a forma com que $w(x)$ é construído nos garante uma bijetividade entre $w(x) - r(x)$ e a palavra em C a ele correspondida. De fato, suponha que exitem $w_1(x) \neq w_2(x)$ tais que $w_1(x) - r_1(x) = w_2(x) - r_2(x)$, logo $w_1(x) - w_2(x) = r_1(x) - r_2(x)$ que é um absurdo, pois (como $w_1(x) \neq w_2(x)$) $grau(w_1(x) - w_2(x)) \geq n-k$ e $grau(r_1(x) - r_2(x)) < n-k$.

Observe que neste caso necessitamos somente de $r = n-k$ informações, que são os coeficientes de $g(t)$, para se fazer a sistemática de codificação.

Assim, vimos que um código cíclico possui uma estrutura algébrica, de um ideal em $\dfrac{\mathbb{F}_q[t]}{\langle t^n-1\rangle}$, que nos ajuda na construção de um algoritmo de codificação mais eficiente que o da matriz geradora. Uma pergunta a fazer é: e se C não é cíclico, podemos encontrar outro tipo de estrutura que nos ajude na construção de um novo algoritmo de codificação?

A resposta para essa pergunta é sim, e passa pela definição de automorfismo de um código.

Sejam $(c_1, \ldots, c_n) \in \mathbb{F}_q^n$ e S_n o grupo simétrico cujos elementos são as permutações do conjunto $\{1, 2, \ldots, n\}$.

Para $\pi \in S_n$, S_n age sobre $\mathbb{F}_q^n$ via: $\pi(c_1, c_2, \ldots, c_n) = (c_{\pi(1)}, c_{\pi(2)}, \ldots, c_{\pi(n)})$.

Então, o grupo de automorfismos de C é dado por:

$$\mathbf{Aut(C)} = \{\pi \in S_n \ ; \ \pi(C) = C\} = \{\pi \in S_n \ ; \ \pi(c) \in C \ , \ \forall c \in C\}.$$

Consideremos C com um $\sigma \in Aut(C)$. O fato de $\sigma \in S_n$, nos diz que ele divide o conjunto $\{1, 2 \ldots, n\}$ em r blocos (ou órbitas) cíclicas, onde r pode variar de 1 (como no caso dos códigos cíclicos) a n. Denotaremos tais órbitas por $O_1, \ldots, O_r$.

Fixemos um elemento $c_{i,0} \in O_i$, para $j = 0, 1, \ldots, |O_i| - 1$, que é um abuso de notação, já que $O_i \subseteq \{1, \ldots, n\}$. Definimos $c_{i,j} = \sigma^j(c_{i,0})$. Logo, vemos que $c_{i,|O_i|} = c_{i,0}$ e, por convenção, escrevemos $c_{i,-1} = \sigma^{-1}(c_{i,0}) = c_{i,|O_i|-1}$.

Portanto, dada $\overrightarrow{c} = (c_1, \ldots, c_n) \in C$ e rearranjando, se necessário, as componentes de $\overrightarrow{c}$ vemos que se pode representar as palavras de C como r-uplas de polinômios em uma variável $(h_1(t), \ldots, h_r(t))$, onde

$$h_i(t) = \sum_{j=0}^{|O_i|-1} c_{i,j} t^j.$$

Podemos ver as r-uplas $(h_1(t), \ldots, h_r(t))$ como elementos do $\mathbb{F}_q[t]$-módulo

$$M = \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{|O_i|} - 1 \rangle}.$$

O $\mathbb{F}_q[t]$-submódulo $\overline{C} \leq \mathbb{F}_q[t]^r$ gerado pelas palavras código de C e por $q_i = (t^{|O_i|} - 1)e_i$, onde para $i = 1, \ldots, r$, e_i é o i-ésimo vetor da base padrão de $\mathbb{F}_q[t]^r$ é dito associado a C. Também podemos ver $\overline{C}$ como sendo a imagem inversa $\pi^{-1}(C)$ da sobrejeção

$$\pi : \mathbb{F}_q^r[t] \to \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{|O_i|} - 1 \rangle}.$$

Portanto, vimos como um $[n, k, d]$-código linear C com um automorfismo σ pode ser associado a um submódulo $\overline{C}$ do módulo livre $\mathbb{F}_q^r[t]$. Com essa estrutura de módulos veremos, nas próximas seções, como fazer um algoritmo de codificação semelhante ao de códigos cíclicos.

1.0.3 O caso de Códigos de Goppa Geométricos

Seja $\mathcal{X}$ uma curva projetiva suave e irredutível sobre $\mathbb{F}_q$.

Definição 1.0.11. Dado $D \in Div(\mathcal{X})$ definimos o espaço $\mathbb{F}_q$-vetorial de Riemann-Roch associado a D como:

$$\mathcal{L}(D) = \{f \in \mathbb{F}_q(\mathcal{X}) \setminus \{0\} \ ; \ D + (f) \succeq 0\} \cup \{0\}$$

onde $D_1 \succeq D_2 \ \Leftrightarrow \ v_P(D_1) \geq v_P(D_2) \ , \forall \ P \in \mathcal{X}$.

Definição 1.0.12. Sejam $P_1, \ldots, P_n$ pontos distintos de $\mathcal{X}$, e $G \in Div(\mathcal{X})$ tal que $v_{P_i}(G) = 0$. Definimos a aplicação

$$ev_{P_1,\ldots,P_n} = ev : \mathcal{L}(G) \to \mathbb{F}_q^n$$
$$f \mapsto ev(f) = (f(P_1), \ldots, f(P_n))$$

que é chamada de *aplicação de avaliação.*

Utilizando tais definições definimos código de Goppa geométrico.

Definição 1.0.13. Sendo $D = P_1 + \ldots + P_n \in Div(\mathcal{X})$, onde $P_i \neq P_j$ se $i \neq j$, e $G \in Div(\mathcal{X})$ com $v_{P_i}(G) = 0$, isto é, $SuppG \cap SuppD = \emptyset$, definimos o *código de Goppa associado a D e G*, e escrevemos $C(D, G)$, como sendo $ev(\mathcal{L}(G))$, ou seja, $C(D, G) = ev(\mathcal{L}(G))$.

Para esses códigos também podemos construir um algoritmo de codificação através da matriz geradora de $C(D, G)$. Tal matriz é dada por

$$M = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_k(P_1) & \ldots & f_k P_n, \end{pmatrix}$$

onde $\{f_1, \ldots, f_k\}$ é uma coleção de funções em $L(G)$, cujas imagens em $\dfrac{L(G)}{L(G-D)}$ formam uma base para tal espaço, e $D = \sum_{i=1}^{n} P_i$.

Analogamente ao caso de códigos lineares construímos um algoritmo de codificação para $C(D, G)$.

Observamos que fazendo operações com as linhas de M e, se necessário, trocas de colunas (que é uma reordenação dos pontos de D), podemos ver M como

$$M' = [I_k \mid B]$$

onde I_k é a matriz identidade $k \times k$ e B é uma matriz $k \times (n-k)$. Logo, a quantidade de informações necessárias para se fazer o algoritmo é $k \times (n-k)$, que é o número de entradas da matriz B.

A seguir, veremos que uma estrutura de módulo de $C(D, G)$ pode reduzir a quantidade de informações para se descrever uma sistemática de codificação. Para isso necessitamos que $C(D, G)$ possua um certo automorfismo, e sobre isso temos os resultados a seguir.

Lema 1.0.14. *([23]) Se $\sigma_{\mathcal{X}}$ é um automorfismo da curva $\mathcal{X}$ que fixa os divisores D e G, então $\sigma_{\mathcal{X}}$ induz um automorfismo não-trivial:*

$$\sigma(f(P_1,\ldots,f(P_n)=((f\circ\sigma_{\mathcal{X}}^{-1})(P_1),\ldots,(f\circ\sigma_{\mathcal{X}}^{-1})(P_n))$$

do código de Goppa $C(D,G)$ construído de $\mathcal{X}$.

Demonstração: Veja a demonstração em [23] sec. VII.3.3.

Corolário 1.0.15. *([13]) Seja H um subgrupo cíclico de $Aut(\mathcal{X})$ gerado por σ, e seja*

$$Supp(D)=O_1\cup\ldots\cup O_r$$

a decomposição do suporte de D em órbitas disjuntas sobre a ação de H. Então as entradas das palavras código correspondem aos pontos em cada O_i, que são permutados ciclicamente por σ.

Observação 1.0.16. O lema 1.0.14 nos diz como conseguir um automorfismo de $C(D,G)$ através de um automorfismo da curva $\mathcal{X}$. Esse resultado tem muito valor, pois se C é um código linear qualquer podemos ter muitas dificuldades em encontrar um automorfismo de C. Logo, vemos a importância de trabalhar com códigos algébricos geométricos sobre curvas com grupo de automorfismos conhecidos, como as curvas Hermitianas ou de Suzuki por exemplo.

Vejamos como dar uma estrutura de módulos para códigos $C(D,G)$ com um automorfismo σ que fixa D e G.

Seja $supp(D)=O_1\cup\ldots\cup O_r$. Renomeamos os pontos de $supp(D)=\{P_1,\ldots,P_n\}$ da seguinte forma: seja $P_{i,0}\in O_i$, um ponto em O_i, para $i=1,\ldots,r$, e para $j=0,1,\ldots,|O_i|-1$ definimos $P_{i,j}=\sigma^j(P_{i,0})$. Portanto, vemos que $P_{i,|O_i|}=P_{i,0}$, e, por convenção, vamos escrever $P_{i,-1}=\sigma^{-1}(P_{i,0})=P_{i,|O_i|-1}$.

Sabemos que se $\in C$, então $=(f(P_1),\ldots,f(P_n))$, com $f\in\mathcal{L}(G)$. Assim, rearranjando as componentes podemos representar as palavras códigos como r-uplas de polinômios em uma variável: $(h_1(t),\ldots,h_r(t))$, onde

$$h_i(t)=\sum_{j=0}^{|O_i|-1}f(P_{i,j})t^j.$$

Como no caso linear, podemos ver as r-uplas $(h_1(t), \ldots, h_r(t))$ como elementos do $\mathbb{F}_q[t]$-módulo

$$M = \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{|O_i|} - 1 \rangle}.$$

E temos, novamente, $C(D, G)$ associado ao submódulo $\overline{C} \leq \mathbb{F}_q[t]^r$ que é a imagem inversa $\pi^{-1}(C)$ da sobrejeção $\pi : \mathbb{F}_q^r[t] \to \bigoplus_{i=1}^{r} \frac{\mathbb{F}_q[t]}{\langle t^{|O_i|} - 1 \rangle}$.

Assim, sabendo que um código $C(D, G)$ com um automorfismo que fixa D e G possui uma estrutura de módulo, Little, Saints e Heegard fizeram uma sistemática de codificação mais eficiente que a da matriz geradora. Veremos essa sistemática na próxima seção.

Para finalizar esta seção vamos dar um importante exemplo de códigos de Goppa geométricos, que são os códigos Hermitianos.

Exemplo 1.0.17. Códigos Hermitianos: Consideremos a curva Hermitiana $\mathcal{X}_m$ definida, sobre F_{m^2}, pela equação no plano $x^{m+1} = y^m + y$.

$\mathcal{X}_m$ tem gênero $g = \dfrac{m(m-1)}{2}$ e possui m^3+1 pontos $\mathbb{F}_{m^2}$-racionais, sendo $P_\infty = (0 : 1 : 0)$ seu único ponto no infinito.

Definimos, para $a \in \mathbb{N}$, $C_a := C(D, aP_\infty)$, onde $D = \sum_{i=1}^{m^3} P_i$ é a soma de todos os pontos $\mathbb{F}_{m^2}$-racionais de $\mathcal{X}_m$, exceto P_∞.

Os códigos C_a são chamados *códigos Hermitianos* (pontuais) e possuem bons parâmetros k e d, e por isso são considerados importantes.

No decorrer deste trabalho faremos alguns estudos sobre esses códigos.

1.0.4 Utilizando bases de Gröbner

Nesta seção veremos como o conceito de base de Gröbner para módulos será utilizado no algoritmo de codificação de Little, Saints e Heegard.

Primeiramente, vejamos o que é uma base de Gröbner. Observamos que uma exposição mais detalhada sobre esse assunto pode ser visto no apêndice A.

Seja $A = k[x_1, \ldots, x_n]$ para algum corpo k. Seja $\{e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1)\}$ uma base de A^m.

Definição 1.0.18. Um *monômio* em A^m é um vetor do tipo $\mathbf{X}e_i$, onde $1 \leq i \leq m$ e $\mathbf{X}$ é monômio (produto de potências) em A.

Se $\mathbb{M}_1 = \mathbf{X}e_i$ e $\mathbb{M}_2 = \mathbf{Y}e_j$ são monômios em A^m, dizemos que $\mathbb{M}_1$ *divide* $\mathbb{M}_2$ se $i = j$ e $\mathbf{X}$ divide $\mathbf{Y}$. Notemos que no caso em que $\mathbb{M}_1$ divide $\mathbb{M}_2$, existe um produto Z em A tal que $\mathbb{M}_2 = Z.\mathbb{M}_1$. Nesse caso definimos $\dfrac{\mathbb{M}_2}{\mathbb{M}_1} = \dfrac{\mathbf{Y}}{\mathbf{X}} = Z$.

Definição 1.0.19. Uma *ordem* sobre monômios de A^m será uma ordem total, $<$, satisfazendo:

i) $\mathbb{M} < Z.\mathbb{M}$, para todo monômio $\mathbb{M}$ de A^m e monômios $Z \neq 1$ de A;

ii) Se $\mathbb{M}_1 < \mathbb{M}_2$, então $Z\mathbb{M}_1 < Z\mathbb{M}_2$, para quaisquer monômios $\mathbb{M}_1, \mathbb{M}_2$ de A^m e qualquer monômio $Z \in A$.

Neste trabalho, a ordem utilizada para a construção das bases de Gröbner é a ordem POT (position over term), que tem a seguinte definição.

Definição 1.0.20. Dada uma ordem total em A e dados dois monômios $\mathbb{M}_1 = \mathbf{X}e_i$ e $\mathbb{M}_2 = \mathbf{Y}e_j$ em A^m, dizemos que $\mathbb{M}_1 <_{POT} \mathbb{M}_2$ se $i > j$ ou $i = j$ e $\mathbf{X} < \mathbf{Y}$ (onde $\mathbf{X}$ e $\mathbf{Y}$ são monômios em A).

Notações: Vejamos agora algumas importantes notações.

Fixada uma ordem $<$ sobre os monômios de A^m, para $f \in A^m$, com $f \neq 0$, temos que $f = a_1\mathbb{M}_1 + a_2\mathbb{M}_2 + \ldots + a_l\mathbb{M}_l$, onde para $1 \leq i \leq l$, $a_i \in k \setminus \{0\}$ e $\mathbb{M}_i$ são monômios em A^m tais que $\mathbb{M}_1 > \mathbb{M}_2 > \ldots > \mathbb{M}_l$. Assim, definimos:

Monômio líder de f= $Lm(f) = \mathbb{M}_1$

Coeficiente líder de f= $Lc(f) = a_1$

Termo líder de f= $Lt(f) = a_1\mathbb{M}_1$

Agora, podemos definir base de Gröbner para módulos.

Definição 1.0.21. Um conjunto de vetores não nulos $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ contido em um submódulo $\mathcal{M}$ de A^m é chamado de *base de Gröbner* para $\mathcal{M}$ se para todo $\mathbf{f} \in \mathcal{M}$ existe $i \in \{1, \ldots, t\}$ tal que $Lm(\mathbf{g}_i)$ divide $Lm(\mathbf{f})$.

Com o conceito de bases de Gröbner, vejamos como será o algoritmo de codificação.

Definição 1.0.22. Dado um código C. Um monômio que aparece como termo líder de algum elemento do submódulo $\overline{C} \leq \mathbb{F}_q[t]^r$ é chamado de monômio "nonstandard". Caso contrário o chamamos de monômio "standard".

Utilizando estas definições temos:

Definição 1.0.23. Dada uma base de Gröbner $\mathcal{G}$ para $\overline{C}$, as posições de informação e os "parity checks"(**verificação de paridade**) para $C(D,G) \leftrightarrow \overline{C}$ são determinadas da seguinte forma:

a) As posições de informação são os coeficientes dos monômios "nonstandard"que aparecem nas r-uplas construídas das palavras $(h_1(t), \ldots, h_r(t))$ do código. Em outras palavras, as posições de informação são os coeficientes dos monômios "nonstandard"da forma $t^l e_j$, onde $l \leq |O_i| - 1$.

b) Os "parity checks"são os monômios "standard".

Seja $\mathcal{G} = \{g_1, \ldots, g_r\}$ uma base de Gröbner de $\overline{C}$. Olhando para os termos líderes de cada g_i obtemos os monômios "nonstandard"que aparecem nas r-uplas construídas das palavras $(h_1(t), \ldots, h_r(t))$ do código. Assim, ordenando (através da ordem POT) tais monômios de forma decrescente obtemos as posições de informação, que serão os $k(= dimC)$ primeiros. Denotaremos esses monômios por $m_l = t^{i_l} e_{j_l}$, para $l = 1, 2, \ldots, k$.

O exemplo abaixo nos mostra exatamente como isto funciona.

Exemplo 1.0.24. Seja $C = C(D, 19P_\infty)$ um código sobre a curva Hermitiana $X^4 = Y^3 + Y$ em $\mathbb{F}_9 = \{1, \alpha, \alpha^2, , \alpha^7\}$ com automorfismo σ dado por $\sigma(x) = \alpha x$ e $\sigma(y) = \alpha^4 y$.

Tal código possui **dimensão** igual a **17** e sob a ação de σ os 27 pontos de D se dividem em 5 órbitas: $O_1 = \{(1, \alpha^7), (\alpha, \alpha^3), (\alpha^2, \alpha^7), (\alpha^3, \alpha^3), (\alpha^4, \alpha^7), (\alpha^5, \alpha^3), (\alpha^6, \alpha^7), (\alpha^7, \alpha^3)\}$, $O_2 = \{(1, \alpha^4), (\alpha, 1), (\alpha^2, \alpha^4), (\alpha^3, 1), (\alpha^4, \alpha^4), (\alpha^5, 1), (\alpha^6, \alpha^4), (\alpha^7, 1)\}$, $O_3 = \{(1, \alpha^5), (\alpha, \alpha), (\alpha^2, \alpha^5), (\alpha^3, \alpha$
$O_4 = \{(0, \alpha^2), (0, \alpha^6)\}$ e $O_5 = \{(0, 0)\}$

Utilizando a ordem POT conseguimos a seguinte base de Gröbner para o submódulo $\overline{C}$:

$g_1 = (1, \alpha^6, \alpha t^5 + \alpha t^4 + \alpha^6 t^3 + \alpha^2 t^2 + \alpha t + \alpha^2, \alpha^2 t + \alpha, 1)$

$g_2 = (0, t + \alpha^5, t^5 + \alpha^5 t^4 + \alpha^7 t^3 + \alpha^7 t + \alpha^7, \alpha^2 t + \alpha^4, 1)$

$g_3 = (0, 0, t^6 + \alpha^6 t^5 + \alpha^2 t^4 + \alpha^7 t^3 + \alpha t^2 + \alpha^4 t + \alpha^5, \alpha^3 t + \alpha^3, \alpha^7)$

$g_4 = (0, 0, 0, t^2 - 1, 0)$

$g_5 = (0, 0, 0, 0, t-1)$

E obtemos as seguintes posições de informação:

$m_1 = t^7 e_1, \ldots, m_7 = te_1, m_8 = e_1$

$m_9 = t^7 e_2, \ldots, m_{15} = te_2$

$m_{16} = t^7 e_3$, $m_{17} = t^6 e_3$.

Observe, pela definição de base de Gröbner, que $LT(g_1)$ tem que dividir $m_1, \ldots, m_8$; $LT(g_2)$ tem que dividir $m_9, \ldots, m_{15}$, e $LT(g_3)$ tem que dividir m_{16} e m_{17}.

Para $h = (h_1(t), \ldots, h_r(t))$, definiremos o vetor $\mathbf{VC}(h) \in \mathbb{F}_q^n$ como sendo o vetor formado pelos coeficientes dos termos de h, listados na ordem POT.

Observação 1.0.25. Utilizando a observação 6.1.9 temos que se $E \leq \mathbb{F}_q[t]^r$ e $\mathcal{G} = \{g_1, \ldots, g_s\}$ é uma base de Gröbner para o submódulo E, então dada $f \in \mathbb{F}_q[t]^r$ temos que

$$f = a_1 g_1 + \ldots + a_s g_s + \overline{f}^{\mathcal{G}}$$

onde $a_1, \ldots, a_s \in \mathbb{F}_q[t]$, $a_1 g_1 + \ldots + a_s g_s \in E$ e $\overline{f}^{\mathcal{G}} \in \mathbb{F}_q[t]^r$ é o resto, que é reduzido com respeito a $\mathcal{G}$.

Com isso se obteve o seguinte algoritmo de codificação.

O Algoritimo de Codificação (Little, Saints e Heegard [13])

Entrada: Base de Gröbner $\mathcal{G}$, $w = (w_1, \ldots, w_k) \in \mathbb{F}_q^k$ e $\{m_1, \ldots, m_k\}$

Saída: $E(w) \in C(D, G)$

Início: Seja $f := \sum_{i=1}^{k} w_i m_i$

Defina $E(w) := \mathbf{VC}(f - \overline{f}^{\mathcal{G}})$

Pela observação 1.0.25 temos que $f - \overline{f}^{\mathcal{G}} \in \overline{C}$, e, portanto, é associado a uma palavra código. Claramente, pela forma com que construímos f (ver definição dos m_i), temos uma bijeção entre $f - \overline{f}^{\mathcal{G}}$ e uma palavra de C. Esta bijeção é mostrada de maneira análoga à que fizemos no caso de códigos cíclicos, só que aqui olhamos cada uma das coordenadas de $f - \overline{f}^{\mathcal{G}} \in \mathbb{F}_q[t]^r$ e usamos que $\overline{f}^{\mathcal{G}}$ é reduzido com respeito a base de Gröbner $\mathcal{G}$ (ver definição 6.1.6 no apêndice).

A quantidade de informações necessárias no algoritmo acima é menor que a quantidade necessária para se desenvolver o algoritmo da matriz geradora, pois se utilizarmos uma base Gröbner reduzida, cada elemento desta base consiste de um termo líder (um termo não standard) e (no máximo) $n-k$ termos standard. Assim o número de informações necessárias neste algoritmo é no máximo $r(n-k)$.

Já o número de operações é praticamente o mesmo, já que no algoritmo da matriz geradora temos que fazer $k(n-k)$ multiplicações e $(k-1)(n-k)$ somas. Por outro lado neste novo algoritmo subtraímos k múltiplos dos elementos da base de Gröbner para remover os monômios standard, onde cada um destes múltiplos consiste de uma constante vezes um monômio vezes um elemento da base de Gröbner, que contém no máximo $n-k$ destes coeficientes não nulos.

Observamos que encontrar uma base de Gröbner para $\overline{C}$ pode ser um tanto complicado, o algoritmo mais conhecido para se fazer isso, o algoritmo de Buchberger (algoritmo 7.13), pode tornar esta tarefa difícil, já que podem ser necessárias muitas divisões polinomiais. Para tornar esta tarefa mais fácil Little et al. fizeram, em [14], um algoritmo, somente para códigos Hermitianos pontuais, mais praticável que o de Buchberger. Veremos como se constrói esse algoritmo na próxima seção.

Para finalizar esta seção vejamos um exemplo que ilustra o funcionamento deste algoritmo de codificação.

Exemplo 1.0.26. Seja $\mathcal{X}_3$ a curva Hermitiana $Y^3 + Y = X^4$ e considere o seguinte automorfismo, cuja ordem é 12

$$\tau(x) = \alpha^2 x \text{ e } \tau(y) = y + \alpha^2.$$

Sabemos que os $m^3 = 27$ pontos $\mathbb{F}_9$-racionais de $\mathcal{X}_3$ são distribuídos em 3 órbitas que são:

$$O_1 = O((1, \alpha^4)) \text{ com 12 elementos}$$

$$O_2 = O((\alpha, 1)) \text{ com 12 elementos}$$

$$O_3 = O((0, 0)) \text{ com 3 elementos}$$

Uma base para $L(19Q)$ é $\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^3y, x^2y^2, xy^3, y^4, x^3y^2, x^2y^2, xy^3\}$.

Dado o código Hermitiano pontual $C = C(D, 19P_\infty)$. Usando a ordem POT em $\mathbb{F}_9[t]^3$ conseguimos a seguinte base de Gröbner para $\overline{C}$:

$g_1 = (1, \alpha^3t^6 + \alpha^7t^4 + \alpha^7t^3 + t^2 + \alpha^6t + \alpha, \alpha^5t^2 + t + \alpha)$

$g_2 = (0, t^7 + \alpha^3t^6 + \alpha^5t^5 + \alpha^4t^4 + \alpha^4t^3 + \alpha^7t^2 + \alpha t + 1, \alpha^2t + \alpha^6)$

$g_3 = (0, 0, t^3 - 1)$

E assim temos as seguintes posições de informação, que são os 17 (que é a dimensão de C) primeiros monômios (com relação a ordem POT) de $\overline{C}$.

$m_1 = t^{11}e_1, \ldots, m_{11} = te_1, m_{12} = e_1$

$m_{13} = t^{11}e_2, \ldots, m_{17} = t^7e_2$

Vamos codificar a mensagem $w = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, \alpha, 1) \in \mathbb{F}_9^{17}$. Com tal vetor e os m_i constuímos $f = (t, \alpha t^8 + t^7, 0)$.

1º) $f - tg_1 = (0, \alpha t^8 + \alpha^6t^7 + \alpha^3t^5 + \alpha^3t^4 - t^3 + \alpha^2t^2 + \alpha^5t, \alpha t^3 - t^2 + \alpha^5t)$.

2º) Dividimos o termo líder de g_2 na segunda componente acima, conseguimos um quociente de $\alpha t + \alpha$ e um resto de $R_2e_2 = (0, \alpha^3t^6 + \alpha^5t^5 + \alpha^6t^4 + \alpha^7t^3 - t^2 + \alpha^3t + \alpha^5, 0)$.

Assim:

$$f - tg_1 - (\alpha t + \alpha)g_2 - R_2e_2 = (0, 0, \alpha t^3 + \alpha t^2 + \alpha^5t + \alpha^3)$$

3º) Dividindo por g_3 obtemos $R_3e_3 = (0, 0, \alpha t^2 + \alpha^5t - 1)$. E assim temos:

$$\overline{f} = (0, R_2, R_3)$$

e portanto

$$f - \overline{f} = (t, \alpha t^8 + t^7 + \alpha^7 t^6 + \alpha t^5 + \alpha^2 t^4 + \alpha^3 t^3 + t^2 + \alpha^7 t + \alpha, \alpha^5 t^2 + \alpha t + 1)$$

é uma palavra do código $C(D, 19P_\infty)$, que será:

$$(0,1,0,0,0,0,0,0,0,0,0,0,\alpha,\alpha^7,1,\alpha^3,\alpha^2,\alpha,\alpha^7,1,\alpha,0,0,0,1,\alpha,\alpha^5) \in \mathbb{F}_9^{27}.$$

1.0.5 Algoritmo mais eficiente para bases de Gröbner

O objetivo de Little, Saints e Heegard foi o de construir um método (algoritmo) para encontrar uma base de Gröbner para uma classe de códigos Hermitianos. Tal método é mais eficiente que o de Buchberger, pois nele se tem menos contas e complexidade em seus passos. Na construção desse algoritmo foi utilizado o conceito de "digrama de raízes"para um código Hermitiano, conceito este que será visto a seguir e também no próximo capítulo.

Os resultados de [14] foram obtidos sobre códigos Hermitianos pontuais $C = C(D, aP_\infty)$ (definidos no exemplo 1.0.26) com o automorfismo σ, de ordem $m^2 - 1$, dado por:

$$\sigma(x) = \alpha x \quad \text{e} \quad \sigma(y) = \alpha^{m+1} y \tag{1.1}$$

onde α é um gerador de $\mathbb{F}_{m^2}^\star$.

Através de σ associamos o código Hermitiano C a um submódulo $\overline{C}$ do módulo livre $\mathbb{F}_{m^2}[t]^{m+2}$, lembrando que $m+2$ é o número de órbitas geradas quando σ age sob os m^3 pontos racionais da curva Hermitiana $\mathcal{X}_m$.

No apêndice apresentamos a proposição 6.1.5 que nos garante a existência de uma base de Gröbner para $\overline{C}$, e a proposição 6.1.10 nos diz que podemos ter uma base de Gröbner diagonal para $\overline{C}$, ou seja, uma base de Gröbner $\mathcal{G} = \{g^{(1)}, \ldots, g^{(m+2)}\}$, onde $g^{(i)} \in \mathbb{F}_{m^2}[t]^{m+2}$, para todo $i = 1, \ldots, m+2$, com a seguinte propriedade:

$g^{(1)} = (g_1^{(1)}(t), \ldots, g_{m+2}^{(1)}(t))$
$g^{(2)} = (0, g_2^{(2)}(t), \ldots, g_{m+2}^{(2)}(t))$
$\vdots$
$g^{(m+2)} = (0, \ldots, 0, g_{m+2}^{(m+2)}(t))$

O resultado que veremos a seguir diz respeito a estes elementos $g^{(i)}$ e será fundamental para a definição de diagrama de raízes.

Proposição 1.0.27. *([14]) Para cada $i \in \{1, 2, \ldots, r\}$, se d_i é o grau da componete diagonal $g_i^{(i)}(t)$, então a equação $g_i^{(i)}(t) = 0$ tem d_i raízes distintas em $\mathbb{F}_{m^2}^{\star}$.*

Demonstração:

Seja C nosso código Hermitiano. Temos que $\pi^{-1}(C) = \overline{C} \leq \mathbb{F}_{m^2}[t]^{m+2}$, onde

$$\pi : \mathbb{F}_{m^2}[t]^{m+2} \longrightarrow \oplus_{i-1}^{m+2} \frac{\mathbb{F}_{m^2}[t]^{m+2}}{\langle t^{|O_i|} - 1 \rangle}$$

Assim, para cada i, temos que $\mathbf{q}_i = (t^{|O_i|} - 1)\mathbf{e}_i \in \overline{C}$, pois $\mathbf{q}_i \in \pi^{-1}(0, 0, \ldots, 0)$.

Sabemos que $|O_i|$ divide $m^2 - 1 = |\sigma|$ (ordem de σ), e portanto $t^{|O_i|} - 1$ divide $t^{m^2-1} - 1$.

Agora, como $\mathcal{G}$ é uma base de Gröbner de $\overline{C}$ e $\mathbf{q}_i \in \overline{C}$ temos que $\mathbf{q}_i$ se reduz a zero por $\mathcal{G}$.

Mas $\mathbf{g}^{(i)}$ tem termo líder $t^k\mathbf{e}_i$ e assim, como $\mathbf{g}^{(i)} \in \mathcal{G}$ temos que o termo líder de $\mathbf{g}^{(i)}$, que é $g_i^{(i)}(t)$, divide $\mathbf{q}_i$.

Logo, temos que $g_i^{(i)}(t)$ divide $t^{|O_i|} - 1$ e $t^{|O_i|} - 1$ divide $t^{m^2-1} - 1$.

Mas $t^{m^2-1} - 1$ tem $m^2 - 1$ raízes distintas em $\mathbb{F}_{m^2}^{\star}$. Logo, $g_i^{(i)}(t) = 0$ tem d_i raízes distintas em $\mathbb{F}_{m^2}^{\star}$. □

Olhando para as raízes dos $g_i^{(i)}(t)$ constrói-se o **diagrama de raízes** da seguinte forma: os elementos da i-ésima linha correspondem a quadradinhos sobre as raízes de $t^{|O_i|} - 1$ com marcas X sobre as raízes de $g_i^{(i)}(t) = 0$.

No próximo capítulo faremos uma definição mais formal de diagrama de raízes e veremos um exemplo de como é feita sua construção, além de dar um resultado que o relaciona com a dimensão de um código.

A idéia de Heegard, Little e Saints foi a de primeiro construir o diagrama de raízes e com ele se obter a base de Gröbner $\mathcal{G}$ para $\overline{C}$. Para isto eles se beneficiaram de certas simetrias que as curvas Hermitianas possuem. Explicitamente tem-se o seguinte lema.

Lema 1.0.28. *([14]) Seja $\mathcal{X}_m$ a curva hermitiana. Sob a ação do automorfismo σ de $\mathcal{X}_m$ dado por (1.1), os m^3 pontos racionais finitos de $\mathcal{X}_m$ sobre $\mathbb{F}_{m^2}$ se agrupam em $m+2$ órbitas, sendo m de comprimento $m^2 - 1$, uma de comprimento $m - 1$ e uma de comprimento 1 (fixaremos a seguinte notação para tais órbitas: as de comprimento $m^2 - 1$ serão $O_1, \ldots, O_m$, a de comprimento $m - 1$ será O_{m+1} e a de comprimento 1 será O_{m+2}). Cada órbita de*

comprimento m^2-1 é uma interseção completa de $\mathcal{X}_m$ com uma curva algébrica redutível de grau $m-1$, definida por uma equação da forma:

$$M_i(y) = \prod_{j=0}^{m-2}(y - \alpha^{l_i+j(m+1)}) = y^{m-1} - \alpha^{l_i(m-1)}$$

(uma união de linhas horizontais).
O mesmo é válido para a órbita O_{m+1} de comprimento $m-1$ se vemos uma multiplicidade de $m+1$ para cada ponto. E a órbita O_{m+2} (com multiplicidade m^2-1) é a interseção completa de $\mathcal{X}_m$ com o conjunto de zeros de $M_{m+2}(y) = y^{m-1}$.

Tem-se também que cada $M_i(y)$, com $i = 1, 2, \ldots, m+2$, é uma constante não nula quando restrita a cada órbita O_k, com $k \neq i$.

Como primeira consequência deste resultado os autores conseguiram a seguinte informação com respeito as linhas do diagrama de raízes do código Hermitiano $C(D, aP_\infty)$.

Teorema 1.0.29. *([14]) Considere o diagrama de raízes do código Hermitiano $C(D, aQ)$.*

1) Seja $i \leq m$. Se $a \geq (i-1)(m^2-1)$, então a i-ésima linha do diagrama de raízes não é toda preenchida (com marcas X).

2) Seja $i \leq m$. Se $a \geq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$, então a i-ésima linha do diagrama de raízes é vazia (não tem marcas X), ou seja, $g_i^{(i)}(t) = 1$.

3) Finalmente, considere o caso $i = m+1$. Se $a \geq m(m^2-1)$, a $m+1$-ésima linha do digrama de raízes não é toda preenchida. E se $a \geq m(m^2-1)+(m-2)(m+1)$ a $m+1$-ésima linha é vazia.

E posteriormente um resultado que diz exatamente como serão as linhas do diagrama.

Teorema 1.0.30. *([14]) Sejam $1 \leq i \leq m$ (analogamente se faz para $i = m+1$ e $i = m+2$) e a no seguinte intervalo:*

$$(i-1)(m^2-1) \leq a \leq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$$

Então (pelo teorema anterior) a i-ésima linha do digrama de raízes não é nem vazia, nem totalmente preenchida.

Sendo A_i o conjunto das raízes maracadas na i-ésima linha do diagrama de raízes, o complementar de A_i é o conjunto de elementos $\alpha^{-k} \in \mathbb{F}_q^*$ tal que $k = r + s(m+1)$, onde $0 \leq r \leq m$, $0 \leq s \leq m-2$ e $rm + s(m+1) + (i-1)(m^2) \leq a$.
Como uma observação, para todo a dado, tem-se no máximo duas linhas do diagrama que são nem vazias, nem totalmente preenchidas.

Vejamos um exemplo de como se construir o diagrama de raízes utilizando estes resultados.

Exemplo 1.0.31. Consideremos o código Hermitiano $C = C(D, 19P_\infty)$ sobre $\mathbb{F}_9$ e o automorfismo σ, dado em 1.1. Vimos no Exemplo 1.0.23 que σ permuta os 27 pontos $\mathbb{F}_9$-racionais finitos em 5 órbitas: três de comprimento 8, uma de comprimento 2 e uma de comprimento 1.

Aqui temos que $a = 19$ e $m = 3$. Usando os teoremas 1.0.29 e 1.0.30 construímos o diagrama de raízes da seguinte forma:

Linhas 1: Como $a = 19 \geq m^2 + (m-2)(m+1)$, então o teorema 1.0.29 nos diz que a linha 1 será vazia.

Linha 2: No caso de $i = 2$ temos $(i-1)(m^2-1) \leq a \leq (i-1)(m^2-1)+m^2+(m-2)(m+1)$, e pelo teorema 1.0.30 marcamos somente α com um X.

Linha 3: Para $i = 3$ também temos $(i-1)(m^2-1) \leq a \leq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$, e usando o teorema 1.0.30, marcamos $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

Linha 4: A linha 4 será totalmente preenchida, só que possui apenas dois quadradinhos, um embaixo do 1 e outro embaixo do α^4.

Linha 5: A linha 5 possui somente um quadradinho, embaixo do 1, e também será totalmente preenchida.

Assim, temos o seguinte diagrama de raízes.

1	α	α^2	α^3	α^4	α^5	α^6	α^7
	X						
	X	X	X	X	X	X	
X				X			
X							

O resultado a seguir foi essencial para a construção do algoritmo.

Teorema 1.0.32. *([14]) Sejam $\{\alpha^{e_1}, \ldots, \alpha^{e_l}\}$ o conjunto das raízes que aparecem na linha i do diagrama de raízes de $C(D, aP_\infty)$. Seja*

$$p(t) = \sum_{k=1}^{l}(t - \alpha^{e_k}) = \sum_{j=0}^{l} c_j t^j,$$

o único polinômio mônico de grau l que possui tais raízes. Então

$$f(x,y) = \prod_{k=1}^{i-1} M_k(y).\sum_{j=0}^{|O_i|-1} c_j \frac{B_{i,j}(x,y)}{B_{i,j}P_{i,j}}$$

é uma função em $L(aP_\infty)$ que fornece um elemento $g^{(i)}$ do módulo $\overline{C}$ com as $i-1$ componentes iniciais nulas, e a i-ésima componente igual a $p(t)$.

Antes de darmos o algoritmo vejamos algumas notações que nele são usadas.

|**RootDiagram**[**i**]|: Denota o número de raízes na linha i.

Get Root Diagram: Denotaremos por **Get Root Diagram** um procedimento onde: dado $a \geq 1$, determina, utilizando os teoremas 1.0.29 e 1.0.30, as raízes de cada componente diagonal dos elementos da base de Gröbner. Assumiremos que **Get Root Diagram** retorna uma lista de $m + 2$ listas de raízes, correspondendo aos lugares marcados no diagrama de raízes.

Get Value List: Denotaremos por **Get Value List** um procedimento no qual toma como entrada uma lista de elementos em $\mathbb{F}_q^\star$ e retorna a lista de coeficientes do único polinômio mônico de grau minimal sobre $\mathbb{F}_q$ com estas raízes, incluindo zeros para potências de t maiores que o número de raízes.

Evaluate Combination: Finalmente denotaremos por **Evaluate Combination**, uma função que toma uma lista de coeficientes $= \{c_j\}$ como os que aparecem no teorema 1.0.32 e evalua a combinação linear das funções $\left(\prod_{k=1}^{i-1} M_k(y)\right).B_{i,j}(x)$ dadas em $f(x,y)$ do teorema 1.0.32, no ponto $P = (x,y) \in \mathbb{F}_q^2$.

Encerramos este capítulo com o tão desejado algoritmo de Heegard, Little e Saints para se computar uma base de Gröbner para o submódulo $\overline{C}$.

Proposição 1.0.33. *([14]) O seguinte algorítmo computa uma base de gröbner POT, não reduzida, para o módulo $\overline{C}$ de $C_L(D, aP_\infty)$.*

Entrada: $a, \{P_{i,j}\}$ (*os* m^3 *pontos racionais finitos de* $\mathcal{X}_m$)

Saída: *um base de Grobner nao reduzida* $\mathcal{G} = \{\mathbf{g}^{(1)}, \mathbf{g}^{(2)}, \ldots, \mathbf{g}^{(m+2)}\}$

Início: $\mathcal{G} := \{\}$ *e* $\mathbf{RootDiagram} := \mathbf{GetRootDiagram}(a)$

Fazer, para i *de 1 a* $m+2$ *:*

•***Se*** $|RootDiagram[i]| < |O_i|$, *então*

Valores= $\{c_j\}$*:=**Get Value List**(RootDiagram[i])*

Fazer $\circ$ *Para* k *de* 1 *a* $i-1$*:* $g_k^{(i)} := 0$

Fazer $\circ$ *Para* k *de* i *a* $m+2$*:*

$g_k^{(i)} := 0$

para j *de* 0 *a* $|O_i| - 1$ *fazer,*

$$g_k^{(i)} := g_k^{(i)} + \mathbf{EvaluateCombination}(valores, P_{i,j}) t^j \mathbf{e}_k$$

• ***Caso contrário*** $\mathbf{g}^{(i)} := (t^{|O_i|} - 1)\mathbf{e}_i$

$\mathcal{G} := \mathcal{G} \bigcup \{\mathbf{g}^{(i)}\}$

Observamos que o algoritmo acima produz uma base de Gröbner diagonal $\mathcal{G}_D\{\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(m+2)}\}$ não reduzida. Assim, se quisermos uma base reduzida basta reduzir $\mathcal{G}_D$. Para isso basta retirar os elementos $\mathbf{g}^{(i)}$ tais que $Lt(\mathbf{g}^{(i)}) \leq Lt(\mathbf{g}^{(j)})$ para algum j.

Vemos que tal algoritmo possui uma complexidade menor que o de Buchberger (algoritmo 7.13), que utiliza divisões polinômiais que é algo complexo quando tratamos de vários elementos e, assim, tendo que efetuar muitas divisões.

CAPÍTULO 2

O Automorfismo η e o diagrama de raízes

A partir de agora começaremos a mostrar nossos resultados. Neste capítulo estudaremos um automorfismo, denotado por η, e o diagrama de raízes construído a partir de η. Este automorfismo será de extrema importância em nosso estudo do caso bipontual. Podemos destacar a Definição 2.0.34, o Lema 2.0.38 e o Teorema 2.0.42.

No capítulo anterior vimos como Little, Saints e Heegard definiram diagrama de raízes para um código Hermitiano pontual com um automorfismo σ de ordem $m^2 - 1$. O que daremos a seguir é uma definição mais "formal"deste conceito.

Definição 2.0.34. Seja $\mathcal{R}_i \subseteq \mathbb{F}_q^\star$, para $i = 1, \ldots, r$, o conjunto das raízes de $t^{|O_i|} - 1$. Um diagrama de raízes de um código C sobre $\mathbb{F}_q$ com um automorfismo σ de ordem $q - 1$ é uma tabela formada por r linhas, onde, para cada $i = 1, \ldots, r$, a linha i é formada por quadradinhos sobre os elementos de $\mathcal{R}_i$ com uma marca X sobre as raízes de $g_i^{(i)}(t)$, que é a i-ésima componente do elemento $g^(i)$ da base de Gröbner diagonal de $\overline{C}$ (veja começo da seção 1.0.5).

Vejamos um exemplo simples de como funciona tal construção.

Exemplo 2.0.35. Mais uma vez considere o código Hermitiano $C = C(D, 19P_\infty)$ sobre $\mathbb{F}_9$ e o automorfismo σ dado em 1.1 de ordem 8. Sabemos, pelo Exemplo 1.0.23, que σ permuta

os 27 pontos $\mathbb{F}_9$-racionais em 5 órbitas: três de comprimento 8, uma de comprimento 2 e uma de comprimento 1. Consegue-se uma base de Gröbner diagonal $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_5\}$, com $g_1^{(1)} = 1$, $g_2^{(2)} = t+\alpha^5$, $g_3^{(3)} = t^6+\alpha^6t^5+\alpha^2t^4+\alpha^7t^3+\alpha t^2+\alpha^4t+\alpha^5$, $g_4^{(4)} = t^2-1$ e $g_5^{(5)} = t-1$.

Assim, como as três primeiras órbitas têm comprimento 8 e as raízes de $t^8 - 1 = 0$ são todos os elementos de $\mathbb{F}_9^\star = \{1, \alpha, \ldots, \alpha^7\}$, colocamos quadradinhos embaixo de todos os α^i, $i = 0, 1, \ldots, 7$. Agora $g_1^{(1)} = 1$, logo não possui raiz e portanto não marcamos nenhum X a linha 1. Já $g_2^{(2)} = t + \alpha^5$ possui $\alpha = -\alpha^5$ como raiz e assim marcamos um X embaixo de α. Na linha 3 marcamos X embaixo de $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ e α^6 que são as raíes de $g_3^{(3)}$. A linha 4 terá somente dois quadradinhos, embaixo de 1 e α^4 que são as raízes de $t^{|O_4|} - 1 = t^2 - 1$, e como $g_4^{(4)} = t^2-1$ marcamos tanto 1 como α^4 na linha 4, ou seja, ela é totalmente preenchida. O mesmo será para a linha 5 que terá apenas um quadradinho, embaixo do 1, que é raiz de $t^{|O_5|} - 1 = t - 1 =$, e que será marcado com um X, já que $t - 1 = g_5^{(5)}$.

1	α	α^2	α^3	α^4	α^5	α^6	α^7
	X						
	X	X	X	X	X	X	
X				X			
X							

Um primeiro resultado utilizando o diagrama de raízes é dado na proposição a seguir.

Proposição 2.0.36. *([14]) A dimensão do código C é igual número de lugares vazios no diagrama de raízes.*

Demonstração:

Pela proposição $II.C.1$ dada em [13], sabemos que existe uma $\mathbb{F}_q$-base de C em uma correspondência $1-1$ com os monômios não-padrões (nonstandard) no módulo $\overline{C}$. Ou seja, os termos $t^k\mathbf{e}_i$ aparecem como termos líderes de alguns elementos do módulo, cujos expoentes satisfazem $k \leq |O_i| - 1$.

Se temos n_i lugares vazios na i-ésima linha do diagrama de raízes, então $g_i^{(i)}(t) = 0$ tem $|O_i| - n_i$ raízes, e o termo líder de $\mathbf{g}^{(i)} \in \mathcal{G}$ é $t^{|O_i|-n_i}\mathbf{e}_i$.

Assim, obtemos n_i monômios não-padrões contendo $\mathbf{e}_i$, que são: $t^{|O_i|-1}\mathbf{e}_i, t^{|O_i|-2}\mathbf{e}_i, \ldots, t^{|O_i|-n_i}\mathbf{e}_i$.

Fazendo isso em cada i, obtemos $n_1 + n_2 + \ldots + n_r$ monômios não-padrões de $\overline{C}$, ou seja, a dimensão de C é igual a $n_1 + n_2 + \ldots + n_r$ que é igual ao número de lugares vazios do diagrama de raízes. □

Observação 2.0.37. Uma pergunta que podemos fazer é se podemos definir o diagrama de raízes para um código C sobre $\mathbb{F}_q$ com um automorfismo que não tenha ordem $q-1$.

A resposta para esta pergunta é sim, mas desde que a ordem do automorfismo usado divida $q-1=|\mathbb{F}_q^\star|$, pois neste caso, utilizando a proposição 1.0.27, as raízes dos $g_i^{(i)}(t)$ serão todas distintas e, assim, podemos dar a definição 2.0.34. Caso contrário as raízes dos $g_i^{(i)}(t)$ podem ter multiplicidade maior que 1 e nossa definição não seria válida, assim como a proposição 2.0.36.

Mais adiante veremos o exemplo do automorfismo η que tem ordem diferente de $q-1$.

Pelo trabalho [4], de Garcia, Stichtenoth e Xing, vimos que o grupo de automorfismos da curva Hermitiana é formado por automorfismos da forma:

$$\pi(x)=ax+b\ ,\ \pi(y)=a^{m+1}y+ab^mx+c$$

onde $a\in\mathbb{F}_{m^2}^\star$, $b\in\mathbb{F}_{m^2}$ e $c^m+c=b^{m+1}$.

Agora vejamos um outro automorfismo sobre a curva Hermitiana, cuja ordem é diferente de m^2-1, que é a ordem de σ (1.1).

Tal automorfismo, denotado por η, é o seguinte:

$$\eta(x)=\alpha^{m-1}x \quad \text{e} \quad \eta(y)=y \tag{2.1}$$

onde α é um gerador de $\mathbb{F}_{m^2}^\star$. Note que a ordem de η é $m+1$.

Observamos que as proposições 1.0.27 e 2.0.36 também valem para o automorfismo η.

Utilizando η construiremos um diagrama de raízes para nosso código $C_L(D,aP_\infty)$ sem utilizar base de Gröbner, e com isso faremos um algoritmo análogo ao obtido a partir de σ, dado na proposição 1.0.33. Depois disso fazeremos uma comparação entre eles.

Os resultados para se contruir o diagrama de raízes do código Hermitiano $C(D,aP_\infty)$ com o automorfismo η são os seguintes.

Lema 2.0.38. *A ação de η, como em 2.1, decompõe os m^3 pontos racionais finitos de $\mathcal{X}_m$ em m^2 órbitas, sendo $m(m-1)$ de comprimento $m+1$ e m de comprimento 1.*

Cada uma destas órbitas é a interseção completa de $\mathcal{X}_m$ com uma curva algébrica de grau 1 definida por:

$$M_i(y) = y - \alpha^{l_i}$$

Cada $M_i(y)$, $i = 1, 2, \ldots, m^2$ é uma constante não nula quando restrita a cada órbita O_k, com $k \neq i$.

Demonstração:

Temos que as órbitas geradas por η são da seguinte forma:

Para $1 \leq i \leq m(m-1)$:

$$O_i = O(\alpha^{t_i}, \alpha^{l_i}) = \{(\alpha^{t_i}, \alpha^{l_i}), (\alpha^{t_i+(m-1)}, \alpha^{l_i}), (\alpha^{t_i+2(m-1)}, \alpha^{l_i}), \ldots, (\alpha^{t_i+m(m-1)}, \alpha^{l_i})\}$$

onde, para cada i, $t_i, l_i \in \{0, 1, \ldots, m^2 - 2\}$.

Para $m(m-1) + 1 \leq i \leq m^2 - 1$:

$$O_i = O(0, \alpha^{l_i}) = \{(0, \alpha^{l_i})\}$$

e $O_{m^2} = \{(0, 0)\}$.

Portanto $M_i(y) = y - \alpha^{l_i}$ intersecta $\mathcal{X}_m$ nos pontos em que $y = \alpha^{l_i}$, ou seja, na órbita O_i.

E obviamente se tomamos $P_{k,j} = (\alpha^{t_k+j(m-1)}, \alpha^{l_k}) \in O_k$, com $k \neq i$, temos $M_i(\alpha^{l_k}) = \alpha^{l_k} - \alpha^{l_i} = constante \neq 0$, pois $\alpha^{l_k} \neq \alpha^{l_i}$. □

Lema 2.0.39. *Sejam $i \leq m(m-1)$ e $P_{i,j} = \eta^j(P_{i,0}) = (\alpha^{t_i+j(m-1)}, \alpha^{l_i})$ o j-ésimo ponto de O_i, com $j \in \{0, 1, \ldots, m\}$. A função*

$$B_{i,j}(x) = \prod_{k=1}^{m} (x - \alpha^{t_i+(j+k)(m-1)})$$

se anula em cada ponto de O_i exceto em $P_{i,j}$.

Demonstração:

Temos que $B_{i,j}(\alpha^{t_i+j(m-1)}) \neq 0$. Vamos considerar $P_{i,s} = (\alpha^{t_i+s(m-1)}, \alpha^{l_i}) \in O_i$, com $s \neq j$. Como $\alpha^{m^2-1} = 1$, existe $k \in \{1, 2, \ldots, m\}$ tal que $s = j + k$, e assim $B_{i,j}(\alpha^{t_i+s(m-1)}) = 0$. □

Observação 2.0.40. Os divisores principais de x e y são dados por

$(x) = P_{0,0} + \sum_{\alpha \in \Lambda} P_{0,\alpha} - mP_\infty$, onde Λ é o conjunto de raízes de $y^{(m-1)} - 1$ e $P_{a,b} \in X_m$ denota o ponto racional finito onde as coordenadas a e b são os zeros de $x - a$ e $y - b$, respectivamente;

$(y) = (m+1)P_{0,0} - (m+1)P_\infty$.

Logo, temos que $M_i(y) \in L((m+1)P_\infty)$, para $1 \leq i \leq m^2$, e $B_{i,j}(x,y) \in L(m^2 P_\infty)$, para $1 \leq i \leq m(m-1)$.

Com isto podemos dar a seguinte informação sobre as linhas do diagrama.

Teorema 2.0.41. *Considere o diagrama de raízes do código Hermitiano $C_L(D, aP_\infty)$.*

1) *Seja $i \leq m(m-1)$. Se $a \geq (i-1)(m+1)$, então a i-ésima linha do diagrama de raízes não é totalmente preenchida.*

2) *Seja $i \leq m(m-1)$. Se $a \geq (i-1)(m+1) + m^2$, então a i-ésima linha do diagrama de raízes é vazia (não tem marcas X), ou seja, a i-ésima componente da diagonal da base de Gröbner de $\overline{C}$ é 1, isto é, $g_i^{(i)}(t) = 1$.*

3) *Para $m(m-1)+1 \leq i \leq m^2$, temos que $|O_i| = 1$, logo teremos apenas um quadradinho, que será embaixo do 1 que é a única raiz de $t - 1 = 0$. Assim se $a \geq (i-1)(m+1)$, então a linha i será vazia.*

Demonstração:

Antes de começarmos lembremos que representamos os elementos de $C_L(D, aP_\infty)$ como m^2-uplas de polinômios $(h_1(t), h_2(t), \ldots, h_{m^2}(t))$, onde para cada i:

$$h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j}) t^j$$

para algum $f \in L(aP_\infty)$.

1) Suponhamos que $i \leq m(m-1)$ e $a \geq (i-1)(m+1)$. Como $M_i(y) \in L((m+1)P_\infty)$ para todo $i \leq m(m-1)$, então:

$$f_i = M_1(y).M_2(y).\ldots.M_{i-1}(y) \in L(aP_\infty)$$

Avaliando f_i nos elementos de O_k, para $k = 1, 2, \ldots, i-1$, temos que o módulo $\overline{C}$ (e portanto C) conterá um elemento da forma: $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t))$ com $i-1$ componentes iniciais (líderes) nulas, já que $f_i(P_{k,j}) = 0$ para todo $P_{k,j} \in O_k$ e todo $k = 1, 2, \ldots, i-1$.

No lema 2.0.38 vimos que cada $M_j(y)$, $j = 1, 2, \ldots, m^2$, é uma constante não nula quando restrita a cada órbita O_k, com $k \neq j$.

Logo, para $P_{i,j} \in O_i$ temos que $f_i(P_{i,j}) = c \neq 0$, onde c é uma constante. Portanto $h_i(t) = 1 + t + t^2 + \ldots + t^m$ não possui 1 como raiz.

Agora, pela definição de base de Gröbner, $g_i^{(i)}(t)$ divide $h_i(t)$ (que é o termo líder de $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t))$), e assim o 1 também não é raiz de $g_i^{(i)}(t)$. Consequentemente a i-ésima linha do diagrama não é totalmente preenchida, pois não marcamos o 1.

2) Agora suponhamos que $i \leq m(m-1)$ e $a \geq (i-1)(m+1) + m^2$. Sabemos que $M_i(y) \in L((m+1)P_\infty)$ e $B_{i,j}(x, y) \in L(m^2 P_\infty)$ para todo $i \leq m(m-1)$. Logo,

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y) \right) . B_{i,0}(x) \in L(aP_\infty).$$

Mas $f_i(P) = 0$ para todo $P \in O_1 \bigcup O_2 \bigcup \ldots \bigcup O_{i-1}$, e mais ainda, $f_i(Q) = 0$ para todo $Q \in O_i \setminus \{P_{i,0}\}$, pois $B_{i,0}$ se anula em todo $Q \in O_i \setminus \{P_{i,0}\}$.

Assim, conseguimos $h_1(t) = h_2(t) = \ldots = h_{i-1}(t) = 0$ e $h_i(t) = f_i(P_{i,0}) + 0 + \ldots + 0 = f_i(P_{i,0}) = c \neq 0$. E temos que $\overline{C}$ possui um elemento da forma $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$.

Como $g_i^{(i)}(t)$ divide $h_i(t) = c$, que não possui raiz, temos que $g_i^{(i)}(t)$ também não possui raiz e, portanto, a i-esima linha do diagrama é vazia.

3) No caso em que $m(m-1) + 1 \leq i \leq m^2$, temos que $|O_i| = 1$. Logo os $h_i(t) = f(P_{i,j})$ são constantes. Assim, se $a \geq (i-1)(m+1)$ tomamos $f_i = M_1(y).M_2(y).\ldots.M_{i-1}(y)$, que estará em $L(aP_\infty)$ e, analogamente ao item anterior, teremos $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$ implicando que a linha i será vazia. □

Teorema 2.0.42. *Sejam $i \leq m(m-1)$ e a no seguinte intervalo:*

$$(i-1)(m+1) \leq a < (i-1)(m+1) + m^2.$$

Então a i-ésima linha do diagrama de raízes não é nem vazia nem totalmente preenchida.

Sendo M o conjunto das raízes marcadas na i-ésima linha do diagrama de raízes, o complementar de M é o conjunto $M^c = \{\alpha^{-k} \in \mathbb{F}_{m^2}^\star;$ tal que $k = r(m-1),$ com $0 \leq r \leq m$ e $rm + (i-1)(m+1) \leq a\}$.

Para demonstrar este teorema necessitamos dos resultados que veremos a seguir.

Consideremos $I(O_i) = \{f(x, y) \in \mathbb{F}_q[x, y]$; $f(P_{i,j}) = 0$, $\forall$ $P_{i,j} \in O_i\}$ o ideal em $\mathbb{F}_q[x, y]$ consistindo dos polinômios que se anulam em todos os pontos de O_i.

E $\dfrac{\mathbb{F}_q[x,y]}{I(O_i)}$ o anel de funções polinomiais sobre O_i.

Lema 2.0.43. *Sejam $i \leq m(m-1)$ e V_i o espaço gerado por $\left(\prod_{k=1}^{i-1} M_k(y)\right).x^r$, para $0 \leq r \leq m$.*

Então a aplicação restrição de V_i a $\dfrac{\mathbb{F}_{m^2}[x,y]}{I(O_i)}$ é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais.

Demonstração:

Para $i \leq m(m-1)$ temos que as órbitas O_i consistem de $m+1$ pontos com coordenadas x distintas e de um único $y = \alpha^{l_i}$. Sabemos que O_i é a interseção de $\mathcal{X}_m$, cuja equação é $x^{m+1} = y^m + y$, com $M_i(y)$ de equação $y - \alpha^{l_i} = 0$. Então, temos que $(y - \alpha^{l_i})^m = 0$, e daí $y^m - \alpha^{l_i.m} = 0 \Rightarrow y^m + y - \alpha^{l_i.m} = y \Rightarrow x^{m+1} - \alpha^{l_i.m} = y$ e, em O_i, conseguimos $x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i} = 0$.

Vejamos que o anel das funções polinomiais $\dfrac{\mathbb{F}_q[x,y]}{I(O_i)}$ é isomorfo a $\dfrac{\mathbb{F}_q[x]}{\langle x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i}\rangle}$.

Seja $\Psi_i : \mathbb{F}_q[x,y] \longrightarrow \dfrac{\mathbb{F}_q[x]}{\langle x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i}\rangle}$ dada por: $\Psi_i(f(x,y)) = \overline{f(x, x^{m+1} - \alpha^{l_i.m})}$.

Temos que Ψ_i é sobrejetora, pois dada $\overline{f(x)} \in \dfrac{\mathbb{F}_q[x]}{\langle x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i}\rangle}$, então $\overline{f(x)} = f(x) + h(x).(x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i})$. Agora tomando $f(x,y) = f(x) \in \mathbb{F}_q[x,y]$ temos que $\Psi_i(f(x)) = \overline{f(x)} \in \dfrac{\mathbb{F}_q[x]}{\langle x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i}\rangle}$. E portanto, Ψ_i é sobrejetora.

Agora, vejamos que $Ker(\Psi_i) = I(O_i)$.

1º) $I(O_i) \subseteq Ker(\Psi_i)$.

De fato, dada $f(x,y) \in I(O_i)$, então $f(P) = 0$, para todo $P \in O_i$. Logo $f(x,y) = h(x,y)(y - \alpha^{l_i}) = h(x,y)(x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i})$, e assim $\Psi_i(f(x,y)) = \overline{f(x,y)} = \overline{0}$. Ou seja, $f(x,y) \in Ker(\Psi_i)$.

2º) $Ker(\Psi_i) \subseteq I(O_i)$.

De fato, dada $f(x,y) \in Ker(\Psi_i)$, temos $\overline{f(x, x^{m+1} - \alpha^{l_i.m})} = 0$, ou seja, $f(x, x^{m+1} - \alpha^{l_i.m}) = h(x).(x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i})$. Logo, dado $P \in O_i$ temos $f(P) = 0$ e, assim, $f(x,y) \in I(O_i)$.

Portanto, pelo Teorema do Isomorfismo, temos que $\dfrac{\mathbb{F}_q[x,y]}{I(O_i)}$ é isomorfo a $\dfrac{\mathbb{F}_q[x]}{\langle x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i}\rangle}$.

Agora, seja $\Phi_i : V_i \longrightarrow \dfrac{\mathbb{F}_q[x,y]}{I(O_i)}$ a aplicação restrição que é uma aplicação linear e sobrejetiva.

Sabendo que $\dfrac{\mathbb{F}_q[x,y]}{I(O_i)}$ é isomorfo a $\dfrac{\mathbb{F}_q[x]}{\langle x^{m+1}-\alpha^{l_i.m}-\alpha^{l_i}\rangle}$, e que $\{1,x,x^2,\ldots,x^m\}$ é uma base para $\dfrac{\mathbb{F}_q[x]}{\langle x^{m+1}-\alpha^{l_i.m}-\alpha^{l_i}\rangle}$, temos que $dim\left(\dfrac{\mathbb{F}_q[x]}{\langle x^{m+1}-\alpha^{l_i.m}-\alpha^{l_i}\rangle}\right)=m+1$.

E $\{\left(\prod_{k=1}^{i-1}M_k(y)\right),\left(\prod_{k=1}^{i-1}M_k(y)\right).x,\ldots,\left(\prod_{k=1}^{i-1}M_k(y)\right).x^m\}$ é uma base para V_i. Logo $dim(V_i)=m+1$.

Portanto, V_i e $\dfrac{\mathbb{F}_q[x,y]}{I(O_i)}$ têm mesma dimensão e, a aplicação restrição Φ_i é um isomorfismo. □

Falaremos agora sobre "Fórmula de Lagrange", que é algo que será utilizado para a demonstração do próximo resultado. Um estudo mais aprofundado sobre o assunto pode ser visto em [20].

Observação 2.0.44. **Fórmula de Lagrange:** Sejam $x_0,x_1,\ldots,x_n$, $n+1$ pontos distintos e $y_i=f(x_i)$. Seja $P_n(x)$ o polinômio de grau $\leq n$ que interpola f em $x_0,x_1,\ldots,x_n$. Então, podemos representar $P_n(x)$ da seguinte forma:

$$P_n(x)=y_0L_0(x)+y_1L_1(x)+\ldots+y_nL_n(x)$$

onde os polinômios $L_k(x)$ são de grau n.

Para cada i queremos que a condição $P_n(x_i)=y_i$ seja satisfeita. A forma mais simples de se satisfazer esta condição é impor:

$$L_i(x_i)=1 \text{ e } L_k(x_i)=0, \text{ se } k\neq i$$

Para isso definimos $L_k(x)=\dfrac{(x-x_0)(x-x_1)\ldots(x-x_{k-1})(x-x_{k+1})\ldots(x-x_n)}{(x_k-x_0)(x_k-x_1)\ldots(x_k-x_{k-1})(x_k-x_{k+1})\ldots(x_k-x_n)}$.

Fazendo tal comentário sobre "Fórmula de Lagrange", veremos o corolário a seguir.

Corolário 2.0.45. *Para toda coleção de valores c_j, com $j=0,1,\ldots,m$, existe uma única função $f(x,y)\in V_i$ a qual satisfaz $f(P_{i,j})=c_j$, para todo j, e que é identicamente nula em $O_1,\ldots,O_{i-1}$.*

Demonstração:

Utilizando técnicas, como a "Fórmula de Lagrange"para interpolação, vista em 2.0.44, encontramos um $P_m(x)\in\dfrac{\mathbb{F}_q[x]}{\langle x^{m+1}-\alpha^{l_i.m}-\alpha^{l_i}\rangle}$, de grau no máximo m, que resolve os problemas de interpolação em O_i.

Assim a função $f(x,y) = \Phi_i^{-1}(P_m(x)) \in V_i$ também se anula nas órbitas $O_1, \ldots, O_{i-1}$. $\square$

Observação 2.0.46. Observamos que as funções $B_{i,j}(x) = \prod_{k=1}^{m}(x - \alpha^{t_i+(j+k)(m-1)})$ multiplicadas pelas funções de órbita $M_1(y), \ldots, M_{i-1}(y)$ estão em V_i. Ou seja,

$$B_{i,j}(x).M_1(y).\ldots.M_{i-1}(y) \in V_i.$$

Mais ainda, aplicando Φ_i em tal elemento de V_i, conseguimos uma função de Lagrange $L_j^{(i)}(x)$ para Φ_i, onde, a menos de uma constante, tem-se:

$$L_k^{(i)}(P_{i,k}) = 1 \text{ e } L_k^{(i)}(P_{i,j}) = 0 \text{ se } j \neq k$$

Agora, vejamos como demonstrar o teorema 2.0.42.

Demonstração do teorema 2.0.42:

Sabemos que x tem pólo de ordem m em P_∞ e, tanto y como $M_i(y)$, têm pólo de ordem $m+1$ em P_∞.

Assim, para todo $i = 1, 2, \ldots, m(m-1)$, as funções $f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).x^r.y^s$, com $rm + s(m+1) + (i-1)(m+1) \leq a$ estão em $L(aP_\infty)$.

Como $M_i(y) = y - \alpha^{l_i}$, podemos excluir o termo y^s de f_i, ou seja, tomar $s = 0$, pois $y = M_i(y) - c$. E como $x^{m+1} = y^m + y$, podemos tomar $0 \leq r \leq m$. Logo $f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).x^r$, com $0 \leq r \leq m$, está em $L(aP_\infty)$ se $rm + (i-1)(m+1) \leq a$.

Seja $h_i(t) = \sum_{j=0}^{|O_i|-1} f_i(P_{i,j})t^j$, para $1 \leq i \leq m(m-1)$.

Como $M_k(y)$ é zero para os elementos de O_k, temos que $h_j(t) = 0$, para $1 \leq j \leq i-1$.

Sabemos, pelo lema 2.0.38, que $M_j(y)$ são constantes não nulas em O_k, para $k \neq j$, e que os elementos de O_i são do tipo $P_{i,j} = \eta^j(P_{i,0}) = (\alpha^{t_i+j(m-1)}, \alpha^{l_i}) = (\alpha^{t_i}\alpha^{j(m-1)}, \alpha^{l_i})$.

Assim, temos que $f(P_{i,j}) = c.\alpha^{rt_i+rj(m-1)}$, onde c é uma constante. Multiplicando pelas suas respectivas inversas, podemos desconsiderar as constantes c e α^{rt_i}, pois elas não alteram os valores das raízes. Logo temos que $h_i(t) = \sum_{j=0}^{m}(\alpha^{r(m-1)}t)^j$, com $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t)) \in \overline{C}$.

Agora $t = \alpha^{-(r(m-1))} \in \mathbb{F}_r^\star$ não é raiz de $h_i(t)$, pois $h_i(\alpha^{-(r(m-1))}) = 1 + 1 + \ldots + 1 = m + 1 \neq 0$. Portanto as raízes de $h_i(t)$ são diferentes de $\alpha^{-(r(m-1))}$.

Como $C_L(D, aP_\infty)$ pode ser visto como um módulo $\overline{C}$ ele conterá um elemento cujas primeiras $i-1$ entradas são zero, e cuja i-ésima entrada é o maior divisor comum dos polinômios $h_i(t)$, com $0 \leq r \leq m$ e $rm + (i-1)(m+1) \leq a$.

Assim, a componente $g_i^{(i)}(t)$ do elemento $g^{(i)}$ da base de Gröbner $\mathcal{G}$ de $\overline{C}$ divide tal mdc dos $h_i(t)$ e, portanto, não tem $\alpha^{-(r(m-1))}$ como raiz.

Então, concluímos que $\mathcal{A} = \{\alpha^{-k} \in \mathbb{F}_{m^2}^\star;$ tal que $k = r(m-1),$ com $0 \leq r \leq m$ e $rm + (i-1)(m+1) \leq a\} \subseteq M^c$, lembrando que M é o conjunto das raìzes marcadas na i-ésima linha do diagrama de raízes.

Agora, vejamos que $M^c \subseteq \mathcal{A}$.

Seja $g(x,y) \in L(aP_\infty)$ uma função que se anula em $O_1, O_2, \ldots, O_{i-1}$ e possua o menor número de raízes no diagrama. Sejam $\{\alpha^{s_1}, \alpha^{s_2}, \ldots, \alpha^{s_l}\}$ o conjunto de tais raízes de g, e, $\prod_{k=1}^{l}(t - \alpha^{s_k}) = \sum_{j=0}^{l} c_j t^j$, o único polinômio mônico de grau l que possua tais raízes.

Queremos uma função cujos valores em O_i são:

$$g(P_{i,j}) = 0, \text{ para todo } j = l+1, \ldots, m$$

e

$$g(P_{i,j}) = c_j, \text{ para todo } j = 0, 1, \ldots, l$$

Pelo corolário 2.0.45, existe única solução para g em V_i. E, assim, vemos que não podemos ter um conjunto menor do que M^c que contenha tais raízes. □

Vejamos agora um exemplo de como construir o diagrama de raízes usando os teoremas 2.0.41 e 2.0.42.

Exemplo 2.0.47. Consideremos o código $C = C_L(D, 19Q)$ na curva Hermitiana sobre $\mathbb{F}_9$ e o automorfismo η, como em 2.1, de ordem 4. O automorfismo η permuta os 27 pontos racionais afins em 9 órbitas, sendo 6 de comprimento 4 e 3 de comprimento 1.

Sabemos que $|O_i| = 4$, para $i = 1, 2, \ldots, 6$. Logo $t^{|O_i|} - 1 = 0$ possui $1, \alpha^2, \alpha^4$ e α^6 como raízes. E $|O_i| = 1$, para $i = 7, 8, 9$. Logo $t^{|O_i|} - 1 = 0$ tem somente o 1 como raiz.

Utilizando os teoremas 2.0.41 e 2.0.42 contruímos o seguinte diagrama de raízes para nosso código C.

Linhas 1,2,3: Para $i = 1, 2, 3$ temos $a \geq (i-1).4 + 9$. Pelo item 2) do teroema 2.0.41 temos que as linhas $1, 2, 3$ são vazias.

Linha 4: Para $i = 4$ temos $12 \leq 19 < 21$. Assim, pelo teorema 2.0.42, não marcaremos $1, \alpha^6$ e α^4 no diagrama.

Linha 5: Para $i = 5$ temos $16 \leq 19 < 25$. Assim, pelo teorema 2.0.42, não marcaremos 1 e α^6 no diagrama.

Linhas 6,7,8,9: Para $i = 6, 7, 8, 9$ temos $a < (i-1).4$. Logo, pelo teorema 2.0.41, tais linhas são totalmente preenchidas, sendo que a linha 6 possui 4 quadradinhos, um para cada raiz de $t^4 - 1 = 0$ e, as linhas $7, 8, 9$, têm somente um quadradinho embaixo do 1, que é a única raiz de $t - 1 = 0$.

Dessa forma constrímos o seguinte diagrama:

1	α^2	α^4	α^6
	X		
	X	X	
X	X	X	X
X			
X			
X			

Da proposição 2.0.36 tem-se que a dimensão do código é 17.

Comparando a complexidade na construção do diagrama, sem usar base de Gröbner, do exemplo acima com a do exemplo 1.0.31, vemos que elas não diferem muito, pois apesar do exemplo acima (utilizando η) possuir mais linhas (na ordem de m^2), ele possui menos raízes a serem analisadas (na ordem de m), ao contrário do exemplo 1.0.31 que possui menos linhas (na ordem de m) mas possui mais raízes a serem analisadas (na ordem de m^2). Assim, vemos que a complexidade na construção dos diagramas utilizando η e σ são praticamente a mesma, como aconteceu no caso das contruções utilizando base de Gröbner diagonal.

Teorema 2.0.48. *Seja $\{\alpha^{s_1}, \alpha^{s_2}, \ldots, \alpha^{s_l}\}$ o conjunto de raízes que aparecem na i-ésima linha do diagrama de raízes de um código Hermitiano $C_L(D, aP_\infty)$. Seja $p(t) = \prod_{k=1}^{l}(t - \alpha^{s_k}) = \sum_{j=0}^{l} c_j t^j$, o único polinômio mônico de grau l com tais raízes.*

Então,

$$f(x,y) = \prod_{k=1}^{i-1} M_k(y).\ \sum_{j=0}^{|O_i|-1} c_j \frac{B_{i,j}(x)}{B_{i,j}(P_{i,j})}$$

é uma função em $L(aP_\infty)$ que fornece um elemento $\mathbf{g}^{(i)}$ do módulo com $i-1$ componentes líderes iguais a zero e a i-ésima comonente $g_i^{(i)}(t)$ igual a $p(t)$.

Demonstração:

Temos que tal $f(x,y)$ é solução do problema de interpolação sobre O_i para os coeficientes c_j de $p(t)$. Assim, só nos resta mostrar que $f(x,y) \in L(aP_\infty)$, ou seja que, $(i-1)(m+1) + m^2 \leq a$. Mas isso segue do teorema 2.0.42 e do lema 2.0.39. □

Utilizando tais resultados e as mesmas notações do algoritmo dado na proposição 1.0.33 daremos, agora, um algoritmo semelhante só que obtido a partir de η.

Proposição 2.0.49. *O seguinte algorítmo computa uma base de gröbner POT, não reduzida, para o módulo $\overline{C}$ de $C_L(D, aP_\infty)$.*

Entrada: $a, \{P_{i,j},$ *os* m^3 *pontos racionais de* $\mathcal{X}_m\}$

Saída: *um base de Grobner nao reduzida* $\mathcal{G} = \{\mathbf{g}^{(1)}, \mathbf{g}^{(2)}, \ldots, \mathbf{g}^{(m^2)}\}$

Início: $\mathcal{G} := \{\}$ *e* $\mathbf{RootDiagram} := \mathbf{GetRootDiagram}(a)$

Fazer, para i de 1 a m^2 :

•***Se*** $|RootDiagram[i]| < |O_i|$, *então*

Valores= $\{c_j\}$*:=**Get Value List**(RootDiagram[i])*

Fazer ∘ *Para k de 1 a $i-1$:* $g_k^{(i)} := 0$

Fazer ∘ *Para k de i a m^2:*

$g_k^{(i)} := 0$

para j de 0 a $|O_i| - 1$ fazer,

$$g_k^{(i)} := g_k^{(i)} + \mathbf{EvaluateCombination}(valores, P_{i,j}) t^j \mathbf{e}_k$$

• ***Caso contrário*** $\mathbf{g}^{(i)} := (t^{|O_i|} - 1)\mathbf{e}_i$

$\mathcal{G} := \mathcal{G} \bigcup \{\mathbf{g}^{(i)}\}$

Demonstração: A veracidade do algoritmo segue dos resultados anteriores.

Uma última questão que podemos levantar é a respeito dos algoritmos dados em 1.0.33 e 2.0.49. Qual é mais complexo, o que utiliza σ ou η?

Para responder esta pergunta temos que olhar para dois pontos: primeiro para o número de iterações que o algoritmo faz, e segundo para a complexidade de tais iterações.

Olhando para o algoritmo 1.0.33, construído a partir de σ, vemos que ele possui um número de iterações na ordem de m, sendo que em cada iteração se calcula um número de valores na ordem de m^2.

Por outro lado, o algoritmo 2.0.49, construído a partir de η, possui um número de iterações na ordem de m^2, mas com iterações tendo cálculos de valores na ordem de m, justamente o oposto do algoritmo construído a partir de σ.

Agora, tanto a complexidade das iterações quanto a dos cálculos dos valores são pequenas, e, portanto, podemos dizer que os algoritmos se equivalem quanto a complexidade.

Para finalizar este capítulo vejamos um exemplo de como encontrar uma base de Grobner utizando o algoritmo da proposição 2.0.49.

Exemplo 2.0.50. Seja $C = C(D, 3P_\infty)$ um código sobre a curva Hermitiana $\mathcal{X}_2$ definida sobre $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ pela equação $x^3 = y^2 + y$.

Com o automorfismo η, dado por $\eta(x) = \alpha x$ e $\eta(y) = y$, temos o seguinte diagrama de raízes para o código C.

1	α	α^2
	X	
	X	X
X		
X		

Entrada: 3, $\{P_{1,0} = (1, \alpha), P_{1,1} = (\alpha, \alpha), P_{1,2} = (\alpha^2, \alpha), P_{2,0} = (1, \alpha^2), P_{2,1} = (\alpha, \alpha^2), P_{2,2} = (\alpha^2, \alpha^2), P_{3,0} = (0, 1), P_{4,0} = (0, \alpha),$ os 8 pontos racionais de $\mathcal{X}_2\}$

i = 1

Root Diagram $[1] = 1 < |O_1|$;

GetRootDiagram= $\{\alpha\}$;

GetValueList: $\{\alpha, 1\}$

$k = 1$

$g_1^{(1)} := EvaluateCombination((\alpha,1,P_{1,0}) + (\alpha,1,P_{1,1}).t + (\alpha,1,P_{1,2})t^2)e_1 \Rightarrow g_1^{(1)} = (t + \alpha)e_1$.

$k = 2$

$g_2^{(1)} := EvaluateCombination((\alpha,1,P_{1,0}) + (\alpha,1,P_{1,1}).t + (\alpha,1,P_{1,2})t^2)e_2 \Rightarrow g_1^{(1)} = (t + \alpha)e_2$.

$k = 3$

$g_3^{(1)} := EvaluateCombination((\alpha,1,P_{1,0}) + (\alpha,1,P_{1,1}).t + (\alpha,1,P_{1,2})t^2)e_3 \Rightarrow g_1^{(1)} = (t + \alpha)e_3$.

$k = 4$

$g_4^{(1)} := EvaluateCombination((\alpha,1,P_{1,0}) + (\alpha,1,P_{1,1}).t + (\alpha,1,P_{1,2})t^2)e_4 \Rightarrow g_1^{(1)} = (t + \alpha)e_4$.

Portanto, $g^{(1)} = (\alpha + t, \alpha + t, \alpha + t, \alpha + t)$.

i = 2

Root Diagram $[2] = 2 < |O_2|$;

GetRootDiagram= $\{\alpha, \alpha^2\}$;

GetValueList: $\{1, 1, 1\}$

$k = 2$

$g_2^{(2)} := EvaluateCombination((1,1,1,P_{2,0}) + (1,1,1,P_{2,1}).t + (1,1,1,P_{2,2})t^2)e_1 \Rightarrow g_2^{(2)} = (1 + t + t^2)e_2$.

$k = 3$

$g_3^{(2)} := EvaluateCombination((1,1,1,P_{2,0}) + (1,1,1,P_{2,1}).t + (1,1,1,P_{2,2})t^2)e_3 \Rightarrow g_3^{(2)} = (1 + t + t^2)e_3$.

$k = 4$

$g_4^{(2)} := EvaluateCombination((1,1,1,P_{2,0}) + (1,1,1,P_{2,1}).t + (1,1,1,P_{2,2})t^2)e_4 \Rightarrow g_4^{(2)} = (1 + t + t^2)e_4$.

Portanto, $g^{(2)} = (0, 1 + t + t^2, 1 + t + t^2, 1 + t + t^2)$.

i = 3

Root Diagram $[3] = 1 = |O_3|$, logo $g^{(3)} = (0, 0, t - 1, 0)$.

i = 4

Root Diagram $[4] = 1 = |O_4|$, logo $g^{(4)} = (0, 0, 0, t - 1)$.

Assim, temos a seguinte base de Gröbner para $\overline{C}$:

$$\mathcal{G} = \{g^{(1)}, g^{(2)}, g^{(3)}, g^{(4)}\}.$$

CAPÍTULO 3

Resultados para códigos Hermitianos com mais pontos

Neste capítulo apresentaremos nossos resultados com respeito a códigos Hermitianos bipontuais e n-pontuais. A motivação para estudar estes códigos é que eles podem possuir melhores parâmetros que os códigos pontuais.

3.1 Caso bipontual

Seja $\mathcal{X}_m$ a curva Hermitiana definida sobre $\mathbb{F}_{m^2}$ e com equação no plano $x^{m+1} = y^m + y$. Sabemos que X_m possui m^3+1 pontos $\mathbb{F}_{m^2}$-racionais, sendo $P_\infty = (0:1:0)$ seu único ponto no infinito e $P_{0,0}$ o ponto sobre $\mathcal{X}_m$ que é um zero comum das funções x e y.

Consideremos $C = C_L(D, aP_\infty + bP_{00})$, com $a, b \geq 0$, um código Hermitiano e η o automorfismo de C dado por

$$\eta : \begin{array}{l} \mathbf{x} \mapsto \alpha^{m-1}x \\ y \mapsto y \end{array} \tag{3.1}$$

Sejam $G = aP_\infty + bP_{00}$ e D formado pelos outros $m^3 - 1$ pontos $\mathbb{F}_{m^2}$-racionais de $\mathcal{X}_m$. Adaptando os resultados obtidos no estudo do automorfismo η, dados no capítulo anterior, obtemos os resultados a seguir, que são relacionados a $C_L(D, aP_\infty + bP_{00})$.

Lema 3.1.1. *A ação de η, definido em 3.1 acima, decompõe os m^3-1 pontos racionais de $\mathcal{X}_m$, diferentes de $P_{0,0}$ e P_∞, em m^2-1 órbitas, sendo $m(m-1)$ de comprimento $m+1$ e $m-1$ de comprimento* 1.

Cada uma destas órbitas é a completa interseção de $\mathcal{X}_m$ com uma curva algébrica de grau 1 *definida por*

$$M_i(y) = y - \alpha^{l_i}$$

Cada $M_i(y)$, $i = 1, 2, \ldots, m^2-1$ é uma constante não nula quando restrita a cada órbita O_k, com $k \neq i$.

Demonstração:

Sobre a ação de η os m^3-1 pontos racionais de $\mathcal{X}_m$, diferentes de $P_{0,0}$ e P_∞, estão decompostos nas seguintes órbitas:

para $1 \leq i \leq m(m-1)$ tem-se

$$O_i = O(\alpha^{t_i}, \alpha^{l_i}) = \{(\alpha^{t_i}, \alpha^{l_i}), (\alpha^{t_i+(m-1)}, \alpha^{l_i}), \ldots, (\alpha^{t_i+m(m-1)}, \alpha^{l_i})\};$$

e para $m(m-1)+1 \leq i \leq m^2-1$ tem-se $O_i = \{(0, \alpha^{l_i})\}$.

Onde, para cada $1 \leq i \leq m^2-1$, α^{t_i} e α^{l_i} são elementos de $F^*_{m^2}$, e $\alpha^{l_i} \neq \alpha^{l_j}$ se $i \neq j$.

Logo, $M_i = y - \alpha^i$ intersecta $\mathcal{X}_m$ nos pontos em que $y = \alpha^{l_i}$, ou seja, na órbita O_i.

Se $P_{k,j} = (\alpha^{t_k+j(m+1)}, \alpha^{l_k}) \in O_k$, com $k \neq i$, então $M_i(\alpha^{l_k}) = \alpha^{l_k} - \alpha^{l_i} \neq 0$. □

Sejam O_i, para $1 \leq i \leq m^2-1$, as órbitas definidas no lema anterior.

Lema 3.1.2. *Sejam $i \leq m(m-1)$ e $P_{i,j} = \eta^j(P_{i,0}) = (\alpha^{t_i+j(m-1)}, \alpha^{l_i})$ o j-ésimo ponto de O_i. A função*

$$B_{i,j}(x) = \prod_{k=1}^{m}(x - \alpha^{t_i+(j+k)(m-1)})$$

se anula em cada ponto de O_i, exceto em $P_{i,j}$.

Demonstração:

1) Vejamos que $B_{i,j}(x)$ não se anula em $P_{i,j} = (\alpha^{t_i+j(m-1)}, \alpha^{l_i})$.

De fato,

$$B_{i,j}(\alpha^{t_i+j(m-1)}) = \prod_{k=1}^{m}(\alpha^{t_i+j(m-1)} - \alpha^{t_i+(j+k)(m-1)}) = (\alpha^{t_i+j(m-1)})^m . \prod_{k=1}^{m}(1 - \alpha^{k(m-1)}),$$

mas $1 - \alpha^{k(m-1)} \neq 0$, para todo $k = 1, \ldots, m$, logo tal produto é não nulo.

2) Vejamos que $B_{i,j}(x)$ se anula em cada ponto de $O_i \setminus \{P_{i,j}\}$.

De fato, seja $P_{i,s} = (\alpha^{t_i+s(m-1)}, \alpha^{l_i}) \in O_i \setminus P_{i,j}$. Logo, $B_{i,j}(\alpha^{t_i+s(m-1)}) = \prod_{k=1}^{m}(\alpha^{t_i+s(m-1)} - \alpha^{t_i+(j+k)(m-1)}) = (\alpha^{t_i})^m.\prod_{k=1}^{m}(\alpha^{s(m-1)} - \alpha^{(j+k)(m-1)})$.

Agora, $s, j \in \{0, 1, \ldots, m\}$ com $s \neq j$, e $k \in \{1, 2, \ldots, m\}$.

2*a*) Se $j > s$, então $j = s + l$, com $l \in \{1, 2, \ldots, m\}$. Como $\alpha^{m^2-1} = 1$, basta tomar $k = m + 1 - l$, já que, dessa forma,

$j + k = s + m + 1 \Rightarrow \alpha^{(j+k)(m-1)} = \alpha^{(s+(m+1))(m-1)} = \alpha^{s(m-1)}.\alpha^{(m+1)(m-1)} = \alpha^{s(m-1)}$.

Assim, existe $k \in \{1, 2, \ldots, m\}$, tal que $\alpha^{(j+k)(m-1)} = \alpha^{s(m-1)}$ e, portanto, $B_{i,j}(x)$ se anula em todo $P_{i,s} \in O_i \setminus \{P_{i,j}\}$.

2*b*) Se $s > j$, então $s = j + l$, com $l \in \{1, 2, \ldots, m\}$, e basta tomar $k = l$ para termos $\alpha^{s(m-1)} - \alpha^{(j+k)(m-1)} = 0$. □

Observação 3.1.3. Como x tem pólo de ordem m em $P_\infty = (0 : 1 : 0)$ e y tem pólo de ordem $m + 1$ em $P_\infty = (0 : 1 : 0)$, então:

$M_i(y) \in L((m + 1)P_\infty)$, para $1 \leq i \leq m^2$;

$B_{i,j}(x, y) \in L(m^2 P_\infty)$, para $1 \leq i \leq m(m - 1)$.

Agora, podemos dar a seguinte informação sobre as linhas do diagrama.

Teorema 3.1.4. *Considere o diagrama de raízes do código Hermitiano* $C_L(D, aP_\infty + bP_{00})$.

1) *Seja* $i \leq m(m - 1)$. *Se existem* $0 \leq r \leq m$ *e* $0 \leq s \leq m - 1$ *tais que*

$a \geq (i - 1)(m + 1) + rm - s(m + 1)$ *e*

$b \geq s(m + 1) - r$.

Então a i-ésima linha do diagrama de raízes não é totalmente preenchida.

2) *Seja* $i \leq m(m - 1)$. *Se existem* $0 \leq r \leq m$ *e* $0 \leq s \leq m - 1$ *tais que*

$a \geq (i - 1)(m + 1) + rm - s(m + 1) + m^2$ *e*

$b \geq s(m + 1) - r$.

Então a i-ésima linha do diagrama de raízes é vazia.

3) *Para* $m(m - 1) + 1 \leq i \leq m^2 - 1$, *temos que* $|O_i| = 1$. *Portanto, teremos apenas um quadradinho, que será embaixo do* 1 *que é a única raiz de* $t - 1 = 0$. *Assim, se existem* $0 \leq r \leq m$ *e* $0 \leq s \leq m - 1$ *tais que*

$a \geq (i-1)(m+1) + rm - s(m+1)$ *e* $b \geq s(m+1)$,

temos que a i-ésima linha do diagrama de raízes não é totalmente preenchida, ou seja, é vazia.

Demonstração:

Primeiramente lembremos que os elementos de $C_L(D, aP_\infty + bP_{00})$ podem ser vistos como (m^2-1)-uplas de polinômios $(h_1(t), h_2(t), \ldots, h_{m^2}(t))$, onde para cada i

$$h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j$$

para algum $f \in L(aP_\infty + bP_{00})$.

1) Suponhamos que $i \leq m(m-1)$ e que existam r e s, com $0 \leq r \leq m$ e $0 \leq s \leq m-1$, tais que $a \geq (i-1)(m+1)+rm-s(m+1)$ e $b \geq s(m+1)-r$. Como $M_i(y) \in L((m+1)P_\infty)$ para todo $i \leq m(m-1)$, e $\dfrac{x^r}{y^s} \in L((rm-s(m+1))P_\infty + (s(m+1)-r)P_{00})$, então

$$f_i = M_1(y).M_2(y).\ldots.M_{i-1}(y).\frac{x^r}{y^s} \in L(aP_\infty + bP_{00}).$$

Utilizando f_i vemos que o módulo $\overline{C}$ (e portanto C) conterá um elemento da forma: $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t))$ com $i-1$ componentes iniciais (líderes) nulas, já que $f_i(P_{k,j}) = 0$ para todo $P_{k,j} \in O_k$ com $k = 1, 2, \ldots, i-1$.

Como $|O_i| = m+1$ e $M_k(P_{i,j}) = c_k = const.$, para $k = 1, 2, \ldots, i-1$, temos

$$h_i(t) = \sum_{j=0}^{m} f(P_{i,j})t^j$$

com $f_i(P_{i,j}) = c.\alpha^{rt_i - sl_i}\alpha^{rj(m-1)}$ e c é uma cosntante não nula.

Assim, $h_i(t) = c.\alpha^{rt_i-sl_i}.\displaystyle\sum_{j=0}^{m}(\alpha^{r(m-1)}t)^j$ e, portanto, $\alpha^{-r(m-1)}$ não será uma raiz de $h_i(t)$.

Pela definição de base de Gröbner, $g_i^{(i)}(t)$ divide $h_i(t)$ (que é o termo líder da m^2-upla $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t))$) assim, $\alpha^{-r(m-1)}$ também não será raiz de $g_i^{(i)}(t)$, e consequentemente a i-ésima linha do diagrama não é totalmente preenchida, pois neste caso não marcaremos $\alpha^{-r(m-1)}$.

2) Agora suponhamos que $i \leq m(m-1)$ e que existam $0 \leq r \leq m$ e $0 \leq sm-1$ tais que $a \geq (i-1)(m+1) + rm - s(m+1) + m^2$ e $b \geq s(m+1) - r$. Assim,

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).B_{i,0}(x).\frac{x^r}{y^s} \in L(aP_\infty + bP_{00}).$$

Logo $f_i(P) = 0$ para todo $P \in O_1 \bigcup O_2 \bigcup \ldots \bigcup O_{i-1}$, pois se $P \in O_k$, para algum $k = 1, 2, \ldots, i-1$, temos $M_k(P) = 0$. Mais ainda, $f_i(Q) = 0$ para todo $Q \in O_i \setminus \{P_{i,0}\}$, pois $B_{i,0}$ se anula em todo $Q \in O_i \setminus \{P_{i,0}\}$.

Portanto, conseguimos $h_1(t) = h_2(t) = \ldots = h_{i-1}(t) = 0$ e $h_i(t) = f_i(P_{i,0}) + 0 + \ldots + 0 = f_i(P_{i,0}) = c \neq 0$. E, assim, temos que o módulo $\overline{C}$ possui um elemento da forma $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$.

Agora, como $g_i^{(i)}(t)$ divide $h_i(t) = c$ que não possui raiz, temos que $g_i^{(i)}(t)$ também não possui raiz e, assim, a i-esima linha do diagrama é vazia.

3) No caso em que $m(m-1) + 1 \leq i \leq m^2$, temos que $|O_i| = 1$, logo os $h_i(t) = f(P_{i,j})$ são constantes. Assim, se existem $0 \leq r \leq m$ e $0 \leq s \leq m-1$ tais que $a \geq (i-1)(m+1) + rm - s(m+1)$ e $b \geq s(m+1)$, tomamos

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y) \right) . \frac{(x-c)^r}{y^s}$$

com $(x - c) \neq 0$ para todo $x = \alpha^{t_k + j(m-1)}$ com $1 \leq k \leq m(m-1)$ e $1 \leq j \leq m$.

Então, tal f_i está em $L(aP_\infty + bP_{00})$ e, novamente, temos um elemento da forma $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$ em $\overline{C}$ e a i-ésima linha será vazia. □

Recordando que V_i é o espaço gerado por $\left(\prod_{k=1}^{i-1} M_k(y) \right) .x^r$, para $0 \leq r \leq m$, e que se $P_{i,j} \in O_i$, então $P_{i,j} = (\alpha^{t_i + j(m-1)}, \alpha^{l_i})$, utilizamos o corolário 2.0.45 conseguimos a seguinte proposição.

Proposição 3.1.5. *Para toda coleção de valores c_j, com $j = 0, 1, \ldots, m$, e para cada $0 \leq s \leq m-1$, existe uma única função $f(x, y) \in V_i$ a qual satisfaz $f(P_{i,j}) = c_j.\alpha^{s.l_i}$, para todo j, e que é identicamente nula em $O_1, \ldots, O_{i-1}$. Isto é, $\dfrac{f(x,y)}{y^s}$ vale c_j quando aplicada a $P_{i,j}$ e, mais ainda, $\dfrac{f(x,y)}{y^s}$ se anula em $O_1, \ldots, O_{i-1}$.*

Demonstração:

Pelos lema 4.0.11, corolário 2.0.45 e usando "forma de Lagrange"temos que existe $P_m(x) \in \dfrac{\mathbb{F}_q[x]}{\langle x^{m+1} - \alpha^{l_i.m} - \alpha^{l_i} \rangle}$, que resolve os problemas de interpolação em O_i, para os valores $c_j.\alpha^{sl_i}$, $j = 0, 1, \ldots, m$.

Com as mesmas notações do lema 4.0.11 e do corolário 2.0.45, temos que $f(x,y) = \Phi_i^{-1}(P_m(x)) \in V_i$ também se anula nas órbitas $O_1, \ldots, O_{i-1}$.

Ou seja, fazemos o mesmo que no corolário 2.0.45, só que para a coleção de valores $c_j.\alpha^{sl_i}$.

□

O resultado a seguir nos diz como serão as linhas do diagrama.

Teorema 3.1.6. *Seja i um inteiro tal que $1 \leq i \leq m(m-1)$.*

1) Se existem r e s, com $0 \leq r \leq m$ e $s \geq 0$, tais que

$$a \geq (i-1)(m+1) + rm - s(m+1) \quad e \quad b \geq s(m+1) - r$$

Então a i-ésima linha do diagrama não é totalmente preenchida.

2) Se existem r e s, com $0 \leq r \leq m$ e $s \geq 0$, tais que

$$a < (i-1)(m+1) + rm - s(m+1) + m^2 \quad ou \quad b < s(m+1) - r.$$

Então, não podemos garantir que a i-ésima linha do diagrama é vazia.

Nestas condições, sendo M o conjunto das raízes marcadas na i-ésima linha do diagrama de raízes, o complementar de M é o conjunto

$$M^c = \{\alpha^{-r(m-1)} \ ; \ 0 \leq r \leq m \text{ e existe } s \geq 0 \text{ tal que}$$

$$a \geq (i-1)(m+1) + rm - s(m+1) \quad e \quad b \geq s(m+1) - r\}.$$

Demonstração:

Sabemos que x tem pólo de ordem m em P_∞, $M_i(y)$ tem pólo de ordem $m+1$ em P_∞ e $\dfrac{1}{y}$ tem pólo de ordem m em P_{00}.

Assim, para todo $i = 1, 2, \ldots, m(m-1)$, as funções $f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).\dfrac{x^r}{y^s}$, com $rm - s(m+1) + (i-1)(m+1) \leq a$ e $s(m+1) - r \leq b$ estão em $L(aP_\infty + bP_{00})$.

Como $y = M_i(y) - c$ e $x^{m+1} = y^m + y$ podemos tomar $0 \leq r \leq m$. Portanto $f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).\dfrac{x^r}{y^s}$, com $0 \leq r \leq m$, está em $L(aP_\infty + bP_{00})$ se $rm - s(m+1) + (i-1)(m+1) \leq a$ e $s(m+1) - r \leq b$.

Sejam $h_i(t) = \sum_{j=0}^{|O_i|-1} f_i(P_{i,j})t^j$, para $1 \leq i \leq m(m-1)$.

Como $M_k(y)$ é zero para os elementos de O_k, temos que $h_j(t) = 0$, para $1 \leq j \leq i-1$.

Sabemos que $M_j(y)$ são constantes não nulas em O_k, para $k \neq j$, e que os elementos de O_i são do tipo $P_{i,j} = \eta^j(P_{i,0}) = (\alpha^{t_i+j(m-1)}, \alpha^{l_i}) = (\alpha^{t_i}\alpha^{j(m-1)}, \alpha^{l_i})$. Então $f_i(P_{i,j}) = c.\alpha^{rt_i-sl_i}\alpha^{rj(m-1)}$, onde c é uma constante.

Multiplicando pelas suas respectivas inversas, podemos desconsiderar as constantes c e $\alpha^{rt_i-sl_i}$, pois elas não alteram os valores das raízes. Assim, temos $h_i(t) = \sum_{j=0}^{m}(\alpha^{r(m-1)}t)^j$, com $(0,\ldots,0,h_i(t),\ldots,h_{m^2}(t)) \in \overline{C}$.

Agora, $t = \alpha^{-(r(m-1))} \in \mathbb{F}_r^\star$ não é raiz de $h_i(t)$, pois $h_i(\alpha^{-(r(m-1))}) = 1+1+\ldots+1 = m+1 \neq 0$. Portanto, as raízes de $h_i(t)$ são diferentes de $\alpha^{-(r(m-1))}$.

Como a componente $g_i^{(i)}(t)$ do elemento $g^{(i)}$ da base de Gröbner $\mathcal{G}$ de $\overline{C}$ divide $h_i(t)$, temos que $g_i^{(i)}(t)$ não tem $\alpha^{-(r(m-1))}$ como raiz.

Então temos $\{\alpha^{-r(m-1)}$; $0 \leq r \leq m$ e existe $s \geq 0$ tal que $a \geq (i-1)(m+1)+rm-s(m+1)$ e $b \geq s(m+1)-r\} \subseteq M^c$.

Agora, vejamos que $M^c \subseteq \{\alpha^{-r(m-1)}$; $0 \leq r \leq m$ e existe $s \geq 0$ tal que $a \geq (i-1)(m+1)+rm-s(m+1)$ e $b \geq s(m+1)-r\}$.

Seja $g(x,y) \in L(aP_\infty + bP_{00})$ uma função que se anula em $O_1, O_2, \ldots, O_{i-1}$, e possua o menor número de raízes no diagrama. Sejam $\{\alpha^{s_1}, \alpha^{s_2}, \ldots, \alpha^{s_l}\}$ o conjunto de tais raízes de g, e $\prod_{k=1}^{l}(t-\alpha^{s_k}) = \sum_{j=0}^{l} c_j t^j$ o único polinômio mônico de grau l que possua tais raízes.

Queremos uma função cujos valores em O_i são:

$$g(P_{i,j}) = \begin{cases} \mathbf{0}, \text{ se } j = l+1,\ldots,m \\ c_j, \text{ se } j = 0,1,\ldots,l \end{cases}$$

Agora pelo corolário 2.0.45, existe única solução para f em V_i, que satisfaz

$$f(P_{i,j}) = \begin{cases} \mathbf{0}, \text{ se } j = l+1,\ldots,m \\ c_j, \text{ se } j = 0,1,\ldots,l \end{cases}$$

Logo tomando $g(x,y) = \dfrac{\alpha^{sl_i}.f(x,y)}{y^s}$ temos o que queríamos. E assim vemos que não podemos ter um conjunto menor do que M^c que contenha tais raízes. □

Teorema 3.1.7. *Sejam $\{\alpha^{s_1}, \alpha^{s_2}, \ldots, \alpha^{s_l}\}$ o conjunto de raízes que aparecem na i-ésima linha do diagrama de raízes de um código Hermitiano $C_L(D, aP_\infty + bP_{00})$, e r e s tais que*

$a \geq (i-1)(m+1)+rm-s(m+1)+m^2$ *e* $b \geq s(m+1)-r$. *Seja* $p(t) = \prod_{k=1}^{l}(t-\alpha^{s_k}) = \sum_{j=0}^{l} c_j t^j$, *o único polinômio mônico de grau* l *com tais raízes.*

Então

$$f(x,y) = \prod_{k=1}^{i-1} M_k(y).\left(\sum_{j=0}^{|O_i|-1} c_j \frac{B_{i,j}(x)}{B_{i,j}(P_{i,j})}.\frac{x^r}{\alpha^{r(t_i+j(m-1))}}\right).\frac{\alpha^{sl_i}}{y^s}$$

é uma função em $L(aP_\infty + bP_{00})$ *que fornece um elemento* $\mathbf{g}^{(i)}$ *módulo com* $i-1$ *componentes líderes iguais a zero e a* i*-ésima comonente* $g_i^{(i)}(t)$ *igual a* $p(t)$.

Demonstração:

Do lema 3.1.2 e do teorema 3.1.6 temos que $f(x,y) \in L(aP_\infty + bP_{00})$, e é claro que $f(x,y)$ é solução do problema de interpolação sobre O_i, que é única, pela proposição 3.1.5. E temos o que queríamos. □

Exemplo 3.1.8. Consideremos o código $C = C_L(D, 7P_\infty + 12P_{00})$ na curva Hermitiana sobre $\mathbb{F}_9$ e η, como em 2.1, de ordem 4. O automorfismo η permuta os 26 pontos racionais, diferentes de $P_{0,0}$ e P_∞, em 8 órbitas, sendo 6 de comprimento 4 e 2 de comprimento 1.

Lembremos que $|O_i| = 4$, para $i = 1, 2, \ldots, 6$. Logo $t^{|O_i|} - 1 = 0$ possui $1, \alpha^2, \alpha^4$ e α^6 como raízes. E $|O_i| = 1$, para $i = 7, 8, 9$. Logo $t^{|O_i|} - 1 = 0$ tem somente o 1 como raiz.

Sabendo que $a = 7$ e $b = 12$ e, utilizando os teoremas 3.1.4 e 3.1.6, contruímos o seguinte diagrama de raízes para nosso código C.

Linha 1: Para $i = 1$, temos que $r = 0$ e $s = 1$ são tais que $7 \geq 3r - 4s + 9$ e $12 \geq 4s - r$. Logo a linha 1 é vazia.

Linha 2: Para $i = 2$, temos que $r = 0$ e $s = 2$ são tais que $7 \geq 3r - 4s + 13$ e $12 \geq 4s - r$. Logo a linha 2 é vazia.

Linha 3: Para $i = 3$, temos que $r = 0$ e $s = 3$ são tais que $7 \geq 3r - 4s + 17$ e $12 \geq 4s - r$. Logo a linha 3 também é vazia.

Linha 4: Para $i = 4$, não conseguimos r e s tais que $7 \geq 3r - 4s + 21$ e $12 \geq 4s - r$. Logo não podemos garantir que a linha 4 é vazia.

Encontramos r e s tais que $7 \geq 12 + 3r - 4s$ e $12 \geq 4s - r$. Logo a linha 4 não é totamente preenchida.

Portanto, utilizando o teorema 3.1.6, maracaremos na linha 4 somente α^2.

Linha 5: Para $i = 5$, novamente não conseguimos r e s tais que $7 \geq 3r - 4s + 21$ e $12 \geq 4s - r$. Logo não podemos garantir que a linha 4 é vazia.

Novamente encontramos r e s tais que $7 \geq 12 + 3r - 4s$ e $12 \geq 4s - r$. Logo a linha 5 não é totamente preenchida.

Portanto, utilizando o teorema 3.1.6, maracaremos na linha 5 α^2 e α^4.

Linha 6: Agora não encontramos $0 \leq r \leq 4$ e $s \geq 0$ tais que $7 \geq 20 + 3r - 4s$ e $12 \geq 4s - r$. Portanto temos que a linha 6 é totalmente preenchida.

Linhas 7,8,9: Existem r e s nas condições do teorema 5.3. Portanto, tais linhas são totalmente preenchidas.

Dessa forma temos o diagrama:

1	α^2	α^4	α^6
	X		
	X	X	
X	X	X	X
X			
X			
X			

Pela proposição 2.0.36, a dimensão do código é 17.

3.2 O caso de n pontos

Nesta seção estudaremos, para $2 \leq n \leq m + 1$, códigos Hermitanos n-pontuais $C(D, aP_\infty + bP_0 + c_1P_{k_1} + \ldots + c_{n-2}P_{k_{n-2}})$, onde P_∞ é o único ponto no infinito, P_0 é a origem, e, para cada $j = 1, \ldots, n-2$, $P_{k_j} = (0, \alpha^{l_{k_j}}) \in O_{k_j}$, com $|O_{k_j}| = 1$, $k_j \in \{m(m-1)+1, \ldots, m^2-1\}$ e $\alpha^{l_{k_j}} \in \mathbb{F}^*_{m^2}$. Para simplificar nossas notações denotaremos $(0, \alpha^{l_{k_j}})$ por $(0, \alpha_{(j)})$.

Considere o código Hermitiano n-pontual $C(D, aP_\infty + bP_0 + c_1P_{k_1} + \ldots + c_{n-2}P_{k_{n-2}})$ com o automorfismo η definido em 3.1 e dado por

$$\eta(x) = \alpha^{m-1}x \quad \text{e} \quad \eta(y) = y.$$

Um primeiro resultado, análogo ao da proposição 3.1.4, é o seguinte.

Proposição 3.2.1. *Sobre a ação de η, os $m^3-(n-1)$ pontos $\mathbb{F}_{m^2}$-racionais que estão em SuppD se decompõem em $m^2-(n-1)$ órbitas, sendo $m(m-1)$ de comprimento $m+1$ e $m-(n-1)$ de comprimento 1. (Fixaremos a notação para tais órbitas da seguinte maneira. As órbitas de comprimento $m+1$, serão denotadas por $O_1,\ldots,O_{m(m-1)}$ e as órbitas de comprimento 1 por $O_{m(m-1)+1},\ldots,O_{m^2-(n-1)}$.) Cada uma destas órbitas é uma completa interseção de $\mathcal{X}_m$ com uma curva algébrica de grau 1, definida pela equação:*

$$M_i(y) = y - \alpha^{l_i}$$

Cada $M_i(y)$, $i=1,\ldots,m^2-(n-1)$, é uma costante não nula quando restrita a cada uma das órbitas O_k, $k\neq i$.

Demonstração: Análoga a demonstração de 3.1.4.

Teorema 3.2.2. *Considere o diagrama de raízes do código Hermitiano $C(D, aP_\infty + bP_0 + c_1P_{k_1} + \ldots + c_{n-2}P_{k_{n-2}})$.*

(1) Seja $i \leq m(m-1)$. Se existem $0\leq r\leq m$ e $s,t_1,\ldots,t_{n-2}\geq 0$ tais que
$a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1)$,
$b \geq s(m+1) - r$ *e* $c_l \geq t_l(m+1) - r$, *para todo* $l=1,\ldots,n-2$.
Então a i-ésima linha do diagrama não é totalmente preenchida.

(2) Seja $i \leq m(m-1)$. Se existem $0\leq r\leq m$ e $s,t_1,\ldots,t_{n-2}\geq 0$ tais que
$a \geq (i-1)(m+1) + rm - s(m+1) - \left(\sum_{j=1}^{n-2} t_j(m+1)\right) + m^2$,
$b \geq s(m+1) - r$ *e* $c_l \geq t_l(m+1) - r$, *para todo* $l=1,\ldots,n-2$.
Então a i-ésima linha do diagrama de raízes é vazia.

(3) Finalmente, considerando o caso $m(m-1)+1 \leq i \leq m^2-(n-1)$, temos $|O_i|=1$, logo em cada uma destas linhas tem-se somente um único quadradinho, que será embaixo do 1 que é é a única raiz de $t-1=0$. Assim, se existem $0\leq r\leq m$ e $s,t_1,\ldots,t_{n-2}\geq 0$ tais que

$$a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1),$$

$b \geq s(m+1)$ e $c_l \geq t_l(m+1)$, para todo $l = 1, \ldots, n-2$.

Então a linha i será vazia.

Demonstração:

Os elementos de $C(D, aP_\infty + bP_0 + c_1P_{k_1} + \ldots + c_{n-2}P_{k_{n-2}})$ podem ser representados por $(m^2-(n-1))$-uplas de polinômios $(h_1(t), h_2(t), \ldots, h_{m^2-(n-1)}(t))$, onde para cada i:

$$h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j$$

para algum $f \in L(aP_\infty + bP_0 + c_1P_{i_1} + \ldots + c_{n-2}P_{i_{n-2}})$.

1) Suponha que $i \leq m(m-1)$ e que existam $0 \leq r \leq m$ e $s, t_1, \ldots, t_{n-2} \geq 0$ tais que $a \geq (i-1)(m+1)+rm-s(m+1)-\sum_{j=1}^{n-2} t_j(m+1)$, $b \geq s(m+1)-r, c_1 \geq t_1(m+1)-r, \ldots, c_{n-2} \geq t_{n-2}(m+1)-r$. Como $M_i(y) \in L((m+1)P_\infty)$ para todo $i \leq m(m-1)$ e $\dfrac{x^r}{y^s.\prod_{j=1}^{n-2}(y-\alpha_{(j)})^{t_j}} \in L((rm-s(m+1)-\sum_{j=1}^{n-2} t_j(m+1))P_\infty + (s(m+1)-r)P_0 + \sum_{j=1}^{n-2}(t_j(m+1)-r)P_{k_j})$,

então:

$$f_i = \prod_{k=1}^{i-1} M_k(y).\frac{x^r}{y^s.\prod_{j=1}^{n-2}(y-\alpha_{(j)})^{t_j}} \in L(aP_\infty + bP_0 + \sum_{j=1}^{n-2} c_jP_{k_j})$$

Evaluando f_i sobre os elementos de O_k, para $k = 1, 2, \ldots, i-1$, vemos que o módulo $\overline{C}$ (e portanto C) conterá um elemento da forma: $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t))$ com $i-1$ componentes nulas, já que $f_i(P_{k,j}) = 0$ para todo $P_{k,j} \in O_k$ e $k = 1, 2, \ldots, i-1$.

Como $|O_i| = m+1$ temos

$$h_i(t) = \sum_{j=0}^{m} f(P_{i,j})t^j$$

com $f_i(P_{i,j}) = \dfrac{c.\alpha^{rt_i-sl_i}}{\prod_{j=1}^{n-2}(\alpha^{l_i}-\alpha_{(j)})^{t_j}}.\alpha^{rj(m-1)}$.

Assim, $h_i(t) = \dfrac{c.\alpha^{rt_i-sl_i}}{\prod_{j=1}^{n-2}(\alpha^{l_i}-\alpha_{(j)})^{t_j}}.\sum_{j=0}^{m}(\alpha^{r(m-1)}t)^j$ e, portanto $\alpha^{-r(m-1)}$ não é raiz de $h_i(t)$.

Pela definição de base de Gröbner, $g_i^{(i)}(t)$ divide $h_i(t)$ (que é o termo líder da m^2-upla $(0, \ldots, 0, h_i(t), \ldots, h_{m^2}(t))$), e assim $\alpha^{-r(m-1)}$ também não será raiz de $g_i^{(i)}(t)$ e, consequentemente, a i-ésima linha do diagrama não é totalmente preenchida.

2) Agora suponha que $i \leq m(m-1)$ e que existam $0 \leq r \leq m$ e $s, t_1, \ldots, t_{n-2} \geq 0$ tais que $a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1) + m^2$, $b \geq s(m+1) - r$, $c_1 \geq t_1(m+1) - r$, $\ldots$, $c_{n-2} \geq t_{n-2}(m+1) - r$.

Logo,

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).B_{i,0}(x).\frac{x^r}{y^s.\prod_{j=1}^{n-2}(y-\alpha_{(j)})^{t_j}} \in L(aP_\infty + bP_0 + \sum_{j=1}^{n-2} c_j P_{i_j})$$

e $f_i(P) = 0$ para $p \in O_1 \bigcup O_2 \bigcup \ldots \bigcup O_{i-1}$, pois $M_k(P) = 0$ se $P \in O_k$, para $k = 1, 2, \ldots, i-1$. Mais ainda, como $B_{i,0}$ é nulo se $Q \in O_i \setminus \{P_{i,0}\}$, temos que $f_i(Q) = 0$ para todo $Q \in O_i \setminus \{P_{i,0}\}$.

Portanto, $h_1(t) = h_2(t) = \ldots = h_{i-1}(t) = 0$ e $h_i(t) = f_i(P_{i,0}) + 0 + \ldots + 0 = f_i(P_{i,0}) = c \neq 0$, e, assim, $\overline{C}$ possui um elemento da forma $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$.

Como $g_i^{(i)}(t)$ divide $h_i(t) = c$ que é uma constante não nula, segue que $g_i^{(i)}(t)$ não possui raiz. Logo, a i-ésima linha do diagrama de raízes é vazia.

3) No caso de $m(m-1) + 1 \leq i \leq m^2 - (n-1)$, tem-se $|O_i| = 1$, logo $h_i(t) = f(P_{i,j})$ é constante, para todo i. Assim, se existem $0 \leq r \leq m$ e $s, t_1, \ldots, t_{n-2} \geq 0$ tais que $a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1)$, $b \geq s(m+1)$, $c_1 \geq t_1(m+1)$, $\ldots$, $c_{n-2} \geq t_{n-2}(m+1)$,

consideremos

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).\frac{(x-c)^r}{y^s.\prod_{j=1}^{n-2}(y-\alpha_{(j)})^{t_j}}$$

uma função com $(x-c) \neq 0$ para todo $x = \alpha^{t_k + j(m-1)}$ com $1 \leq k \leq m(m-1)$ e $1 \leq j \leq m$.

Então, $f_i \in L(aP_\infty + bP_0 + \sum_{j=1}^{n-2} c_j P_{k_j})$ e, novamente, temos um elemento da forma $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$ em $\overline{C}$, e portanto a linha i será vazia. □

Teorema 3.2.3. *Seja* $1 \leq i \leq m(m-1)$.

1) Se existem r *e* $s, t_1, \ldots, t_{n-2}$ *inteiros, com* $0 \leq r \leq m$ *e* $s, t_1, \ldots, t_{n-2} \geq 0$ *tais que:*

$$a \geq (i-1)(m+1) + rm - s(m+1) \quad , \quad b \geq s(m+1) - r \text{ e } c_j \geq t_j(m+1) - r$$

onde $j = 1, \ldots, n-2$.

Então a i-ésima linha do diagrama não é totalmente preenchida.

2) Se existem r *e* $s, t_1, \ldots, t_{n-2}$ *inteiros, com* $0 \leq r \leq m$ *e* $s, t_1, \ldots, t_{n-2} \geq 0$ *tais que:*

$$a < (i-1)(m+1) + rm - s(m+1)m^2 \quad ou \quad b < s(m+1) - r \text{ ou } c_j < t_j(m+1) - r$$

para algum $j = 1, \ldots, n-2$. *Então não garantimos que a linha* i *é vazia.*

Sobre essas condições, se M *é o conjunto das raízes marcadas sobre a linhao* i, *o complementar de* M *é o conjunto*

$$M^c = \{\alpha^{-r(m-1)} \text{ ; } 0 \leq r \leq m \text{ e existem } s, t_1, \ldots, t_{n-2} \geq 0 \text{ tais que}$$

$$a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1) \quad , \quad b \geq s(m+1) - r \text{ e } c_j \geq t_j(m+1) - r\}.$$

Demonstração:

Sabemos que x tem pólo de ordem m e $M_i(y)$ tem pólo de ordem $m+1$ em P_∞, $\dfrac{1}{y}$ tem pólo de ordem $m+1$ em P_0 e $\dfrac{1}{y - \alpha_{(j)}}$ tem pólo de ordem $m+1$ em P_{k_j}, para $j = 1, \ldots, n-2$. Então, para $i = 1, 2, \ldots, m(m-1)$ e $j = 1, \ldots, n-2$, temos que

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y) \right) . \frac{x^r}{y^s . \prod_{j=1}^{n-2} (y - \alpha_{(j)})^{t_j}},$$

é um elemento de $L(aP_\infty + bP_0 + \sum_{j=1}^{n-2} c_j P_{k_j})$ se

$rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1) + (i-1)(m+1) \leq a$;

$s(m+1) - r \leq b$;

$t_j(m+1) \leq c_j$.

Como $y = M_i(y) - c$ e $x^{m+1} = y^m + y$ podemos tomar $0 \leq r \leq m$.

Seja $h_i(t) = \sum_{j=0}^{|O_i|-1} f_i(P_{i,j}) t^j$, para $1 \leq i \leq m(m-1)$.

Como $M_k(y)$ vale zero sobre os elementos de O_k, temos que $h_j(t) = 0$, para $1 \leq j \leq i-1$.

Sabemos que $M_j(y)$ são constantes não nulas sobre O_k, para $k \neq j$, e que os elementos de O_i são $P_{i,j'} = \eta^{j'}(P_{i,0}) = (\alpha^{t_i + j'(m-1)}, \alpha^{l_i}) = (\alpha^{t_i} \alpha^{j'(m-1)}, \alpha^{l_i})$. Assim, podemos escrever $f_i(P_{i,j'}) = \dfrac{c . \alpha^{r t_i - s l_i}}{\prod_{j=1}^{n-2} (\alpha^{l_i} - \alpha_{(j)})^{t_j}} . \alpha^{r j'(m-1)}$, onde c é uma constante.

Removendo fatores comuns $(\frac{c . \alpha^{r t_i - s l_i}}{\prod_{j=1}^{n-2} (\alpha^{l_i} - \alpha_{(j)})^{t_j}})$, que não influirão no conjunto de raízes, conseguimos $h_i(t) = \sum_{j'=0}^{m} (\alpha^{r(m-1)} t)^{j'}$. Note que as raízes deste polinômio são todas diferentes de $\alpha^{-(r(m-1))} \in \mathbb{F}_r^\star$, já que $h_i(\alpha^{-(r(m-1))}) = 1 + 1 + \ldots + 1 = m + 1 \neq 0$.

Como $C(D, aP_\infty + bP_0 + \sum_{j=1}^{n-2} c_j P_{i_j})$ é um $\mathbb{F}_q[t]$-módulo, ele conterá um elemento cujas primeiras $i-1$ entradas são 0, e a i-ésima entrada é o maior divisor comum dos polinômios $\sum_{j'=0}^{m} (\alpha^{r(m-1)}t)^{j'}$, onde $0 \leq r \leq m$, $s, t_1, \ldots, t_{n-2} \geq 0$ e $a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1)$, $b \geq s(m+1) - r$ e $t_j(m+1) \leq c_j$, para todo $j = 1, \ldots, n-2$. A componente diagonal $g_i^{(i)}(t)$ do elemento $g^{(i)}$ da base de Gröbner $\mathcal{G}$ deve dividir tal MDC.

Então, temos que $\{\alpha^{-r(m-1)}$; $0 \leq r \leq m$ e existem $s, t_1, \ldots, t_{n-2} \geq 0$ tais que $a \geq (i-1)(m+1) + rm - s(m+1) - \sum_{j=1}^{n-2} t_j(m+1)$, $b \geq s(m+1) - r$ e $c_j \geq t_j(m+1) - r\} \subseteq M^c$.

Analogamente ao caso bipontual mostra-se a inclusão contrária. □

Utilizando esses resultados e os do capítulo anterior conseguimos, analogamente ao caso bipontual, a construção do algoritmo de bases de Gröbner para o caso n-pontual.

Para finalizar este capítulo vamos dar um exemplo de como construir o diagrama de raízes para um código Hermitiano $C(D, G)$ com $Supp(G)$ tendo mais de dois pontos.

Exemplo 3.2.4. Seja $C = C(D, 5P_\infty + 8P_{0,0} + 4P_1 + 3P_2)$ um código Hermitiano sobre $\mathbb{F}_9$, onde $P_1 = (0, \alpha^{l_1})$ e $P_2 = (0, \alpha^{l_2})$, com $\alpha^{l_1}, \alpha^{l_2} \in \mathbb{F}_9^\star$ são raízes de $y^3 + y = 0$. O automofismo

$$\eta : \begin{array}{l} \mathbf{x} \mapsto \alpha^2 x \\ y \mapsto y \end{array}$$

permuta os outros 24 pontos $\mathbb{F}_9$-racionais da curva Hermitiana $y^3 + y = x^4$ em 6 órbitas de comprimento 4.

Assim, para $i = 1, 2, \ldots, 6$, $t^{|O_i|} - 1 = t^4 - 1$ que possui $1, \alpha^2, \alpha^4$ e α^6 como raízes.

Neste exemplo temos que: $m = 3$, $1 \leq i \leq 6$, $a = 5$, $b = 8$, $c_1 = 4$ e $c_2 = 3$. Com tais valores o teorema 3.2.2 possui as seguintes condições.

(1) Seja $i \leq 6$. Se existem $0 \leq r \leq 3$ e $s, t_1, \ldots, t_{n-2} \geq 0$ tais que

$5 \geq 4(i-1) + 3r - 4s - 4t_1 - 4t_2$,

$8 \geq 4s - r$, $4 \geq 4t_l - r$ e $3 \geq 4t_2 - r$.

Então a i-ésima linha do diagrama não é totalmente preenchida.

(2) Seja $i \leq 6$. Se existem $0 \leq r \leq m$ e $s, t_1, \ldots, t_{n-2} \geq 0$ tais que

$5 \geq 4(i-1) + 3r - 4s - 4t_1 - 4t_2 + 9$,

$8 \geq 4s - r$, $4 \geq 4t_l - r$ e $3 \geq 4t_2 - r$.

Então a i-ésima linha do diagrama de raízes é vazia.

E do teorema 3.2.3 temos que se M é o conjunto das raízes marcadas sobre a linhao i, o complementar de M é o conjunto

$$M^c = \{\alpha^{-2r} \ ; \ 0 \leq r \leq 3 \text{ e existem } s, t_1, \ldots, t_{n-2} \geq 0 \text{ tais que}$$

$$5 \geq 4(i-1) + 3r - 4s - 4t_1 - 4t_2 \ \ , \ \ 8 \geq 4s - r \ , \ 4 \geq 4t_l - r \text{ e } 3 \geq 4t_2 - r\}.$$

Assim, construímos o seguinte diagrama de raízes para o código C.

Linha 1: Para $i = 1$, temos que $r = 0$, $s = 1$ e $t_1 = t_2 = 0$ satisfazem a condição 2) do teorema 3.2.2 e, então, a linha 1 será vazia.

Linha 2: Para $i = 2$, temos que $r = 0$, $s = t_1 = 1$ e $t_2 = 0$ satisfazem a condição 2) do teorema 3.2.2 e, então, a linha 2 também será vazia.

Linha 3: Para $i = 3$, temos que $r = 0$, $s = 2$, $t_1 = 1$ e $t_2 = 0$ satisfazem a condição 2) do teroema 3.2.2 e, assim, a linha 3 também será vazia.

Linha 4: Para $i = 4$ não encontramos r, s, t_1 e t_2 que satisfazem a condição 2) do teorema 3.2.2, mas pelo teorema 3.2.3 veremos que essa linha também será vazia.

De fato,

I) Se $r = 0$, $s = t_1 = 1$ e $t_2 = 0$, então, pelo teorema 3.2.3, não marcamos $\alpha^0 = 1$;

II) Se $r = 1$, $s = 2$, $t_1 = 1$ e $t_2 = 0$, pelo teorema 3.2.3, não marcamos $\alpha^{-2} = \alpha^6$;

III) Se $r = 2$, $s = 2$, $t_1 = 1$ e $t_2 = 1$, pelo teorema 3.2.3, não marcamos $\alpha^{-4} = \alpha^4$;

IV) Se $r = 3$, $s = 2$, $t_1 = 1$ e $t_2 = 1$, pelo teorema 3.2.3, não marcamos $\alpha^{-6} = \alpha^2$.

Portanto, a linha 4 será vazia, pois não marcaremos nenhuma das raízes.

Linha 5: Para $i = 5$ temos:

I) Se $r = 0$, $s = 2$, $t_1 = 1$ e $t_2 = 0$, pelo teorema 3.2.3, não marcamos $\alpha^0 = 1$;

II) Se $r = 1$, $s = 2$, $t_1 = 1$ e $t_2 = 1$, pelo teorema 3.2.3, não marcamos $\alpha^{-2} = \alpha^6$;

III) Se $r = 2$, não existem $s, t_1, t_2 \geq 0$ tais que

$$\begin{aligned} 5 &\geq 22 - 4s - 4t_1 - 4t_2 \\ 8 &\geq 4s - 2 \\ 4 &\geq 4t_1 - 2 \\ 3 &\geq 4t_2 - 2 \end{aligned}$$

Logo, pelo teorema 3.2.3, marcamos $\alpha^{-4} = \alpha^4$;

IV) Se $r = 3$, não existem $s, t_1, t_2 \geq 0$ tais que

$$\begin{aligned} 5 &\geq 25 - 4s - 4t_1 - 4t_2 \\ 8 &\geq 4s - 3 \\ 4 &\geq 4t_1 - 3 \\ 3 &\geq 4t_2 - 3 \end{aligned}$$

Assim, pelo teorema 3.2.3, marcamos $\alpha^{-6} = \alpha^2$.

Linha 6: Para $i = 6$ n4ao existem $r, s, t_1, t_2 \geq 0$, com $0 \leq r \leq 3$, tais que

$$\begin{aligned} 5 &\geq 20 + 3r - 4s - 4t_1 - 4t_2 \\ 8 &\geq 4s - r \\ 4 &\geq 4t_1 - r \\ 3 &\geq 4t_2 - r \end{aligned}$$

Portanto, pelo condição 1) do teorema 3.2.2 temos que a linha 6 é totalmente preenchida.

E temos o digrama a seguir.

1	α^2	α^4	α^6
	X	X	
X	X	X	X

CAPÍTULO 4

Os Resultados sobre a curva Norma-traço

Considere q uma potência de um número primo e $r \geq 2$ um inteiro positivo.

Definição 4.0.5. Para $\alpha \in \mathbb{F}_{q^r}$ a *norma* $\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ de α sobre $\mathbb{F}_q$ é definida por

$$\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) := \alpha^{\frac{q^r-1}{q-1}}.$$

E o *traço* $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ de α sobre $\mathbb{F}_q$ é dado por

$$Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) := \alpha^{q^{r-1}} + \alpha^{q^{r-2}} + \ldots + \alpha^q + \alpha.$$

Ou seja, temos a soma e o produto dos conjugados de α.

Sejam $\mathcal{X}_{q,r}$ curvas sobre $\mathbb{F}_{q^r}$ de equação no plano

$$x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y. \tag{4.1}$$

Como os zeros de $F(X,Y) = X^{\frac{q^r-1}{q-1}} - (Y^{q^{r-1}} + Y^{q^{r-2}} + \ldots + Y)$ em $\mathbb{F}_{q^r}$, são os pontos $(\alpha, \beta) \in \mathbb{F}_{q^r}^2$ tais que $\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$, tais curvas são chamadas de *norma-traço*.

Sabemos, de [5], que $\mathcal{X}_{q,r}$ possui um único ponto $P_\infty = (0:1:0)$ no infinito e outros q^{2r-1} pontos $\mathbb{F}_{q^r}$-racionais. No próximo capítulo veremos qual é o gênero de $\mathcal{X}_{q,r}$.

Observação 4.0.6. Colocando $r = 2$ na equação 4.1 tem-se a equação no plano para a curva hermitiana. Assim, pode-se considerar que as curvas norm-trace são uma generalização das hermitianas.

Assim, sabendo que a estrutura dessas curvas $\mathcal{X}_{q,r}$ é similar a da curva Hermitiana, nos motivamos a estudá-las e construir um algoritmo, semelhante ao caso hermitiano, para se encontrar bases de Gröbner.

Primeiramente vamos nos concentrar em códigos pontuais sobre tal curva, ou seja, códigos $C(D, aP_\infty)$, onde D é a soma dos q^{2r-1} pontos racionais de $\mathcal{X}_{q,r}$ e $a \in \mathbb{N}$.

Consideremos a aplicação η dada por:

$$\eta(x) = \alpha^{q-1}x \quad \text{e} \quad \eta(y) = y \tag{4.2}$$

onde α é um gerador de $\mathbb{F}_{q^r}^\star$.

Como $\alpha^{q^r-1} = 1$, temos que η é um automorfismo de $\mathcal{X}_{q,r}$, de ordem $q^{r-1}+q^{r-2}+\ldots+q+1$, que fixa D e $G = aP_\infty$.

Lema 4.0.7. *Os q^{2r-1} pontos $\mathbb{F}_{q^r}$-racionais de $\mathcal{X}_{q,r}$ estão, sobre a ação de η, decompostos em q^r órbitas, sendo $q^{r-1}(q-1)$ órbitas, denotadas por $O_1, \ldots, O_{q^{r-1}(q-1)}$, de comprimento $\frac{q^r-1}{q-1}$, e q^{r-1} órbitas, $O_{q^{r-1}(q-1)+1}, \ldots, O_{q^r}$, de comprimento 1.*

Cada umas dessas órbitas é a interseção completa de $\mathcal{X}_{q,r}$ com uma curva algébrica de grau 1 dada por:

$$M_i(y) = y - \alpha^{l_i}.$$

Cada $M_i(y)$, $i = 1, 2, \ldots, q^r$, é uma constante não nula quando restrita a cada órbita O_k, com $k \neq i$.

Demonstração:

Sabemos que os pontos racionais da curva $\mathcal{X}_{q,r}$ são da forma $P = (a, b)$ com $a, b \in \mathbb{F}_{q^r}$.

Assim, as órbitas geradas por η são:

Para $1 \leq i \leq q^{r-1}(q-1)$

$$O_i = O(\alpha^{t_i}, \alpha^{l_i}) = \{(\alpha^{t_i}, \alpha^{l_i}), (\alpha^{t_i+(q-1)}, \alpha^{l_i}), \ldots, (\alpha^{t_i+(q^{r-1}+q^{r-2}+\ldots+q)(q-1)}, \alpha^{l_i})\}.$$

Denotaremos $P_{i,0} := (\alpha^{t_i}, \alpha^{l_i})$, onde $t_i, l_i \in \{0, 1, \ldots, q^r - 2\}$.

Para $q^{r-1}(q-1)+1 \leq i \leq q^r-1$, temos $O_i = O(0,\alpha^{l_i})$. E nossa última órbita será $O_{q^r} = O(0,0) = \{(0,0)\}$.

Portanto, $M_i(y) = y - \alpha^{l_i}$ intersecta $\mathcal{X}_{q,r}$ nos pontos em que $y = \alpha^{l_i}$, ou seja, na órbita O_i.

Agora, tomando $P_{k,j} = (\alpha^{t_k+j(q-1)}, \alpha^{l_k}) \in O_k$, com $k \neq i$, temos $M_i(\alpha^{l_k}) = \alpha^{l_k} - \alpha^{l_i} = const \neq 0$, pois $\alpha^{l_k} \neq \alpha^{l_i}$. □

Lema 4.0.8. *Sejam $i \leq q^{r-1}(q-1)$ e $P_{i,j} = \eta^j(P_{i,0}) = (\alpha^{t_i+j(q-1)}, \alpha^{l_i})$ o j-ésimo ponto de O_i. A função*

$$B_{i,j}(x) = \prod_{k=1}^{\frac{q^r-1}{q-1}-1} (x - \alpha^{t_i+(j+k)(q-1)})$$

se anula em cada ponto de O_i, exceto em $P_{i,j}$.

Demonstração:

Primeiramente vejamos que $B_{i,j}(x)$ não se anula em $P_{i,j}$.

De fato,

$$B_{i,j}(\alpha^{t_i+j(q-1)}) = \prod_{k=1}^{\frac{q^r-1}{q-1}-1} (\alpha^{t_i+j(q-1)} - \alpha^{t_i+j(q-1)+k(q-1)}) = \alpha^{t_i+j(q-1)} \cdot \prod_{k=1}^{\frac{q^r-1}{q-1}-1} (1 - \alpha^{k(q-1)}) \neq 0.$$

Agora, consideremos $P_{i,s} = (\alpha^{t_i+s(q-1)}, \alpha^{l_i}) \in O_i$, com $s \neq j$. Assim, temos

$$B_{i,j}(\alpha^{t_i+s(q-1)}) = \prod_{k=1}^{\frac{q^r-1}{q-1}-1} (\alpha^{t_i+s(q-1)} - \alpha^{t_i+(j+k)(q-1)}),$$

Como $s \in \{0,1,2,\ldots,\dfrac{q^r-1}{q-1}-1\}$, vejamos que dado $j \in \{0,1,2,\ldots,\dfrac{q^r-1}{q-1}-1\}$, existe $k \in \{1,2,\ldots,\dfrac{q^r-1}{q-1}-1\}$, tal que $\alpha^{s(q-1)} = \alpha^{(j+k)(q-1)}$. De fato, se $s > j$, então $s = j+l$ e basta tomar $k = l$. Se $s < j$, então $j = s+l$ e, como $\alpha^{q^r-1} = 1$, basta tomar $k = \dfrac{q^r-1}{q-1} - l$. Portanto, $B_{i,j}(\alpha^{t_i+s(q-1)}) = 0$. □

Observação 4.0.9. Em $\mathcal{X}_{q,r}$ temos que x tem pólo de ordem q^{r-1} e y tem pólo de ordem $\dfrac{q^r-1}{q-1}$ em P_∞.

Logo, $M_i(y) \in L(\frac{q^r-1}{q-1}P_\infty)$, para $1 \leq i \leq q^r$, e $B_{i,j} \in ((\dfrac{q^r-1}{q-1}-1)q^{r-1}P_\infty)$, com $1 \leq i \leq q^{r-1}(q-1)$ e $0 \leq j \leq |O_i|-1$.

Com estes fatos conseguimos o seguinte resultado.

Teorema 4.0.10. *Considere o diagrama de raízes do código $C(D, aP_\infty)$ sobre $\mathcal{X}_{q,r}$. Temos que:*

1) Seja $1 \leq i \leq q^{r-1}(q-1)$. Se $a \geq (i-1)(\frac{q^r-1}{q-1})$, então a i-ésima linha do diagrama de raízes não é totalmente preenchida;

2) Seja $1 \leq i \leq q^{r-1}(q-1)$. Se $a \geq (i-1)(\frac{q^r-1}{q-1}) + (\frac{q^r-1}{q-1} - 1)q^{r-1}$, então a i-ésima linha do diagrama é vazia;

3) Para $q^{r-1}(q-1)+1 \leq i \leq q^r$, temos $|O_i| = 1$, logo temos apenas um quadradinho, embaixo do 1, que é a única raiz de $t-1=0$, portanto, se $a \geq (i-1)(\frac{q^r-1}{q-1})$, a linha i será vazia.

Demonstração:

1) Para $1 \leq i \leq q^{r-1}(q-1)$ consideremos $f_i(y) = \prod_{k=1}^{i-1} M_k(y)$. Então, se $a \geq (i-1)(\frac{q^r-1}{q-1})$, temos que $f_i(y) \in L(aP_\infty)$.

Agora, f_i se anula em cada ponto $P \in O_k$, para $k = 1, \ldots, i-1$, e, pelo lema 4.0.7, f_i será uma constante quando evaluada em qualquer $P \in O_i$. Logo, o submódulo $\overline{C}$ associado ao código $C(D, aP_\infty)$ terá um elemento da forma $(0, \ldots, 0, h_i(t), \ldots, h_{q^r}(t))$ onde

$$h_i(t) = \sum_{j=0}^{\frac{q^r-1}{1-1}-1} f_i(P_{i,j})t^j = c. \sum_{j=0}^{\frac{q^r-1}{1-1}-1} t^j,$$

onde c é uma constante não nula.

$h_i(t)$ não possui o 1 como raiz, pois $h_i(1) = 1+1+\ldots+1 = q^{r-1}+q^{r-2}+\ldots+q+1 \neq 0$. Portanto, a i-ésima componente $g_i^{(i)}(t)$ do elemento $g^{(i)}$ da base de Gröbner de $\overline{C}$ também não possui o 1 como raiz. Assim, a i-ésima linha do diagrama não é totalmente preenchida.

2) Agora, suponhamos que $1 \leq i \leq q^{r-1}(q-1)$ e $a \geq (i-1)(\frac{q^r-1}{q-1}) + (\frac{q^r-1}{q-1} - 1)q^{r-1}$. Sabemos que $M_i(y) \in L(\frac{q^r-1}{q-1}P_\infty)$, para $1 \leq i \leq q^r$, e $B_{i,j} \in ((\frac{q^r-1}{q-1} - 1)q^{r-1}P_\infty)$, para $1 \leq i \leq q^{r-1}(q-1)$ e $0 \leq j \leq |O_i| - 1$. Logo,

$$f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).B_{i,0}(x) \in L(aP_\infty).$$

Mas $f_i(P) = 0$ para todo $P \in O_1 \bigcup O_2 \bigcup \ldots \bigcup O_{i-1}$, e mais ainda, $f_i(Q) = 0$ para todo $Q \in O_i \setminus \{P_{i,0}\}$, pois $B_{i,0}$ se anula em todo $Q \in O_i \setminus \{P_{i,0}\}$.

Assim, conseguimos $h_1(t) = h_2(t) = \ldots = h_{i-1}(t) = 0$ e $h_i(t) = f_i(P_{i,0}) + 0 + \ldots + 0 = f_i(P_{i,0}) = c \neq 0$. Então, o módulo $\overline{C}$ possui um elemento da forma $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{q^r}(t))$.

Como $g_i^{(i)}(t)$ divide $h_i(t) = c$, que não possui raiz, temos que $g_i^{(i)}(t)$ também não possui raiz e, portanto, a i-esima linha do diagrama é vazia.

3) No caso em que $q^{r-1}(q-1)+1 \leq i \leq q^r$, temos que $|O_i| = 1$. Logo, os $h_i(t) = f(P_{i,j})$ são constantes. Assim, se $a \geq (i-1)(m+1)$ tomamos $f_i = M_1(y).M_2(y).\ldots.M_{i-1}(y)$, que estará em $L(aP_\infty)$ e, analogamente ao item anterior, teremos $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_{m^2}(t))$ implicando que a linha i será vazia. □

Sejam $I(O_i) = \{f(x,y) \in \mathbb{F}_{q^r}[x,y] \ ; \ f(P_{i,j}) = 0 \ , \ \forall \ P_{i,j} \in O_i\}$ que é um ideal em $\mathbb{F}_{q^r}[x,y]$, e $\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)}$ o anel de funções polinomiais sobre O_i.

Lema 4.0.11. *Para $i \leq q^r(q-1)$ seja V_i o espaço gerado por $\left(\prod_{k=1}^{i-1} M_k(y)\right).x^r$, para $0 \leq r \leq \dfrac{q^r-1}{q-1} - 1$.*

A aplicação restrição de V_i a $\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)}$ é um isomorfismo de $\mathbb{F}_q$-espaços vetoriais.

Demonstração:

Em O_i temos $y - \alpha^{l_i} = 0$, logo $(y-\alpha^{l_i})^{q^{r-1}} = 0$, ou seja, $y^{q^{r-1}} - \alpha^{l_i.q^{r-1}} = 0 \Rightarrow y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y - \alpha^{l_i.q^{r-1}} = +y^{q^{r-2}} + \ldots + y$. Assim, em O_i, temos $x^{\frac{q^r-1}{q-1}} - \alpha^{l_i.q^{r-1}} - \alpha^{l_i.q^{r-2}} - \ldots - \alpha^{l_i} = 0$.

Vejamos que $\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)}$ é isomorfo a $G := \dfrac{\mathbb{F}_{q^r}[x]}{< x^{\frac{q^r-1}{q-1}} - \alpha^{l_i.q^{r-1}} - \alpha^{l_i.q^{r-2}} - \ldots - \alpha^{l_i} >}$

Seja $\psi_i : \mathbb{F}_{q^r}[x,y] \to G$, dada por $\psi_i(f(x,y)) = \overline{f(x, x^{\frac{q^r-1}{q-1}} - \alpha^{l_i.q^{r-1}} - \alpha^{l_i.q^{r-2}} - \ldots - \alpha^{l_i})}$, que é uma aplicação sobrejetiva.

Temos também que $Ker(\psi_i) = I(O_i)$. Portanto, pelo teorema dos isomorfismos, segue que $\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)} \sim G$.

Agora, seja $\varphi_i : V_i \to \dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)}$ a aplicação restrição, que é linear e sobrejetiva. Sabendo que $\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)} \sim G$, e que $\{1, x, x^2, \ldots, x^{\frac{q^r-1}{q-1}-1}\}$ é uma base para G, temos que $dim\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)} = \dfrac{q^r-1}{q-1}$.

Por outro lado, $dim V_i = \dfrac{q^r-1}{q-1}$, já que $\{\prod_{k=1}^{i-1} M_k(y), (\prod_{k=1}^{i-1} M_k(y)).x, \ldots, (\prod_{k=1}^{i-1} M_k(y)).x^{\frac{q^r-1}{q-1}-1}\}$ é uma base para V_i.

Logo, V_i e $\dfrac{\mathbb{F}_{q^r}[x,y]}{I(O_i)}$ têm a mesma dimensão, e segue que a aplicação restrição é um isomorfismo. □

Corolário 4.0.12. *Para toda coleção de valores c_j, com $j = 0, 1, 2, \ldots, \dfrac{q^r-1}{q-1} - 1$, existe uma única função $f(x,y) \in V_i$ tal que $f(P_{i,j}) = c_j$, para todo j, e que é identicamente nula em $O_1, \ldots, O_{i-1}$.*

Demonstração:

Usando forma de Lagrange para interpolação, encontramos um $P_{q,r}(x) \in G$, de grau no máximo $\dfrac{q^r-1}{q-1} - 1$, que resolve o problema de interpolação em O_i. Logo a função $f(x,y) = \varphi^{-1}(P_{q,r}(x)) \in V_i$ é a função procurada. □

Com tais resultados obtemos o teorema a seguir.

Teorema 4.0.13. *Sejam $1 \leq i \leq q^{r-1}(q-1)$ e*

$$(i-1)(\frac{q^r-1}{q-1}) \leq a \leq (i-1)(\frac{q^r-1}{q-1}) + (\frac{q^r-1}{q-1} - 1)q^{r-1}.$$

Então a i-ésima linha do diagrama de raízes não é nem vazia, nem totalmente preenchida.

Se M é o conjunto das raïzes marcadas na i-ésima linha do diagrama, o complementar de M é o conjunto

$$M^c = \{\alpha^{-k} \in \mathbb{F}_{q^r}^* \ ; k = r(q-1) \text{ com } 0 \leq r \leq \frac{q^r-1}{q-1} - 1 \text{ e } rq^{r-1} + (i-1)(\frac{q^r-1}{q-1}) \leq a\}.$$

Demonstração:

Consideremos, para $1 \leq i \leq q^{r-1}(q-1)$, as funções $f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).x^r.y^s$. Se $rq^{r-1} + s(\frac{q^r-1}{q-1}) + (i-1)(\frac{q^r-1}{q-1}) \leq a$, então tais funções estão em $L(aP_\infty)$.

O fato de $M_i(y) = y - \alpha^{l_i}$, nos permite excluir o termo y^s de f_i, ou seja, tomar $s = 0$, pois $y = M_i(y) - c$. E, como $x^{\frac{q^r-1}{q-1}} = y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y$, podemos tomar $0 \leq r \leq \frac{q^r-1}{q-1} - 1$. Logo, $f_i = \left(\prod_{k=1}^{i-1} M_k(y)\right).x^r$, com $0 \leq r \leq \frac{q^r-1}{q-1} - 1$, está em $L(aP_\infty)$ se $rq^{r-1} + (i-1)(\frac{q^r-1}{q-1}) \leq a$.

Seja $h_i(t) = \sum_{j=0}^{|O_i|-1} f_i(P_{i,j})t^j$, para $1 \leq i \leq q^{r-1}(q-1)$.

Como $M_k(y)$ é zero para os elementos de O_k, temos que $h_j(t) = 0$, para $1 \leq j \leq i-1$.

Sabemos, pelo lema 4.0.7, que $M_j(y)$ são constantes não nulas em O_k, para $k \neq j$, e que os elementos de O_i são do tipo $P_{i,j} = \eta^j(P_{i,0}) = (\alpha^{t_i+j(q-1)}, \alpha^{l_i}) = (\alpha^{t_i}\alpha^{j(q-1)}, \alpha^{l_i})$.

Assim, podemos escrever $f(P_{i,j}) = c.\alpha^{rt_i+rj(q-1)}$, onde c é uma constante não nula. Desconsiderando tais constantes, temos:

$$h_i(t) = \sum_{j=0}^{\frac{q^r-1}{q-1}-1} (\alpha^{r(q-1)})^j,$$

e $(0, \ldots, 0, h_i(t), \ldots, h_{q^r}(t)) \in \overline{C}$.

Agora, $t = \alpha^{-(r(q-1))} \in \mathbb{F}_{q^r}^*$ não é uma raiz de $h_i(t)$, pois $h_i(\alpha^{-(r(q-1))}) = 1+1+\ldots+1 = \dfrac{q^r-1}{q-1} = q^{r-1}+q^{r-2}+\ldots+q+1 \neq 0$.

Portanto, as raízes de $h_i(t)$ são diferentes de $\alpha^{-(r(q-1))}$, e segue que $g_i^{(i)}(t)$ não tem $\alpha^{-(r(q-1))}$ como raiz.

Assim, concluímos que $A = \{\alpha^{-k} \in \mathbb{F}_{q^r}^* \ ; \ k = r(q-1) \text{ com } 0 \leq r \leq \frac{q^r-1}{q-1} - 1 \text{ e } rq^{r-1} + (i-1)(\frac{q^r-1}{q-1}) \leq a\} \subseteq M^c$.

Para vermos que $M^c \subseteq A$ basta utilizar o corolário anterior, do mesmo modo visto no caso hermitiano. □

Teorema 4.0.14. *Sejam $\{\alpha^{s_1}, \alpha^{s_2}, \ldots, \alpha^{s_l}\}$ o conjunto de raízes que aparecem na i-ésima linha do diagrama do código $C(D, aP_\infty)$ sobre $\mathcal{X}_{q,r}$.*

Seja $P(t) = \sum_{j=0}^{l} c_j t^j$ o único polinômio mônico de grau l com tais raízes. Então $f(x,y) = \prod_{k=1}^{i-1} M_k(y) . \sum_{j=0}^{|O_i|-1} c_j \dfrac{B_{i,j}(x)}{B_{i,j}(P_{i,j})}$ é uma função em $L(aP_\infty)$ que fornece um elemento $g^{(i)}$ com $i-1$ componentes líderes iguais a zero e a i-ésima componente $g_i^{(i)}(t)$ igual a $P(t)$.

Demonstração: Análoga aos casos anteriores (teorema 2.15).

E, assim, se constrói um algoritmo análogo ao caso hermitiano, que será o seguinte.

Entrada: $a, \{P_{i,j},$ os q^{2r-1} pontos racionais de $\mathcal{X}_{q^r} distintos de P_\infty\}$

Saída: um base de Grobner nao reduzida $\mathcal{G} = \{\mathbf{g}^{(1)}, \mathbf{g}^{(2)}, \ldots, \mathbf{g}^{(q^r)}\}$

Início: $\mathcal{G} := \{\}$ e **RootDiagram** := **GetRootDiagram**(a)

Fazer, para i de 1 a q^r :

•**Se** $|RootDiagram[i]| < |O_i|$, então

Valores= $\{c_j\}$:=**Get Value List**(RootDiagram[i])

Fazer $\circ$ Para k de 1 a $i-1$: $g_k^{(i)} := 0$

Fazer $\circ$ Para k de i a q^r:

$g_k^{(i)} := 0$

para j de 0 a $|O_i| - 1$ fazer,

$$g_k^{(i)} := g_k^{(i)} + \textbf{EvaluateCombination}(valores, P_{i,j}) t^j \mathbf{e}_k$$

• **Caso contrário** $\mathbf{g}^{(i)} := (t^{|O_i|} - 1)\mathbf{e}_i$

$\mathcal{G} := \mathcal{G} \bigcup \{\mathbf{g}^{(i)}\}$

CAPÍTULO 5

Semigrupo de Weierstrass $H(P_{0,0}, P_\infty)$ da curva Norma-Traço e resultados para códigos de Goppa geométricos sobre essa curva

Seja $\mathbb{F}_q$ um corpo finito. Denotaremos por $F/\mathbb{F}_q$, ou simplesmente F, um corpo de funções algébricas sobre $\mathbb{F}_q$.

$\mathcal{X}$ denotará uma curva suave, projetiva e irredultível sobre $\mathbb{F}_q$, e $\mathbb{F}_q(\mathcal{X})$ será o corpo de funções racionais de $\mathcal{X}$ definidas sobre $\mathbb{F}_q$.

Nos resultados e definições que veremos a seguir usaremos F ou $\mathcal{X}$, uma vez que ambos são equivalentes.

Vamos relembrar a seguinte definição.

Definição 5.0.15. Chama-se de *lugar racional* (ponto racional) um lugar de $F/\mathbb{F}_q$ que tem grau um. O conjunto de todos os lugares racionais de $F/\mathbb{F}_q$ será denotado por $\mathbb{P}_F$.

5.1 Semigrupo de Weierstrass

Definição 5.1.1. Seja $P \in \mathbb{P}_F$. Um inteiro $n > 0$ é chamado de **nongap** (não-lacuna ou ordem do pólo) de P se existe $f \in F$ com $(f)_\infty = nP$. Caso contrário n é dito número **gap** (ou lacuna) de P.

Observamos que $(f)_\infty$ denota o divisor de pólos de f.

Para uma curva $\mathcal{X}$ suave, projetiva e irredutível de gênero $g > 1$ sobre um corpo finito $\mathbb{F}_q$ temos a seguinte definição:

Definição 5.1.2. Se P é um ponto $\mathbb{F}_q$-racional de $\mathcal{X}$, definimos o semigrupo de Weierstrass do ponto P por

$$H(P) = \{n \in \mathbb{N}_0 \ ; \text{ existe } f \in \mathbb{F}(\mathcal{X}) \text{ com } (f)_\infty = nP\}$$

Assim, temos que $H(P)$ é o conjunto de nongaps (não-lacunas) de P. O conjunto finito $\mathbb{N} \setminus H(P)$ formado pelos gaps (lacunas) de P será denotado por $Gaps(P)$, ou simplesmente $G(P)$.

Definição 5.1.3. O *condutor* de $H(P)$ é o menor inteiro $c \in H(P)$ tal que $c + n \in H(P)$, para todo $n \in \mathbb{N}_0$.

Se $c = 2g$ dizemos que o semigrupo é *simétrico*.

O teorema a seguir mostra uma relação entre lugar racional e gênero.

Teorema 5.1.4. ***(Teorema das lacunas de Weierstrass ou Weierstrass gap)*** *Suponha que $F/\mathbb{F}_q$ tem gênero $g \geq 1$ e que P é um lugar racional. Então existem exatamente g gaps (lacunas) $\alpha_1 < \ldots < \alpha_g$ de P, e temos*

$$\alpha_1 = 1 \quad e \quad \alpha_g \leq 2g - 1.$$

No caso de 2 pontos racionais distintos temos a seguinte definição.

Definição 5.1.5. Se P_1 e P_2 são dois pontos $\mathbb{F}_q$-racionais distintos de $\mathcal{X}$, o semigrupo de Weierstrass $H(P_1, P_2)$ do par (P_1, P_2) é definido por

$$H(P_1, P_2) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 \ ; \ \exists f \in \mathbb{F}_q(\mathcal{X}) \text{ com } (f)_\infty = \alpha_1 P_1 + \alpha_2 P_2\}.$$

O conjunto de gaps do par (P_1, P_2) é dado por

$$G(P_1, P_2) = \mathbb{N}_0^2 \setminus H(P_1, P_2),$$

e também é um conjunto finito.

Agora, vejamos alguns resultados, vistos em [12], relacionados a $H(P_1, P_2)$ e que serão utilizados quando formos construir $H(P_{0,0}, P_\infty)$.

Definição 5.1.6. Dados $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in \mathbb{N}_0^2$, definimos o *lub* (least upper bound) de α e β por

$$lub\{\alpha, \beta\} = (max\{\alpha_1, \beta_1\}, max\{\alpha_2, \beta_2\}) \in N_0^2.$$

Lema 5.1.7. *([11]) Se $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2) \in H(P_1, P_2)$, então $lub\{\alpha, \beta\} \in H(P_1, P_2)$.*

Demonstração: Podemos assumir que $\alpha_1 > \alpha_2$ e $\beta_1 < \beta_2$. Sejam f e g funções racionais tais que $(f)_\infty = \alpha_1 P_1 + \alpha_2 P_2$ e $(g)_\infty = \beta_1 P_1 + \beta_2 P_2$. Logo, $(f+g)_\infty = \alpha_1 P_1 + \beta_2 P_2$, e assim, $(\alpha_1, \beta_2) \in H(P_1, P_2)$. □

Lema 5.1.8. *([11]) Para $\alpha \in G(P_1)$, definimos $\beta_\alpha := min\{\beta \in \mathbb{N}_0 \ ; (\alpha, \beta) \in H(P_1, P_2)\}$. Então, $(\gamma, \beta_\alpha) \notin H(P_1, P_2)$, para todo $\gamma < \alpha$. Ou seja, $\alpha = min\{\gamma | (\gamma, \beta_\alpha) \in H(P_1, P_2)\}$.*

Utilizando este lema conseguimos.

Lema 5.1.9. *([11]) Seja β_α como no lema anterior. Então, $\{\beta_\alpha \ ; \alpha \in G(P_1)\} = G(P_2)$.*

Demonstração: O lema anterior implica que $\beta_\alpha \notin H(P_2)$, e que $\beta_\alpha \neq \beta_\gamma$, se $\alpha \neq \gamma$. Assim, o conjunto $\{\beta_\alpha \ ; \alpha \in G(P_1)\}$ está contido em $G(P_2)$ e sua cardinalidade é extamente g. Portanto, devemos ter $\{\beta_\alpha \ ; \alpha \in G(P_1)\} = G(P_2)$. □

Observação 5.1.10. Sejam $\alpha_1 < \alpha_2 < \ldots < \alpha_g$ a sequência de gaps de P_1, e $\alpha'_1 < \alpha'_2 < \ldots < \alpha'_g$ a sequência de gaps de P_2. Sabemos, pelo lema anterior, que existe uma aplicação bijetiva entre $G(P_1)$ e $G(P_2)$, logo temos que $\beta_{\alpha_i} = \alpha'_{\sigma(i)}$, onde σ é uma permutação do conjunto $\mathbb{N}_{\leq g} := \{1, 2, \ldots, g\}$. Tal permutação é denotada por $\sigma(P_1, P_2)$, e o gráfico da aplicação bijetiva será

$$\Gamma(P_1, P_2) = \{(\alpha_i, \alpha'_{\sigma(i)}) \ ; i = 1, 2, \ldots, g\} = \{(\alpha_i, \beta_{\alpha_i}) \ ; i = 1, 2, \ldots, g \text{ e } \alpha_i \in G(P_1)\}.$$

Um primeiro resultado, visto em [11], sobre $\Gamma(P_1, P_2)$ é o seguinte.

Lema 5.1.11. *Seja Γ' um subconjunto de $(G(P_1) \times G(P_2)) \cap H(P_1, P_2)$. Se existe uma permutação τ de $\mathbb{N}_{\leq g} := \{1, \ldots, g\}$ tal que $\Gamma' = \{(\alpha_i, \alpha'_{\tau(i)})$; $i = 1, \ldots, g\}$, então $\Gamma' = \Gamma(P_1, P_2)$.*

O lema a seguir, visto em [12] e [17], nos diz como $\Gamma(P_1, P_2)$, $H(P_1)$ e $H(P_2)$ geram o semigrupo $H(P_1, P_2)$.

Lema 5.1.12. *Sejam P_1 e P_2 lugares racionais distintos de F (corpo de funções algébricas sobre um corpo finito). O semigrupo de Weierstrass do par $(P_1, P_2) \in \mathbb{P}_F^2$ é dado por*

$$H(P_1, P_2) = \{lub\{\gamma_1, \gamma_2\} \text{ ; } \gamma_1, \gamma_2 \in S\},$$

onde $S := \Gamma(P_1, P_2) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2))$.

Em [9] vimos os seguintes resultados.

Proposição 5.1.13. *Seja g o número de gaps de um certo $H(P)$. Então $c \leq 2g$. E $c = 2g$ se, e somente se, para qualquer inteiro não-negativo s, se s é um gap, então $c - 1 - s$ é um não-gap.*

Proposição 5.1.14. *Sejam $a, b \in \mathbb{N}$ tais que $mdc(a, b) = 1$. O semigrupo gerado por a e b é simétrico, tem $ab - a - b$ como maior gap, $(a-1)(b-1)$ como condutor e o número de gaps é igual a $\dfrac{(a-1)(b-1)}{2}$.*

Demonstração:

Como $mdc(a, b) = 1$, todo inteiro m possui uma única representação $m = xb + ya$, onde x e y são inteiros tais que $0 \leq y < b$. Assim, todo gap m tem uma única representação $m = xb + ya$, onde $0 \leq y < b$ e $x < 0$, e todo não-gap m tem uma única representação $m = xb + ya$, onde $0 \leq y < b$ e $x \geq 0$.

Seja c o condutor do semigrupo $\Lambda\langle a, b\rangle$ (gerado por a e b). Temos que $c-1$ é o maior gap. Os números $ya \in \Lambda$, $y = 0, 1, \ldots, b-1$, formam um conjunto completo de representantes

do coset $\{0, 1, \ldots, b-1\}$ módulo b, e $ya - b$ é o maior elemento no coset de ya sem uma representação com coeficientes inteiros não-negativos.

Logo, $(b-1)a - b$ é o maior gap, que é igual a $c-1$, e segue que $c = (a-1)(b-1)$.

Para vermos que $\langle a, b\rangle$ é simétrico, assumimos que s e t são gaps com $s+t = c-1$. Como s e t podem ser escritos como

$$s = x_1 b + y_1 a, \quad t = x_2 b + y_2 a, \quad 0 \leq y_1, y_2 < b \text{ e } x_1, x_2 < 0,$$

conseguimos $c - 1 = ab - a - b = (x_1 + x_2)b + (y_1 + y_2)a$.

Assim, $(-x_1 - x_2 - 1)b = (y_1 + y_2 - b + 1)a$, onde $0 \leq y_1 + y_2 \leq 2b - 2$ e $x_1 + x_2 \leq -2$. Logo, $(-x_1 - x_2 - 1) > 0$ e $(y_1 + y_2 - b + 1)a < ab$, contradição, já que $mdc(a, b) = 1$. Portanto, Λ é simétrico e, pela proposição anterior, $c = 2g$, onde g é o número de gaps. E segue que $g = \dfrac{(a-1)(b-1)}{2}$. □

Observação 5.1.15. Sendo $P_{a,b}$ um ponto $\mathbb{F}_{q^r}$-racional da curva norma-traço $\mathcal{X}_{q,r}$ (definida no capítulo anterior) e um zero comum de $x - a$ e $y - b$, temos os seguintes divisores das funções x e y.

$(x) = P_{0,0} + \sum_{\alpha} P_{0,\alpha} - q^{r-1} P_\infty$, onde os α´s são as raízes de $t^{q^{r-2}} + t^{q^{r-3}} + \ldots + t + 1 = 0$;

$(y) = \dfrac{(q^r - 1)}{q-1} P_{0,0} - \dfrac{(q^r - 1)}{q-1} P_\infty$.

Sabemos que $mdc(q^{r-1}, \dfrac{(q^r-1)}{q-1}) = 1$. Assim, utilizando o teorema de Weierstrass gaps, a proposição 5.1.14 e as funções x e y temos que $H(P_\infty) = \langle q^{r-1}, \dfrac{(q^r-1)}{q-1}\rangle$ e que o gênero de $\mathcal{X}_{q,r}$ é $g = \dfrac{(q^{r-1} - 1)(\frac{(q^r-1)}{q-1}) - 1)}{2}$.

5.2 O semigrupo de Weierstrass $H(P_{0,0}, P_\infty)$ para $q = 2$

Sejam P_∞ o ponto no infinito e $P_{0,0}$ o ponto $\mathbb{F}_{q^r}$-racional de $\mathcal{X}_{q,r}$ que é um zero comum de x e y.

De agora até o final desta seção vamos fixar $q = 2$ e supor $r \geq 3$, já que para $r = 2$ temos a curva curva Hermitiana que possui $H(P_{0,0}, P_\infty)$ conhecido.

Da observação 5.1.15 temos, para $q = 2$, que $H(P_\infty) = \langle 2^{r-1}, 2^r - 1\rangle$, ou seja,

$$H(P_\infty) = \{0, 2^{r-1}, 2^r - 1, 2.2^{r-1}, 2^{r-1} + 2^r - 1, 2.(2^r - 1), \ldots\},$$

que é obtido pelas funções $\{0, x, y, x^2, xy, y^2, \ldots\}$.

Assim, sendo $a = 2^{r-1}$, o conjunto de gaps $G(P_\infty)$ será dado por

$$\begin{array}{cccccc}
1 & 2 & 3 & \ldots & a-2 & a-1 \\
a+1 & a+2 & a+3 & \ldots & a+(a-2) & \\
2a+1 & 2a+2 & 2a+3 & \ldots & 2a+(a-2) & \\
3a+1 & 3a+2 & 3a+3 & & & \\
4a+1 & 4a+2 & 4a+3 & & & \\
\vdots & \vdots & \vdots & & & \\
(2(a-4)+1)a+1 & (2(a-4)+1)a+2 & & & & \\
2(a-3)a+1 & 2(a-3)a+2 & & & & \\
(2(a-3)a+1)a+1 & & & & & \\
2(a-2)a+1 & & & & &
\end{array}$$

Logo
$|G(P_\infty)| = (a-1) + 2.(a-2) + 2.(a-3) + \ldots + 2.(a-(2^{r-1}-1))$
$= (a-1) + 2.(a(a-2) - (2+3+\ldots+a-1))$
$= (2^{r-1}-1) + 2.(2^{2r-2} - 2^r - \dfrac{(2^{r-1}-2)(2^{r-1}+1)}{2})$
$= (2^{r-1}-1)^2 = g$, estando de acordo com o teorema 5.1.4, já que P_∞ é racional.

Tal conjunto de gaps pode ser visto como a seguinte união disjunta:

$$G(P_\infty) = \{2(i-j)a + j \ ; \ 1 \leq j \leq i \leq a-1\} \sqcup \{(2(i-j)+1)a + j \ ; \ 1 \leq j \leq i \leq a-2\},$$

onde $\{2(i-j)a + j \ ; \ 1 \leq j \leq i \leq a-1\}$ é dado por

$$\begin{array}{cccccc}
1 & 2 & \ldots & \ldots & a-2 & a-1 \\
2a+1 & 2a+2 & \ldots & \ldots & 2a+(a-2) & \\
4a+1 & 4a+2 & \ldots & 4a+(a-3) & & \\
\vdots & & & & & \\
2(a-3)a+1 & 2(a-3)a+2 & & & & \\
2(a-2)a+1 & & & & &
\end{array}$$

e $\{(2(i-j)+1)a+j \ ; \ 1 \leq j \leq i \leq a-2\}$ por

$$\begin{array}{ccccccc} a+1 & & a+2 & \ldots & \ldots & & a+(a-2) \\ 3a+1 & & 3a+2 & \ldots & 3a+(a-3) & & \\ \vdots & & & & & & \\ (2(a-4)+1)a+1 & & (2(a-4)+1)a+2 & & & & \\ (2(a-3)+1)a+1 & & & & & & \end{array}$$

Para simplificar, seja $\gamma = 2(a-1)$, lembrando que $a = 2^{r-1}$. Vejamos que

$$H(P_{0,0}) = \langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}.\gamma - (\frac{\gamma}{2}-1) \rangle.$$

Para isso basta ver que $\langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}.\gamma - (\frac{\gamma}{2}-1) \rangle$ possui g gaps.

Observamos que o conjunto $\{\gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}.\gamma - (\frac{\gamma}{2}-1)\}$ é obtido pelas funções $\left\{ \frac{x}{y}, \frac{1}{y}, \frac{x^3}{y^2}, \frac{x^5}{y^3}, \ldots, \frac{x^{\gamma-1}}{y^{\frac{\gamma}{2}}} \right\}$.

O conjunto $G(P_{0,0})$ de gaps, em $P_{0,0}$, de $\langle \gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}.\gamma - (\frac{\gamma}{2}-1) \rangle$ será

$$\begin{array}{ccccccc} 1 & 2 & 3 & \ldots & \ldots & \ldots & \gamma-1 \\ \gamma+2 & \gamma+3 & \gamma+4 & \ldots & \ldots & \gamma+(\gamma-2) & \\ 2\gamma+3 & 2\gamma+4 & 2\gamma+5 & \ldots & 2\gamma+(\gamma-3) & & \\ \vdots & & & & & & \\ (\frac{\gamma}{2}-2)\gamma+(\frac{\gamma}{2}-1) & (\frac{\gamma}{2}-2)\gamma+\frac{\gamma}{2} & (\frac{\gamma}{2}-2)\gamma+(\frac{\gamma}{2}+1) & & & & \\ (\frac{\gamma}{2}-1)\gamma+\frac{\gamma}{2} & & & & & & \end{array}$$

Assim, $|G(P_{0,0})| = (\gamma-1)+(\gamma-3)+(\gamma-5)+\ldots+3+1 = \frac{\gamma.(\frac{\gamma}{2})}{2} = (a-1)^2 = g$.
Logo, $H(P_{0,0})$ é de fato gerado por $\{\gamma, \gamma+1, 2\gamma-1, 3\gamma-2, \ldots, \frac{\gamma}{2}.\gamma - (\frac{\gamma}{2}-1)\}$.

Agora, sabendo como são os conjuntos $G(P_\infty)$ e $G(P_{0,0})$ para $q=2$, e utilizando resultados da seção 5.1 conseguimos o seguinte resultado.

Teorema 5.2.1. *Para o par P_∞ e $P_{0,0}$ de pontos de Weierstrass da curva Norma-Traço $\mathcal{X}_{2,r}$ temos*

$$\beta_{2(i-j)a+j} = (2a-1)j - 2i \ ; \ 1 \leq j \leq i \leq a-1$$

e

$$\beta_{(2(i-j)+1)a+j} = (2a-1) - (2i+1) \ ; \ 1 \leq j \leq i \leq a-2.$$

Demonstração:

1º caso) Consideremos $1 \leq j \leq i \leq a-1$.

Para todo par (i, j), temos, pelo que vimos dos conjuntos $G(P_\infty)$ e $G(P_{0,0})$, que $2(i-j)a + j \in G(P_\infty)$ e $j(2a-1) - 2i = (j-1)\lambda + (\lambda - 2i + j) \in G(P_{0,0})$, lembrando que $\lambda = 2(a-1)$.

I) Primeiramente, vejamos que $2(i-j)a + j \neq 2(i'-j')a + j'$ se $i \neq i'$ ou $j \neq j'$.

De fato, suponhamos que existam $(i, j) \neq (i', j')$ tais que $2(i-j)a + j = 2(i'-j')a + j'$.

Se $i - j = i' - j'$, então $2(i-j)a + j = 2(i'-j')a + j' \Rightarrow j = j'$ e, como $i - j = i' - j'$, teríamos $i = i'$, absurdo, pois supomos $(i, j) \neq (i', j')$. Logo, $i - j \neq i' - j'$.

Sem perda de generalidade, vamos assumir que $i - j > i' - j'$. Então $i - j = i' - j' + k$, para algum $0 < k \in \mathbb{N}$. Assim, teríamos $2(i'-j'+k)a + j = 2(i'-j')a + j' \Rightarrow j' = 2ak + j$, absurdo, pois, por hipótese $1 \leq j, j' \leq a-1$.

Portanto, $2(i-j)a + j \neq 2(i'-j')a + j'$ se $(i, j) \neq (i', j')$.

II) Agora, vejamos que $j(2a-1) - 2i \neq j'(2a-1) - 2i'$ se $(i, j) \neq (i', j')$.

Novamente vamos supor que existam $(i, j) \neq (i', j')$ tais que $j(2a-1)-2i = j'(2a-1)-2i'$.

Como $j(2a-1) - 2i = j'(2a-1) - 2i'$, temos que se $i = i'$, então $j = j'$, e se $j = j'$, então $i = i'$. Logo $i \neq i'$ e $j \neq j'$. Suponhamos que $i > i'$, ou seja, $i = i' + k$ com $k \in \mathbb{N}$. Como $1 \leq i, i' \leq a-1$, então $1 \leq k < a-1$, e temos $j(2a-1) = j'(2a-1) + 2k$ e, assim, $(j-j')(2a-1) = 2k < 2a-1$, absurdo, pois $j \neq j'$.

Então, $j(2a-1) - 2i \neq j'(2a-1) - 2i'$ se $i \neq i'$ ou $j \neq j'$.

Ordenando $2(i-j)a + j$ e $j(2a-1) - 2i$ de forma crescente obtemos as sequências $\alpha_1 < \alpha_2 < \ldots < \alpha_g$, e $\alpha'_1 < \alpha'_2 < \ldots < \alpha'_g$, de gaps de P_∞ e $P_{0,0}$, respectivamente, onde, para cada $l, l' = 1, \ldots, g$, $\alpha_l = 2(i-j)a+j$, para algum par (i, j), e $\alpha'_{l'} = j'(2a-1)-2i'$, para algum par (i', j') satisfazendo $1 \leq j' \leq i' \leq a-1$. Como exemplo, para $(i, j) = (i', j') = (1, 1)$, conseguimos $\alpha_1 = 1$ e $\alpha'_{2(a-1)} = 2a - 3$.

Agora, $\left(\dfrac{x^{2i}}{y^j}\right)_\infty = (2(i-j)a + j)P_\infty + (j(2a-1) - 2i)P_{0,0}$.

Portanto, $(2(i-j)a + j, j(2a-1) - 2i) \in H(P_\infty, P_{0,0})$.

Assim, se $\alpha_l = 2(i-j)a+j$ e $\alpha'_{l'} = j(2a-1)-2i$ temos que $(\alpha_l, \alpha'_{l'}) \in (G(P_\infty) \times G(P_{0,0})) \cap H(P_\infty, P_{0,0})$. Seja τ a permutação de $\mathbb{N}_{\leq g}$ tal que $\tau(l) = l'$. Portanto, pelo lema 5.1.11, temos que $\Gamma' = \{\alpha_l, \alpha'_{\tau(l)} \; ; \; l = 1, \ldots, g\} = \Gamma(P_\infty, P_{0,0})$, e segue que, para $1 \leq j \leq i \leq a-1$, $\beta_{2(i-j)a+j} = (2a-1)j - 2i$.

2º caso) Utilizando que $\left(\frac{x^{2i+1}}{y^j}\right)_\infty = ((2(i-j)+1)a+j)P_\infty + (j(2a-1)-(2i+1))P_{0,0}$, mostra-se, analogamente ao primeiro caso, que $\beta_{(2(i-j)+1)a+j} = (2a-1)-(2i+1)$, para $1 \leq j \leq i \leq a-2$. □

Uma forma de vermos como os gaps de P_∞ e de $P_{0,0}$ são associados é a seguinte: sejam $\alpha_{m,n}$ e $\beta_{m,n}$ elementos da linha m e coluna n de $G(P_\infty)$ e $G(P_{0,0})$, respectivamente. Atribuindo valores a i e a j conseguimos todos os pares $(\alpha_{m,n}, \beta_{m,n})$ desejados, ou seja, associamos todos os gaps de P_∞ com os de $P_{0,0}$.

Como exemplo podemos tomar $i = j = 1, 2, \ldots, a-1$. Dessa forma conseguimos todos os pares $(\alpha_{1,j}, \beta_{1,j})$ em $H(P_\infty, P_{0,0})$, onde $\alpha_{1,j}$ são todos os elementos da linha 1 de $G(P_\infty)$, e $\beta_{1,j}$ são todos os elementos da linha 1 de $G(P_{0,0})$.

Observação 5.2.2. Observamos que se $P_{a,b} \neq P_{0,0}$ é um ponto $\mathbb{F}_q$-racional de $\mathcal{X}_{q,r}$ e que se existem funções racionais $\overline{x}$ e $\overline{y}$ tais que

$(\overline{x}) = P_{a,b} + \sum_\alpha P_{a,\alpha} - q^{r-1}P_\infty$, onde os α´s são as raízes de $t^{q^{r-1}} + t^{q^{r-2}} + \ldots + t = a$ distintas de b;

$(\overline{y}) = \frac{(q^r-1)}{q-1}P_{a,b} - \frac{(q^r-1)}{q-1}P_\infty$.

Teremos que $H(P_{a,b}) = H(P_{0,0})$ e, assim, conseguiremos os mesmos resultados para o par $(P_{a,b}, P_\infty)$.

Exemplo 5.2.3. Vejamos um exemplo de como encontrar tais $(\alpha_{m,n}, \beta_{m,n})$ em $H(P_\infty, P_{0,0})$.

Sejam $q = 2$ e $r = 3$.

Temos que $H(P_\infty) = \langle 4, 7\rangle$ e $H(P_{0,0}) = \langle 6, 7, 11, 16\rangle$. Assim, $G(P_\infty)$ é dado por

1	2	3
5	6	
9	10	
13		
17		

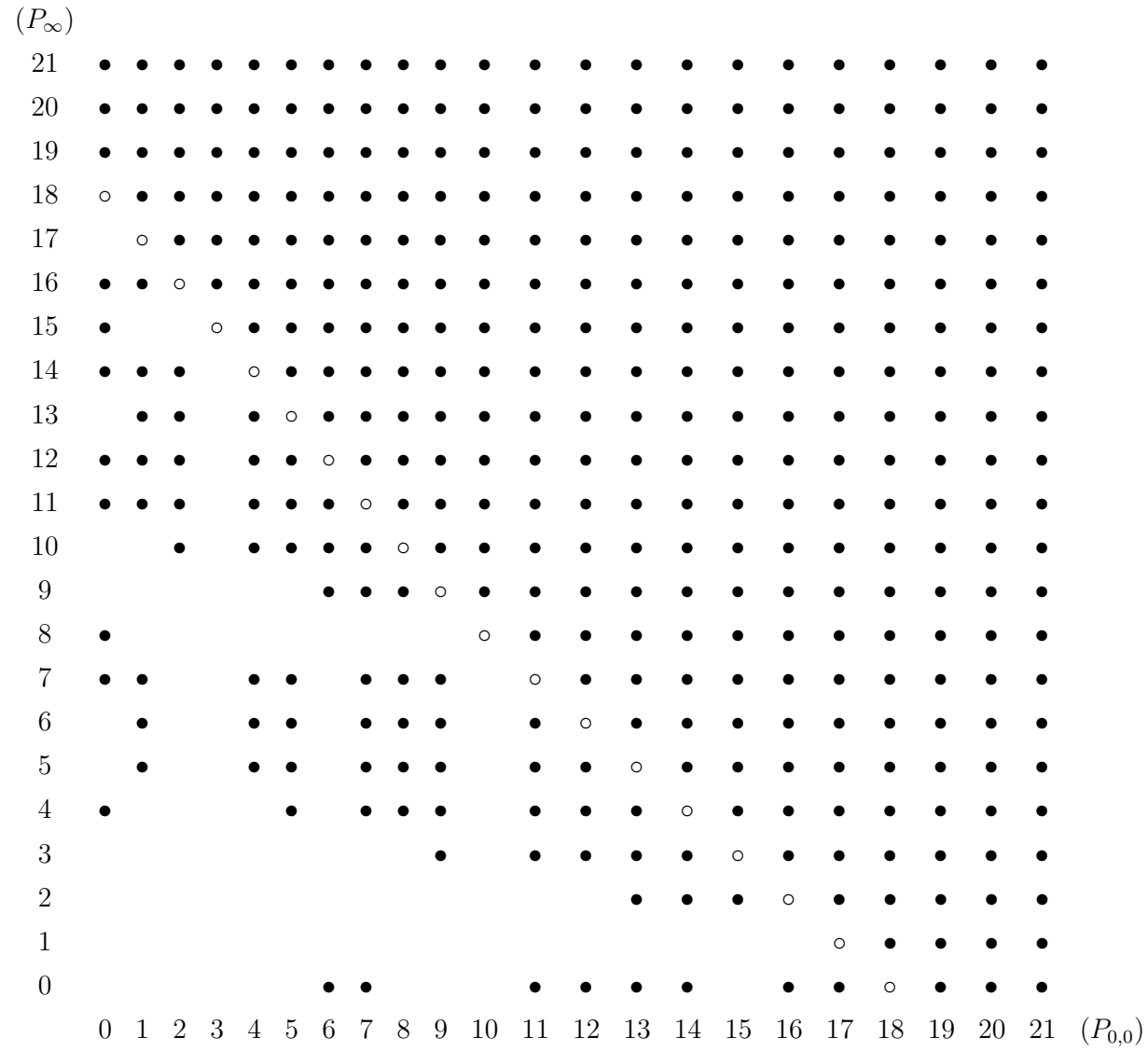
e $G(P_{0,0})$ será

$$\begin{array}{lll} 5 & 10 & 15 \\ 4 & 9 & \\ 3 & 8 & \\ 2 & & \\ 1 & & \end{array}$$

Logo, pelo teorema 5.2.1, temos que

$$\{(5,1),(10,2),(15,3),(4,5),(9,6),(3,9),(8,10),(2,13),(1,17)\} \subseteq H(P_{0,0}, P_\infty).$$

Utilizando lema 5.1.7 encontramos o seguinte diagrama para o conjunto $H(P_\infty, P_{0,0})$.



Observamos que os pontos denotados por $\circ$ pertencem a $H(P_\infty, P_{0,0})$ e estão sobre a reta $x + y = 2g$ do diagrama.

5.3 O semigrupo de Weierstrass $H(P_{0,0}, P_\infty)$ para q qualquer

Sejam q uma potência de um número primo qualquer, $r \geq 3$ e $X_{q,r}$ a curva Norma-Traço. Vejamos como encontrar $H(P_{0,0}, P_\infty)$.

Lembremos que

$(x) = P_{0,0} + \sum_{\alpha} P_{0,\alpha} - q^{r-1}P_\infty$, onde os α´s são as raízes de $t^{q^{r-2}} + t^{q^{r-3}} + \ldots + t + 1 = 0$.

$$(y) = \frac{(q^r-1)}{q-1}P_{0,0} - \frac{(q^r-1)}{q-1}P_\infty.$$

E que $H(P_\infty) = \left\langle q^{r-1}, \frac{q^r-1}{q-1} \right\rangle$.

Sendo $a = \frac{q^r-1}{q-1} - 1$ temos

$\left(\frac{x}{y}\right)_\infty = aP_{0,0}$

$\left(\frac{1}{y}\right)_\infty = (a+1)P_{0,0}$

e, para $0 \leq \lambda \leq q^{r-2} + q^{r-3} + \ldots + q - 1$

$$\left(\frac{x^{\lambda q+q+1}}{y^{\lambda(q-1)+q}}\right)_\infty = (((\lambda+1)q - \lambda)a - (\lambda+1))P_{0,0}.$$

Assim, utilizando as funções $\frac{x}{y}, \frac{1}{y}$ e $\frac{x^{\lambda q+q+1}}{y^{\lambda(q-1)+q}}$ definimos

$$\overline{H} = \langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda'+1)q-\lambda')a - (\lambda'+1)\rangle,$$

onde $\lambda' = q^{r-2} + q^{r-3} + \ldots + q - 1$. Vejamos que $\overline{H} = H(P_{0,0})$.

Observação 5.3.1. Para $\widetilde{\lambda} = \lambda' + 1 = q^{r-2} + q^{r-3} + \ldots + q$ temos:

$$((\widetilde{\lambda}+1)q - \widetilde{\lambda})a - (\widetilde{\lambda}+1) = (q^{r-1}-1)(a+1)$$

e, portanto, tal elemento não pode pertencer ao grupo de geradores de $\overline{H}$.

Para vermos que $\overline{H} = H(P_{0,0})$ vamos mostrar que $\overline{H}$ possui g gaps em $P_{0,0}$, onde $g = \frac{(q^{r-1}-1)(\frac{q^r-1}{q-1}-1)}{2}$ é o gênero de $X_{q,r}$.

Então vejamos que $\overline{H}$ possui g gaps em $P_{0,0}$.

Seja $\widehat{H}$ o conjunto gerado por $\langle a, a+1\rangle$. Logo, pela proposição 5.1.14, $|\mathbb{N}\setminus\widehat{H}| = \frac{a(a-1)}{2}$.

Seja $\widehat{G} = \mathbb{N}\setminus\widehat{H}$. Vamos distribuir os elementos de $\widehat{G}$ da seguinte maneira:

$$\begin{array}{cccccc}
1 & 2 & \dots & \dots & \dots & a-1 \\
(a+1)+1 & (a+1)+2 & \dots & \dots & (a+1)+(a-2) & \\
2(a+1)+1 & (a+1)+2 & \dots & 2(a+1)+(a-3) & & \\
\vdots & & & & & \\
(a-3)(a+1)+1 & (a-3)(a+1)+2 & & & & \\
(a-2)(a+1)+1 & & & & &
\end{array}$$

Ou seja, em $a-1$ linhas, onde a linha i, com $1 \leq i \leq a-1$, é formada por $\{(i-j)a+j \ ; \ 1 \leq j \leq i \leq a-1\}$ e possui $(a-1)-(i-1)$ elementos.

Vejamos quantos dos elementos de $\widehat{G}$ deixam de existir quando, para $0 \leq \lambda \leq q^{r-2} + q^{r-3} + \ldots + q - 1$, acrescentamos $((\lambda+1)q-\lambda)a-(\lambda+1)$ ao conjunto de geradores $\langle a, a+1\rangle$.

Passo 1: Da linha 1 à linha $q-1$ não tiramos nenhum dos elementos de $\widehat{G}$, já que todos os elementos de tais linhas são menores que $qa-1$, que é o primeiro elemento acrescentado ao conjunto de geradores. Logo, tais elementos serão gaps em $P_{0,0}$.

Passo 2: Da linha q à linha $2q-2$ tiraremos 1 elemento em cada uma dessas linhas. Tais elementos são obtidos por uma combinação de a, $a+1$ e $qa-1$, e são os seguintes: $qa-1, (q+1)a-1, \ldots, (2q-2)a-1$.

Passo 3: Da linha $2q-1$ à linha $3q-3$ tiramos 2 elementos em cada uma dessas linhas, que são $(2q-1)a-2, (2q-1)a-1, (2q)a-2, (2q)a-1, \ldots, (3q-3)a-2, (3q-3)a-1$, obtidos através de a, $a+1$, $qa-1$ e $(2q-1)a-2$.

Continuando este processo, temos, para $1 \leq n \leq q^{r-2} + q^{r-3} + \ldots + q$.

Passo n+1: Da linha $nq-(n-1)$ à linha $(n+1)q-(n+1)$ tiramos n elementos em cada uma dessas linhas. Tais elementos são

$(nq-(n-1))a-n, (nq-(n-1))a-(n-1), \ldots, (nq-(n-1))a-1$
$(nq-(n-2))a-n, (nq-(n-2))a-(n-1), \ldots, (nq-(n-2))a-1$

$\vdots$

$((n+1)q-(n+1))a-n, ((n+1)q-(n+1))a-(n-1), \ldots, ((n+1)q-(n+1))a-1,$
obtidos através de $a, a+1, qa-1, (2q-1)a-2, \ldots, (nq-(n-1))a-n$.

Portanto, tiramos elementos de $(q-1)(q^{r-2}+q^{r-3}+\ldots+q+1)-1 = q^{r-1}-2$ linhas de $\widehat{G}$, num total de $(q-1)+2(q-1)+\ldots+(q^{r-2}+q^{r-3}+\ldots+q)(q-1)$ elementos .

Lembrando que nas $q-1$ primeiras não tiramos nenhum elemento, nos resta analisar as $(a-1)-(q^{r-1}-1) = q^{r-2}+q^{r-3}+\ldots+q$ últimas linhas de $\widehat{G}$, que são as linhas i, com $a-(q^{r-2}+q^{r-3}+\ldots+q) \leq i \leq a-1$. Vejamos que os elementos destas linhas podem ser obtidos pelos novos geradores $((\lambda+1)q-\lambda)a-(\lambda+1)$ e, assim, não serão gaps de $P_{0,0}$.

De fato, o primeiro elemento da $(a-(q^{r-2}+q^{r-3}+\ldots+q))$-ésima linha é

$$(a-(q^{r-2}+q^{r-3}+\ldots+q)-1)a+(a-(q^{r-2}+q^{r-3}+\ldots+q)) = q^{r-1}a-(q^{r-2}+q^{r-3}+\ldots+q)$$

que pode ser escrito como a soma de $(q-1)a$ com $((q^{r-2}+q^{r-3}+\ldots+q)q-(q^{r-2}+q^{r-3}+\ldots+q-1))a-(q^{r-2}+q^{r-3}+\ldots+q)$, e, portanto, não será um gap. Utilizando $a+1$ obtemos todos os demais elementos dessa linha.

Agora, os primeiros elementos das linhas seguintes são obtidos acrescentando $a+1$. Portanto, não teremos mais gaps em $P_{0,0}$.

Assim, o número de elementos de $\mathbb{N} \setminus \overline{H}$ será

$$\frac{a(a-1)}{2}-((q-1)+2(q-1)+\ldots+(q^{r-2}+q^{r-3}+\ldots+q)(q-1))-(q^{r-2}+q^{r-3}+\ldots+3+2+1)$$

$$= \frac{a(a-1)}{2} - q(1+2+\ldots+(q^{r-2}+q^{r-3}+\ldots+q))$$
$$= \frac{(\frac{q^r-1}{q-1}-1)(\frac{q^r-1}{q-1}-2)}{2} - \frac{(q^{r-2}+q^{r-3}+\ldots+q)(\frac{q^r-1}{q-1}-1)}{2}$$
$$= \frac{(q^{r-1}-1)(\frac{q^r-1}{q-1}-1)}{2} = g.$$

Logo, $\overline{H} = H(P_{0,0})$.

Sabendo que $H(P_\infty) = \left\langle q^{r-1}, \frac{q^r-1}{q-1} \right\rangle$ e que $\overline{H} = \langle a, a+1, qa-1, (2q-1)a-2, (3q-2)a-3, \ldots, ((\lambda'+1)q-\lambda')a-(\lambda'+1)\rangle$, onde $\lambda' = q^{r-2}+q^{r-3}+\ldots+q-1$, conseguimos o seguinte resultado que nos dará um dos conjuntos geradores de $H(P_{0,0}, P_\infty)$.

Teorema 5.3.2. *Sejam q potência de um número primo, $r \geq 3$ e $a = q^{r-1}+q^{r-2}+\ldots+q^2+q$. Para o par $P_{0,0}$ e P_∞ de pontos de Weierstrass da curva Norma-Traço $\mathcal{X}_{q,r}$ temos, para cada $1 \leq s \leq^{r-2} +q^{r-3}+\ldots+q+1$:*

$$\beta_{(i-j)(a+1)+j} = (q^{r-1}-(i-j+1))(a+1) - jq^{r-1} \tag{5.1}$$

onde i, j são tais que

$$1 \leq j \leq i \leq a-s \ , \ \ com \ \ (s-1)q-(s-1) \leq i-j \leq sq-(s+1).$$

Demonstração:

Seja $1 \leq s \leq q^{r-2}+q^{r-3}+\ldots+q+1$. Consideremos $1 \leq j \leq i \leq a-s$, com $(s-1)q-(s-1) \leq i-j \leq sq-(s+1)$. Nestas condições vimos, quando analisamos os gaps de $P_{0,0}$, que $(i-j)(a+1)+j \in Gaps(P_{0,0})$.

I) Vejamos que se $(i,j) \neq (i',j')$, então $(i-j)(a+1)+j \neq (i'-j')(a+1)+j'$.

De fato, suponhamos que exitam $(i,j) \neq (i',j')$ tais que $(i-j)(a+1)+j = (i'-j')(a+1)+j'$.

Se $i-j = i'-j'$, então da igualdade acima temos que $j = j'$ e como $i-j = i'-j'$, segue que $i = i'$, absurdo, pois supomos $(i,j) \neq (i',j')$. Logo $i-j \neq i'-j'$. Suponhamos que $i-j > i'-j'$, assim $i-j = i'-j'+m$, com $1 \leq m \leq q-1$, já que $(s-1)q-(s-1) \leq i-j, i'-j' \leq sq-(s+1)$. Então, $(i-j)(a+1)+j = (i'-j')(a+1)+j' \Rightarrow m(a+1)+j = j'$, que é um absurdo, pois, por hipótese, $j' \leq a-1$.

II) Vejamos que $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$ também são distintos para cada par (i,j).

Mais uma vez faremos uma prova por absurdo. Suponhamos que existam $(i,j) \neq (i',j')$ tais que $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} = (q^{r-1}-(i'-j'+1))(a+1)-j'q^{r-1}$. Usando o mesmo argumento de I) acima, vemos que $i-j \neq i'-j'$. Assim, suponhamos que $i-j > i'-j'$, logo $i-j = i'-j'+m$, onde $1 \leq m \leq q-1$, pois $(s-1)q-(s-1) \leq i-j, i'-j' \leq sq-(s+1)$. Da igualdade $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} = (q^{r-1}-(i'-j'+1))(a+1)-j'q^{r-1}$, segue que $(j-j')q^{r-1} = m(a+1) = m(q^{r-1}+\ldots+q+1)$, logo terímaos que q^{r-1} divide $m(q^{r-1}+\ldots+q+1)$, absurdo.

Portanto, se $(i,j) \neq (i',j')$, então $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} \neq (q^{r-1}-(i'-j'+1))(a+1)-j'q^{r-1}$.

III) Agora, vejamos que $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} \in Gaps(P_\infty)$, ou seja, que $(q^{r-1}-(i-j+1))(a+1)-jq^{r-1} \notin \langle q^{r-1}, q^{r-1}+\ldots+q+1\rangle = H(P_\infty)$.

De fato, suponhamos que exista um par (i_0,j_0) tal que $(q^{r-1}-(i_0-j_0+1))(a+1)-j_0q^{r-1} \in \langle q^{r-1}, q^{r-1}+\ldots+q+1\rangle$. Então, existem $\alpha, \beta \in \mathbb{N}\cup\{0\}$ tais que

$$\alpha q^{r-1}+\beta(q^{r-1}+\ldots+q+1) = (q^{r-1}-(i_0-j_0+1))(a+1)-j_0q^{r-1}$$

$$= (q^{r-1}-(i_0-j_0+1))(q^{r-1}+\ldots+q+1)-j_0q^{r-1}$$

logo, $(\alpha+j_0)q^{r-1} = (q^{r-1}-(i_0-j_0+1+\beta))(q^{r-1}+\ldots+q+1)$. Mas, $\alpha+j_0>0$ e $i_0-j_0+1+\beta>0$, assim, a igualdade acima nos diz que q^{r-1} divide $(q^{r-1}-(i_0-j_0+1+\beta))(q^{r-1}+\ldots+q+1)$, que é um absurdo, já que $q^{r-1}-(i_0-j_0+1+\beta) < q^{r-1}$ e q é potência de um número primo.

Usando que $\left(\frac{x^{a+1-j}}{y^{i-j+1}}\right)_\infty = ((i-j)(a+1)+j)P_{0,0}+((q^{r-1}-(i-j+1))(a+1)-jq^{r-1})P_\infty$, vemos que $((i-j)(a+1)+j, (q^{r-1}-(i-j+1))(a+1)-jq^{r-1}) \in H(P_{0,0},P_\infty)$.

Portanto, $((i-j)(a+1)+j, (q^{r-1}-(i-j+1))(a+1)-jq^{r-1}) \in (G(P_{0,0})\times G(P_\infty))\cap H(P_{0,0},P_\infty)$.

Assim, se $\alpha_1<\ldots<\alpha_g$ e $\alpha'_1<\ldots<\alpha'_g$ são as sequências de gaps de $P_{0,0}$ e P_∞, respectivamente, e τ é a permutação de $\mathbb{N}_{\leq g}$ tal que, para cada $l=1,\ldots,g$, $\alpha'_{\tau(l)} = (q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$, se $\alpha_l = (i-j)(a+1)+j$. Então, $\Gamma' = \{(\alpha_l, \alpha'_{\tau(l)})\ ;\ l=1,\ldots,g\} \subseteq (G(P_{0,0})\times G(P_\infty))\cap H(P_{0,0},P_\infty)$ e, pelo lema 5.1.11, temos que $\Gamma' = \Gamma(P_{0,0},P_\infty)$. Logo $\beta_{(i-j)(a+1)+j} = (q^{r-1}-(i-j+1))(a+1)-jq^{r-1}$. □

Exemplo 5.3.3. Sejam $q=3$ e $r=3$. Assim, temos que

$a=12$;

$H(P_\infty) = \langle 9, 13\rangle$;

$G(P_\infty) = \{1,\ldots,8,10,11,12,14,15,16,17,19,20,21,23,24,25,28,29,30,32,33,34,$

$37,38,41,42,43,46,47,50,51,55,56,59,60,64,68,69,73,77,82,86,95\}$;

$H(P_{0,0}) = \langle 12,13,35,58,81\rangle$;

e $G(P_{0,0})$ é dado por:

1	2	3	4	5	6	7	8	9	10	11
14	15	16	17	18	19	20	21	22	23	
27	28	29	30	31	32	33	34			
40	41	42	43	44	45	46				
53	54	55	56	57						
66	67	68	69							
79	80									
92										

Agora, utilizando o teorema 5.3.2, temos

1ª Parte: $1 \leq j \leq i \leq 11$ e $0 \leq i - j \leq 1$.

$\{(1,95),(2,86),(3,77),(4,68),(5,59),(6,60),(7,41),(8,32),(9,23),(10,14),(11,5)$
$(14,82),(15,73),(16,64),(17,55),(18,46),(19,37),(20,28),(21,19),(22,10),(23,1)\} \subseteq H(P_{0,0}, P_\infty)$

2ª Parte: $1 \leq j \leq i \leq 10$ e $2 \leq i - j \leq 3$.

$\{(27,69),(28,60),(29,51),(30,42),(31,33),(32,24),(33,15),(34,6)$
$(40,56),(41,47),(42,38),(43,29),(44,20),(45,11),(46,2)\} \subseteq H(P_{0,0}, P_\infty)$

3ª Parte: $1 \leq j \leq i \leq 9$ e $4 \leq i - j \leq 5$.

$\{(53,43),(54,34),(55,25),(56,16),(57,7),(66,30),(67,21),(68,12),(69,3)\} \subseteq H(P_0, P_\infty)$

4ª Parte: $1 \leq j \leq i \leq 8$ e $6 \leq i - j \leq 7$.

$\{(79,17),(80,8),(92,4)\} \subseteq H(P_{0,0}, P_\infty)$

E, conseguimos

$\Gamma(P_{0,0}, P_\infty) = \{(1,95),(2,86),(3,77),(4,68),(5,59),(6,60),(7,41),(8,32),(9,23),(10,14),$
$(11,5),(14,82),(15,73),(16,64),(17,55),(18,46),(19,37),(20,28),(21,19),(22,10),(23,1),$
$(27,69),(28,60),(29,51),(30,42),(31,33),(32,24),(33,15),(34,6),(40,56),(41,47),(42,38),$
$(43,29),(44,20),(45,11),(46,2),(53,43),(54,34),(55,25),(56,16),(57,7),(66,30),(67,21),$
$(68,12),(69,3),(79,17),(80,8),(92,4)\}$.

Portanto, pelo lema 5.1.12, o semigrupo de Weierstrass $H(P_{0,0}, P_\infty)$ é gerado por

$$\Gamma(P_{0,0}, P_\infty) \cup (\langle 12,13,35,58,81\rangle \times \{0\}) \cup (\{0\} \times \langle 9,13\rangle).$$

Seja $S := \Gamma(P_1, P_\infty) \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_\infty))$, como no lema 5.1.12, onde $P_1 \neq P_\infty$ é um ponto $\mathbb{F}_{q^r}$-racional de $\mathcal{X}_{q,r}$. Como $S \subseteq H(P_1, P_\infty)$, se $(a_1, a_2) \in S$ então existe uma função racional f_{a_1} tal que

$$(f_{a_1})_\infty = a_1 P_1 + a_2 P_\infty.$$

De acordo com o lema 5.1.12, existem $(a_1', a_2'), (a_1'', a_2'') \in S$ tais que $(a_1, a_2) = lub\{(a_1', a_2'), (a_1'', a_2'')\}$.

Assim, existem constantes $c', c'' \in \mathbb{F}_{q^r}$ tais que a função $f_{a_1,a_2} := c' f_{a_1'} + c'' f_{a_1''}$ tem divisor de pólo dado por

$$(f_{a_1,a_2})_\infty = a_1 P_1 + a_2 P_\infty \tag{5.2}$$

Definindo a ordem parcial $\preceq$ sobre $\mathbb{N}_0^2$ dada por: $(n_1, n_2) \preceq (m_1, m_2)$ se, e somente se, $n_1 \leq m_1$ e $n_2 \leq m_2$, e sabendo que $f \in L(mP_1 + nP_\infty)$ se, e somente se, $(f)_\infty = aP_1 + bP_\infty$, com $a \leq m$ e $b \leq n$, obtemos o seguinte resultado.

Proposição 5.3.4. *Seja P_1 um ponto racional de $\mathcal{X}_{q,r}$ distinto de P_∞, e sejam $m, n \in \mathbb{N}$. O espaço vetorial $L(mP_1 + nP_\infty)$ é gerado por*

$$\{f_{a_1,a_2} \,:\, (a_1, a_2) \in H(P_1, P_\infty) \ , \ (a_1, a_2) \preceq (m, n)\},$$

onde f_{a_1,a_2} é definida como na equação 5.2.

5.4 Códigos sobre curvas Norma-Traço:

Nesta última parte deste trabalho vejamos alguns resultados relacionados a códigos de Goppa geométricos sobre as curvas norma-traço $\mathcal{X}_{q,r}$.

G. Matthews mostrou em [16] o seguinte resultado que fornece uma melhor cota para a distância mínima de um código de Goppa geométrico sobre uma curva arbitrária.

Teorema 5.4.1. *Assuma que $(\alpha_1, \alpha_2) \in Gaps(P_1, P_2)$ com $\alpha_1 \geq 1$ e $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Suponha que $(\gamma_1, \gamma_2 - t - 1) \in Gaps(P_1, P_2)$, para todo t, $0 \leq t \leq min\{\gamma_2 - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$. Sejam $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2$ e $D = \sum_{j=1}^{n} Q_j$, onde $Q_1, \ldots, Q_n$ são pontos $\mathbb{F}_q$-racionais distintos e que não pertencem ao suporte de G.*

Se a dimensão de $C_\Omega(D, G)$ é positiva, então sua distância mínima é maior ou igual a $degG - 2g + 3$.

No teorema 5.3.2 vimos quais são os pares (α, β_α) que compõem $\Gamma(P_{0,0}, P_\infty)$, e com a definição 5.1.6 construímos $H(P_{0,0}, P_\infty)$, que será um subconjunto de $\mathbb{N}_0^2$. Aproveitando a distribuição dos elementos de $H(P_{0,0}, P_\infty)$ podemos melhorar tal cota de d para códigos sobre $\mathcal{X}_{q,r}$. Vejamos.

Teorema 5.4.2. *Considere o código $C_\Omega(D, G)$ sobre $\mathcal{X}_{q,r}$, com $G = (\alpha_1 + \gamma_1 - 1)P_{0,0} + (\alpha + \gamma - 1)P_\infty$ e $D = \sum_{j=1}^{n} Q_j$, onde $P_{0,0}, P_\infty, Q_1, \ldots, Q_n$ são pontos $\mathbb{F}_{q^r}$-racionais distintos. Suponhamos que:*

a) $(\alpha_1, \alpha) \in Gaps(P_{0,0}, P_\infty)$, $\alpha \geq 1$ *e* $l(\alpha_1 P_{0,0} + \alpha P_\infty) = l(\alpha_1 P_{0,0} + (\alpha - 1)P_\infty)$.

b) $(\gamma_1 - t - 1, \gamma), (\gamma_1 - t - 1, \gamma + 1), (\gamma_1 - t - 1, \gamma + \dfrac{q^r - 1}{q - 1}), (\gamma_1, \gamma) \in Gaps(P_{0,0}, P_\infty)$, *para todo* t, $0 \leq t \leq min\{\gamma_1 - 1, 2g - 1 - (\alpha_1 + \alpha)\}$.

Se a dimensão de $C_\Omega(D, G)$ é positiva, então sua distância mínima é maior ou igual a $degG - 2g + 4$.

Demonstração:

Pelo teorema anterior sabemos que a distância mínima de $C = C_\Omega(D, G)$ é $\geq deg(G) - 2g + 3$. Seja $d = deg(G) - 2g + 3$. Se existe $c \in C$ com peso igual a d, então existe um diferencial $\omega \in \Omega(G - D)$ com extamente d pólos simples $Q_1, \ldots, Q_d$. Agora, $deg(\omega) = 2g-2 = deg(G)-d+1$, ou seja, $(\omega) \geq G-(Q_1+\ldots+Q_d)$, e temos $(\omega) = G-(Q_1+\ldots+Q_d)+P$, onde P é um ponto $\mathbb{F}_{q^r}$-racional, com $P \neq Q_i$, para $1 \leq i \leq d$.

Como $l(\alpha_1 P_{0,0} + \alpha P_\infty) = l(\alpha_1 P_{0,0} + (\alpha - 1)P_\infty)$, o teorema de Riemann-Roch nos diz que $l(W-(\alpha_1 P_{0,0}+\alpha P_\infty)) = l(W-(\alpha_1 P_{0,0}+(\alpha-1)P_\infty))-1$, ou seja, $L(W-(\alpha_{0,0}P_1+(\alpha-1)P_\infty)) \neq L(W - (\alpha_1 P_{0,0} + \alpha P_\infty))$, onde W é um divisor canônico. Logo, existe uma função racional h onde:

$$(h) = (\alpha - 1)P_\infty + (\alpha_1 + t)P_{0,0} - W + E,$$

sendo E um divisor efetivo cujo suporte não contém $P_{0,0}$ e P_∞, e $0 \leq t \leq 2g - 1 - (\alpha_1 + \alpha)$, t está em tal intervalo pois $deg(h) = 0$. Portanto, temos

$$(\omega) = G - (Q_1 + \ldots + Q_d) + P = (\omega) \sim W \sim (\alpha - 1)P_\infty + (\alpha_1 + t)P_{0,0} + E.$$

Mas $G = (\alpha_1 + \gamma_1 - 1)P_{0,0} + (\alpha + \gamma - 1)P_\infty$, assim, existe uma função racional f tal que:

$$(f) = -\gamma P_\infty - (\gamma_1 - t - 1)P_{0,0} - P + (Q_1 + \ldots + Q_d) + E.$$

Vejamos que isto não pode ocorrer. Consideremos os seguintes casos.

1º) Suponhamos $t \leq \gamma_1 - 1$.

1ºa) Se $P \in Supp(E)$, então $(f)_\infty = \gamma P_\infty + (\gamma_1 - t - 1)P_{0,0}$, que é uma contradição, pois supomos $(\gamma_1 - t - 1, \gamma) \in Gaps(P_{0,0}, P_\infty)$.

1ºb) Se $P = P_\infty$, então $(f)_\infty = (\gamma + 1)P_\infty + (\gamma_1 - t - 1)P_{0,0}$, que contradiz o fato de $(\gamma_1 - t - 1, \gamma + 1) \in Gaps(P_{0,0}, P_\infty)$. O mesmo ocorre se supomos $P = P_{0,0}$, pois teríamos $(\gamma_1 - t, \gamma) \in H(P_{0,0}, P_\infty)$, que é um absurdo, lembrando que $(\gamma_1, \gamma) \in Gaps(P_{0,0}, P_\infty)$.

Logo $P = Q_j$, para algum j, $d+1 \leq j \leq n$. Sabemos que $(y) = \dfrac{(q^r-1)}{q-1}P_{0,0} - \dfrac{(q^r-1)}{q-1}P_\infty$.

Portanto, $(f.y)_\infty = (\gamma + \dfrac{q^r-1}{q-1})P_\infty + (\gamma_1 - t - 1)P_{0,0}$, que é um absurdo, já que supomos $(\gamma_1 - t - 1, \gamma + \dfrac{q^r-1}{q-1}) \in Gaps(P_{0,0}, P_\infty)$.

2º) Consideremos agora o caso $\gamma_1 - 1 < t \leq 2g - 1 - (\alpha_1 + \alpha)$.

2ºa) Se $P \in Supp(E)$ ou $P = P_{0,0}$, então $(f)_\infty = \gamma P_\infty$, contradição com o fato de γ ser um gap.

2ºa) Se $P = P_\infty$, também teremos uma contradição, pois $\gamma + 1$ também é um gap.

Logo nos resta $P = Q_j$, para algum j, $d+1 \leq j \leq n$, que também será uma contradição, pois $\gamma + \dfrac{q^r-1}{q-1}$ é um gap.

Portanto temos que $d \geq degG - 2g + 4$. □

Observação 5.4.3. Se temos uma função racional $f \in \mathbb{F}_q(\mathcal{X}_{q,r})$ tal que $(f) = \dfrac{(q^r-1)}{q-1}P_1 - \dfrac{(q^r-1)}{q-1}P_\infty$, com $P_1 \neq P_{0,0}$ ponto $\mathbb{F}_q$-racional de $\mathcal{X}_{q,r}$, temos que o teorema também será válido para P_1.

Definição 5.4.4. Seja C um código $[n, k, d]$. Definimos $\delta = \dfrac{d}{n}$ como sendo a *distância mínima relativa* de C. E $R = \dfrac{k}{n}$ será a *taxa de informação* de C.

Nota: Observamos que a comparação entre dois códigos é feita baseada em δ e R, cujos valores estão dentro do intervalo $[0, 1]$, ou seja, $0 \leq \delta \leq 1$ e $0 \leq R \leq 1$.

Assim, podemos representar um código C por um ponto (δ, R) que está dentro do quadrado unitário $[0, 1] \times [0, 1]$. Quanto mais próximo (δ, R) estiver do vértice $(1, 1)$ melhor serão os parâmetros relativos δ, R de C. Na maioria dos casos ocorre justamente o contrário, isto é, o ponto (δ, R) está mais próximo de $(0, 0)$, e mais ainda, uma parte deste quadrado,

incluindo o vértice $(1,1)$, nunca conterá (δ, R). Isto ocorre devido a algumas restrições, relacionadas a cotas, sobre os parâmetros de C.

No resultado a seguir veremos uma comparação entre códigos bipontuais e pontuais de mesma dimensão sobre a curva Norma-Traço.

Teorema 5.4.5. *Existem códigos bipontuais $C_\Omega(D,G)$ sobre $\mathcal{X}_{q,r}$ que possuem possui melhores parâmetros R, δ do que códigos pontuais $C_L(\overline{D}, mq^{r-1}P_\infty)$ sobre $\mathcal{X}_{q,r}$, de mesma dimensão que $C_\Omega(D,G)$.*

Demonstração:

Seja $C_L(\overline{D}, mq^{r-1}P_\infty)$ um código pontual sobre $\mathcal{X}_{q,r}$, onde $\overline{D} = \sum_{i=1}^{q^{2r-1}} P_i$, é o divisor formado pelos q^{2r-1} pontos $\mathbb{F}_{q^r}$-racionais de $\mathcal{X}_{q,r}$ diferentes de P_∞.

De [23] sabemos que se d é a distância mínima de $C_L(\overline{D}, mq^{r-1}P_\infty)$, então $d \geq n - deg(G) = q^{2r-1} - mq^{r-1}$.

Seja $f = \prod_{i=1}^{m}(x - \alpha^i) \in L(mq^{r-1}P_\infty)$, onde α é um gerador de $\mathbb{F}_{q^r}^\star$.

Sabemos que os q^{2r-1} pontos $\mathbb{F}_{q^r}$-racionais de $\mathcal{X}_{q,r}$ são da forma

$(0, \alpha_s^{(0)})$ onde $\alpha_s^{(0)}$, são as q^{r-1} raízes de $y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y = 0$;

$(\alpha^j, \alpha_s^{(j)})$, com $0 \leq j \leq q^r - 2$, e $\alpha_s^{(j)}$ sendo as q^{r-1} raízes de $y^{q^{r-1}} + y^{q^{r-2}} + \ldots + y = \alpha^j$.

Assim f possui mq^{r-1} zeros e nos dá uma palavra-código de peso $q^{2r-1} - mq^{r-1}$.

Portanto, a distância mínima de $C_L(\overline{D}, mq^{r-1}P_\infty)$ é exatamente $q^{2r-1} - mq^{r-1}$, e tal código terá os seguintes parâmetros

comprimento $n = q^{2r-1}$;

dimensão $k = mq^{r-1} - g + 1$;

distância mínima $d = q^{2r-1} - mq^{r-1}$.

Agora vamos ver quais serão os parâmetros do bipontual $C_\Omega(D,G)$.

Temos que $D = \sum_{j=1}^{q^{2r-1}-1} Q_j$ é o divisor formado pelos $q^{2r-1} - 1$ pontos $\mathbb{F}_{q^r}$-racionais de $\mathcal{X}_{q,r}$ distintos de $P_{0,0}$ e P_∞.

Sabemos pelo teorema 5.3.2 que $\beta_1 = 2g - 1$, isto é, $(1, 2g-1) \in H(P_{0,0}, P_\infty)$ e $(1, \lambda) \in Gaps(P_{0,0}, P_\infty)$, para todo $\lambda \leq 2g - 2$.

Seja $(\alpha_1, \alpha) = (1, 2g-2) \in Gaps(P_{0,0}, P_\infty)$, que satisfaz a condição $l(\alpha_1 P_{0,0} + \alpha P_\infty) = l((\alpha_1 - 1)P_{0,0} + \alpha P_\infty)$.

Seja $q^r - (q^{r-1} + q^{r-2} + \ldots + q^2 + q) + q \leq m < q^r$. Como $2g - 1 = q^{2r-2} + q^{2r-3} + \ldots + q^r - (q^{r-1} + \ldots q + 1) - 1$, então $0 \leq q^{2r-1} - mq^{r-1} - 1 < 2g - 1$, para todo m e $(\gamma_1, \gamma) = (1, q^{2r-1} - mq^{r-1} - 1) \in Gaps(P_{0,0}, P_\infty)$ satisfaz a condição $(\gamma_1, \gamma - t - 1) \in Gaps(P_{0,0}, P_\infty)$, para todo t, $0 \leq t \leq min\{\gamma - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$.

Por fim para estar nas condições do teorema 5.4.1 temos que $G = (\alpha_1 + \gamma_1 - 1)P_{0,0} + (\alpha + \gamma - 1)P_\infty$, logo $G = P_{0,0} + (q^{2r-1} + 2g - mq^{r-1} - 4)P_\infty$ e usando tal teorema, temos que a distância mínima de $C_\Omega(D, G)$ será

$$d \geq degG - 2g + 3 = q^{2r-1} - mq^{r-1}.$$

Sabemos que $C_\Omega(D, G)$ tem comprimento $n = q^{2r-1} - 1$. Agora vejamos que sua dimensão também será $k = mq^{r-1} - g + 1$.

De fato, sendo W um divisor canônico sabemos de [23] que

$$i(G) = l(W - G) \text{ e } dimC_\Omega(D, G) = i(G - D) - i(G).$$

Mas $degG > 2g - 2$, logo $i(G) = l(W - G) = 0$ e portanto

$$dimC_\Omega(D, G) = i(G - D) = l(W - G + D).$$

Agora $deg(W - G + D) \geq 2g - 2$, assim pelo teorema de Riemann-Roch temos

$$l(W - G + D) = deg(W - G + D) - g + 1.$$

Sabemos que $deg(W) = 2g - 2$, $deg(G) = q^{2r-1} + 2g - mq^{r-1} - 3$ e $deg(D) = q^{2r-1} - 1$. Logo

$$dimC_\Omega(D, G) = mq^{r-1} - g + 1.$$

Portanto os códigos $C_\Omega(D, G)$, que é bipontual, e $C_L(\overline{D}, mq^{r-1}P_\infty)$ que é pontual, ambos sobre $\mathcal{X}_{q,r}$ possuem mesma dimensão e assim podem ser comparáveis.

Como $C_\Omega(D, G)$ possui uma distância mínima maior e um comprimento menor que os respectivos de $C_L(\overline{D}, mq^{r-1}P_\infty)$, então também terá uma maior distância mínima relativa e um maior raio de informação, e assim podemos dizer que possui melhores parâmetros relativos que $C_L(\overline{D}, mq^{r-1}P_\infty)$. □

Exemplo 5.4.6. Sejam $q = r = 3$ e $\mathcal{X}_{3,3}$ a curva Norma-Traço sobre $\mathbf{F}_{27}$ de gênero $g = 48$. Consideremos os códigos $C_L(\overline{D}, 180P_\infty)$ e $C_\Omega(D, P_{0,0} + 155P_\infty)$, onde $\overline{D}$ é a soma de todos os 243 pontos racionais finitos. Assim, os parâmetros relativos do código $C_L(\overline{D}, 180P_\infty)$ são $\delta_1 = 63/243$ e $R_1 = 133/243$.

Pelos teoremas 5.4.1 e 5.4.5, temos que os parâmetros relativos do código bipontual $C_\Omega(D, P_{0,0} + 155P_\infty)$ são $\delta_2 \geq 63/242$ e $R_2 = 133/242$.

CAPÍTULO 6

Apêndice

6.1 Apêndice A: Bases de Gröbner

Os conceitos de base de Gröbner e ordem POT foram ferramentas de extremo valor utilizadas em todo o trabalho. Nesta seção daremos um breve estudo sobre tais conceitos.

Então vejamos.

Seja $A = k[x_1, \ldots, x_n]$ para algum corpo k. Seja $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_m = (0, \ldots, 0, 1)$ uma base de A^m.

Um *monômio* em A^m é um vetor do tipo $\mathbf{X}e_i$, onde $1 \leq i \leq m$ e $\mathbf{X}$ é um monômio em A. Ou seja, um monômio é um vetor cujas coordenadas são todas nulas exceto uma que é um produto em A.

Se $\mathbb{M}_1 = \mathbf{X}e_i$ e $\mathbb{M}_2 = \mathbf{Y}e_j$ são monômios em A^m, dizemos que $\mathbb{M}_1$ *divide* $\mathbb{M}_2$ se $i = j$ e $\mathbf{X}$ divide $\mathbf{Y}$.

Notemos que no caso em que $\mathbb{M}_1$ divide $\mathbb{M}_2$, existe um produto Z em A tal que $\mathbb{M}_2 = Z.\mathbb{M}_1$. Nesse caso definimos $\dfrac{\mathbb{M}_2}{\mathbb{M}_1} = \dfrac{\mathbf{Y}}{\mathbf{X}} = Z$.

Similarmente, um *termo* é um vetor do tipo $c\mathbb{M}$, onde $c \in k \setminus 0$ e $\mathbb{M}$ é um monômio. Assim $\mathbb{T} = (0, 5x_1^2x_3^4, 0, 0) = 5\mathbb{M}$, onde $\mathbb{M} = (0, x_1^2x_3^4, 0, 0) = x_1^2x_3^4.e_2$ é um termo de A^4 mas não um monômio.

Também se $\mathbb{T}_1 = c_1\mathbf{X}e_i$ e $\mathbb{T}_1 = c_2\mathbf{Y}e_j$ são termos de A^m, dizemos que $\mathbb{T}_1$ *divide* $\mathbb{T}_2$ se $i = j$ e $\mathbf{X}$ divide $\mathbf{Y}$, e escrevemos $\dfrac{\mathbb{T}_2}{\mathbb{T}_1} = \dfrac{c_2\mathbf{Y}}{c_1\mathbf{X}}$.

Agora podemos definir uma ordem para monômios em A^m.

Definição 6.1.1. Uma *ordem* sobre monômios de A^m será uma ordem total, $<$, sobre esses monômios satifazendo :

i) $\mathbb{M} < Z.\mathbb{M}$, para todo monômio $\mathbb{M}$ de A^m e monômios $Z \neq 1$ de A;

ii) Se $\mathbb{M}_1 < \mathbb{M}_2$, então $Z\mathbb{M}_1 < Z\mathbb{M}_2$, para quaisquer monômios $\mathbb{M}_1, \mathbb{M}_2$ de A^m e todo monômio $Z \in A$.

Em todo o trabalho, a ordem utilizada para a construção das bases de Gröbner foi a ordem POT, que tem a seguinte definição:

Definição 6.1.2. Dada uma ordem total em A e dados dois monômios $\mathbb{M}_1 = \mathbf{X}e_i$ e $\mathbb{M}_2 = \mathbf{Y}e_j$ de A^m, dizemos que $\mathbb{M}_1 <_{POT} \mathbb{M}_2$ se $i > j$ ou $i = j$ e $\mathbf{X} < \mathbf{Y}$ (onde X e Y são monômios em A).

Notações: Vejamos agora alguma notações.

Primeiramente fixamos uma ordem $<$ sobre os monômios de A^m. Então para $f \in A^m$, com $f \neq 0$ temos que :

$$f = a_1\mathbb{M}_1 + a_2\mathbb{M}_2 + \ldots + a_l\mathbb{M}_l$$

onde, para $1 \leq i \leq l$, $0 \neq a_i \in k$ e $\mathbb{M}_i$ é um monômio em A^m. E com tais monômios satisfazendo $\mathbb{M}_1 > \mathbb{M}_2 > \ldots > \mathbb{M}_l$. Assim definimos :

Monômio líder de f= $Lm(f) = \mathbb{M}_1$

Coeficiente líder de f= $Lc(f) = a_1$

Termo líder de f= $Lt(f) = a_1\mathbb{M}_1$

Podemos, então, dar a seguinte definição:

Definição 6.1.3. Um conjunto de vetores não nulos $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ contido em um submódulo $\mathcal{M}$ é chamado de *base de Gröbner* para $\mathcal{M}$ se para todo $\mathbf{f} \in \mathcal{M}$ existe $i \in \{1, \ldots, t\}$ tal que $Lm(\mathbf{g}_i)$ divide $Lm(\mathbf{f})$.

Observação 6.1.4. Tal definição nos diz que se $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ é uma base de Gröbner para um submódulo $\mathcal{M}$ e $Lm(\mathbf{g}_2)$ divide $Lm(\mathbf{g}_1)$, então $\mathcal{G} = \{\mathbf{g}_2, \ldots, \mathbf{g}_t\}$ continua sendo uma base de Gröbner para o submódulo $\mathcal{M}$.

Dois resultados, vistos em [2], que podemos citar estão na proposição a seguir:

Proposição 6.1.5. 1) *Todo submódulo não nulo $\mathcal{M}$ de A^m tem uma base de Gröbner.*

2) *Se $\mathcal{G} = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t\}$ é uma base de Gröbner para o submódulo $\mathcal{M}$ de A^m, então $\mathcal{M} = \langle \boldsymbol{g}_1, \ldots, \boldsymbol{g}_t \rangle$.*

Definição 6.1.6. Dados $\mathbf{f}, \mathbf{g}, \mathbf{h}$ em A^m, $\mathbf{g} \neq 0$, dizemos que $\mathbf{f}$ é reduzido a $\mathbf{h}$ módulo $\mathbf{g}$, e escrevemos

$$\mathbf{f} \rightarrow^{\mathbf{g}} \mathbf{h}$$

se, e somente se, $Lt(\mathbf{g})$ divide um termo $\mathbf{X}$ que aparece em $\mathbf{f}$ e $\mathbf{h} = \mathbf{f} - \frac{\mathbf{X}}{Lt(\mathbf{g})}\mathbf{g}$.

Usando tal definição conseguimos:

Definição 6.1.7. Sejam $\mathbf{f}, \mathbf{h}$ e $\mathbf{f}_1, \ldots, \mathbf{f}_s$ vetores em A^m, com $\mathbf{f}_1, \ldots, \mathbf{f}_s$ não nulos. Seja $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$, dizemos que $\mathbf{f}$ é reduzido a $\mathbf{h}$ módulo F, denota-se

$$\mathbf{f} \rightarrow_+^F \mathbf{h}$$

se, e somente se, existe um sequência de índices $i_1, \ldots, i_t \in \{1, \ldots, s\}$ e vetores $\mathbf{h}_1, \ldots, \mathbf{h}_{t-1} \in A^m$ tais que

$$\mathbf{f} \rightarrow^{\mathbf{f}_{i_1}} \mathbf{h}_1 \rightarrow^{\mathbf{f}_{i_2}} \mathbf{h}_2 \rightarrow^{\mathbf{f}_{i_3}} \ldots \rightarrow^{\mathbf{f}_{i_{t-1}}} \mathbf{h}_{t-1} \rightarrow^{\mathbf{f}_{i_t}} \mathbf{h}$$

Definição 6.1.8. Um vetor $\mathbf{r}$ em A^m é dito *reduzido* com respeito a um conjunto $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\}$ de vetores não nulos em A^m se $\mathbf{r} = 0$ ou se nenhum dos monômios que aparecem em $\mathbf{r}$ é divisível por qualquer um dos $Lm(\mathbf{f}_i)$, $i = 1, \ldots, s$.

Se $\mathbf{f} \rightarrow_+^F \mathbf{r}$ e $\mathbf{r}$ é reduzido com respeito a F, então diremos que $\mathbf{r}$ é um **resto** para $\mathbf{f}$ com respeito a F.

A observação a seguir é de extrema importância na construção do algoritmo de codificação dado na seção 2.

Observação 6.1.9. Este processo de redução permite a construção de um "algoritmo de divisão"que imita o algoritmo de divisão para polinômios.

Dados $\mathbf{f}, \mathbf{f}_1, \ldots, \mathbf{f}_s \in A^m$, com $\mathbf{f}_1, \ldots, \mathbf{f}_s \neq \mathbf{0}$, tal algoritmo nos dá coeficientes $a_1, \ldots, a_s \in A = k[x_1, \ldots, x_n]$, e um resto $\mathbf{r} \in A^m$, que é reduzido com respeito a F, tais que

$$\mathbf{f} = a_1\mathbf{f}_1 + \ldots + a_s\mathbf{f}_s + \mathbf{r}.$$

Este algoritmo pode ser visto em [2] ou em [3].

O resultado a seguir, visto em [13], é de muita importância para nosso trabalho, pois ele nos garante a existência de um tipo muito especial de base de Gröbner: uma base de Gröbner diagonal, que é peça chave na construção do diagrama de raízes. Tal resultado é o seguinte.

Proposição 6.1.10. *Se M é um submódulo do módulo livre $\mathbb{F}_q[t]^r$, então M possui uma base de Gröbner $\mathcal{G}$ com a propriedade: para cada $j = 1, 2, \ldots, r$, existe no máximo um elemento de $\mathcal{G}$ cujo monômio líder é da forma $t^i\mathbf{e}_j$. Portanto, é uma base de Gröbner $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_r\}$ tal que:*

$$\begin{aligned}
\mathbf{g}^{(1)} &= (g_1^{(1)}(t), g_2^{(1)}(t), \ldots, g_r^{(1)}(t)) \\
\mathbf{g}^{(2)} &= (0, g_2^{(2)}(t), \ldots, g_r^{(2)}(t)) \\
&\vdots \\
\mathbf{g}^{(r)} &= (0, \ldots, 0, g_r^{(r)}(t))
\end{aligned}$$

Em particular, M possui uma base de Gröbner com no máximo r elementos.

Demonstração:

Sabemos de [2] que todo submódulo de $\mathbb{F}_q[t]^r$ possui uma base de Gröbner. Seja $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$ uma base de Gröbner genérica para M.

Suponha que dentre os elementos de $\mathcal{G}$ existam dois, $\mathbf{g}_i$ e $\mathbf{g}_k$, com $Lt(\mathbf{g}_i) = t^u\mathbf{e}_j$ e $Lt(\mathbf{g}_k) = t^v\mathbf{e}_j$ para o mesmo j.

Sem perda de generalidade, suponhamos $u \leq v$. Logo, $Lt(\mathbf{g}_k)$ é divisível por $Lt(\mathbf{g}_i)$ e os termos líderes de $\mathcal{G}_1 = \mathcal{G} \setminus \{\mathbf{g}_k\}$ geram o mesmo submódulo M que é gerado por $\mathcal{G}$. Portanto, pela observação 2.4, $\mathcal{G}_1$ também é uma de Gröbner para M.

Repetindo o mesmo argumento para $\mathcal{G}_1$ e assim, sucessivamente, conseguimos uma base de Gröbner $\mathcal{G}$ com a propriedade desejada.

Em particular tal $\mathcal{G}$ possui no máximo r elementos, já que temos $\mathbf{e}_1, \ldots, \mathbf{e}_r$ fazendo parte dos geradores dos $Lt(\mathbf{g}_i)$. □

Agora, vejamos o algoritmo de Buchberger para se encontrar uma base de Gröbner para módulos.

Primeiramente introduziremos o conceito de "S-polinômio".

Sejam $\mathbb{X} = \mathbf{X}e_i$ e $\mathbb{Y} = \mathbf{Y}e_j$ dois monômios em A^m. Assim, vamos dizer que:

$$mmc(\mathbb{X}, \mathbb{Y}) = \begin{cases} \mathbf{0}\ , \text{ se } i \neq j \\ Le_i\ , \text{ se } i = j, \text{ onde } L = mmc(\mathbf{X}, \mathbf{Y}) \end{cases}$$

Por exemplo, $mmc((x^2yz, 0), (xy^3, 0)) = (x^2y^3z, 0)$ e $mmc((x^2y, 0), (0, xy^3)) = (0, 0)$.

Definição 6.1.11. Sejam $0 \neq \mathbf{f}, \mathbf{g} \in A^m$. Seja $\mathbb{L} = mmc(Lm(\mathbf{f}), Lm(\mathbf{g}))$. O vetor $S(\mathbf{f}, \mathbf{g}) = \frac{\mathbb{L}}{Lt(\mathbf{f})}.\mathbf{f} - \frac{\mathbb{L}}{Lt(\mathbf{g})}.\mathbf{g}$ é chamado de *S-polinômio* de $\mathbf{f}$ e $\mathbf{g}$.

Teorema 6.1.12. *Seja $\mathcal{G} = \{\boldsymbol{g}_1, \ldots, \boldsymbol{g}_t\}$ um conjunto de vetores não nulos em A^m. Então $\mathcal{G}$ é uma base de Gröbner para o submódulo $\mathcal{M}\langle \boldsymbol{g}_1, \ldots, \boldsymbol{g}_t \rangle$ de A^m se, e só se, para todo $i \neq j$ temos $S(\boldsymbol{g}_i, \boldsymbol{g}_j) \xrightarrow{\mathcal{G}}_+ \boldsymbol{0}$.*

Agora estamos prontos pra descrever o algoritmo de Buchberger para módulos que é o seguinte:

Algoritmo 7.13:

Entrada: $F = \{\mathbf{f}_1, \ldots, \mathbf{f}_s\} \subseteq A^m$ com $\mathbf{f}_i \neq 0, 1 \leq i \leq s$

Saída: $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_t\}$ base de Gröbner para $\langle \mathbf{f}_1, \ldots, \mathbf{f}_s \rangle$

Inicialização : $\mathcal{G} := F$, $\mathbf{G} := \{\{\mathbf{f}_i, \mathbf{f}_j\}\ ;\ \mathbf{f}_i \neq \mathbf{f}_j \in \mathcal{G}\}$

Enquanto G $\neq \emptyset$ faça

escolha algum $\{\mathbf{f}, \mathbf{g}\} \in \mathbf{G}$

$\mathbf{G} := \mathbf{G} \setminus \{\{\mathbf{f}, \mathbf{g}\}\}$

$S(\mathbf{f}, \mathbf{g}) \xrightarrow{\mathcal{G}}_+ \mathbf{h}$

Se $h \neq 0$ **então**
$\mathbf{G} := \mathbf{G} \bigcup \{\{\mathbf{u}, \mathbf{h}\} \ ; \ \forall u \in \mathcal{G}\}$
$\mathcal{G} := \mathcal{G} \bigcup \{\mathbf{h}\}$

6.2 Apêndice B: Um Estudo do Diagrama de Raízes

Nesta seção vamos fazer um estudo sobre o diagrama de raízes. Veremos como fazer sua construção e como podemos relacioná-la ao semigrupo de Weiertrass, se podemos dar uma relação de equivalência entre diagramas, dentre outras questões. Para começar vejamos, passo a passo, como é feita sua construção.

6.2.1 Como se constrói um diagrama de raízes

Seja $C = C(D, G)$ um código de Goppa geométrico. Para se definir um diagrama de raízes relacionado a C é necessário que C possua um automorfismo σ que fixe D e G. Assim o diagrama de raízes $\mathcal{D}(C, \sigma)$ de C é associado a σ. A construção de tal diagrama é feita da seguinte forma.

1º Passo: Seja C com o automorfismo σ, assim, através de σ, podemos associar C a um submódulo $\overline{C}$ do módulo livre $\mathbb{F}_q[t]^r$ (veja seção 1.0.2 no capítulo 1), onde r é o número de órbitas, $O_1, \ldots, O_r$, geradas por σ quando aplicado aos pontos de $Supp(D)$.

2º Passo: Verificar que as raízes de $t^{|O_i|} - 1 = 0$ são distintas, onde $i = 1, \ldots, r$.

3º Passo: O submódulo $\overline{C}$ possui uma base de Gröbner diagonal com r elementos, ou seja, uma base do tipo

$$\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_r\}$$

onde, para cada i, $\mathbf{g}_i = (0, \ldots, 0, g_i^{(i)}(t)), g_{i+1}^{(i)}(t), \ldots, g_r^{(i)}(t))$.

4º Passo: Seja $\mathbb{F}_q^\star = \{1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$. Para cada $i = 1, \ldots, r$, olhamos para as raízes de $t^{|O_i|} - 1 = 0$ que estão em $\mathbb{F}_q^\star$ e colocamos um quadradinho em cada uma delas.

5º Passo: Vemos quais são as raízes de $t^{|O_1|} - 1 = 0$ que também são raízes de $g_i^{(i)}(t)$ e marcamos, com um X, os respectivos quadradinhos. E, assim, a i-ésima linha do diagrama de raízes $\mathcal{D}(C, \sigma)$ está construída.

Questão 6.2.1. Podemos comparar diagramas de um código C com diferentes automorfismos?

Vejamos. Seja C um código sobre $\mathbb{F}_q$ com dois automorfismos σ e σ', onde, sem perda de generalidade, $|\sigma| < |\sigma'|$, com $|\sigma|$ e $|\sigma|'$ dividindo $q-1$. Assim C é associado a um submódulo $\overline{C}$ por σ, e associado a um submódulo $\overline{C}'$ por σ'.

Pela forma como $\overline{C}$ e $\overline{C}'$ são construídos a partir de C temos que eles possuem um mesmo número de elementos (geradores), e portanto a complexidade do algorítmo de Buchberger para se encontrar as bases de Gröbner $\mathcal{G}$ e $\mathcal{G}'$ para este módulos é praticamente a mesma, assim como transformação destas bases em bases diagonais, para ver isto basta olhar para a demonstração da proposição 6.1.10.

A primeira diferença relevante entre os dois automorfismos na construção do diagrama será o número de órbitas. O automorfismo σ possui um menor número de órbitas e levará vantagem sobre σ' quanto ao número de elementos de sua base diagonal, pois este número será menor, porém os graus dos elementos $g_i^{(i)}(t)$ serão maiores e consequentemente pode se tornar mais difícil a obtenção de suas raízes, que é uma desvagem de σ. Assim concluímos que a complexidade na construção do diagrama será praticamente a mesma para os dois automorfismos.

Para códigos Hermitianos podemos fazer um outro tipo de construção, sem utilizar a base de Gröbner. Tal construção é feita da seguinte forma:

• **Para códigos Hermitanos pontuais $C(D, aP_\infty)$:**

I : Utilizando o automorfismo $\sigma \in Aut(C)$, de ordem m^2-1, dado por: $\sigma(x) = \alpha x$ e $\sigma(y) = \alpha^{m+1}y$.

Este automorfismo decompõe os m^3 pontos de D em $m+2$ órbitas, e, assim, teremos $m+2$ linhas no diagrama $\mathcal{D}(C, \sigma)$, que serão preenchidas da seguinte maneira:

1º **Passo:** Para cada $i = 1, \ldots, m+2$, olhamos para as raízes de $t^{|O_i|} - 1 = 0$ que estão em $\mathbb{F}_{m^2}^\star$ e colocamos um quadradinho em cada uma delas.

2º **Passo:** Olhamos para o valor de a e, temos:

1) Para $i \leq m+1$. Se $a < (i-1)(m^2-1)$, então a i-ésima linha do diagrama de raízes é toda preenchida (com marcas X). E, se $a \geq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$, então a i-ésima linha do diagrama de raízes é vazia (não tem marcas X).

2) Para $1 \leq i \leq m$ (analogamente se faz para $i = m+1$ e $i = m+2$) e a no seguinte intervalo:

$$(i-1)(m^2-1) \leq a \leq (i-1)(m^2-1) + m^2 + (m-2)(m+1)$$

Então, a i-ésima linha do digrama de raízes não é nem vazia, nem totalmente preenchida.

Sendo A_i o conjunto das raízes maracadas na i-ésima linha do diagrama de raízes, o complementar de A_i é o conjunto de elementos $\alpha^{-k} \in \mathbb{F}_q^*$ tal que $k = r + s(m+1)$, onde $0 \leq r \leq m$, $0 \leq s \leq m-2$ e $rm + s(m+1) + (i-1)(m^2) \leq a$.

II : Utilizando o automorfismo $\eta \in Aut(C)$, de ordem $m+1$, dado por: $\eta(x) = \alpha^{m-1}x$ e $\eta(y) = y$.

O automorfismo η decompõe os m^3 pontos racinais de $\mathcal{X}_m$ em m^2 órbitas, sendo $m(m-1)$ de comprimento $m+1$ e m de comprimento 1. Logo teremos m^2 linhas no diagrama de raízes $\mathcal{D}(C, \eta)$, que são construídas de uma maneira semelhante a de σ, só com intervalos diferentes de a. Esta construção é feita da seguinte forma:

Mais uma vez o primeiro passo será:

1º **Passo:** Para cada $i = 1, \ldots, m^2$, olhamos para as raízes de $t^{|O_i|} - 1 = 0$ que estão em $\mathbb{F}_{m^2}^\star$ e colocamos um quadradinho em cada uma delas.

2º **Passo:** Olhamos para a e temos:

1) Para $i \leq m(m-1)$. Se $a < (i-1)(m+1)$, então a i-ésima linha do diagrama de raízes é totalmente preenchida. E, se $a \geq (i-1)(m+1) + m^2$, então a i-ésima linha do diagrama de raízes é vazia (não tem marcas X).

2) Para $m(m-1)+1 \leq i \leq m^2$, temos que $|O_i| = 1$, logo teremos apenas um quadradinho, que será embaixo do 1 que é a única raiz de $t - 1 = 0$. Assim se $a \geq (i-1)(m+1)$, então a linha i será vazia.

3) Se $i \leq m(m-1)$ e $(i-1)(m+1) \leq a < (i-1)(m+1) + m^2$

Então a i-ésima linha do diagrama de raízes não é nem vazia nem totalmente preenchida.

Sendo M o conjunto das raízes marcadas na i-ésima linha do diagrama de raízes, o complementar de M é o conjunto $M^c = \{\alpha^{-k} \in \mathbb{F}_{m^2}^\star;$ tal que $k = r(m-1),$ com $0 \leq r \leq m$ e $rm + (i-1)(m+1) \leq a\}$.

Vemos que estas construções do diagrama de raízes são mais fáceis, já que basta olhar o valor de a e compará-lo a certos valores, e não é necessário encontrar uma base de Gröbner para C.

Também podemos fazer uma construção deste tipo para códigos Hermitianos n-pontuais $C(D, aP_\infty + bP_0 + c_1P_{k_1} + \ldots + c_{n-2}P_{k_{n-2}})$ (com $2 \leq n \leq m+1$), onde P_∞ é o único ponto no infinito, P_0 é a origem, e para cada $j = 1, \ldots, n-2$, $P_{k_j} \in O_{k_j}$ onde $k_j \in \{m(m-1)+1, \ldots, m^2-1\}$, que é $P_{k_j} = (0, \alpha^{l_{k_j}}) \in O_{k_j}$, onde $|O_{k_j}| = 1$.

6.2.2 Outra interpretação para encontrar o conjunto de raízes sobre a linha i do diagrama de raízes de um código Hermitiano pontual

Nesta secão vamos fornecer uma outra interpretação, utilizando o semi-grupo de Weierstrass $H(P_\infty)$ para a curva Hermitiana, para encontrar as raízes marcadas sobre a linha i do diagrama de raízes de um código Hermitiano pontual $C_L(D, aP_\infty)$ sobre $\mathbb{F}_{m^2}$ com o automorfismo σ, de ordem m^2-1. A base para tal interpretação são os resultados obtidos por J. Little et al. em [14].

Antes de começarmos a falar desta nova interpretação daremos os resultados obtidos por J. Little et al. em [14], que são os seguintes:

Teorema 6.2.2. *Considere o diagrama de raízes do código Hermitano $C_L(D, aQ)$.*

(1) Seja $i \leq m$. Se $a \geq (i-1)(m^2-1)$, então a i-ésima linha do diagrama de raíes para o código não é totalmente preenchida.

(2) Seja $i \leq m$. Se $a \geq (i-1)(m^2-1)+m^2+(m-2)(m+1)$, então a i-ésima linha do diagrama de raízes é vazia.

(3) Finalmente consideremos o caso $i = m+1$. A $(m+1)$-ésima linha do diagrama de raízes não é toda preenchida se $a \geq m(m^2-1)$. E ela é vazia se $a \geq m(m^2-1)+(m-2)(m+1)$.

O próximo resultado é onde baseamos nossa nova interpretação. Através dele construímos uma outra forma de encontrar as raízes marcadas na i-ésima linha do diagram.

Teorema 6.2.3. *Sejam $1 \leq i \leq m$ e a no seguinte intervalo:*

$$(i-1)(m^2-1) \leq a < (i-1)(m^2-1)+m^2+(m-2)(m+1)$$

então a linha i do nosso diagrama não é nem totalmente preenchida, nem vazia. Sendo M_i o conjunto das raízes marcadas na i-ésima linha do diagrama, o complementar de M_i, ou seja, M_i^c é o conjunto dos elementos $\alpha^{-k} \in \mathbb{F}_{m^2}^\star$ tais que $k = r+s(m+1)$, $0 \leq r \leq m$, $0 \leq s \leq m-2$, e $rm+s(m+1)+(i-1)(m^2-1) \leq a$.

Observação 6.2.4. Note que para todo a dado, existe no máximo duas linhas do diagrama que não são totalmente preenchidas, nem vazias.

Para vermos isto primeiramente notemos que se j_1 e j_2, com $j_1 < j_2$, são tais linhas, então pelo terorema 1.2 $(j_1-1)(m^2-1) \leq a < (j_1-1)(m^2-1)+m^2+(m-2)(m+1)$ e $(j_2-1)(m^2-1) \leq a < (j_2-1)(m^2-1)+m^2+(m-2)(m+1)$, se existe i entre j_1 e j_2, então $(i-1)(m^2-1) \leq a < (i-1)(m^2-1)+m^2+(m-2)(m+1)$ e consequentemente a linha i também não será totalmente preenchida, nem vazia. Portanto concluímos que as linhas do diagrama que não são totalmente preenchidas, nem vazias, são consecutivas.

Agora suponhamos que existem três linhas do diagrama que não são totalmente preenchidas, nem vazias. Sejam $j, j+1$ e $j+2$ tais linhas. Assim a está nos seguintes intervalos:

$$(j-1)(m^2-1) \leq a < (j-1)(m^2-1)+m^2+(m-2)(m+1)$$

$$j(m^2-1) \leq a < j(m^2-1)+m^2+(m-2)(m+1)$$

$$(j+1)(m^2-1) \leq a < (j+1)(m^2-1)+m^2+(m-2)(m+1)$$

mas $(j+1)(m^2-1) = (j-1+2)(m^2-1) = (j-1)(m^2-1)+2m^2-2 \geq (j-1)(m^2-1)+2m^2-2-m = (j-1)(m^2-1)+m^2+(m-2)(m+1)$ que é uma contradição, pois temos $a < (j-1)(m^2-1)+m^2+(m-2)(m+1) \leq (j+1)(m^2-1)$ e $a \geq (j+1)(m^2-1)$.

Portanto não podemos ter três ou mais linhas deste tipo em nosso diagrama.

Observação 6.2.5. Observamos que $m^2-1 = |\mathbb{F}^{\star}_{m^2}| = |\sigma|$ e $(m-2)(m+1) = 2g-2$, onde g é o gênero de nossa curva. Estes fatos podem ser importantes para estudarmos o diagrama de de raízes para outro tipos de códigos.

A nova interpretação:

Seja $\mathcal{X}_m$ a curva Hermitiana $X^{m+1} = Y^m + Y$, cujo gênero é $g = \dfrac{m(m-1)}{2}$. Sabemos que $P_\infty = (0:1:0)$ é o ponto no infinito de tal curva.

O semi-grupo de Weierstrass, ou conjunto de não-gaps de $\mathcal{X}_m$, $H(P_\infty)$ em P_∞ é:

$$H(P_\infty) = \langle m, m+1, 2m, 2m+1, 2m+2, \ldots, (m-1)m, (m-1)m+1, \ldots, (m-1)(m+1) = m^2-1, \ldots \rangle$$

Sejam:

$g_{01} = 0$

$g_{11} = m, g_{12} = m+1$

$g_{21} = 2m, g_{22} = 2m+1, g_{23} = 2m+2$

$\vdots$

$g_{(m-1)1} = (m-1)m, g_{(m-1)2} = (m-1)m+1, \ldots, g_{(m-1)m} = (m-1)(m+1) = m^2-1$

e

$g_{m1} = m^2, g_{m2} = m^2+1, \ldots, g_{m(m-1)} = m^2+(m-2)$

$g_{(m+1)2} = (m+1)m+1, g_{(m+1)3} = (m+1)m+2, \ldots, g_{(m+1)(m-1)} = (m+1)m+(m-2)$

$g_{(m+2)3} = (m+2)m+2, g_{(m+2)4} = (m+2)m+3, \ldots, g_{(m+2)(m-1)} = (m+2)m+(m-2)$

$\vdots$

$g_{(2m-3)(m-2)} = (2m-3)m+(m-3), g_{(2m-3)(m-1)} = (2m-3)m+(m-2)$

isto é, nós apenas demos uma notação para alguns não-gaps específicos. Isso será importante para explicar nossa interpretação. Seja $\widetilde{\mathcal{T}}$ o conjunto formado por estes não-gaps citados acima menos $\{g_{(m-1)m} = m^2-1\}$. Tal conjunto tem ordem $1 + \frac{(m-1)(2+m)}{2} + \frac{(m-2)(m+1)}{2} - 1 = m^2-2$. Note que se a linha i do diagrama não é totalmente preenchida, então esse número , m^2-1, é o número máximo de raízes marcadas em tal linha, ou seja podemos preencher tal linha com no máximo m^2-1 raízes marcadas.

Agora sejam:

$\mathbf{g_{02}} = 1, \mathbf{g_{03}} = 2, \ldots, \mathbf{g_{0m}} = m-1$

$\mathbf{g_{13}} = m+2, \mathbf{g_{14}} = m+3, \ldots, \mathbf{g_{1m}} = 2m-1$

$\mathbf{g_{24}} = 2m+3, \mathbf{g_{25}} = 2m+4, \ldots, \mathbf{g_{2m}} = 3m-1$

$\vdots$

$\mathbf{g_{(m-3)(m-1)}} = (m-2)m-2, \mathbf{g_{(m-3)m}} = (m-2)m-1$

$\mathbf{g_{(m-2)m}} = (m-1)m-1$

que são os gaps menores que m^2-1.

Definimos a seguinte ordem para os g_{ij} e $\mathbf{g_{ij}}$:

$$g_{ij} > g_{rs} \Leftrightarrow j > s \text{ or } j = s \text{ and } i > r$$

analogamente para os $\mathbf{g_{ij}} > \mathbf{g_{rs}}$.

Utilizando esta ordem construímos um conjunto ordenado $\mathcal{T}$ da seguinte maneira: Primeiramente tomamos $g_{01} = 0$, depois tomamos, em ordem decrescente, os non-gaps menores que $m^2 - 1$, e finalmente tomamos, também em ordem decrescente, os gaps. Assim temos:

$$\mathcal{T} := \{0, g_{(m-1)(m-1)}, g_{(m-2)(m-1)}, g_{(m-1)(m-2)}, g_{(m-2)(m-2)}, g_{(m-3)(m-2)}, \ldots, g_{(m-1)1}, g_{(m-2)1}, \ldots, g_{11},$$

$$\mathbf{g_{(m-2)m}}, \mathbf{g_{(m-3)m}}, \ldots, \mathbf{g_{0m}}, \mathbf{g_{(m-3)(m-1)}}, \mathbf{g_{(m-4)(m-1)}}, \ldots, \mathbf{g_{0(m-1)}}, \ldots, \mathbf{g_{13}}, \mathbf{g_{03}}, \mathbf{g_{02}} = 1\}$$

Feita estas construções podemos começar nossa nova interpretação para o teorema 1.2. Seja a no intervalo:

$$(i-1)(m^2-1) \leq a < (i-1)(m^2-1) + m^2 + (m-2)(m+1)$$

e seja M_i^c o conjunto dos elementos $\alpha^{-k} \in \mathbb{F}_{m^2}^\star$ tais que $k = r + s(m+1)$, $0 \leq r \leq m$, $0 \leq s \leq m-2$, e $rm + s(m+1) + (i-1)(m^2-1) \leq a$.

Tomemos $a' = a - (i-1)(m^2-1)$, então $a' < m^2 + (m-2)(m+1)$. Agora vejamos quantos não-gaps $g_{ij} \in \widetilde{\mathcal{T}}$ são menores ou iguais a a'. Seja n este número. Assim tomamos os n primeiros elementos do conjunto ordenado $\mathcal{T}$, suponhamos $0, a_1, a_2, \ldots, a_{n-1}$. Com isso podemos construir M_i^c sa seguinte maneira:

$$M_i^c = \{\alpha^0 = 1, \alpha^{a_1}, \alpha^{a_2}, \ldots, \alpha^{a_{n-1}}\}$$

E portanto o conjunto M_i das raízes marcadas na i-ésima linha será $\mathbb{F}_{m^2}^\star \setminus M_i^c$.

Exemplo 6.2.6. Daremos agora um exemplo de como funciona nossa interpretação. Seja $m = 5$, Assim temos $\mathcal{X}_5$ dada por $X^6 = Y^5 + Y$. Let α be a generator for $\mathbb{F}_{25}^\star$. Então $\mathbb{F}_{25}^\star = \{1, \alpha, \alpha^2, \ldots, \alpha^{23}\}$.

Seja $a = 80$. Vejamos como é feito o diagrama de raízes para o código $C_L(D, aP_\infty)$ sobre $\mathcal{X}_5$.

Aqui temos:

$$\widetilde{\mathcal{T}} := \{0, 5, 6, 10, 11, 12, 15, 16, 17, 18, 20, 21, 22, 23, 25, 26, 27, 28, 31, 32, 33, 37, 38\}$$

e o conjunto ordenado

$$\mathcal{T} := \{0, 23, 18, 22, 17, 12, 21, 16, 11, 6, 20, 15, 10, 5, 19, 14, 9, 4, 13, 8, 3, 7, 2, 1\}$$

• Para a linha 1, que é, $i = 1$, temos:

$(i-1)(m^2-1) = 0 \leq a$ and $(i-1)(m^2-1)+m^2+(m-2)(m+1) = 25+3.6 = 43 \leq a = 80$

assim, pelo teorema 6.2.2, temos que a linha 1 do nosso diagrama é vazia.

• Para $i = 2$ temos:

$$(i-1)(m^2-1) = 24 < a \text{ and } (i-1)(m^2-1)+m^2+(m-2)(m+1) = 67 \leq a$$

assim, pelo teorema 6.2.2, a linha 2 do diagrama também será vazia.

• Para $i = 3$:

$$(i-1)(m^2-1) = 48 < a = 124 < (i-1)(m^2-1)+m^2+(m-2)(m+1) = 91$$

logo a está no intervalo do teorema 6.2.3. Assim seja $a' = a-(3-1)(5^2-1) = 80-48 = 32$, logo $a' = 32$. Olhando para $\widetilde{\mathcal{T}}$ vemos que 20 de seus elementos são menores ou iguais a $a' = 32$. Os 20 primeiros elementos do conjunto ordenado $\mathcal{T}$ são $\{0, 23, 18, 22, 17, 12, 21, 16, 11, 6, 20, 15, 10, 5,$ e assim $M_3^c = \{1, \alpha^{23}, \alpha^{18}, \alpha^{22}, \ldots, \alpha^8\}$. Portanto $M_3 = \mathbb{F}_{25}^\star \setminus M_3^c = \{\alpha, \alpha^2, \alpha^3, \alpha^7\}$, e temos que as raízes marcadas na linha 3 serão $\{\alpha, \alpha^2, \alpha^3, \alpha^7\}$.

• Para $i = 4$ temos:

$$(i-1)(m^2-1) = 72 < a = 80 < (i-1)(m^2-1)+m^2+(m-2)(m+1) = 115$$

e novamente a está no intervalo do teorema 6.2.3. Assim seja $a' = a-(4-1)(5^2-1) = 80-72 = 8$, logo $a' = 8$. Olhando para $\widetilde{\mathcal{T}}$ vemos que 3 de seus elementos são menores ou iguais a $a' = 8$. E os 3 primeiros elementos de $\mathcal{T}$ são $\{0, 23, 18\}$, e temos $M_4^c = \{1, \alpha^{23}, \alpha^{18}\}$. Portanto $M_4 = \mathbb{F}_{25}^\star \setminus M_4^c = \{\alpha, \alpha^2, \ldots, \alpha^{17}, \alpha^{19}, \alpha^{20}, \alpha^{21}, \alpha^{22}\}$, que são as $21(= |M_4|)$ raízes marcadas na linha 4.

• Para $i = 5, 6$:

$$(i-1)(m^2-1) = 4.(25-1) = 96 > a = 80$$

portanto, pelo teorema 6.2.2, as linhas 5 e 6 são totalmente preenchidas.

Questão 6.2.7. Poderíamos fazer algo similar utilizando o automorfismo η?

Sim, vejamos.

No caso do automorfismo η conseguimos funções $B_{i,j}(x) = \prod_{k=1}^{m}(x - \alpha^{t_i+(j+k)(m-1)})$, e sendo M o conjunto das raízes marcadas na i-ésima linha do diagrama de raízes $\mathcal{D}(C, \eta)$, o complementar de M é o conjunto $M^c = \{\alpha^{-k} \in \mathbb{F}^{\star}_{m^2};$ tal que $k = r(m-1),$ com $0 \leq r \leq m$ e $rm + (i-1)(m+1) \leq a\}$. Mais ainda, temos o seguinte resultado:

Teorema 6.2.8. *Considere o diagrama de raízes do código Hermitiano $C_L(D, aP_\infty)$.*

1) Seja $i \leq m(m-1)$. Se $a \geq (i-1)(m+1)$, então a i-ésima linha do diagrama não é totalmente preenchida.

2) Seja $i \leq m(m-1)$. Se $a \geq (i-1)(m+1) + m^2$, então a i-ésima linha do diagrama é vazia.

3) Para $m(m-1)+1 \leq i \leq m^2$, temos que $|O_i| = 1$, logo teremos apenas um quadradinho, que será embaixo do 1 que é a única raiz de $t - 1 = 0$. Assim se $a \geq (i-1)(m+1)$, então a linha i será vazia.

Novamente construimos um subconjunto $\overline{H_\eta(P\infty)}$ de $H(P\infty)$ composto por elementos de $H(P\infty)$ que não são múltiplos de $m+1$ e que são menores que m^2, que serão somente os m (incluindo o 0) primeiros elementos da primeira coluna do semi-grupo $H(P_\infty)$, isto pois o lado direito da desigualdade $a' < m.m$, onde $a' = a - (i-1)(m+1)$, não depende de $m+1$ e temos $m.m = m^2$.

Agora vemos quantos elementos de $\overline{H_\eta(P\infty)}$ são menores ou iguais a $a' = a-(i-1)m(m+1)$. Sendo n esse número, vamos até o conjunto $R_i\{1, \alpha^{m-1}, \alpha^{2(m-1)} \ldots, \alpha^{m(m-1)}\}$, formado pelas raízes de $t^{|O_i|} - 1 = 0$, para $1 \leq i \leq m(m-1)$, e excluímos n de seus elementos na seguinte ordem: primeiro 1, depois $\alpha^{m(m-1)}$, depois $\alpha^{(m-1)(m-1)}$, e assim sucessivamente até o último que será α^{m-1}. O restante,$|R_i| - n$, serão as raízes marcadas na i-ésima linha do diagrama.

Para os demais valores de i, ou seja, $m(m-1)+1 \leq i \leq m^2$ temos $t^{|O_i|} - 1 = t - 1$ que possui somente o 1 como raiz e assim só temos que analisar a parte 3) do terorema 6.2.8.

Exemplo 6.2.9. Seja $m = 4$, com $\alpha^{15} = 1$. Assim teremos o seguinte automorfismo:

$$\eta(x) = \alpha^3 x \ , \ \eta(y) = y$$

Portanto $|\eta| = 5$ e teremos 16 órbitas, sendo 12 de comprimento $m+1 = 5$ e 4 órbitas de comprimento 1.

Para $1 \leq i \leq 12$ temos $t^{|O_i|-1=t^5-1}$, logo $R_i = \{1, \alpha^1 2, \alpha^9, \alpha^6, \alpha^3\}$, onde obviamente cada raiz tem multiplicidade 1.

Sabemos que $H(P_\infty)$ é dado por:

0

4 5

8 9 10

12 13 14 15

⋮

Logo $\overline{H_\eta(P\infty)} = \{0, 4, 8, 12\}$.

Para $a = 35$ construímos o seguinte diagrama de raízes para o código Hermitiano $C_L(D, 35P_\infty)$.

Linhas 1,2,3,4: Para $i = 1, 2, 3, 4$ temos $a \geq (i-1).5+16$, logo pelo item 2) do teorema 2 temos que as linhas $1, 2, 3, 4$ são vazias.

Linha 5: Para $i = 5$ temos $20 \leq 35 < 36$, assim tomando $a' = a - 20 = 15$ vemos que 4 elementos de $\overline{H_\eta(P\infty)}$ são menores ou iguais a $a' = 15$. Assim só marcaremso α^3 na linha 5.

Linha 6: Para $i = 6$ temos $25 \leq a < 41$, logo $a' = a - 25 = 10$, e temos 3 elementos de $\overline{H_\eta(P\infty)}$ que são menores ou iguais a $a' = 10$. E assim marcamos α^3 e α^6 na linha 6 do diagrama.

Linha 7: Para $i = 7$ temos $30 \leq a < 41$, logo $a' = a - 30 = 5$, e temos 2 elementos de $\overline{H_\eta(P\infty)}$ que são menores ou iguais a $a' = 5$. E assim marcamos α^3, α^6 e α^9 na linha 7 do diagrama.

Linha 8: Para $i = 8$ temos $35 \leq a < 41$, logo $a' = a - 35 = 0$, e temos somente um elemento de $\overline{H_\eta(P\infty)}$ que é menor ou igual a $a' = 0$. E assim marcamos α^3, α^6, α^9 e α^{12} na linha 8 do diagrama.

Linhas 9,10,11,12,13,14,15,16: Para $i = 9, 10, 11, 12, 13, 14, 15, 16$ temos $a < (i - 1).5$, logo tais linhas são totalmente preenchidas, sendo que as linhas $9, 10, 11, 12$ possuem 5 quadradinhos, um para cada elemento de R_i, e as linhas $13, 14, 15, 16$ têm somente um quadradinho, que é embaixo do 1.

Assim teremos o seguinte diagrama:

Linha	1	α^3	α^6	α^9	α^{12}
1					
2					
3					
4					
5		X			
6		X	X		
7		X	X	X	
8		X	X	X	X
9	X	X	X	X	X
10	X	X	X	X	X
11	X	X	X	X	X
12	X	X	X	X	X
13	X				
14	X				
15	X				
16	X				

Conclusão:

Fixemos as seguintes notações:

$|O_i|$ = ordem da órbita O_i;

X_{O_i} = número de coordenadas X diferentes na órbita O_i;

Y_{O_i} = número de coordenadas Y diferentes na órbita O_i;

Após estudarmos o comportamento do diagrama de raízes de um código Hermitiano $C_L(D, aP_\infty)$ com estes dois diferentes tipos de automorfismos, conseguimos expressar o diagrama de raízes da seguinte forma:

1) Se $a \leq (i-1).|automorfismo|$, então a i-ésima linha do diagrama é totalmente preenchida;

2) Caso X_{O_i} e Y_{O_i} não são múltiplos nenhum do outro, se $a \geq (i-1).|automorfismo| + (X_{O_i} - 1)m. + (Y_{O_i} - 1)(m+1)$, então a i-esima linha do diagrama é vazia.
Caso X_{O_i} e Y_{O_i} sejam múltiplos, ou seja, $X_{O_i} = c.Y_{O_i}$, então se $a \geq (i-1).|automorfismo| + (c-1)m. + (Y_{O_i} - 1)(m+1)$, então a i-ésima linha do diagrama é vazia.

3) No caso em que a está entre as desigualdades dos itens anteriores, então a i-ésima linha do diagrama não será nem vazia nem totalmente preenchida, e assim construímos os seguintes conjuntos:

• Seja R_i o conjundo formado pelas raízes de $t^{|O_i|} - 1 = 0$.

• $\overline{H_{autom}(P_\infty)}$ composto por elementos de $H(P_\infty)$ e formado da seguinte maneira:

1ºCaso: Quando $(X_{O_i} - 1)$ e $(Y_{O_i} - 1)$ são não nulos, caso de σ. Assim as funções $B_{i,j}$ dependem de x e de y.
Sabemos que os elementos de $H(P_\infty)$ são da forma $rm + s(m+1)$, incluindo o 0. Neste caso tomamos $\overline{H_{autom}(P_\infty)}$ como sendo o conjunto formado pelos elementos $h = rm + s(m+1)$ de $H(P_\infty)$ tais que $s \leq (Y_{O_i} - 1)$ e que são menores que $(X_{O_i} - 1)m. + (Y_{O_i} - 1)(m+1)$, ou no caso de σ, menores que $(c-1)m. + (Y_{O_i} - 1)(m+1)$, onde $X_{O_i} = c.Y_{O_i}$.

2ºCaso: Será quando $(Y_{O_i} - 1) = 0$, caso do automotfismo η. Assim as funções $B_{i,j}$ dependem apenas de x. E formaremos $\overline{H_{autom}(P_\infty)}$ pelos elementos $h = rm + s(m+1)$ de $H(P_\infty)$, com $s \leq 0 = Y_{O_i} - 1$, ou seja, $s = 0$, e que sejam menores que $(X_{O_i} - 1)m$.

Com estes dois conjuntos em mãos tomamos $a' = a - (i - 1.|autom.|)$ e vemos quantos elementos de $\overline{H_{autom}(P_\infty)}$ são menores ou iguais a a', sendo n esse número, vamos até R_i e excluímos n de seus elementos em ordem. Assim marcaremos sobre a linha i do diagrama os $|R_i| - n$ elementos que restaram em R_i.

Questão 6.2.10. Poderíamos fazer algo semelhante para códigos Hermitianos bi-pontuais, ou seja, construir suas linhas através de seu semi-grupo de Weierstrass?

6.2.3 Associando diagramas a códigos

Dado um diagrama $\mathcal{D}$, como na definição 2.0.34, podemos associá-lo a um determinado código $C(D, G)$?

A resposta é sim se este diagrama $\mathcal{D}$ satisfaz algumas condições.

1º) Se o número de lugares vazios de $\mathcal{D}$ é igual a dimensão de $C(D, G)$;

2º) Se existe $\sigma \in Aut(C)$ tal que o número de linhas de $\mathcal{D}$ é igual ao número de órbitas $|O_i|$ geradas por σ, agindo sobre os pontos de D. Mais ainda, as raízes de $t^{|O_i|} - 1 = 0$ têm que ser distintas em $\mathbb{F}_q^\star$;

3º) Se os quadradinhos na linha i do diagrama estão abaixo das raízes de $t^{|O_i|} - 1 = 0$;

4º) E, por fim, se existe uma base de Gröbner diagonal de $\overline{C}$ tal que as marcas da linha i estão sobre as raízes de $g_i^{(i)}(t)$.

Está análise é feita baseada na definição e construção de um diagrama de raízes dada na primeira seção.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] W. Adams e P. Loustaunau, *An Introduction to Gröbner bases*, Providence, RI: Amer. Math. Soc. 1994.

[2] C. Carvalho e F. Torres, *On Goppa codes and Weierstrass gaps at several points*, Des. Codes Cryptogr. 35(2) (2005), 211-225.

[3] D. Cox, J. Little e D. O'Shea, *Ideals, Varieties and Algorithms*, Springer, New York, 1992.

[4] A. Garcia, H. Stichtenoth e C.P. Xing, *On Subfield of the Hermitian Function Field*, Composito Mathematica **120** (2000), 137-170.

[5] O. Geil, *On codes from norm-trace curves*, Finite Fields and Their Applications, 9, 2003, 351-371.

[6] M. Giulietti, G. Korchmáros e F. Torres, *Quotient curves of the Suzuki curve*, Pre-print, May 2005.

[7] J. P. Hansen e H. Stichtenoth, *Group codes on certain curves with many rational points*, AAECC 1, 67-77 (1990).

[8] A. Hefez e M. L. T. Villela, *Códigos Corretores de Erros*, IMPA - Série de Computação e Matemática 2002.

[9] T. Høholdt, J. van Lint e R. Pellikaan, *Algebraic geometry codes*, V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, v. 1, Elsevier, Amsterdam, 1998.

[10] M. Homma e S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra, 162 (2001), 273-290.

[11] M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. 67 (1996), 337-348

[12] S.J. Kim, *On index of the Weierstrass semigroup of a pair of points on a curve*, Arch. Math. 62 (1994), 73-82

[13] J. Little, C. Heegard e K. Saints, *Systematic encoding via Gröbner bases for class of algebraic geometric Goppa codes*, IEEE Trans. Infor. Theory **41**(6) (1995), 1752–1761.

[14] J. Little, C. Heegard e K. Saints, *On the structure of Hermitian codes*, J. Pure Appl. Algebra **121** (1997), 293-314.

[15] G. L. Matthews, *Codes from the Suzuki function field*, IEEE Transactions on Information Theory vol. 50 (2004), no. 12, 3298-3302.

[16] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Designs, Codes and Cryptography, 22, 107-121, 2001.

[17] G. L. Matthews, *The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve*, Lecture Notes in Computer Science vol. 2948 (2004), 12-24.

[18] C. Munuera e J. Tena, *Codificacion de la Informacion*, Univ. de Valladolid 1997.

[19] R. Pellikaan, B. Z. Shen e G.J.M. van Wee, *Which linear codes are algebraic-geometric?*, IEEE Trans. Inform. Theory, vol. 37, n.3, p. 583-602, May 1991.

[20] M.G. Ruggiero e V.R. Lopes, *Cálculo Numérico: Aspectos teóricos e computacionais*, Makron Books, 2ªed. 1997.

[21] J. T. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[22] J. H. Silvervam e J. Tate, *Rational points on Elliptic Curves*, Springer, 1992.

[23] H. Stichtenoth, *Algebraic Function Fields and Codes*, Berlin, Germany: Springer, 1993

[24] H. Stichtenoth, *On Automorphism of Geometric Goppa Codes*, Journal of Algebra 130, p. 113-121, 1990

[25] J. H. van Lint, *Introduction to Coding Theory*, New York: Springer 1982.

[26] S. Wesemeyer, *On the automorphism group of various Goppa codes*, IEEE Trans. Inform. Theory, vol. 44, n. 2, March 1998

[27] C. Xing *Automorphism Group of Elliptic Codes*, Comm. in Algebra, 23(11), 4061-4072 (1995).