Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Tese de Doutorado

SOBRE CÓDIGOS HERMITIANOS GENERALIZADOS

por

Alonso Sepúlveda Castellanos

Doutorado em Matemática - Campinas - SP

Orientador: **Prof. Dr. Fernando Eduardo Torres Orihuela**

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

SOBRE CÓDIGOS HERMITIANOS GENERALIZADOS

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Alonso Sepúlveda Castellanos** e aprovada pela comissão julgadora.

Campinas, 21 de Fevereiro de 2008.

Prof. Dr. Fernando E. Torres Orihuela

Banca examinadora:

Prof. Dr. Fernando E. Torres Orihuela.
Prof. Dr. Cícero Fernandes de Carvalho.
Prof. Dr. Reginaldo Palazzo Junior.
Prof. Dr. Paulo Roberto Brumatti.
Prof[a]. Dr[a]. Sueli Irene Rodrigues Costa.

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

Castellanos, Alonso Sepúlveda
C276g Sobre códigos hermitianos generalizados / Alonso Sepúlveda Castellanos-- 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. Códigos hermitianos. 3. Distância mínima. 4. Corpos de funções algébricas . I. Torres Orihuela, Fernando Eduardo. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: On generalized hermitian codes.

Palavras-chave em inglês (Keywords): 1. Goppa codes. 2. Hermitian codes. 3. Minimum distance. 4. Algebraic function fields.

Área de concentração: Álgebra (Geometria Algébrica)

Titulação: Doutor em Matemática

Banca examinadora: Prof. Dr. Fernando Eduardo Torres Orihuela (IMECC-UNICAMP)
Prof. Dr. Cícero Fernandes de Carvalho (UFU)
Prof. Dr. Reginaldo Palazzo Junior (FEEC-UNICAMP)
Prof. Paulo Roberto Brumatti (IMECC-UNICAMP)
Profa. Dra. Sueli Irene Rodrigues Costa (IMECC-UNICAMP)

Data da defesa: 21/02/2008

Programa de pós-graduação: Doutorado em Matemática

Tese de Doutorado defendida em 21 de fevereiro de 2008 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

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

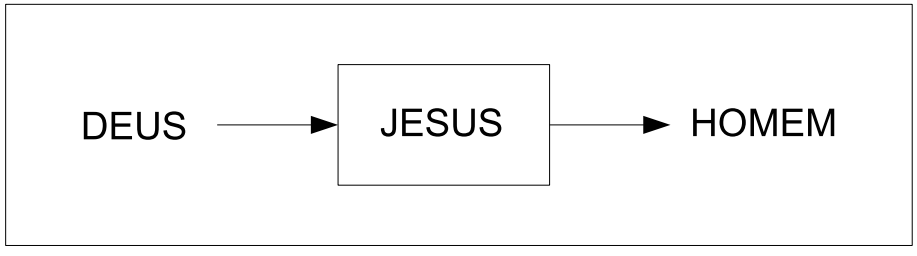
Prof(a). Dr(a). CÍCERO FERNANDES DE CARVALHO

Prof(a). Dr(a). REGINALDO PALAZZO JÚNIOR

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

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

Jesus o Código para a Vida Eterna



"Quando o HOMEM entender a mensagem de DEUS para sua vida, através de JESUS, ele entenderá o verdadeiro propósito da sua existência. Este código é simples, só para quem quiser"

A Deus

João 3:16

Á minha esposa

Juliana Bueno Castellanos

Por seu Amor, paciência, apoio, companhia e por estar sonhado junto comigo os sonhos de Deus em nossas vidas.

Á minha grande Família

Meus pais José Alonso e Yolanda

Meus painhos Keyla e Sergio

Meus sogros Sebastião e Lucélia

Meus Pastores Paulo e Valeria

Meus líderes Marcos e Day

Agradecimentos

Agradeço:

Em especial, ao meu Senhor e Salvador Jesus Cristo, pelo apoio, atenção, força, bom ânimo e Amor proporcionados durante a realização deste trabalho.

A igreja Batista Vida Nova, que me acolheram e tem vivido do meu lado cada uma das conquistas que tenho alcançado neste país abençoado, o Brasil.

A minhas famílias em Bucaramanga (Colômbia), Campinas e Pernambuco (Brasil).

Ao meu orientador Prof. Dr. Fernando Torres, pela sua orientação, ensinamentos e em especial pelos momentos que compartilhamos como amigos durante este trabalho.

Ao Prof. Dr. Paulo Brumatti, pelo tempo que me dedicou na fase final do trabalho que foi essencial para terminar.

Ao Prof. Dr. Carlos Munuera, pelo apoio, incentivo e valiosos comentários do trabalho.

Aos professores da banca examinadora, por todas suas sugestões, importantes para melhorar o trabalho.

Aos funcionários da Unicamp, que direta e indiretamente fizeram parte desta conquista pela sua presença e trabalho, em particular Cidinha, Ednaldo e Tânia.

Aos meus amigos e colegas, em especial ... a TODOS.

Aos meus irmãos, Daniel, Carol Paola, Johana, Dimas, Fabio, Josiney, Kedla, Kaio, Silvano, Rogerio, Eliel, Thyago, Lúcio, Benedita, Alcione, a minha sobrinha Daniela, e a todos os outros que não dá para escrever seu nome aqui mas que também foram importantes.

Ao ministério de teatro da IBVN.

Ao Cnpq e à Unicamp, pelo seu apoio financeiro durante o período do doutorado.

Resumo

Estudamos os códigos de Goppa (códigos GH) sobre certos corpos de funções algébricas com muitos lugares racionais. Estes códigos generalizam os bem conhecidos códigos Hermitianos; portanto podemos esperar que estes códigos tenham bons parâmetros.

Bulygin (IEEE Trans. Inform. Theory **52 (10)**, 4664–4669 (2006)) inicia o estudo dos códigos GH; enquanto Bulygin considerou somente característica par, nosso trabalho é feito em qualquer característica. Em qualquer caso, nosso trabalho é fortemente influenciado pelo de Bulygin. A seguir, listamos alguns dos nossos resultados com respeito aos códigos GH.

- Calculamos "distâncias mínimas exatas", em particular, melhoramos os resultados de Bulygin;
- Encontramos cotas para os pesos generalizados de Hamming, além disso, mostramos um algoritmo para aplicar estes cálculos na criptografia;
- Calculamos um subgrupo de Automorfismos;
- Consideramos códigos em determinados subcorpos dos corpos usados para construir os códigos GH.

Abstract

We study Goppa codes (GH codes) based on certain algebraic function fields whose number of rational places is large. These codes generalize the well-known Hermitian codes; thus we might expect that they have good parameters.

Bulygin (IEEE Trans. Inform. Theory **52 (10)**, 4664–4669 (2006)) initiate the study of GH-codes; while he considered only the even characteristic, our work is done regardless the characteristic. In any case our work was strongly influenced by Bulygin's. Next we list some of the results of our work with respect to GH-codes.

- We calculate "true minimum distances", in particular, we improve Bulygin's results;
- We find bounds on the generalized Hamming weights, moreover, we show an algorithm to apply these computations to the cryptography;
- We calculate an Automorphism subgroup;
- We consider codes on certain subfields of the fields used for to construct GH-codes.

SUMÁRIO

Introdução

Códigos de Goppa fazem parte dos códigos chamados de *corretores de erros*, que participam da vida moderna de inúmeras formas como, por exemplo, nas comunicações via satélite, na telefonia celular e na comunicação entre computadores, etc. A teoria dos Códigos Corretores de erros foi introduzida pelo matemático C.E. Shannon, num trabalho publicado no ano de 1948. Houve um desenvolvimento considerável nas décadas de 50 e 60, e a partir da década de 70, com as pesquisas espaciais e a grande popularização dos computadores, essa teoria teve um impulso ainda maior. Hoje em dia, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados, garantindo sua confiabilidade. Em geral, o processo de trasmissão de informação esta dado na seguinte figura:

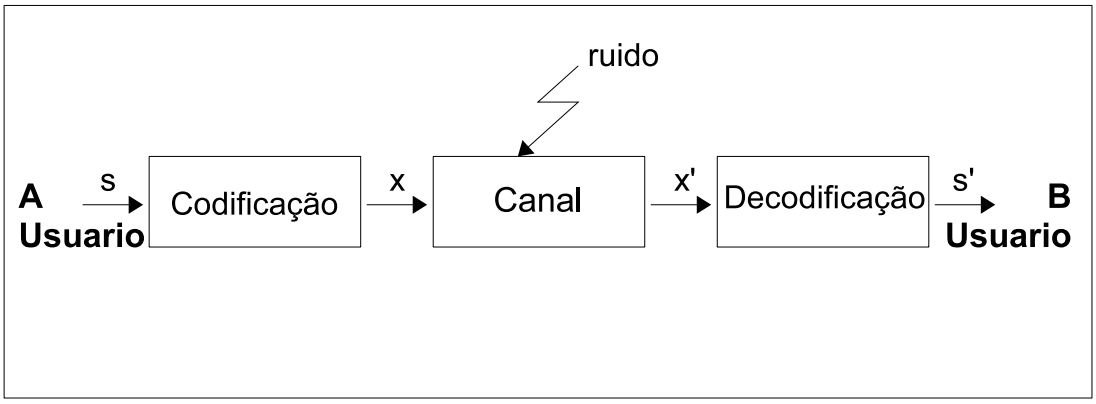


Figura 1: Processo de Transmissão de Informação

O usuário **A** deseja enviar uma mensagem **s** para o usuário **B**. Quase sempre acontece que

esta informação não esta escrita convenientemente para ser transmitida, pois pode ocupar muito espaço ou pode ser vulnerável a interferências e ataques na sua privacidade. Então, é codificada para adaptar-la as características do canal e as nossas necessidades.

Depois, os blocos de mensagens codificadas são associados a sinais contínuos, que desde um ponto de vista geométrico, podem ser representados como pontos em esferas euclideanas. Este fato, abre uma linha de estudo direcionada a desenvolver uma teoria mias geométrica dos códigos, buscando aumentar a confiabilidade da mensagem durante a transmissão. Nesta direção aparecem códigos como: *códigos esféricos euclideanos* [6], *códigos de grupo cíclico e comutativo* [2], [15], [26].

O canal de transmissão pode ser uma linha telefônica, fibra ótica, canal de radiofreqüência, circuito integrado digital, fita magnética, disco de armazenamento, etc. Codificar a informação significa reescrever-la de novo em forma diferente, seguindo determinadas regras. Um dos objetivos perseguidos com a codificação é detectar e corrigir (possíveis) erros aparecidos durante a transmissão. Com esta perspectiva, a seguir descrevemos algébricamente o tipo de códigos a serem estudados nesta tese.

A classe de códigos mais utilizada na prática é a classe dos *Códigos Lineares*. Um código linear C é um subespaço vetorial de $\mathbb{F}_q^n$, caracterizado pelos parâmetros $[n, k, d]$, onde n é seu comprimento, k é a sua dimensão e $d = \min\{d(a,b) = |\{i : a_i \neq b_i\}| : a, b \in C \text{ com } a \neq b\}$ é a sua distância mínima. Este último parâmetro também é conhecido como o *peso do código* C, denotado por $\omega(C)$, onde $\omega(C) = \min\{\omega(c) = |\{i : c \in C \text{ e } c_i \neq 0\}| : c \in C \setminus \{0\}\}$, pois $d = \omega(c)$. Um grande desenvolvimento da teoria de códigos corretores de erros ocorreu a partir dos anos 80, devido a Goppa [11], com a introdução de métodos da geometria algébrica para construir códigos que melhorassem os anteriores, por exemplo com respeito à distância mínima. Estes códigos são chamados de *Códigos Geométricos de Goppa (CGG)*. Em 1982, se produze a primeira aplicação relevante devido a Tsfasman, Vladut e Zink [29], os quais usaram a ideia de Goppa para mostrar que era possível uma construção de códigos geométricos de Goppa com bons parêmtros que assintóticamente eram melhor que a cota de Gilbert-Varshamov [28], [30].

A seguir, descrevemos a problemática a ser considerada para obter códigos de Goppa com bons parâmetros, para isto, utilizaremos a linguagem de corpos de funções algébricas (ver [28]):

Seja F um corpo de funções algébricas sobre $\mathbb{F}_q$. Denotamos por $N = N(F)$ o número de lugares de grau 1 sobre $\mathbb{F}_q$ e $g = g(F)$ o gênero do corpo de funções F. Sabe-se que a

dimensão k e a distância mínima d do código geométrico de Goppa $C_{\mathcal{L}}(D,G)$ de comprimento n sobre F satisfazem (ver Teorema 1.2):

$$k = \dim \mathcal{L}(G) - \dim \mathcal{L}(G-D) \quad \text{e} \quad d \geq n - \deg(G)\,.$$

Se $\deg(G) < n$, então

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

Denotando por $R = k/n$ a *taxa de informação* e $\delta = d/n$ a *taxa de correção de erros* tem-se que $R+\delta \geq \frac{n+1}{n} - \frac{g}{n}$. Fixando *delta*, para que a taxa de informação R seja a maior possível, devemos ter que g/n seja o menor possível, ou em outras palavras, que o quociente N/g seja o maior possível.

Problema *Achar um corpo de funções algébricas F, tal que o quociente N/g seja o maior possível.*

Na literatura existem diversos candidatos para F. Nosso trabalho, com o intuito de abordar esta problemática, construímos códigos geométricos de Goppa sobre o corpo de funções algébricas que tem como curva base com equação afim

$$y^{q^{r-1}} + \cdots + y^q + y = x^{1+q} + \cdots + x^{1+q^{r-1}} + x^{q+q^2} + \cdots + x^{q+q^{r-1}} + \cdots + x^{q^{r-2}+q^{r-1}}\,. \quad (1)$$

Estas curvas foram construídas por Garcia e Stichtenoth em [9], com o propósito de construir curvas com muitos pontos racionais. Bulygin obteve um recorde na distância mínima para o CGG sobre $\mathbb{F}_8$ com parâmetros $[32, 16, \geq 12]$, comparando com as cotas das distâncias mínimas de todos os códigos lineares em [12]. Este resultado foi obtido aplicando os resultados do trabalho de Kirfel e Pellikaan em [16], com respeito a estimativa da *distância mínima de Feng-Rao* δ_{FR} (ver Subseção 1.2.1), a qual melhora a distância mínima designada de Goppa em alguns casos.

Neste trabalho, generalizamos os resultados de Bulygin para qualquer valor de $q = p^t$, p um primo. Aquí, surge uma pergunta: porque é importante estudar os códigos introduzidos por Bulygin para $q > 2$? A resposta é que o quociente N/g do corpo de funções construídos sobre estas curvas cresce quando q também cresce, e é o menor possível quando $q = 2$.

Devido ao fato que a equação (1) para o caso particular em que $r = 2$ é a Curva Hermitiana (ver Subseção 1.1.1), conseguimos estender os resultados de Stichtenoth [28], de Kumar e Yang [17], para calcular distâncias mínimas exatas dos códigos definidos sobre as curvas com equação (1).

Além disso, calculamos também um subgrupo Σ do grupo de *Automorfismos* dos códigos propostos devido a sua utilidade na construção de códigos equivalentes e na implementação de algoritmos de decodificação.

Em [31], Wei introduz a noção de *pesos generalizados de Hamming* e o *peso hierárquico* de um código linear, mostrando que o peso hierárquico de um código linear caracteriza o desempenho do código sobre o canal de comunicação *Wire-Tap* do Tipo II. Em outras palavras, o peso hierárquico de um código determina o nível de equivocação que um *intruso*, ou usuário não autorizado, pode ter ao adquirir parte da informação transmitida com respeito a mensagem original. Para um código $C \subseteq F_q^n$ de dimensão k, o r-ésimo peso generalizado de Hamming é definido por

$$d_r(C) = \min\{|\chi(D)| : D \subseteq C \text{ é subcódigo de dimensão } r\},$$

onde $\chi(D) = \{i : \exists\ (c_1, \ldots, c_n) \in D \text{ com } c_i \neq 0\}$ é chamado o suporte do subcódigo D, e o peso hierárquico é a seqüência $\{d_1, \ldots, d_k\}$. Em [13], Guruswami fornece uma relação para códigos binários entre os pesos generalizados de Hamming e a Lista de Decodificação da mensagem recebida com erros. Esta relação esta descrita na seguinte figura:

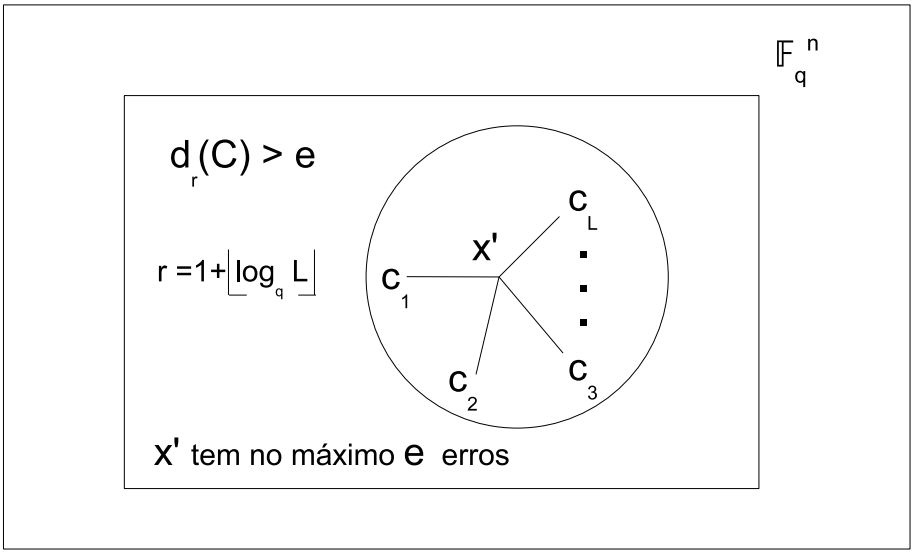


Figura 2: Interpretação do r-ésimo peso de Hamming

Assim, dado C um código linear, se $d_r(C) > e$ onde $r = 1 + \lfloor \log_2 L \rfloor$ então para qualquer palavra recebida, com no máximo e erros conhecidos sua posição, o número de palavras do código coerentes com a palavra recebida é no máximo L.

Seguindo a idéia de Kumar, Stichtenoth e Yang [18], e de Munuera [21], obtemos resultados exatos para o segundo peso generalizado de Hamming, assim como algumas cotas para d_r com $1 \leq r \leq k$. Devido ao fato de não conhecermos a seqüência de gonalidade da curva (ver Definição 1.33), fica difícil apresentar os valores exatos dos pesos generalizados de Hamming para todo r, $1 \leq r \leq k$.

Em 2003, Deolalikar apresenta uma subcobertura $E^1 = F(y_1)$ do corpo de funções $E = F(y)$, onde $F = \mathbb{F}_{q^3}(x)$, y satisfaz

$$y^{q^2} + y^q + y = x^{1+q} + x^{1+q^2} + x^{q+q^2}\,,$$

e y_1 satisfaz

$$y_1^q + (1 + b^{q^2-q})y_1 = x^{1+q} + x^{1+q^2} + x^{q+q^2}, \text{ com } b \in \mathbb{F}_{q^3} \text{ tal que } b^{q^2} + b^q + b = 0\,.$$

O objetivo deste exemplo foi mostrar que o quociente $N(E^1)/g_1(E^1) = 8.5$ era maior que o quociente $N(E)/g(E) = 5.5$. Devido a esta propriedade, o estudo das subextensões do corpo GH para qualquer valor de r é de grande importância para construir códigos com bons parâmetros.

A seguir, descrevemos sucintamente a organização deste trabalho.

O Capítulo 1 é dedicado à apresentação de conceitos relacionados com a Teoria de Códigos. Nele, introduzimos os códigos geométricos de Goppa que são baseados em conhecimentos de curvas algébricas e os códigos avaliados propostos por Høholdt, van Lint e Pellikaan [14], utilizando rudimentos de Álgebra Linear. Como exemplo e base do nosso trabalho estudamos os códigos Hermitianos, exemplo que desempenha um papel importante nas aplicações da teoria de códigos. Também apresentamos a noção de pesos generalizados de Hamming, assim como várias de suas propriedades que serão usadas em nossos cálculos. Damos a definição do conceito de *r-gonalidade*, importante na obtenção dos resultados sobre pesos generalizados de Hamming.

No Capítulo 2 encontram-se os resultados obtidos no trabalho dentre os quais destacamos: (1) O cálculo dos geradores do semigrupo de Weierstrass $H(Q_\infty)$ para todo $q \geq 2$ (Teorema 2.6), assim como a determinação de uma base para o espaço vetorial $\mathcal{L}(sQ_\infty)$. Desta forma, generalizamos os códigos propostos por Bulygin. (2) O cálculo das distâncias mínimas exatas para quase todos os valores em $H(Q_\infty)$ (Proposição 2.13) dos códigos propostos; (3) cotas para os pesos generalizados de Hamming dos códigos introduzidos (Seção 2.5). Em particular, o valor exato do segundo peso generalizado de Hamming para alguns valores

de $s \in H(Q_\infty)$. (4) Expressamos formulas explícitas para os subcorpos dos corpos GH e estudamos os códigos construídos sobre estes subcorpos (Seção 2.6).

No Capítulo 3 apresentamos conclusões do resultados conseguidos e propostas de pesquisa futuras a serem feitas.

CAPÍTULO 1

Preliminares

1.1 Códigos Geométricos de Goppa

Os códigos geométricos de Goppa formam uma subclasse especial da classe de códigos lineares, usados na correção de erros introduzidos na mensagem por usar um canal ruidoso. Aqui apresentamos fatos básicos, mas uma referência mais completa é [28].

Fixemos $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g, onde $\mathbb{F}_q$ é o corpo finito de q elementos. Sejam $P_1, \ldots, P_n$ lugares distintos dois a dois de $F/\mathbb{F}_q$ de grau 1, e G um divisor de $F/\mathbb{F}_q$ tal que $\mathrm{Sup}(G) \cap \mathrm{Sup}(D) = \emptyset$, onde $D = P_1 + \cdots + P_n$ e seja o espaço vetorial $\mathcal{L}(G) := \{f \in F : (f) + G \succeq\}$.

Definição 1.1. O código geométrico de Goppa (CGG) associado aos divisores D e G, denotado por $C_{\mathcal{L}}(D, G)$, é definido como a imagem da seguinte aplicação:

$$\alpha : f \in \mathcal{L}(G) \mapsto (f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n \,.$$

Note que a aplicação α está bem definida, pois como os lugares P_i tem grau 1 então $[F_{P_i} : \mathbb{F}_q] = 1$, onde $F_{P_i} := \mathcal{O}_{P_i}/P_i$ para $i = 1, \ldots, n$. Além disso, temos $v_{P_i}(f) \geq 0$ para $f \in \mathcal{L}(G)$, pois $\mathrm{Sup}(G) \cap \mathrm{Sup}(D) = \emptyset$. Então $f(P_i) \in \mathbb{F}_q$ para todo $i = 1, \ldots, n$.

Teorema 1.2. O código $C_{\mathcal{L}}(D, G)$ têm parâmetros $[n, k, d]$ dados por:

$$k = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D) \quad \text{e} \quad d \geq n - \deg(G).$$

Demonstração: A aplicação α é sobrejetora sobre sua imagem $C_{\mathcal{L}} := C_{\mathcal{L}}(D,G)$ e o núcleo desta aplicação é dada por

$$N(\alpha) = \{f \in \mathcal{L}(G) : v_{P_i}(f) > 0, i = 0, \ldots, n\} = \mathcal{L}(G - D),$$

assim tem-se que $\mathcal{L}(G)/\mathcal{L}(G-D) \cong C_{\mathcal{L}}(D,G)$, portanto $k = \dim \mathcal{L}(G) - \dim \mathcal{L}(G-D)$. Suponhamos $C_{\mathcal{L}} \neq 0$ e seja $d = w(\alpha(f))$ o peso de uma palavra para alguma função $f \in \mathcal{L}(G)$. De fato f existe, pois o subespaço linear é finito e pontual. Sendo assim, existem $n-d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}} \in \mathrm{Sup}(D)$ tal que $f(P_{i_j}) = 0$ e, conseqüêntemente $f \in \mathcal{L}(G - \{P_{i_1} + \cdots + P_{i_{n-d}}\})$, como $f \neq 0$ tem-se que $\deg(G - \{P_{i_1} + \cdots + P_{i_{n-d}}\}) \geq 0$ logo $d \geq n - \deg(G)$. □

Do teorema anterior podemos concluir que a menor distância mínima que um código C-$[n,k]$ pode ter é $d^* = n - \deg(G)$ que chamaremos de *distância mínima designada* do código $C_{\mathcal{L}}(D,G)$.

Corolário 1.3. Se $\deg(G) < n$ então:

1) A aplicação α é injetiva e o código $C_{\mathcal{L}}(D,G)$ é $[n,k,d]$ onde

$$d \geq n - \deg(G) \quad , \quad k = \dim \mathcal{L}(G) \geq \deg(G) + 1 - g.$$

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

2) Se $2g - 2 < \deg(G) < n$ então $k = \deg(G) + 1 - g$.

3) Se $\{f_1, \ldots, f_k\}$ é uma base de $\mathcal{L}(G)$ então a matriz M é uma matriz geradora do código $C_{\mathcal{L}}(D,G)$

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

Demonstração: Como $\deg(G-D) < 0$ segue-se que $\dim(\mathcal{L}(G-D)) = 0$ e desta forma concluímos que α é injetiva. Para o item (2), considerando $\deg(G) > 2g-2$ segue que $\dim(\mathcal{L}(W-G)) = 0$ e do Teorema de Riemman-Roch obtém-se que $k = \deg(G) + 1 - g$. O item (3) decorre da definição de base e do código. □

Exemplo 1.4. Seja $\mathcal{X}$ a curva irredutível de Fermat $x^3 + y^3 + z^3 = 0$ de gênero $g = 1$ sobre $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$ onde α é raiz do polinômio $x^2 + x + 1$ e $\bar{\alpha} := \alpha + 1$. Então temos que

$\mathcal{X}(\mathbb{F}_4) = \{Q = (0:1:1), P_1 = (0:\alpha:1), P_2 = (0:\bar{\alpha}:1), P_3 = (1:0:1), P_4 = (\alpha:0:1), P_5 = (\bar{\alpha}:0:1), P_6 = (1:1:0), P_7 = (\alpha:1:0), P_8 = (\bar{\alpha}:1:0)\}$. Escolhendo $D = P_1 + \cdots + P_8$ e $G = 2Q$, como $\mathrm{Sup}(D) \cap \mathrm{Sup}(G) = \emptyset$ então podemos definir o código $C_{\mathcal{L}}(D,G)$. Temos que $\mathcal{L}(2Q) = \left\langle 1, \frac{x}{y+z} \right\rangle$, pois $v_Q\left(\frac{x}{y+z}\right) = v_Q\left(\frac{x(y^2+yz+z^2)}{y^3+z^3}\right) = v_Q\left(\frac{y^2+yz+z^2}{x^2}\right) = -2$. A matriz geradora deste código é dada por:

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & \alpha & \bar{\alpha} & 1 & \alpha & \bar{\alpha} \end{pmatrix}$$

Para este código tem-se que $n = 8$, $k = 2$ e $d = 6$. Este tipo de código é chamado de código quase MDS (máxima distância de separação), pois $k + d = n$.

Teorema 1.5. [28, Teorema II.2.7] O código dual de $C_{\mathcal{L}}(D,G)$ é $(C_{\mathcal{L}}(D,G))^{\perp} = C_{\Omega} := C_{\Omega}(D,G)$ e têm parâmetros $[n,k',d']$ onde

$$k' = i(G-D) - i(G) \quad \text{e} \quad d' \geq \deg(G) - 2g + 2.$$

Além disso, se $\deg(G) > 2g-2$, então $k' = i(G-D) \geq n + g - 1 - \deg(G)$. Se $2g-2 < \deg(G) < n$ então temos a igualdade. O valor $d'^{*} = \deg(G) - 2g + 2$ é chamado distância mínima designada de Goppa para $C_{\Omega}(D,G)$.

1.1.1 Códigos Hermitianos

Nesta seção estudamos os códigos Hermitianos com alguns detalhes devido ao fato de que estes cálculos foram essenciais para os resultados obtidos neste trabalho. Os códigos Hermitianos são códigos geométricos de Goppa construídos a partir do corpo de funções Hermitianas sobre $\mathbb{F}_{q^2}$ (ver [28, Seção VII.4.]).

O corpo de funções algébricas Hermitiano H sobre $\mathbb{F}_{q^2}$ é representado por $H := \mathbb{F}_{q^2}(x,y)$ onde a curva Hermitiana tem equação afim

$$y^q + y = x^{q+1}. \tag{1.1}$$

O número de lugares de grau 1 de H é $N = q^3 + 1$, pois para cada $\alpha \in \mathbb{F}_{q^2}$ temos que $\alpha^{q+1} = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) \in \mathbb{F}_q$, onde $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}$ é a norma em $\mathbb{F}_{q^2}/\mathbb{F}_q$. Como o traço $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta) = \beta^q + \beta \in \mathbb{F}_q$ é uma aplicação linear sobrejetora de $\mathbb{F}_{q^2}$ em $\mathbb{F}_q$. Assim, tem-se que $\#(Tr^{-1}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha^{q+1})) = q$, logo existem $\beta_1, \ldots, \beta_q$ elementos distintos em $\mathbb{F}_{q^2}$ tal que os pontos (α, β_i) satisfazem

a equação (1.1). Portanto, tem-se q^3 elementos mais o ponto no infinito Q_∞. De [28, Proposição III.3.8(c)] temos que para cada $(\alpha, \beta) \in \mathcal{X}(\mathbb{F}_{q^2})$ está associado um único lugar $P_{\alpha,\beta}$ tal que $P_{\alpha,\beta}|P_\alpha$ de grau 1.

Como a curva que representa o corpo de funções Hermitianas é irredutível e não singular, então da teoria de curvas algébricas podemos dizer que seu gênero é:

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

Do feito acima vemos que a nossa curva é maximal, isto é, atinge a cota máxima de *Hasse-Weil*, pois o número de lugares de grau 1 é $N = q^2 + 1 + 2gq$.

Definição 1.6. Para $r \in \mathbb{N}_0$, definimos

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

onde $D = \sum_{i=1}^{q^3} P_i$ são todos os lugares de grau 1 menos Q_∞.

Se $r > q^3 + 2g - 2 = q^3 + q^2 - q - 2$ então temos da teoria já vista que $\dim(H_r) = k_r = \ell(rQ_\infty) - \ell(rQ_\infty - D) = r + 1 - g - (r - q^3 + 1 - g) = q^3 = n$, portanto $H_r = \mathbb{F}_{q^2}^{q^3}$ e a distância mínima $d = 1$, logo seriam códigos com máxima distância de separação (MDS), porém, nada bons pois seriam todas as palavras do alfabeto.

Logo, os códigos Hermitianos são interessantes para $0 \leq r \leq q^3 + 2g - 2$.

Proposição 1.7. [28, Proposição VII.4.2] O código dual de H_r é

$$H_r^\perp = H_{q^3+2g-2-r}$$

Demonstração: Seja $z = \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha) = x^{q^2} - x$. Então desta construção tem-se que a função z é um parâmetro local para todos os $P_i \in \mathrm{Sup}(D)$, pois $v_{P_i}(z) = 1$ para todo i, e $(z) = D - q^3 Q_\infty$. Como $dz = d(x^{q^2} - x) = -dx$ segue-se que $(dz) = (dx) = (2g-2)Q_\infty$, isto de [28, Lema VI.4.4]. Assim de [28, Teorema II.2.8] obtemos que o divisor da diferencial $\eta = \frac{1}{z} dz$ satisfaz:

$$H_r^\perp = C_\Omega(D, rQ_\infty) = C_{\mathcal{L}}(D, D - rQ_\infty + (dz) - (z)) = H_{q^3+2g-2-r}\,.$$

□

Para determinar os parâmetros dos códigos H_r com $0 \leq r \leq q^3 + 2g - 2$, descrevemos o espaço de funções $\mathcal{L}(rQ_\infty)$.

Sabemos que $f \in \mathcal{L}(rQ_\infty)$ se, e somente se, o único pólo da função f é Q_∞, e sua ordem é menor que r. Tais funções estão fortemente ligadas ao semigrupo de Weierstrass $H(Q_\infty)$ de Q_∞ em H.

Proposição 1.8. O semigrupo de Weierstrass de Q_∞ no corpo de funções hermitianas é

$$H(Q_\infty) = \langle q, q+1 \rangle .$$

Demonstração: Como q e $q+1$ são coprimos, e da equação (1.1) tem-se que $v_{Q_\infty}(x) = -q$ e $v_{Q_\infty}(y) = -(q+1)$, logo $\langle q, q+1 \rangle \subseteq H(Q_\infty)$. Agora tomando o complementar desses dois conjuntos temos que $\mathbb{N} \setminus H(Q_\infty) \subseteq \langle q, q+1 \rangle^C$, como $\langle q, q+1 \rangle$ é um semigrupo numérico sabemos que o número de elementos do complementar é $\frac{q(q-1)}{2}$ e pelo teorema das lacunas de Weierstrass segue-se que o número de elementos do complementar de $H(Q_\infty)$ é o gênero da curva $g = \frac{q(q-1)}{2}$, o que mostra a igualdade. □

Pela proposição acima podemos ver que as funções com pólo apenas em Q_∞ são combinações de elementos da forma $x^i y^j$. Assim, tem-se que

$$\mathcal{L}(rQ_\infty) = \left\langle x^i y^j \,|\, iq + j(q+1) \leq r, 0 \leq i, 0 \leq j \leq q-1 \right\rangle .$$

Definimos o conjunto $I(s) = \{n \in H(Q_\infty) : n \leq s\}$, logo $\dim(\mathcal{L}(sQ_\infty)) = |I(s)|$.

Proposição 1.9. Suponhamos que $0 \leq r \leq q^3 + q^2 - q - 2$. Então

1. A dimensão de H_r é dada por

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

   onde $s = q^3 + q^2 - q - 2 - r$.

2. A distância mínima de H_r satisfaz $d \geq q^3 - r$. Se $0 \leq r \leq q^3$ e os números r e $q^3 - r$ são pólos de Q_∞, então

$$d = q^3 - r.$$

Demonstração: (a) Para $0 \leq r < q^3$ sabemos que

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

Para $q^3 \leq r \leq q^3 + q^2 - q - 2$ seja $s = q^3 + q^2 - q - 2 - r$. Então $0 \leq s \leq q^2 - q - 2 < q^3$, logo da proposição (1.7) obtemos que

$$\dim(H_r) = q^3 - \dim(H_s) = q^3 - |I(s)| .$$

(b) Para códigos lineares tem-se que a distância mínima satisfaz $d \geq n - \deg(G) = q^3 - r$. Agora para mostrar a igualdade vamos dividir a demonstração em três casos. A idéia vai ser construir palavras do código tal que o peso de cada palavra seja $q^3 - r$.

Caso 1. $r = q^3 - q^2$. Sejam $\alpha_i \in \mathbb{F}_{q^2}$ com $i = 1, \ldots, q^2 - q$ elementos distintos. Assim

$$z = \prod_{i=1}^{q^2-q} (x - \alpha_i) \in \mathcal{L}(rQ_\infty),$$

pois os zeros são exatamente $q(q^2 - q) = r$ pontos do suporte de D e o peso da palavra codificada correspondente é $w(\alpha(z)) = q^3 - r$, portanto $d = q^3 - r$.

Caso 2. $r < q^3 - q^2$. Como $r \in H(Q_\infty)$, pode-se escrever então que $r = iq + j(q+1)$, com $i \geq 0$ e $0 \leq j \leq q - 1$. Logo, tem-se que $i \leq q^2 - q - 1$. Fixemos $\gamma \in \mathbb{F}_q \setminus \{0\}$, e seja $A = \{\alpha \in \mathbb{F}_{q^2} : \alpha^{q+1} \neq \gamma\}$. Portanto $|A| = q^2 - (q+1)$, logo defina

$$z_1 := \prod_{j=1}^{i} (x - \alpha_j) \qquad \alpha_j \in A,\ \alpha_j \neq \alpha_k.$$

esta função tem iq zeros distintos no suporte de D. Agora, escolha os elementos $\beta_1, \ldots, \beta_j \in \mathbb{F}_{q^2}$ tais que $\beta_\mu^q + \beta_\mu = \gamma$ e defina

$$z_2 := \prod_{k=1}^{j} (y - \beta_k)\,.$$

Esta função tem $j(q+1)$ zeros distintos dos zeros de z_1 por construção. Logo $z = z_1 z_2 \in \mathcal{L}(G)$ tem r zeros distintos, portanto o peso de $w(\alpha(z)) = q^3 - r$ e conseqüêntemente $d = q^3 - r$.

Caso 3. $q^3 - q^2 < r < q^3$. Seja $s = q^3 - r$ então $0 < s < q^3 - q^2$, logo existe $z \in \mathcal{L}(sQ_\infty)$ tal que tem $q^3 - s = r$ zeros distintos no suporte de D. Assim, $\mathrm{div}(z) = D' - sQ_\infty$ onde $0 \preceq D' \preceq D$ e $\deg(D') = s$. Seja $u = x^{q^2} - x$, então $\mathrm{div}(u) = D - Q_\infty$, assim $\mathrm{div}(z^{-1}u) = \mathrm{div}(u) - \mathrm{div}(z) = \bar{D} - rQ_\infty \in \mathcal{L}(G)$. Portanto, tem-se que o peso é $w(\alpha(z^{-1}u)) = q^3 - r$, donde conclui-se que $d = q^3 - r$. □

1.2 Códigos Avaliados

Aqui veremos os chamados *códigos avaliados* e sua importante conexão com os códigos de Goppa pontuais. Esta seção é introduzida com o intuito de preparar-nos para definir a

distância mínima de Feng-Rao δ_{FR}, e assim entender os resultados equivalentes de Kirfel e Pellikaan para semigrupos telescópicos enunciados neste trabalho (ver Proposições (2.25),(2.26)). Para maiores detalhes pode-se referir a [14].

Seja $K(\mathcal{X})$ o corpo de funções de uma curva $\mathcal{X}$ irredutível e não singular sobre K. Seja P um ponto K-racional. Seja

$$\mathbf{R} := R(P) = \bigcap_{Q \neq P} \mathcal{O}_Q,$$

uma K-álgebra, onde $\mathcal{O}_Q$ é o anel local de $K(\mathcal{X})$ no ponto Q. Seja υ_P a valorização em P. Portanto, $\upsilon_P(f) < 0$ para todo f não nulo em $\mathbf{R}$. Definimos $\rho(f) := -\upsilon_P(f)$ para $f \in \mathbf{R}$. Pelas propriedades de valorização discreta temos, como conseqüência, as seguintes propriedades que definem uma **função peso** sobre $\mathbf{R}$.

Em geral, $\mathbf{R}$ pode ser uma K-álgebra qualquer.

Definição 1.10. Seja $\mathbf{R}$ uma K-álgebra. Uma função $\rho : \mathbf{R} \to \mathbb{N}_0 \cup \{-\infty\}$ é chamada uma **função ordem** sobre $\mathbf{R}$ se as seguintes propriedades são satisfeitas. Sejam $r, g, h \in \mathbf{R}$.

1. $\rho(f) = -\infty$ se, e somente se, $f = 0$;
2. Para $\lambda \in K^*$, $\rho(\lambda f) = \rho(f)$;
3. $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$, e a igualdade vale sempre que $\rho(f) \neq \rho(g)$;
4. Se $\rho(f) < \rho(g)$ e $h \neq 0$, então $\rho(fh) < \rho(gh)$;
5. Se $\rho(f) = \rho(g) \neq 0$, então existe $\lambda \in K^*$ tal que $\rho(f - \lambda g) < \rho(g)$.

   A função ρ é chamada uma **função peso** sobre $\mathbf{R}$, se além de satisfazer as propriedades $(1) - (5)$ também satisfaz:

6. $\rho(fg) = \rho(f) + \rho(g)$.

Observação 1.11. Acima podemos ver que $\rho(\mathbf{R}^*) = H(P)$ onde $\mathbf{R}^* = \mathbf{R} - \{\mathbf{0}\}$ e $H(P)$ é o semigrupo de Weierstrass no ponto P.

Agora veremos que a existência de funções ordem sobre $\mathbf{R}$ está ligada à existência de certas K-bases de $\mathbf{R}$. O próximo teorema nos mostra que se existe uma função ordem sobre uma certa K-álgebra $\mathbf{R}$, então existe uma K-base de $\mathbf{R}$, $\mathbf{R}$ visto como K-espaço vetorial, com certas propriedades. Tal base nos permite construir os chamados códigos avaliados e suas respectivas propriedades serão de fundamental importância para a determinação da cota Feng-Rao δ_{FR}.

Teorema 1.12. Seja $\mathbf{R}$ uma K-álgebra com função ordem ρ. Suponha que $\mathbf{R} \neq \mathbf{K}$.

1. Então existe uma base $\{f_i : i \in \mathbb{N}\}$ de $\mathbf{R}$ sobre K tal que $\rho(f_i) < \rho(f_{i+1})$ para todo i.
2. Se $f \in \mathbf{R}$ e $f = \lambda_1 f_1 + \cdots + \lambda_i f_i$, onde $\lambda_1, \ldots, \lambda_i \in K$ e $\lambda_i \neq 0$, então $\rho(f) = \rho(f_i)$.
3. Seja $\ell(i,j) := \ell$ tal que $\rho(f_i f_j) = \rho(f_\ell)$. Assim, $\ell(i,j) < \ell(i+1,j)$ para todo i e j.
4. Seja $\rho_i := \rho(f_i)$. Se ρ é uma função peso, então $\rho_{\ell(i,j)} = \rho_i + \rho_j$.

Seja $\mathbf{R} = R(P)$, P um ponto $\mathbb{F}_q$-racional. Agora, tome $P_1, \ldots, P_n$ pontos, distintos dois a dois, $\mathbb{F}_q$-racionais de $\mathcal{X}$ diferentes de P e considere o divisor $D := P_1 + \cdots + P_n$. Sejam $(f_i : i \in \mathbb{N})$ base de $\mathbf{R}$ tal que $\rho_i := \rho(f_i) < \rho(f_{i+1}) =: \rho_{i+1}$. Da observação (1.11) segue que $H(P) = \{\rho_i : i \in \mathbb{N}\}$ é o semigrupo de Weierstrass de P. Como $\mathcal{L}(\rho_\ell P) = \{f \in \mathbf{R} : \rho(f) \leq \rho_\ell\}$, então os elementos da base de $\mathbf{R}$ que estão em $\mathcal{L}(\rho_\ell P)$ formam uma $\mathbb{F}_q$-base de $\mathcal{L}(\rho_\ell P)$. Portanto, $\mathcal{L}(\rho_\ell P) = \langle f_1, \ldots, f_\ell \rangle = L_\ell$. Assim, definimos a aplicação avaliação

$$av_{\mathcal{P}} : \mathbf{R} \to \mathbb{F}_q^n,$$

dada por $av_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$.

Então o código avaliado E_ℓ e seu dual C_ℓ são dados por

$$E_\ell := av_{\mathcal{P}}(L_\ell) = av_{\mathcal{P}}(\mathcal{L}(\rho_\ell P)) = C(D, \rho_\ell P),$$

onde $C(D, \rho_\ell P)$ denota o *código geométrico de Goppa* associado aos divisores D e $\rho_\ell P$,e

$$C_\ell := E_\ell^\perp = C(D, \rho_\ell P)^\perp = C_\Omega(D, \rho_\ell P),$$

onde a última igualdade vem do Teorema 1.5.

A seqüência de códigos $(E_\ell : \ell \in \mathbb{N})$ é crescente com respeito à inclusão e todos eles são subespaços de $\mathbb{F}_q^n$. Logo, existe um N natural tal que $E_\ell = E_N$ para todo $\ell \geq N$. Naturalmente, $E_N = av_{\mathcal{P}}(\mathbf{R})$. Seja $h_i := av_{\mathcal{P}}(f_i)$ para todo $i \leq N$.

1.2.1 Distância mínima de Feng-Rao

A seguir construiremos a cota inferior para a distância mínima d_ℓ de C_ℓ, chamada de *distância mínima de Feng-Rao, denotada por* $\delta_{FR}(\ell)$. Pelo feito acima, esta cota será uma cota inferior para distância mínima d_ℓ de $C_\Omega(D, \rho_\ell P)$. Goppa mostrou que neste caso

$$d_\ell \geq \rho_\ell - (2g - 2),$$

onde g denota o gênero da curva $\mathcal{X}$. No exemplo (2.28) vemos que para alguns valores de ℓ a cota $\delta_{FR}(\ell)$ é melhor do que a cota de Goppa. Mais precisamente, temos

$$d_\ell \geq \delta_{FR}(\ell) \geq \rho_\ell - (2g-2).$$

Agora vamos trilhar o caminho que fornecerá $\delta_{FR}(\ell)$. Para isto, recordamos que $h_i = av_{\mathcal{P}}(f_i)$ para todo $i \leq N$ e $E_\ell = E_N = av_{\mathcal{P}}(\mathbf{R})$ para todo $\ell \geq N$. Seja $\mathbf{H}$ a matriz $N \times n$ cuja i-ésima linha é dada pelo vetor h_i. Se $av_{\mathcal{P}}$ não é sobrejetora então $\mathbf{H}$ não gera $\mathbb{F}_q^n$. Nesta situação, sejam $h_{N+1}, \ldots, h_{N+t}$ em $\mathbb{F}_q^n$ e $\tilde{\mathbf{H}}$ a matriz $(N+t) \times n$ obtida acrescentando os vetores $h_{N+1}, \ldots, h_{N+t}$ abaixo da última linha de $\mathbf{H}$, de forma que $\tilde{\mathbf{H}}$ gera $\mathbb{F}_q^n$. Para $y \in \mathbb{F}_q^n$ considere as matrizes $\tilde{\mathbf{S}}(y)$ e $\mathbf{S}(y)$ das *síndromes* de y dadas por

$$\tilde{\mathbf{S}}(y) = (s_{ij}(y) : 1 \leq i,j \leq N+t) \text{ e } \mathbf{S}(y) = (s_{ij}(y) : 1 \leq i,j \leq N) ,$$

tal que $s_{ij}(y) := y \cdot (h_i * h_j)$, onde para $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$ é definido o produto $a * b := (a_1 b_1, \ldots, a_n b_n)$. Assim, $\mathbf{S}(y)$ é uma submatriz de $\tilde{\mathbf{S}}(y)$ e, portanto, $posto\,(\mathbf{S}(y)) \leq posto\left(\tilde{\mathbf{S}}(y)\right)$. O próximo resultado nos mostra uma relação entre o peso de um elemento $y \in \mathbb{F}_q^n$, denotado por $\omega(y)$, com o posto das matrizes acima construídas.

Lema 1.13. Seja $y \in \mathbb{F}_q^n$ e $D(y)$ a matriz diagonal com y na diagonal. Então

$$\tilde{\mathbf{S}}(y) = \tilde{\mathbf{H}} D(y) \tilde{\mathbf{H}}^{\mathbf{T}} \text{ e } \omega(y) = (\tilde{\mathbf{S}}(y)) \geq posto\,(\mathbf{S}(y)) .$$

Observação 1.14. Em [14], os autores trabalham a todo momento com a hipótese de que $av_{\mathcal{P}}$ seja sobrejetora. Neste caso, $\tilde{\mathbf{H}} = \mathbf{H}$ e $\tilde{\mathbf{S}}(y) = \mathbf{S}(y)$. Na verdade, eles provaram o lema acima nesta situação específica. Mas isso não trará nenhum problema pois a demonstração é exatamente a mesma para $\tilde{\mathbf{S}}(y)$ e $\tilde{\mathbf{H}}$. O que mais importa é que $\omega(y) \geq posto\,(\mathbf{S}(y))$ sendo $av_{\mathcal{P}}$ sobrejetora ou não.

O lema abaixo vale apenas para os elementos de $\mathbf{S}(y)$.

Lema 1.15. [14, Proposição 4.9]

1. Se $y \in C_\ell$, e $\ell(i,j) \leq \ell$ então $s_{ij}(y) = 0$;

2. Se $y \in C_\ell \setminus C_{\ell+1}$ e $\ell(i,j) = \ell + 1$, então $s_{ij}(y) \neq 0$.

Para $\ell \in \mathbb{N}_0$ considere as seguintes definições:

$$\begin{aligned} N_\ell &:= \{(i,j) \in \mathbb{N}^2 : \ell(i,j) = \ell + 1\}; \\ \nu_\ell &:= \#N_\ell \ . \end{aligned}$$

Se ρ é uma função peso, então

$$N_\ell = \{(i,j) \in \mathbb{N}_0^2 : \rho(f_i) + \rho(f_j) = \rho(f_{\ell+1})\} \, .$$

Uma outra forma de descrever este conjunto é

$$N_\ell = \{\rho_i \in H(P) : \exists \ \rho_j \in H(P) \text{ tais que } \rho_i + \rho_j = \rho_{\ell+1}\} \, .$$

O lema anterior prova o seguinte resultado. Este por sua vez, só pode ser aplicado para os valores de ℓ tais que $\ell + 1 \leq N$.

Proposição 1.16. [14, Proposição 4.11] Se $y \in C_\ell \setminus C_{\ell+1}$ então $\omega(y) \geq \nu_\ell$.

A seguir enunciamos o resultado principal desta seção. Este é consequência da Proposição 1.16. Para isto, considere o seguinte número:

$$\delta_{FR}(\ell) := Min\{\nu_m : m \geq \ell\} \ .$$

Teorema 1.17. [14, Teorema 4.13] O número $\delta_{FR}(\ell)$ é cota inferior para a distância mínima de C_ℓ, ou seja,

$$d(C_\ell) \geq \delta_{FR}(\ell) \ .$$

Teorema 1.18. [14, Teorema 5.24] Temos que

$$\delta_{FR}(\ell) \geq d_G(\ell) = \rho_\ell - (2g-2) \ ,$$

onde $d_G(\ell)$ é a distância mínima designada de Goppa do código $C_\Omega(D, \rho_\ell P)$.

Exemplo 1.19. [14, Exemplo 4.17] Seja a curva Hermitiana $Y^4+Y = X^5$ sobre $\mathbb{F}_{16}$ de gênero 6. Seja $\mathbf{R}$ a $\mathbb{F}_{16}$-álgebra dada por $\mathbf{R} = \mathbb{F}_{16}[X,Y]/(Y^4+Y-X^5)$. Então $\mathbf{R}$ tem $\{x^\alpha y^\beta : \alpha < 5\}$ como base e $\rho(x^\alpha y^\beta) = 4\alpha + 5\beta$ dá uma função peso sobre $\mathbf{R}$. Neste caso, para qualquer ponto $\mathbb{F}_{16}$-racional é sabido que seu semigrupo de Weierstrass é $\{0,4,5,8,9,10,12,13,\ldots\}$.

Em particular, para $P = (0 : 1 : 0)$ temos que $\mathbf{R} = R(P)$. A tabela abaixo nos fornece uma lista dos valores de $\rho_\ell, \nu_\ell, d(\ell)$ e $d_G(\ell)$ onde $1 \leq \ell \leq 16$.

ℓ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ρ_ℓ	0	4	5	8	9	10	12	13	14	15	16	17	18	19	20	21
ν_ℓ	2	2	3	4	3	4	6	6	4	5	8	9	8	9	10	12
$d(\ell)$	2	2	3	3	3	4	4	4	4	5	8	8	8	9	10	12
$d_G(\ell)$	-10	-6	-5	-2	-1	0	2	3	4	5	6	7	8	9	10	11

Temos também que $d(\ell) = \nu_\ell = \ell - 5 = d_G(\ell)$, para todo $\ell > 16$.

1.3 Automorfismos de Códigos

O grupo simétrico S_n (seus elementos são permutações do conjunto $\{1, \ldots, n\}$) age sobre o espaço vetorial $\mathbb{F}_q^n$ via

$$\pi(c_1, \ldots, c_n) := (c_{\pi(1)}, \ldots, c_{\pi(n)}),$$

para $\pi \in S_n$ e $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$. A seguir damos a definição de automorfismo para um código (ver [28, Seção VII.3]).

Definição 1.20. O grupo de automorfismos de um código linear $C \subseteq \mathbb{F}_q^n$ é definido por

$$Aut(C) := \{\pi \in S_n : \pi(C) = C\}.$$

Claramente, $Aut(C)$ é um subgrupo de S_n. Nesta seção, veremos automorfismos de códigos geométricos de Goppa que são induzidos por automorfismos do correspondente corpo de funções.

Definição 1.21. Seja $F/\mathbb{F}_q$ um corpo de funções e $Aut(F/\mathbb{F}_q)$ o grupo de automorfismos de F sobre $\mathbb{F}_q$. Sejam D e G divisores associados a um código geométrico de Goppa. Então

$$Aut_{D,G}(F/\mathbb{F}_q) := \{\sigma \in Aut(F/\mathbb{F}_q) : \sigma(D) = D \text{ e } \sigma(G) = G\}.$$

A razão pela qual a Definição 1.21 é útil está dada na seguinte proposição.

Proposição 1.22. [28, Proposição VII.3.3]

1. $Aut_{D,G}(F/\mathbb{F}_q)$ age sobre o código $C_{\mathcal{L}}(D,G)$ por

$$\sigma((x(P_1),\ldots,x(P_n))) := (x(\sigma(P_1)),\ldots,x(\sigma(P_n)))\,,$$

para $x \in \mathcal{L}(G)$. Isto produz um homomorfismo de $Aut_{D,G}(F/\mathbb{F}_q)$ em $Aut(C_{\mathcal{L}}(D,G))$.

2. Se $n > 2g+2$, então elementos diferentes de $Aut_{D,G}(F/\mathbb{F}_q)$ induzem diferentes automorfismos de $C_{\mathcal{L}}(D,G)$. Portanto, para $n > 2g+2$ identificamos $Aut_{D,G}(F/\mathbb{F}_q)$ com um subgrupo de $Aut(C_{\mathcal{L}}(D,G))$.

Os seguintes lemas são fatos básicos concernientes à ação de $Aut(F/\mathbb{F}_q)$ sobre códigos e os espaços $\mathcal{L}(G)$ para certos divisores G.

Lema 1.23. [33, Lema 2.7] Para todo $\sigma \in Aut(F/\mathbb{F}_q)$ temos que

$$C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(\sigma(D),\sigma(G))\,.$$

Lema 1.24. [33, Lema 2.8] Seja $\sigma \in Aut(F/\mathbb{F}_q)$. Seja $G = kP \succ 0$ um divisor de F com $\dim(G) > 1$. Se $\sigma(\mathcal{L}(G)) = \mathcal{L}(G)$ então $\sigma(G) = G$.

O cálculo do grupo de automorfismos de um código geométrico de Goppa é essencial para construir códigos equivalentes e também podem ser usados para a implementação de certos algoritmos de decodificação.

1.4 Pesos Generalizados de Hamming

Em [31], Wei introduz a noção de *pesos generalizados de Hamming* e o *peso hierárquico* de um código linear, mostrando que o peso hierárquico de um código linear caracteriza o desempenho do código sobre certo canal de comunicação. Seja C um $[n,k]$ código linear. Definimos o *suporte* de C como sendo:

$$\chi(C) := \{i |\, \exists\, (c_1,\ldots,c_n) \in C \ \text{ com } \ c_i \neq 0\}\,.$$

Definição 1.25. Seja $1 \leq r \leq k$. O *r-ésimo peso generalizado de Hamming* de C é definido por

$$d_r(C) := \min\{|\chi(D)| : D \text{ é subcódigo de } C \text{ de dimensão } r\}\,.$$

Exemplo 1.26. Seja o código $C = \{(0000), (1000), (0100), (1100)\}$ de dimensão $k = 2$. $D_1 = \{(0000),\ (1000)\}$, $D_2 = \{(0000), (0100)\}$, $D_3 = \{(0000), (1100)\}$ são subcódigos de C de dimensão 1. Então $\chi(D_1) = \{1\}$, $\chi(D_2) = \{2\}$, $D_3 = \{(0000),\ (1100)\} = \{1, 2\}$, $d_1(C) = 1$ e $d_2(C) = 2$.

Definição 1.27. O *peso hierárquico* de um código linear é o conjunto de números inteiros

$$\{d_r(C) : 1 \leq r \leq k\}.$$

Observação 1.28. Em particular, $d_1(C)$ é a distância mínima de Hamming do código C.

O peso hierárquico de vários códigos lineares tem sido estudado, incluindo os códigos BCH, Goppa [7], e códigos produto [32]. Em [18], Kumar, Stichtenoth e Yang mostraram uma cota inferior sobre os pesos de Hamming generalizados similar a cota inferior da distância mínima de Goppa. Também mostraram uma cota superior para os pesos de Hamming generalizados de códigos Hermitianos para alguns casos especiais.

A seguir enunciamos algumas propriedades básicas desses pesos.

Teorema 1.29. [Monotonicidade] Para C um $[n, k]$ código linear, temos:

$$0 < d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Demonstração: Da definição temos que $d_{r-1}(C) \leq d_r(C)$ para todo r. Para a desigualdade estrita, seja D um subcódigo de C de dimensão r tal que $|\chi(D)| = d_r(C)$. Escolha $i \in \chi(D)$ e defina $D_i := \{c \in D : c_i = 0\}$. Assim, da construção tem-se que a dimensão de D_i é $r - 1$ e

$$d_{r-1}(C) \leq |\chi(D_i)| \leq |\chi(D)| - 1 = d_r(C) - 1.$$

□

Corolário 1.30. [Cota Generalizada de Singleton] Seja C um $[n, k]$ código linear e para $1 \leq r \leq k$, temos que:

$$d_r(C) \leq n - k + r.$$

(Quando $r = 1$ é a cota de Singleton)

Proposição 1.31. [Dualidade] Seja C um $[n, k]$ código linear e $C^\perp$ seu dual. Então,

$$\{d_r(C) : 1 \leq r \leq k\} = \{1, 2, \ldots, n\} \setminus \{n + 1 - d_r(C^\perp)\}.$$

Demonstração: Ver [31]. □

Corolário 1.32. Seja $C_{\mathcal{L}}(D,G)$ o código geométrico de Goppa. Se $\deg(G) > 2g-2$, então

$$d_r(C) = n - k + r, \quad \text{para } g+1 \leq r \leq k,$$

onde k é a dimensão de $C_{\mathcal{L}}(D,G)$.

Demonstração: Do Teorema (1.5) temos que $d_1(C^{\perp}) \geq \deg(G) - (2g-2)$. Da proposição (1.31) segue que

$$d_{k-i}(C_{\mathcal{L}}(D,G)) = n - i,$$

para $0 \leq i \leq \deg(G) - 2g$. Se $\deg(G) > 2g-2$, então $k \leq \dim(\mathcal{L}(G)) = \deg(G) + 1 - g$, e daí que $k - (\deg(G) - 2g) \leq g+1$, logo para $r = k - i$ obtemos o resultado. □

Agora introduzimos o conceito de *seqüência de gonalidade*, com o objetivo de melhorar a cota inferior para os pesos generalizados de Hamming (ver [21]).

Definição 1.33. Seja F/K um corpo de funções algébricas com corpo constante K, e $\mathcal{D}_F$ o conjunto de todos os divisores de F/K. Para $r \geq 1$ definimos a r-gonalidade como

$$\gamma_r = \min\{\deg(A) : A \in \mathcal{D}_F \, \text{e} \, \ell(A) \geq r\}.$$

A seqüência $SG(F) = \{\gamma_r : r \geq 1\}$ é chamada a *seqüência de gonalidade* de F/K.

As seguintes propriedades são satisfeitas [18]:

- $0 = \gamma_1 < \gamma_2 < \cdots < \gamma_r < \gamma_{r+1} < \cdots$
- $\gamma_r = r + g - 1$, para $r > g$, onde g é o gênero do corpo F/K.
- $\gamma_g = 2g-2$ e $\gamma_r \geq 2(r-1)$ para todo r tal que $1 \leq r \leq g$.

Proposição 1.34. [23, Proposição 2.8] Suponhamos $F/K \neq 0$. Então

1. $a \in SG(F)$ se, e somente se, $2g - 1 - a \notin SG(F)$;
2. Para $i = 1, \ldots, g$ temos que

$$\gamma_{g-\gamma_i+i-1} < 2g - 1 - \gamma_i < \gamma_{g-\gamma_i+i}.$$

O seguinte teorema dá uma cota inferior para os pesos generalizados de Hamming usando a seqüência de gonalidade do corpo de funções algébricas.

Teorema 1.35. [18, Teorema 12] Para o CGG $C_{\mathcal{L}}(D,G)$ temos que

$$d_r(C_{\mathcal{L}}(D,G)) \geq n - \deg(G) + \gamma_r, \quad \text{para } 1 \leq r \leq k,$$

onde $k = \dim(C_{\mathcal{L}}(D,G))$.

A seguir definimos a *abundância* de um código geométrico de Goppa.

Definição 1.36. Seja $C_{\mathcal{L}}(D,G)$ um CGG. O número $a = \ell(G-D)$ é chamado de abundância do código.

Como no caso da distância mínima d_1, o r-ésimo peso generalizado de Hamming tem uma interpretação aritmética correspondente à aritmética da curva.

Teorema 1.37. [21, Teorema 1] Seja $C = C_{\mathcal{L}}(D,G)$ um código linear de abundância $a \geq 0$.

a) Se $d_r(C) = d$, então existem $n-d$ pontos distintos $P_{d+1}, \ldots, P_n$ tal que $\ell(G - P_{d+1} - \cdots - P_n) \geq r + a$;

b) Se existem $n-d$ pontos distintos $P_{d+1}, \ldots, P_n$ tal que $\ell(G - P_{d+1} - \cdots - P_n) \geq r + a$, então $d_r(C) \leq d$.

Demonstração: a) Se $d_r(C) = d$ então existe um subcódigo V_r de C de dimensão r e com d elementos no suporte. Seja $V_r = \langle \alpha(f_1), \ldots, \alpha(f_r) \rangle$. Assim, $f_1, \ldots, f_r$ são funções independentes que se anulam em $P_{d+1}, \ldots, P_n$, n-d pontos distintos. Logo, $f_1, \ldots, f_r \in \mathcal{L}(G - P_{d+1} - \cdots - P_n) \setminus \mathcal{L}(G-D)$, assim, se $\{\phi_1, \ldots, \phi_a\}$ é uma base de $\mathcal{L}(G-D)$ então o conjunto $\{\phi_1, \ldots, \phi_a, f_1, \ldots, f_r\}$ é independente, portanto $\ell(G - P_{d+1} - \cdots - P_n) \geq r + a$.
b) Seja $\{\phi_1, \ldots, \phi_a\}$ uma base de $\mathcal{L}(G-D)$. Pode-se estender esta para uma base $\{\phi_1, \ldots, \phi_a, f_1, \ldots, f_r, \ldots\}$ de $\mathcal{L}(G - P_{d+1} - \cdots - P_n)$. Seja $V_r = \langle \alpha(f_1), \ldots, \ \alpha(f_r) \rangle$, assim, $\chi(V_r) \leq d$ e $\dim(V_r) = r$. □

Corolário 1.38. [21, Corolário 1] Seja $C = C_{\mathcal{L}}(D,G)$ um código de dimensão k e abundância $a \geq 0$. Então para todo r, $1 \leq r \leq k$

$$d_r(C) = \min\{\deg(D') : 0 \preceq D' \preceq D, \ell(G - D + D') \geq r + a\},$$

$$d_r(C) = \min\{n - \deg(D'') : 0 \preceq D'' \preceq D, \ell(G - D'') \geq r + a\}.$$

Proposição 1.39. [21, Proposição 6] Seja $C = C_{\mathcal{L}}(D, G)$ um código de dimensão k e abundância $a > 0$. Então, para $1 \leq r \leq k$, temos que $d_r(C) \leq \deg(D')$ para todo divisor efetivo $D' \preceq D$ tal que $\ell(D') > r$.

Demonstração: Como $\ell(D') + \ell(G - D) \leq \ell(G - D + D') + 1$, se $D'' = D - D'$, temos que $\ell(G - D'') \geq r + \ell(G - D)$, e o resultado segue do corolário (1.38). □

Proposição 1.40. [21, Colorário 2] Seja $C = C_{\mathcal{L}}(D, G)$ um $[n, k]$ código linear de abundância $a \geq 0$. Então para todo r, $1 \leq r \leq k$ temos que:

a) $d_r(C) \geq n - \deg(G) + \gamma_{r+a}$;

b) Se $r + a > g$, então $d_r(C) = n - k + r$;

c) Se $r + a = g$, então $d_r(C) = n - k + r$ ou $d_r(C) = n - k + r - 1$.

A proposição a seguir é um resultado importante no cálculo dos pesos de Hamming generalizados do código.

Proposição 1.41. [21, Proposição 4] Se $C_m = C_{\mathcal{L}}(D, mQ_\infty)$ um $[n, k]$ código linear de abundância $a \geq 0$. Seja $\rho_{r+a} \in H(Q_\infty)$. Então para todo r, $1 \leq r \leq k$ temos que:

$$d_r(C_m) \leq d_1(C_{\mathcal{L}}(D, (m - \rho_{r+a})Q_\infty)).$$

Observação 1.42. Como $\ell(\rho_{r+a}Q_\infty) \leq \ell(mQ_\infty)$, pois $r + a \leq k + a$, então é possível considerar o código $C_{m-\rho_{r+a}} = C_{\mathcal{L}}(D, (m - \rho_{r+a})Q_\infty)$ na proposição 1.41.

CAPÍTULO 2

Códigos Hermitianos Generalizados

Neste capítulo generalizamos os resultados de Bulygin [3]. Além disso, calculamos as distâncias mínimas exatas para alguns valores do semigrupo de Weierstrass $H(Q_\infty)$ no ponto Q_∞ da curva definida abaixo pela equação (2.1) e aplicamos estes cálculos para obter informação sobre os pesos generalizados de Hamming dos códigos introduzidos.

A seguir apresentamos uma família de corpos de funções que foi considerada por Garcia e Stichtenoth em [9], definidas por equações usando polinômios simétricos elementares, e com o propósito de construir corpos de funções com grande número de lugares de grau 1. Denotamos estes tipos de corpos por GH.

2.1 Corpo de Funções Hermitianos Generalizados

Teorema 2.1. [9, Teorema 4.1] Seja $q = p^t$, p um primo. Então a curva dada pela equação

$$y^{q^{r-1}} + \cdots + y^q + y - (x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-2}+q^{r-1}}) = 0\,, \tag{2.1}$$

é absolutamente irredutível sobre $\mathbb{F}_{q^r}$. O correspondente corpo de funções $GH/\mathbb{F}_{q^r}$ desta curva tem gênero

$$g = \frac{q^{r-1}(q^{r-1}-1)}{2}\,,$$

e o número de lugares de grau 1 é

$$N = 1 + q^{2r-1}\,.$$

Em particular, quando $r = 2$ obtemos o corpo de funções Hermitianas.

Observação 2.2. i) A equação (2.1) pode ser escrita como $s_{r,1}(y) = s_{r,2}(x)$, onde $s_{r,1}(y)$ e $s_{r,2}(x)$ são o primeiro e segundo polinômios simétricos de $(y, y^q, \ldots, y^{q^{r-1}})$ e $(x, x^q, \ldots, x^{q^{r-1}})$ respectivamente (ver [19]).

ii) Note que $s_{r,1}(\beta) = \mathrm{Tr}_{\mathbb{F}_{q^r}|\mathbb{F}_q}(\beta)$, onde Tr é a função traço de $\mathbb{F}_{q^r}$ para $\mathbb{F}_q$, e $\beta \in \mathbb{F}_{q^r}$, logo temos que $s_{r,1}(\beta) \in \mathbb{F}_q$. Veja que para $\alpha \in \mathbb{F}_{q^r}$ também temos que $s_{r,2}(\alpha) \in \mathbb{F}_q$, pois $s_{r,2}(\alpha)^q - s_{r,2}(\alpha) = (\alpha^{q^r} - \alpha)(\alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{r-1}}) = 0$, assim segue-se que $s_{r,2}(\alpha) \in \mathbb{F}_q$.

iii) Tomando $r = 3$ e $q = 2$ na equação (2.1), obtem-se um corpo de funções GH de gênero 6 com 33 lugares de grau 1 sobre $\mathbb{F}_8$. Não se conhece um corpo de funções racionais sobre $\mathbb{F}_8$ de gênero 6 com mais de 33 lugares de grau 1, ver [10].

iv) Tomando $r = 3$ e $q = 3$ na equação (2.1), obtem-se um corpo de funções GH de gênero 36 com 244 lugares de grau 1 sobre $\mathbb{F}_{27}$. Não se conhece um corpo de funções racionais sobre $\mathbb{F}_{27}$ de gênero 36 com mais de 244 lugares de grau 1, ver [10].

Com o propósito de entender melhor a família de curvas definidas pela equação (2.1), esboçamos a demonstração da proposição a seguir.

Proposição 2.3. [3, Proposição 1.4] Seja $GH/\mathbb{F}_{q^r}$ o corpo de funções definido pela curva (2.1), e $\mathbb{P}_{GH}$ o conjunto de lugares de $GH/\mathbb{F}_{q^r}$. Então temos que:

a) O pólo P_∞ de x em $\mathbb{F}_{q^r}(x)$ tem uma única extensão $Q_\infty \in \mathbb{P}_{GH}$, e $e(Q_\infty|P_\infty) = q^{r-1}$. Logo, Q_∞ é um lugar em $GH/\mathbb{F}_{q^r}$ de grau 1.

b) O divisor de pólos de x é $(x)_\infty = q^{r-1}Q_\infty$, e de y é $(y)_\infty = (q^{r-2} + q^{r-1})Q_\infty$.

c) Para cada $\alpha \in \mathbb{F}_{q^r}$, existem q^{r-1} elementos $\beta \in \mathbb{F}_{q^r}$ tal que

$$\beta^{q^{r-1}} + \cdots + \beta^q + \beta = \alpha^{1+q} + \alpha^{1+q^2} + \cdots + \alpha^{q^{r-2}+q^{r-1}} := f(\alpha)\,,$$

e para todo (α, β) existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_{GH}$ de grau 1 com $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$.

Demonstração: a) Segue do fato que a equação (2.1) é absolutamente irredutível, isto é, $[GH : \mathbb{F}_{q^r}(x)] = q^{r-1}$.
b) De (a) temos que $(x)_\infty = q^{r-1}Q_\infty$. Da equação (2.1), observe que x e y possuem os mesmos pólos, logo Q_∞ é o único pólo de y. Como

$$q^{r-1}\upsilon_{Q_\infty}(y) = (q^{r-2} + q^{r-1})\upsilon_{Q_\infty}(x)\,,$$

então $(y)_\infty = (q^{r-2} + q^{r-1})Q_\infty$.
c) Como $s_{r,2}(\alpha) = \phi \in \mathbb{F}_q$ para todo $\alpha \in \mathbb{F}_{q^r}$, e a função traço é linear e sobrejetora, então existem q^{r-1} elementos $\lambda \in \mathbb{F}_{q^r}$ tal que $\lambda^{q^{r-1}} + \cdots + \lambda^q + \lambda = \phi$. Agora suponha que $\beta \in \mathbb{F}_{q^r}$ tal que $\beta^{q^{r-1}} + \cdots + \beta^q + \beta = f(\alpha)$. Assim, para todo $\gamma \in \mathbb{F}_{q^r}$ tal que $\gamma^{q^{r-1}} + \cdots + \gamma^q + \gamma = 0$, se cumpre que

$$(\beta+\gamma)^{q^{r-1}} + \cdots + (\beta+\gamma)^q + (\beta+\gamma) = f(\alpha)\,,$$

logo,

$$T^{q^{r-1}} + \cdots + T^q + T - f(\alpha) = \prod_{i=1}^{q^{r-1}} (T - \beta_i)\,,$$

com $\beta_i \neq \beta_j$ para $i \neq j$ e $\beta_i \in \mathbb{F}_{q^r}$ para $i = 1, \ldots, q^{r-1}$. Segue de [28, Corolário III.3.8(c)] que para cada $i = 1, \ldots, q^{r-1}$ existe um único lugar $P_i \in \mathbb{P}_{GH}$ tal que $P_i | P_\alpha$ e $y - \beta_i \in P_i$ e $\deg(P_i) = 1$, logo $x(P_i) = \alpha$ e $y(P_i) = \beta_i$. □

2.2 Semigrupo de Weierstrass no Ponto Q_∞

Por semigrupo entendemos um subconjunto S dos inteiros não negativos $\mathbb{N}_0$ tal que para todo $a, b \in S$ tem-se que $a + b \in S$, e o conjunto $\mathbb{N}_0 \setminus \{S\}$ é finito. Chamamos os elementos de $\mathbb{N}_0 \setminus \{S\}$ de *lacunas* e os elementos de S de não lacunas. Denotamos o número de lacunas por $g = g(S)$. No contexto de curvas algébricas o semigrupo de um ponto racional da curva é chamado semigrupo de Weierstrass e o número g representa o gênero da curva. Enumeramos as lacunas de S pela seqüência $\ell_1 < \cdots < \ell_g$. Assim, ℓ_g é a maior lacuna de S. Dizemos que o semigrupo S é *simétrico* se $\ell_g = 2g - 1$, isto vem do fato de satisfazer a propriedade de simetria que o par (s, t) de inteiros não negativos deve satisfazer, isto é, $s + t = \ell_g$. Conseqüêntemente tem-se que um desses números é uma lacuna e o outro é uma não lacuna.

O objetivo nesta seção é determinar uma base para o espaço $\mathcal{L}(sQ_\infty)$ para todo s, importante para estudar os códigos pontuais com suporte no ponto Q_∞. Este problema está

fortemente ligado com a obtenção de um conjunto de geradores do semigrupo de Weierstrass no ponto Q_∞.

Observação 2.4. Ao contrário de Bulygin, que considerou a curva (2.1) somente no caso em que $q = 2$ em [3], aquí consideramos todas as famílias de curvas com $q = p^t$, onde p é primo. Além disso, veja que para todo q e r tal que q^r é fixo e q uma potência de p, o número máximo N de pontos da curva vai ser obtido quando $q = p$. Isto segue do fato que $N = 1 + q^{2r-1} = 1 + \dfrac{(q^r)^2}{q}$, logo, quando q cresce, N decresce.

Uma da razões pelas quais é interessante o estudo da curva (2.1) para q uma potência de $p > 2$ é porque o quociente

$$\frac{N}{g} = \frac{2(1+q^{2r-1})}{q^{r-1}(q^{r-1}-1)} = \frac{2(1+\frac{(q^r)^2}{q})}{\frac{q^r}{q}(\frac{q^r}{q}-1)},$$

é o menor possível quando $q = 2$, e cresce quando q também cresce.

No lema a seguir, encontraremos a ordem de algumas funções no ponto Q_∞, essenciais para determinar o conjunto de geradores do semigrupo de Weierstrass de Q_∞. A construção da função $z := x^{q+1} - y^q + x^{q-1}y$, foi o que permitiu generalizar todos os resultados obtidos por Bulygin em [3].

Lema 2.5. Sejam as funções $w := x^{q+1} - y^q$, $z := w + x^{q-1}y$. Definimos $\mathrm{ord}(f) := -v_{Q_\infty}(f)$, onde v_{Q_∞} é a valorização no ponto Q_∞. Então:

- $\mathrm{ord}(x) = q^{r-1}$;
- $\mathrm{ord}(y) = q^{r-2} + q^{r-1}$;
- $\mathrm{ord}(z) = q^r + 1$;
- $\mathrm{ord}(w) = \mathrm{ord}(x^{q-1}y) = q^{r-2} + q^r$.

Demonstração: Como notado anteriormente, x e y tem ordens q^{r-1} e $q^{r-2} + q^{r-1}$, respectivamente. Observe que $\mathrm{ord}(x^{q+1}) = \mathrm{ord}(y^q)$. Portanto, pela propriedade de valorizações $\mathrm{ord}(w) \leq \mathrm{ord}(x^{q+1}) = \mathrm{ord}(y^q)$. Elevando à potência q a equação (2.1) temos que

$$y^{q^r} + \cdots + y^{q^2} + y^q = x^{q+q^2} + x^{q+q^3} + \cdots + x^{q^{r-1}+q^r},$$

e como $w^{q^{r-1}} = x^{q^{r-1}+q^r} - y^{q^r}$ então segue que:

$$\begin{aligned} w^{q^{r-1}} &= y^{q^{r-1}} + \cdots + y^{q^2} + y^q - (x^{q+q^2} + x^{q+q^3} + \cdots + x^{q^{r-2}+q^{r-1}}) \\ &= -y + (x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-2}+q^{r-1}}) - (x^{q+q^2} + x^{q+q^3} + \cdots + \\ &\quad x^{q^{r-2}+q^{r-1}}) \end{aligned}$$

vemos que os termos da forma $x^{q^i+q^j}, i, j > 0$ do primeiro parêntesis, se anulam com os termos da forma $x^{q^i+q^j}$, $1 \leq j < i \leq r-1$ do segundo parêntese. Assim,

$$w^{q^{r-1}} = -y + x^{1+q} + x^{1+q^2} + \cdots + x^{1+q^{r-1}} - x^{q+q^r} - x^{q^2+q^r} - \cdots - x^{q^{r-2}+q^r} .$$

As ordens dos termos na igualdade acima são duas a duas distintas, assim $(q^{r-1})\mathrm{ord}(w) = (q^{r-2} + q^r)\mathrm{ord}(x)$, é o maior. Logo,

$$\mathrm{ord}(w) = q^{r-2} + q^r .$$

Observe também que

$$\mathrm{ord}(x^{q-1}y) = (q-1)\mathrm{ord}(x) + \mathrm{ord}(y) = q^r - q^{r-1} + q^{r-2} + q^{r-1} = q^{r-2} + q^r = \mathrm{ord}(w) .$$

Agora, considere a função $z := x^{q+1} - y^q + x^{q-1}y$. Então

$$\begin{aligned} z^{q^{r-1}} &= w^{q^{r-1}} + x^{q^r - q^{r-1}} y^{q^{r-1}} \\ &= w^{q^{r-1}} + x^{q^r - q^{r-1}} (x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-1}+q^{r-2}} - y^{q^{r-2}} - \cdots - y^q - y) \\ &= -y + x^{1+q} + x^{1+q^2} + \cdots + x^{1+q^{r-1}} - x^{q+q^r} - x^{q^2+q^r} - \cdots - x^{q^{r-2}+q^r} \\ &\quad + x^{q^r - q^{r-1}+q+1} + \cdots + x^{q^r - q^{r-1}+q^{r-2}+1} + x^{q^r+1} + \cdots + x^{q^r - q^{r-1}+q^{r-3}+q^{r-2}} \\ &\quad + x^{q^r+q^{r-3}} + x^{q^r+q^{r-2}} - x^{q^r - q^{r-1}} y^{q^{r-2}} - x^{q^r - q^{r-1}} y^{q^{r-3}} - \cdots - x^{q^r - q^{r-1}} y^q \\ &\quad - x^{q^r - q^{r-1}} y \\ &= -y + x^{1+q} + \cdots + x^{1+q^{r-1}} + x^{q^r - q^{r-1}+q+1} + \cdots + x^{q^r - q^{r-1}+q^{r-2}+1} \\ &\quad + x^{q^r+1} + x^{q^r - q^{r-1}+q^2+q} + \cdots + x^{q^r - q^{r-1}+q^{r-2}+q} + \cdots + x^{q^r - q^{r-1}+q^{r-3}+q^{r-2}} \\ &\quad - x^{q^r - q^{r-1}} y^{q^{r-2}} - x^{q^r - q^{r-1}} y^{q^{r-3}} - \cdots - x^{q^r - q^{r-1}} y^q - x^{q^r - q^{r-1}} y . \end{aligned}$$

É necessário que as maiores ordens dos termos na igualdade acima sejam diferentes, pois se algumas das ordens menores são repetidas, então é suficiente agrupar todas as funções com a mesma ordem em uma única função. Assim, basta comparar as ordens das funções x^{q^r+1} e $x^{q^r - q^{r-1}} y^{q^{r-2}}$, pois estas são as funções de maior potência. Logo,

$$\mathrm{ord}(x^{q^r+1}) = (q^r + 1)q^{r-1} ,$$

e

$$\mathrm{ord}(x^{q^r-q^{r-1}}y^{q^{r-2}}) = (q^r-q^{r-1})q^{r-1}+q^{r-2}(q^{r-1}+q^{r-2}) = q^{r-1}(q^r-q^{r-1}+q^{r-2}+q^{r-3})\,.$$

Como $q^2 > q+1$ para todo q, então $q^{r-1} > q^{r-2}+q^{r-3}$ para todo $r \geq 3$ e disso segue que

$$\mathrm{ord}(x^{q^r+1}) > \mathrm{ord}(x^{q^r-q^{r-1}}y^{q^{r-2}})\,.$$

Portanto, $\mathrm{ord}(z^{q^{r-1}}) = (q^r+1)q^{r-1}$, implicando que $\mathrm{ord}(z) = q^r+1$. □

Podemos observar que $\mathrm{ord}(z) = q^r+1$ não é combinação linear de q^{r-1} e $q^{r-2}+q^{r-1}$. A seguir enunciamos o teorema principal desta seção.

Teorema 2.6.

$$H(Q_\infty) = \left\langle q^{r-1}, q^{r-2}+q^{r-1}, q^r+1 \right\rangle\,.$$

Para demonstrar este teorema lembramos o conceito de *semigrupos telescópicos* dado em [16].

Definição 2.7. [16, Definição 6.1] Seja $a_1,\ldots,a_k$ uma seqüência de inteiros positivos com máximo divisor comum (mdc) igual a 1. Defina

$$d_i = \mathrm{mdc}(a_1,\ldots,a_i) \quad e \quad A_i = \{a_1/d_i,\ldots,a_i/d_i\}$$

para $i = 1,\ldots,k$. Seja $d_0 := 0$. Seja S_i o semigrupo gerado por A_i. Se $a_i/d_i \in S_{i-1}$ para $i = 2,\ldots,k$, então a seqüência $(a_1,\ldots,a_k)$ é chamada de *telescópica*. Um semigrupo é chamado telescópico se este é gerado por uma seqüência telescópica.

Proposição 2.8. [16, Lema 6.5] Seja S_k o semigrupo gerado pela seqüência telescópica $(a_1,\ldots,a_k)$. Então

$$\begin{aligned}
\ell_g(S_k) &= d_{k-1}(\ell_g(S_{k-1})-1)+(d_{k-1}-1)a_k \\
&= \textstyle\sum_{i=1}^{k}(d_{i-1}/d_i-1)a_i\,, \\
g(S_k) &= d_{k-1}g(S_{k-1})+(d_{k-1}-1)(a_k-1)/2 \\
&= (\ell_g(S_k)+1)/2\,.
\end{aligned}$$

Assim, da fórmula do gênero para um semigrupo telescópico tem-se que semigrupos telescópicos são simétricos.

Demonstração: (Teorema 2.6) Seja

$$S(r) = \left\langle q^{r-1}, q^{r-2}+q^{r-1}, q^r+1 \right\rangle\,, r \geq 3$$

o semigrupo gerado por $a_1 := q^{r-1}$, $a_2 := q^{r-2} + q^{r-1}$ e $a_3 := q^r + 1$ para $r \geq 3$. Temos que $\mathrm{mdc}(a_1, a_2, a_3) = 1$. A seguir checamos a definição de semigrupo telescópico.

$$\begin{array}{lll} d_1 = \mathrm{mdc}(a_1) = q^{r-1}, & A_1 = \{1\}, & S_1 = \mathbb{N}; \\ d_2 = \mathrm{mdc}(a_1, a_2) = q^{r-2}, & A_2 = \{q, q+1\}, & S_2 = \langle q, q+1 \rangle\,; \\ d_3 = \mathrm{mdc}(a_1, a_2, a_3) = 1, & A_3 = \{a_1, a_2, a_3\} & S_3 = S(r)\,. \end{array}$$

Observamos que $A_2 = \{q, q+1\} \subseteq \mathbb{N} = S_1$ e $q^r + 1 = q(q^{r-1} - 1) + (q+1) \cdot 1 \in S_2 = \langle q, q+1 \rangle$. Isto significa que $S(r)$ é um semigrupo telescópico. Assim, aplicando a Proposição 2.8 a $S(r)$, obtemos

$$\ell_g(S(r)) = (d_0/d_1 - 1)a_1 + (d_1/d_2 - 1)a_2 + (d_2/d_3 - 1)a_3 + 1\,,$$

logo,

$$\ell_g(S(r)) = -a_1 + (q-1)a_2 + (q^{r-2} - 1)a_3 + 1 = q^{2r-2} - q^{r-1} = q^{r-1}(q^{r-1} - 1)\,.$$

Como semigrupos telescópicos são simétricos então segue que:

$$g(S(r)) = \frac{\ell_g(S(r)) + 1}{2} = \frac{q^{r-1}(q^{r-1} - 1)}{2}\,.$$

Note que $g(S(r)) = g(H(Q_\infty)) = \#(\mathbb{N} \setminus H(Q_\infty))$, e como $S(r) \subseteq H(Q_\infty)$ concluímos que $S(r) = H(Q_\infty)$. □

A seguir uma importante conseqüência deste teorema.

Proposição 2.9. Para $s \geq 0$. $\mathcal{L}(sQ_\infty) = \left\langle x^i y^j z^k \right\rangle_{i,j,k}$ onde $z = x^{q+1} - y^q + x^{q-1}y$ e

$$i \cdot q^{r-1} + j \cdot (q^{r-2} + q^{r-1}) + k \cdot (q^r + 1) \leq s, \text{ tal que } i \geq 0, 0 \leq j < q, 0 \leq k < q^{r-2}\,.$$

Demonstração: Podemos ver que

$$\dim(\mathcal{L}(sQ_\infty)) = |H(Q_\infty) \cap \{0, 1, \ldots, s\}|\,,$$

e que as funções da forma $x^i y^j z^k$ como no enunciado são linearmente independentes, pois elas tem diferentes ordens em Q_∞. Para ver isto, é suficiente mostrar que os números da forma

$$i \cdot q^{r-1} + j \cdot (q^{r-2} + q^{r-1}) + k \cdot (q^r + 1)\,,$$

são diferentes para cada $i \geq 0, 0 \leq j < q$ e $0 \leq k < q^{r-2}$. Suponhamos que existem inteiros positivos $i_0, i_1, j_0, j_1, k_0, k_1$ tais que:

$$i_0 q^{r-1} + j_0(q^{r-2} + q^{r-1}) + k_0(q^r + 1) = i_1 q^{r-1} + j_1(q^{r-2} + q^{r-1}) + k_1(q^r + 1)\,.$$

Então,

$$(i_0 - i_1)q^{r-1} + (j_0 - j_1)(q^{r-2} + q^{r-1}) + (k_0 - k_1)(q^r + 1) = 0\,.$$

Logo, q^{r-2} divide $k_0 - k_1$, e do fato que $k_0, k_1 < q^{r-2}$ obtém-se que $k_0 = k_1$. Assim,

$$(i_0 - i_1)q + (j_0 - j_1)(q + 1) = 0.$$

Como conseqüência q divide $j_0 - j_1$, e como $j_0, j_1 < q$ então $j_0 = j_1$ e, portanto $i_0 = i_1$.

Por último, mostraremos que um elemento qualquer

$$aq^{r-1} + b(q^{r-2} + q^{r-1}) + c(q^r + 1) \in H(Q_\infty)\,,$$

com $a \geq 0, b \geq 0$ e $c \geq 0$ se escreve da forma $iq^{r-1} + j(q^{r-2} + q^{r-1}) + k(q^r + 1)$ com $0 \leq j < q$ e $o \leq k < q^{r-2}$. Sabemos existem $c_1, c_2 \in \mathbb{N}_0$, com $0 \leq c_2 < q^{r-2}$ tais que $c = c_1 q^{r-2} + c_2$ e disso temos que

$aq^{r-1} + b(q^{r-2} + q^{r-1}) + c(q^r + 1) = aq^{r-1} + b(q^{r-2} + q^{r-1}) + (c_1 q^{r-2} + c_2)(q^r + 1)$
$= aq^{r-1} + b(q^{r-2} + q^{r-1}) + c_1 q^{2r-2} + c_1 q^{r-2} + c_2(q^r + 1)$
$= (a + c_1 q^{r-1} - c_1)q^{r-1} + (b + c_1)(q^{r-2} + q^{r-1}) + c_2(q^r + 1)\,.$

Sejam agora $d_1, d_2 \in \mathbb{N}_0$, com $0 \leq d_2 < q$, tais que $b + c_1 = d_1 q + d_2$. Então temos que

$(a + c_1 q^{r-1} - c_1)q^{r-1} + (b + c_1)(q^{r-2} + q^{r-1}) + c_2(q^r + 1)$
$= (a + c_1 q^{r-1} - c_1)q^{r-1} + (d_1 q + d_2)(q^{r-2} + q^{r-1}) + c_2(q^r + 1)$
$= (a + c_1 q^{r-1} - c_1)q^{r-1} + d_1 q^{r-1} + d_1 q^r + d_2(q^{r-2} + q^{r-1}) + c_2(q^r + 1)$
$= (a + c_1 q^{r-1} - c_1 + d_1 q + d_1)q^{r-1} + d_2(q^{r-2} + q^{r-1}) + c_2(q^r + 1).$

Isto completa a demonstração de que as ordens de pólo em Q_∞ das funções dadas de fato são todos os elementos de $H(Q_\infty)$. □

2.3 Códigos sobre Corpos Hermitianos Generalizados

Códigos Hermitianos são uma classe importante de exemplos em teoria dos códigos de Goppa. Assim, pela semelhança do corpo de funções GH com o corpo de funções Hermitianas definimos os códigos GH_s de forma análoga à Definição 1.6.

Definição 2.10. Para $s \in \mathbb{N}$, seja

$$GH_s := C_{\mathcal{L}}(D, sQ_\infty)\,,$$

onde

$$D := \sum_{\beta^{q^{r-1}}+\cdots+\beta=\alpha^{1+q}+\cdots+\alpha^{q^{r-2}+q^{r-1}}} P_{\alpha,\beta}\,,$$

é a soma de todos os lugares de grau 1, exceto Q_∞, do corpo de funções $GH/\mathbb{F}_{q^r}$ (ver Teorema 2.1). Chamamos estes códigos GH_s de códigos Hermitianos generalizados.

códigos GH_s são códigos de comprimento $n = q^{2r-1}$ sobre $\mathbb{F}_{q^r}$. Para $t \leq s$ temos que $GH_t \subseteq GH_s$. Agora discutimos um caso trivial. Se $s > q^{2r-1}+2g-2 = q^{2r-1}+q^{2r-2}-q^{r-1}-2$, então pelo Teorema de Riemann-Roch e do Teorema 1.2 segue que

$$\begin{aligned}\dim(GH_s) &= \dim(\mathcal{L}(sQ_\infty)) - \dim(\mathcal{L}(sQ_\infty - D)) \\ &= (s+1-g) - (s+1-g-q^{2r-1}) \\ &= q^{2r-1} = n\,.\end{aligned}$$

Assim, códigos GH_s são interessantes para

$$0 < s \leq q^{2r-1} + q^{2r-2} - q^{r-1} - 2\,.$$

A proposição a seguir será de grande ajuda na hora de calcular a dimensão e as distâncias mínimas do código.

Proposição 2.11. [3, Corolário 4.5] O código dual de GH_s é

$$GH_s^\perp = GH_{q^{2r-1}+2g-2-s} = GH_{q^{2r-1}+q^{r-1}(q^{r-1}-1)-2-s}\,.$$

Assim, GH_s é auto-ortogonal se $2s \leq q^{2r-1} + q^{r-1}(q^{r-1}-1) - 2$, e GH_s é auto-dual (este caso só pode ocorrer se q é uma potência de 2) se, e somente se, $s = (q^{2r-1} + q^{r-1}(q^{r-1} - 1) - 2)/2$.

A seguir determinaremos os parâmetros para GH_s. Considere o conjunto

$$I(s) := H(sQ_\infty) \cap \{0, 1, \ldots, s\}\,.$$

Tem-se para $s \geq 2g - 1 = q^{r-1}(q^{r-1}-1) - 1$ que

$$|I(s)| = s + 1 - g = s + 1 - \frac{q^{r-1}(q^{r-1}-1)}{2}\,,$$

Da seção anterior segue

$$I(s) = \{\ell \leq s : \ell = i \cdot q^{r-1} + j \cdot (q^{r-2} + q^{r-1}) + k \cdot (q^r + 1);\, i \geq 0, 0 \leq j < q, 0 \leq k < q^{r-2}\}\,.$$

Proposição 2.12. Suponhamos que $0 \leq s \leq q^{2r-1} + q^{2r-2} - q^{r-1} - 2$. Então

1. A dimensão de GH_s é dada por

$$\dim(GH_s) = \begin{cases} |I(s)|, & \text{para } 0 \leq s < q^{2r-1}\,, \\ q^{2r-1} - |I(t)|, & q^{2r-1} \leq s \leq q^{2r-1} + q^{2r-2} - q^{r-1} - 2\,, \end{cases}$$

onde $t := q^{2r-1} + q^{2r-2} - q^{r-1} - 2 - s$. Para $q^{2r-2} - q^{r-1} - 2 < s < q^{2r-1}$, tem-se que

$$\dim(GH_s) = s + 1 - \frac{q^{r-1}(q^{r-1}-1)}{2}\,.$$

2. A distância mínima d de GH_s, satisfaz

$$d \geq q^{2r-1} - s\,.$$

Demonstração: 1) Para $0 \leq s < q^{2r-1}$, segue do Corolário 1.3 que

$$\dim(GH_s) = \dim(\mathcal{L}(sQ_\infty)) = |I(s)|\,,$$

e que

$$\dim(GH_s) = s + 1 - \frac{q^{r-1}(q^{r-1}-1)}{2}\,,$$

se $q^{2r-2} - q^{r-1} - 2 < s < q^{2r-1}$.

Se $q^{2r-1} \leq s \leq q^{2r-1} + q^{2r-2} - q^{r-1} - 2$ e $t = q^{2r-1} + q^{2r-2} - q^{r-1} - 2 - s$ tem-se que $0 \leq t \leq q^{2r-2} - q^{r-1} - 2 < q^{2r-1}$, logo da proposição (2.11) obtemos que

$$\begin{aligned} \dim(GH_s) &= q^{2r-1} - \dim(GH_s^{\perp}) \\ &= q^{2r-1} - \dim(GH_t) \\ &= q^{2r-1} - |I(t)|\,. \end{aligned}$$

2) A desigualdade segue do Teorema 1.2. □

No quadro da proposição a seguir apresentamos a distância mínima exata para uma ampla quantidade de valores de $s \in H(Q_\infty)$.

Proposição 2.13.

	$\mathbf{s} \in H(Q_\infty) = \langle q^{r-1}, q^{r-2}+q^{r-1}, q^r+1\rangle$	**Distância Mínima**
1)	$0 \leq s = iq^{r-1} < q^{2r-1}$	$q^{2r-1} - s$
	$r = 3, q = p^t, p \neq 2$ $H(Q_\infty) = \langle q^2, q+q^2, q^3+1\rangle$	
2)	$0 \leq s < q^5 - q^4 - q^3$ $s = iq^2 + j(q+q^2)$	$q^5 - s$
3)	$q^5 - q^4 - q^3 < s < q^5 - q^2;$ $s = q^5 - q^4 - q^3 + aq^2 + bq,$ $0 \leq a \leq q^2 - 1 + b, 1 \leq b \leq q-1$	$q^5 - s$
4)	$q^5 - q^4 - q^3 < s < q^5 - q^2;$ $s = q^5 - q^4 - q^3 + aq^2 + bq,$ $q^2 + b \leq a \leq q^2 + q - 2, 1 \leq b \leq q-1$	$q^5 - s + bq$
5)	$q^{2r-1} - q^{r-1} \leq s \leq q^{2r-1}$	q^{r-1}

Demonstração:

1. Seja $s = iq^{r-1}$. Observe que para $\alpha \in \mathbb{F}_{q^r}$ o divisor de $x - \alpha$ tem exatamente q^{r-1} zeros distintos P_{α,β_t} de grau 1 em $\mathbb{P}_{GH}$. Isto vem do fato que a aplicação traço de $\mathbb{F}_{q^r}$ em $\mathbb{F}_q$ é sobrejetora e linear. Assim, escolha $J \subseteq F_{q^r}$ tal que $|J| = i$, logo o elemento

$$h = \prod_{\alpha \in J}(x - \alpha),$$

tem exatamente iq^{r-1} zeros distintos no suporte de D, o que implica que o peso da palavra $\alpha(h) \in GH_s$ é $q^{2r-1} - s$.

2. Para $0 \leq s < q^5 - q^4 - q^3$, com $s = iq^2 + j(q+q^2)$ tem-se que $i < q^3 - q^2 - q$, e fixe $\gamma \in \mathbb{F}_q \setminus \{0\}$. Escolha $\gamma \notin \Sigma_3$, onde Σ_3 é um subconjunto de $\mathbb{F}_q$ tal que o polinômio $H(x) = x^{1+q} + x^{1+q^2} + x^{q+q^2} - \gamma$ tem raízes múltiplas em $\bar{\mathbb{F}}_q$. Então de [9, Observação 3.8] tem-se que $\#(\Sigma_3) = (q+1)/2$, e que no caso em que $\gamma \notin \Sigma_3$ segue que o polinômio $H(x)$ tem q^2+q raízes simples em $\mathbb{F}_{q^3}$. Portanto, obtém-se que o conjunto $A := \{\alpha \in \mathbb{F}_{q^3} : \alpha^{1+q} + \alpha^{1+q^2} + \alpha^{q+q^2} \neq \gamma\}$ tem $|A| = q^3 - q^2 - q \geq i$ elementos. Considere $\alpha_1, \ldots, \alpha_i \in A$ elementos distintos e defina

$$z_1 := \prod_{\mu=1}^{i}(x - \mu)\,.$$

Por construção obtém-se que z_1 tem iq^2 zeros distintos no suporte de D. Agora, tomando j elementos distintos $\beta_1, \ldots, \beta_j \in \mathbb{F}_{q^3}$ tal que $\beta_\nu^{q^2} + \beta_\nu^q + \beta_\nu = \gamma$ e para $\nu = 1, \ldots, j$, defina a função

$$z_2 := \prod_{\nu=1}^{j} r_\nu,$$

onde $r_\nu = y - \beta_\nu$. Logo z_2 tem $j(q+q^2)$ zeros distintos no suporte de D, e todos diferentes dos zeros de z_1, pois, $\beta_\nu^{q^2} + \beta_\nu^q + \beta_\nu = \gamma \neq \alpha_\mu^{1+q} + \alpha_\mu^{1+q^2} + \alpha_\mu^{q+q^2}$, para todo $\nu = 1, \ldots, j$ e $\mu = 1, \ldots, i$. Assim,

$$z := z_1 z_2 \in \mathcal{L}(sQ_\infty),$$

tem s zeros distintos $P_{\alpha,\beta} \preceq D$, portanto a palavra do código $\alpha(z) \in GH_s$ tem peso $q^5 - s$.

3. Seja $q^5 - q^4 - q^3 < s < q^5 - q^2$, com $s = q^5 - q^4 - q^3 + aq^2 + bq$, $0 \leq a \leq q^2 - 1 + b$ e $1 \leq b \leq q-1$. Para demonstrar esta parte, necessitamos do seguinte lema.

   Lema 2.14. Suponha $0 \leq s \leq n = q^5$ e seja $\delta = n - s$. Então, existe uma função $f \in \mathcal{L}(sQ_\infty)$ com exatamente s zeros distintos no suporte de D se, e somente se, existe $h \in \mathcal{L}(\delta Q_\infty)$ com exatamente δ zeros distintos no suporte de D.

   Demonstração: Seja $u = x^{q^3} - x$. Note que $(u) = D - q^5 Q_\infty$ e considere a função u/f ou u/h para f e h satisfazendo a condição do lema. □

   Note que $\delta = n - s = q^5 - s = (q^2 - 1 - a + b)q^2 + (q-b)(q+q^2)$, tal que $q^2 - 1 - a + b \geq 0$ e $0 < q - b \leq q - 1$, portanto $\delta \in H(Q_\infty)$. Como $\delta < q^5 - q^4 - q^3$ para $q \geq 3$, segue do item (b) que existe uma função $f \in \mathcal{L}(\delta Q_\infty)$ com exatamente δ zeros distintos no suporte de D. Assim, do Lema 2.14 existe uma função $g \in \mathcal{L}(sQ_\infty)$ com exatamente s zeros distintos no suporte de D. Então concluímos que a palavra do código $\alpha(g) \in GH_s$ tem peso $q^5 - s$.

4. Seja $q^5 - q^4 - q^3 < s < q^5 - q^2$ com $s = q^5 - q^4 - q^3 + aq^2 + bq$, $q^2 + b \leq a \leq q^2 + q - 2$ e $1 \leq b \leq q-2$. Do Lema 2.15 segue que $\delta = n - s + v$, $0 \leq v < bq$ é uma lacuna do semigrupo de Weierstrass $H(Q_\infty)$, pois $\delta = (q^2 + q - a - 1)q^2 + (q-b)q + v$ tal que $q^2 + q - a - 1 < q - b$ e $q^2 - bq + v < q^2$. Logo, do item 1 obtém-se que $d(GH_s) = n - s + bq$.

   5) Do item 1) tem-se que $d(GH_{q^{2r-1}-q^{r-1}}) = q^{r-1}$. Por outro lado, note que a abundância do código $GH_{q^{2r-1}}$ é $a = \ell(q^{2r-1}Q_\infty - D) = 1$ e portanto da Proposição 1.40 tem-se

que $d(GH_s) \geq q^{2r-1}$. Além disso, $d(GH_{s_1}) \geq d(GH_{s_2})$ para $s_1 \leq s_2$, então segue-se que $d(GH_s) = q^{r-1}$ para s no intervalo $q^{2r-1} - q^{r-1} \leq s \leq q^{2r-1}$. □

Agora restringimos nossa atenção para $q^{2r-1} \leq s \leq q^{2r-1} + q^{2r-2} - q^{r-1} - 2$. Para simplificar a notação definimos $s^\perp = q^{2r-1} + q^{2r-2} - q^{r-1} - 2 - s$. Assim, $GH_s^\perp = GH_{s^\perp}$ e $0 \leq s^\perp \leq 2g - 2 = q^{2r-2} - q^{r-1} - 2$.

Lema 2.15. Seja $m \in \mathbb{Z}$, com $m \geq 0$. Então, s tem representação única da forma

$$m = aq^{r-1} + bq^{r-2} + c, \tag{2.2}$$

onde $a \geq 0$, $0 \leq b < q$, e $0 \leq c < q^{r-2}$. Além disso, $s \in H(Q_\infty)$ se, e somente se, $a \geq b + cq$.

Demonstração: Suponhamos que $a_1q^{r-1}+b_1q^{r-2}+c_1 = a_2q^{r-1}+b_2q^{r-2}+c_2$ para $a_1, a_2 \geq 0$, $0 \leq b_1, b_2 < q$ e $0 \leq c_1, c_2 < q^{r-2}$. Logo, $(a_1 - a_2)q^{r-1} + (b_1 - b_2)q^{r-2} + (c_1 - c_2) = 0$. Portanto tem-se que $q^{r-2}|(c_1 - c_2)$ e como $0 \leq c_1, c_2 < q^{r-2}$ então segue que $c_1 = c_2$. Assim, $(a_1 - a_2)q + (b_1 - b_2) = 0$. Analogamente obtemos que $b_1 = b_2$ e por conseqüência $a_1 = a_2$, portanto temos a unicidade. Agora, seja m da forma (2.2). Se $a \geq b + cq$, então $u = x^{a-b-cq}y^b z^c \in \mathcal{L}(sQ_\infty)$ e

$$\text{ord}(u) = (a - b - cq)q^{r-1} + b(q^{r-2} + q^{r-1}) + c(q^r + 1) = m,$$

o que mostra que $m \in H(Q_\infty)$. Para mostrar o outro lado, suponha que $a < b + cq$ e que $m \in H(Q_\infty)$. Podemos escrever $m = iq^{r-1} + j(q^{r-2} + q^{r-1}) + k(q^r + 1)$ com $i \geq 0$, $0 \leq j < q$ e $0 \leq k < q^{r-2}$. Então $j = b$, $k = c$ e $a = i + b + cq$, o que contradiz a suposição, que $a < b + cq$ pois $i \geq 0$. □

Desta demonstração temos que o conjunto de lacunas do ponto Q_∞ é dado por

$$\left\{aq^{r-1} + bq^{r-2} + c : 0 \leq a < b + cq \leq q^{r-1} - 1,\ 0 \leq b < q, 0 \leq c < q^{r-2}\right\}.$$

Do Lema 2.15, podemos escrever $s^\perp$ na forma (2.2) com $0 \leq b + cq \leq a \leq q^{r-1} - 2$, pois $0 \leq s^\perp \leq 2g - 2 = q^{2r-2} - q^{r-1} - 2$. Provamos o resultado a seguir de forma similar a [17, Teorema 5].

Proposição 2.16. Se $s^\perp = aq^{r-1} + bq^{r-2} + c \in H(Q_\infty)$ onde $0 \leq b + cq \leq a = b' + c'q \leq q^{r-1} - 2$, com $0 \leq b, b' < q$ e $0 \leq c, c' < q^{r-2}$. Então

$$d(GH_s) \leq \begin{cases} a + 2, & \text{se } a = b + cq\,; \\ a + 2, & \text{se } a > b + cq \text{ e } b' < b\,; \\ a + 1, & \text{se } a > b + cq \text{ e } b' \geq b\,. \end{cases}$$

Demonstração: Seja $\mathbf{H}$ uma matriz geradora para o código $GH_{s^\perp}$, isto é, uma matriz teste de paridade para GH_s, obtida de uma base de $\mathcal{L}(s^\perp Q_\infty)$. Observe que cada linha de $\mathbf{H}$ corresponde a uma função da base. O objetivo é encontrar colunas linearmente dependentes de $\mathbf{H}$ sobre $\mathbb{F}_{q^r}$. Seja o conjunto $\{P_i : P_i = (0, \beta_i), i = 1, \ldots, q^{r-1}\} \subseteq \mathrm{Sup}(D)$, com $\beta_i \neq \beta_j$ para $i \neq j$ e $a + 2 \leq q^{r-1}$.

i) Se $a = b + cq$. Uma base para $\mathcal{L}(s^\perp Q_\infty) = \mathcal{L}((b(q^{r-2} + q^{r-1}) + c(q^r + 1))Q_\infty)$ é $\{1, x, y, x^2, xy, y^2, \ldots, x^{q-1}, x^{q-2}y, \ldots, y^{q-1}, x^q, z, x^{q-1}y, \ldots, xy^{q-1}, x^{q+1}, xz, x^q y, yz, x^{q-1}y^2, \ldots, x^a, \ldots, x^{a-b}y^b, x^{a-b-q}y^b z, \ldots, x^{a+q-b-cq}y^b z^{c-1}, y^b z^c\}$. Lembrando que a função $z = x^{q+1} - y^q + x^{q-1}y$, observe que $z(P_i) = -(\beta_i)^q$. Considere uma submatriz $\mathbf{H_1}$ de $\mathbf{H}$ com colunas correspondentes a $P_1, P_2, \ldots, P_{a+2}$ e usando propriedades de matrizes conseguimos uma matriz equivalente da seguinte forma:

$$\mathbf{H_1} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \beta_3 & \cdots & \beta_{a+2} \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \cdots & \beta_{a+2}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_1^{q-1} & \beta_2^{q-1} & \beta_3^{q-1} & \cdots & \beta_{a+2}^{q-1} \\ -\beta_1^q & -\beta_2^q & -\beta_3^q & \cdots & -\beta_{a+2}^q \\ -\beta_1^{q+1} & -\beta_2^{q+1} & -\beta_3^{q+1} & \cdots & -\beta_{a+2}^{q+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (-1)^c\beta_1^a & (-1)^c\beta_2^a & (-1)^c\beta_3^a & \vdots & (-1)^c\beta_{a+2}^a \\ 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Assim, o $posto(\mathbf{H_1}) = a + 1$ e como $\mathbf{H_1}$ tem $a + 2$ colunas, então segue que as colunas de $\mathbf{H_1}$ são linearmente dependentes. Portanto, $d(GH_s) \leq a + 2$.

ii) Se $a > b + cq$. Seja $a = b' + c'q$, então temos dois casos: (1) Se $b' < b$. Assim tem-se que $b'q + c' < bq + c$, de fato, $b' \leq b - 1 \Rightarrow b'q \leq bq - q \Rightarrow b'q + c' \leq bq - q + c' < bq \leq bq + c$, e também que a função $y^{b'}z^{c'} \in \mathcal{L}(s^\perp Q_\infty)$, pois $b'(q^{r-2} + q^{r-1}) + c'(q^r + 1) = aq^{r-1} + b'q^{r-2} + c' < s^\perp$. (2) Se $b' \geq b$. Assim tem-se que a função $y^{b'}z^{c'} \notin \mathcal{L}(s^\perp Q_\infty)$, pois $b'(q^{r-2} + q^{r-1}) + c'(q^r + 1) = aq^{r-1} + b'q^{r-2} + c' > s^\perp$. Logo, para o caso (1) temos que $d(GH_s) \leq a + 2$ e para o caso (2) apagando a linha correspondente a $y^{b'}z^{c'}$ na matriz

$\mathbf{H_1}$ acima, obtemos uma matriz $\mathbf{H_2}$ com $posto(\mathbf{H_2}) = a$, desse modo, quaisquer $a+1$ colunas de $\mathbf{H_2}$ são linearmente dependentes sobre $\mathbb{F}_{q^r}$. Portanto, $d(GH_s) \leq a+1$. □

Este teorema dá uma cota superior para $d(GH_s)$ no intervalo em que $q^{2r-1} \leq s \leq q^{2r-1} + q^{2r-2} - q^{r-1} - 2$. A seguir, encontraremos uma cota inferior para obter a distância mínima exata. A prova do seguinte lema segue a mesma idéia de [17, Lema 3]. A seguir introduzimos uma notação e um lema a ser usado na demonstração.

Primeiro, para o caso em que $s^{\perp} = aq^{r-1} + bq^{r-2} + c$ com $a = b + cq$, logo $s^{\perp} = b(q^{r-2} + q^{r-1}) + c(q^r + 1)$. Considere A uma submatriz de H obtida por escolha de $a+1$ colunas distintas de H arbitrariamente. Cada coluna de H corresponde a um lugar $P_{\alpha,\beta}$ de grau 1, podemos reordenar as colunas de A de acordo com α. Isto é,

$$\begin{array}{cccc} P_{\alpha_1,\beta_{1,1}}, & P_{\alpha_1,\beta_{1,2}}, & \cdots & P_{\alpha_1,\beta_{1,b_1}} \\ P_{\alpha_2,\beta_{2,1}}, & P_{\alpha_2,\beta_{2,2}}, & \cdots & P_{\alpha_2,\beta_{2,b_2}} \\ \vdots & \vdots & \vdots & \vdots \\ P_{\alpha_l,\beta_{l,1}}, & P_{\alpha_l,\beta_{l,2}}, & \cdots & P_{\alpha_l,\beta_{l,b_l}} \end{array} \tag{2.3}$$

onde os α_i são distintos dois a dois e $b_1 + b_2 + \cdots + b_l = a+1$ com $b_1 \geq b_2 \geq \cdots \geq b_l \geq 1$. Veja que se cumpre

$$x^{i-1}y^{k_i}z^{t_i} \in \mathcal{L}(s^{\perp}Q_{\infty}),\ 0 \leq t_i + k_i q \leq b_i - 1, 0 \leq k_i < q;\ 1 \leq i \leq l\,. \tag{2.4}$$

Aplicando a função ordem tem-se que $\mathrm{ord}(x^{i-1}y^{k_i}z^{t_i}) = (i-1)q^{r-1} + t_i(q^{r-2}+q^{r-1}) + k_i(q^r + 1) = (i-1+t_i+k_iq)q^{r-1} + t_iq^{r-2} + k_i \leq (b_i + i - 2)q^{r-1} + t_iq^{r-2} + k_i$. Por outro lado, pela escolha dos b_i's, tem-se que $b_i + i - 2 \leq a - 1 - \dfrac{(i-3)i}{2}$, o que implica a equação (2.4) para cada $i = 1, \ldots, l$. Reescrevemos esses elementos da base da seguinte forma.

$$\begin{array}{ccccccccccc} 1, & y, & y^2, & \cdots & y^{q-1}, & z, & \cdots & y^{r_1}z^{s_1}, & r_1 + s_1q = b_1 - 1 \\ x, & xy, & xy^2, & \cdots & xy^{q-1}, & xz, & \cdots & xy^{r_2}z^{s_2}, & r_2 + s_2q = b_2 - 1 \\ x^2, & x^2y, & x^2y^2, & \cdots & x^2y^{q-1}, & x^2z, & \cdots & x^2y^{r_3}z^{s_3}, & r_3 + s_3q = b_3 - 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x^{l-1}, & x^{l-1}y, & x^{l-1}y^2, & \cdots & x^{l-1}y^{q-1}, & x^{\ell-1}z, & \cdots & x^{l-1}y^{r_l}z^{s_l}, & r_l + s_lq = b_l - 1 \end{array} \tag{2.5}$$

Então podemos escolher uma submatriz B de A de tamanho $(a+1) \times (a+1)$ como segue: i) Cada linha corresponde a uma função em (2.5) na ordem dada; ii) Cada coluna corresponde a um lugar de grau 1 de (2.3) na ordem dada; iii) Cada entrada de B é obtida por avaliação. Isto é,

$$B = [B_{ij}]\ \ i, j = 1, \ldots, l$$

onde B_{ij} é de tamanho $(b_i \times b_j)$ e cada entrada (u, v) é

$$\alpha_j^{i-1}\beta_{j,v}^{u_1} z^{u_2}(P_{\alpha_j,\beta_{j,v}}),\ u_1 + u_2 q = u - 1$$

logo

$$B_{ij} = \alpha_j^{i-1} D_{ij}\,,$$

onde

$$D_{ij} := \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \beta_{j,1} & \beta_{j,2} & \beta_{j,3} & \cdots & \beta_{j,b_j} \\ \beta_{j,1}^2 & \beta_{j,2}^2 & \beta_{j,3}^2 & \cdots & \beta_{j,b_j}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{j,1}^{q-1} & \beta_{j,2}^{q-1} & \beta_{j,3}^{q-1} & \cdots & \beta_{j,b_j}^{q-1} \\ z(P_{\alpha_j,\beta_{j,1}}) & z(P_{\alpha_j,\beta_{j,2}}) & z(P_{\alpha_j,\beta_{j,3}}) & \cdots & z(P_{\alpha_j,\beta_{j,b_j}}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{j,1}^{r_i} z^{s_i}(P_{\alpha_j,\beta_{j,1}}) & \beta_{j,2}^{r_i} z^{s_i}(P_{\alpha_j,\beta_{j,2}}) & \beta_{j,3}^{r_i} z^{s_i}(P_{\alpha_j,\beta_{j,3}}) & \cdots & \beta_{j,b_j}^{r_i} z^{s_i}(P_{\alpha_j,\beta_{j,b_j}}) \end{bmatrix}$$

tal que $r_i + s_i q = b_i - 1$. Note que a matriz $D_{i,j}$ é equivalente à matriz $\bar{D}_{ij}$ da forma:

$$\bar{D}_{ij} := \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ \beta_{j,1} & \beta_{j,2} & \beta_{j,3} & \cdots & \beta_{j,b_j} \\ \beta_{j,1}^2 & \beta_{j,2}^2 & \beta_{j,3}^2 & \cdots & \beta_{j,b_j}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \beta_{j,1}^{q-1} & \beta_{j,2}^{q-1} & \beta_{j,3}^{q-1} & \cdots & \beta_{j,b_j}^{q-1} \\ -\beta_{j,1}^{q} & -\beta_{j,2}^{q} & -\beta_{j,3}^{q} & \cdots & -\beta_{j,b_j}^{q} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (-1)^{s_i}\beta_{j,1}^{b_i-1} & (-1)^{s_i}\beta_{j,2}^{b_i-1} & (-1)^{s_i}\beta_{j,3}^{b_i-1} & \cdots & (-1)^{s_i}\beta_{j,b_j}^{b_i-1} \end{bmatrix}$$

Usando o método de eliminação de Gauss e por indução obtemos o seguinte lema.

Lema 2.17. Com as notações acima,

$$\det(B) = \left(\prod_{i=1}^{l} \det(D_{i,i})\right)\left(\prod_{j=2}^{l} \tau_j^{b_j}\right) = \left(\prod_{i=1}^{l} \det(\bar{D}_{i,i})\right)\left(\prod_{j=2}^{l} \tau_j^{b_j}\right)$$

onde

$$\tau_j = \prod_{i=1}^{j-1}(\alpha_j - \alpha_i),\ j = 2, 3, \ldots, l\,.$$

Lema 2.18. Seja $s^{\perp} = aq^{r-1} + bq^{r-2} + c$, onde $a = b + cq$, $0 \leq a \leq q^{r-1} - 2$. Então, quaisquer $a+1$ colunas de H são linearmente independentes sobre $\mathbb{F}_{q^r}$.

Demonstração: Considere quaisquer $a+1$ colunas distintas de H e, reordene essas colunas de acordo com α para os pontos $P_{\alpha,\beta}$. Então podemos construir matrizes A e B como acima. Visto que os α_i são distintos dois a dois para $i = 1, 2, \ldots, l$, temos que $\tau_j \neq 0$ para todo $j = 2, 3, \ldots, l$. Como os $\beta_{i,j}$ são distintos dois a dois para $j = 1, 2, \ldots, b_i$ e para um i qualquer tem-se que $\det(D_{i,i}) = \det(\bar{D}_{i,i}) \neq 0$. Assim, $\det(B) \neq 0$ pelo Lema (2.17). Isto significa que $a + 1 = posto(B) \leq posto(A) \leq a + 1$, logo $posto(A) = a + 1$. Portanto, as colunas de A são linearmente independentes sobre $\mathbb{F}_{q^r}$. □

Proposição 2.19. Seja $s^{\perp} = aq^{r-1} + bq^{r-2} + c \in H(Q_{\infty})$ onde $0 \leq b + cq \leq a = b' + c'q \leq q^{r-1} - 2$. Então

$$d(GH_s) = \begin{cases} a+2 & a = b + cq\,; \\ a+2 & a > b + cq \text{ e } b' < b\,; \\ a+1 & a > b + cq \text{ e } b' \geq b\,. \end{cases}$$

Demonstração: Se $a = b + cq$ então da Proposição (2.16) e do Lema (2.18) segue a afirmação. Suponha que $a = b' + c'q > b + cq \geq 0$ e $b' < b$. Seja $s' = n + 2g - 2 - b'(q^{r-2} + q^{r-1}) - c'(q^r + 1) = q^{2r-1} + q^{2r-2} - q^{r-1} - 2 - b'(q^{r-2} + q^{r-1}) - c'(q^r + 1)$. Então $s'^{\perp} = b'(q^{r-2} + q^{r-1}) + c'(q^r + 1)$ e assim $s'^{\perp} < s^{\perp}$, logo $s < s'$ e, portanto,

$$d(GH_s) \geq d(GH_{s'}) = a + 2.$$

Da Proposição 2.16 temos que $d(GH_s) \leq a+2$. Agora suponha que $a = b'+c'q > b+cq \geq 0$ e $b' \geq b$. Seja $\bar{s} = n+2g-2-\bar{b}(q^{r-2}+q^{r-1})-\bar{c}(q^r+1) = q^{2r-1}+q^{2r-2}-\bar{b}(q^{r-2}+q^{r-1})-\bar{c}(q^r+1)$ tal que $\bar{b} + \bar{c}q = a - 1$. Então $\bar{s}^{\perp} = \bar{b}(q + q^2) + \bar{c}(q^3 + 1)$ e assim $\bar{s}^{\perp} < s^{\perp}$, logo $s < \bar{s}$ e, portanto,

$$d(GH_s) \geq d(GH_{\bar{s}}) = (a - 1) + 2 = a + 1.$$

Da Proposição 2.16 temos que $d(GH_s) \leq a + 1$. □

Exemplo 2.20. Para $q = 2$ e $r = 3$, temos que o gênero da curva definida por $\mathcal{X}_{\mathbb{F}_8}$: $y^4 + y^2 + y = x^3 + x^5 + x^6$ é $g = 6$, e o número de pontos racionais é $N = 33$. Seja α uma raiz do polinômio irredutível $F(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Então $\mathbb{F}_8 = \{0, \alpha, \alpha^2, \alpha^3 = \alpha + 1, \alpha^4 = \alpha^2 + \alpha, \alpha^5 = \alpha^2 + \alpha + 1, \alpha^6 = \alpha^2 + 1, \alpha^7 = 1\}$ e assim,

$\mathcal{X}(\mathbb{F}_8) = \{P_1 = (0,0), P_2 = (0,\alpha), P_3 = (0,\alpha^2), P_4 = (0,\alpha^4), P_5 = (1,1), P_6 = (1,\alpha^3), P_7 = (1,\alpha^5), P_8 = (1,\alpha^6), P_9 = (\alpha,1), P_{10} = (\alpha,\alpha^3), P_{11} = (\alpha,\alpha^5), P_{12} = (\alpha,\alpha^6), P_{13} =$

$(\alpha^2, 1),\ P_{14} = (\alpha^2, \alpha^3), P_{15} = (\alpha^2, \alpha 5), P_{16} = (\alpha^2, \alpha^6), P_{17} = (\alpha^4, 1), P_{18} = (\alpha^4, \alpha^3), P_{19} = (\alpha^4, \alpha^5),\ P_{20} = (\alpha^4, \alpha^6), P_{21} = (\alpha^3, 0), P_{22} = (\alpha^3, \alpha), P_{23} = (\alpha^3, \alpha^2), P_{24} = (\alpha^3, \alpha^4), P_{25} = (\alpha^5, 0), P_{26} = (\alpha^5, \alpha), P_{27} = (\alpha^5, \alpha^2), P_{28} = (\alpha^5, \alpha^4), P_{29} = (\alpha^6, 0), P_{30} = (\alpha^6, \alpha), P_{31} = (\alpha^6, \alpha^2), P_{32} = (\alpha^6, \alpha^4), Q_\infty = (0 : 1 : 0)\}$.

Além disso, $\deg(D) = 32$ e $H(Q_\infty) = \{0, 4, 6, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, \ldots\}$.

Calculamos o divisor de algumas funções que usaremos para calcular distâncias mínimas exatas. Então,

$$(y) = 3P_1 + P_{21} + P_{25} + P_{29} - 6Q_\infty\,,$$

$$(x) = P_1 + P_2 + P_3 + P_4 - 4Q_\infty\,,$$

$$(x-1) = P_5 + P_6 + P_7 + P_8 - 4Q_\infty\,,$$

$$(x+y+1) = P_{10} + P_{16} + P_{19} + P_{22} + P_{28} + P_{31} - 6Q_\infty\,,$$

$$(z+y+1) = P_9 + P_{13} + P_{17} + P_{23} + P_{24} + P_{26} + P_{27} + P_{30} + P_{32} - 9Q_\infty\,.$$

Os parâmetros dos códigos GH_s deste exemplo são listados na tabela (2.1).

Tabela 2.1: Parâmetros para o código $GH_s = C_{\mathcal{L}}(D, sQ_\infty)$

s	$[\mathbf{n}, \mathbf{k}, \mathbf{d}]$	**s**	$[\mathbf{n}, \mathbf{k}, \mathbf{d}]$	**s**	$[\mathbf{n}, \mathbf{k}, \mathbf{d}]$
4	$[32, 2, 28]$	**19**	$[32, 14, 13]$	31	$[32, 26, 4]$
6	$[32, 3, 26]$	**20**	$[32, 15, 12]$	32	$[32, 26, 4]$
8	$[32, 4, 24]$	**21**	$[32, 16, 12]$	**33**	$[32, 27, 4]$
9	$[32, 5, 23]$	22	$[32, 17, 10]$	34	$[32, 28, 3]$
10	$[32, 6, 22]$	23	$[32, 18, 9]$	**35**	$[32, 29, 3]$
12	$[32, 7, 20]$	24	$[32, 19, 8]$	36	$[32, 29, 3]$
13	$[32, 8, 19]$	25	$[32, 20, 8]$	**37**	$[32, 30, 2]$
14	$[32, 9, 18]$	26	$[32, 21, 6]$	38	$[32, 30, 2]$
15	$[32, 10, 17]$	27	$[32, 22, 6]$	**39**	$[32, 31, 2]$
16	$[32, 11, 16]$	28	$[32, 23, 4]$	40	$[32, 31, 2]$
17	$[32, 12, 15]$	29	$[32, 24, 4]$	41	$[32, 31, 2]$
18	$[32, 13, 14]$	30	$[32, 25, 4]$	42	$[32, 31, 2]$

Observação 2.21. Na tabela (2.1), . Em [12], pode-se encontrar as melhores cotas conhecidas para as distâncias mínimas dos códigos lineares definidos sobre $\mathbb{F}_8$.

Agora especificamos a matriz geradora do código GH_s sobre $\mathbb{F}_{q^r}$. Fixando uma ordem para o conjunto

$$T := \{(\alpha,\beta) \in \mathbb{F}_{q^r} \times \mathbb{F}_{q^r} | \, \beta^{q^{r-1}} + \cdots + \beta^q + \beta = \alpha^{1+q} + \alpha^{1+q^2} + \cdots + \alpha^{q^{r-2}+q^{r-1}}\}\,.$$

Para $\ell = i \cdot q^{r-1} + j \cdot (q^{r-2} + q^{r-1}) + k \cdot (q^r + 1), i \geq 0, 0 \leq j < q, 0 \leq k < q^{r-2}$ definimos o vetor

$$u_\ell := (\alpha^i \beta^j (\alpha^{q+1} - \beta^q + \alpha^{q-1}\beta)^k)_{(\alpha,\beta)\in T} \in (\mathbb{F}_{q^r})^{q^{2r-1}}\,.$$

Da Proposição 2.9 e do Corolário 1.3 tem-se a seguinte proposição.

Proposição 2.22. Suponhamos que $0 \leq s < q^{2r-1}$ e seja $m := |I(s)|$. Então a matriz $m \times q^{2r-1}$

$$GHM_s := (u_\ell)_{\ell \in I(s)}\,,$$

é uma matriz geradora do código GH_s.

Em [16], Kirfel e Pellikaan estimaram a distância mínima de Feng-Rao δ_{FR}, ver subseção 1.2.1, para o caso em que o semigrupo de Weierstrass é telescópico. A seguir enunciamos dois resultados de [16] que aplicamos para fazer estimativas da distância mínima exata.

Teorema 2.23. [16, Teorema 6.10] Seja o semigrupo de Weierstrass $H(Q_\infty) = (\rho_i)_{i\in\mathbb{N}}$, gerado por uma seqüência telescópica $(a_1, \ldots, a_k)$. Suponha que $a_k = \max(A_k)$ e $d_{k-1} = \text{mdc}(a_1, \ldots, a_{k-1}) > 1$. Para códigos $C(r) = C_\Omega(D, \rho_r Q_\infty)$ tem-se que

$$\delta_{FR}(r) = \min\{\rho_t : \rho_t \geq r + 1 - g\}\,,$$

se $3g - 2 - (d_{k-1} - 1)a_k < r \leq 3g - 2$ e $g \leq r$.

Teorema 2.24. [16, Teorema 6.11] Seja o semigrupo de Weierstrass $H(Q_\infty)$ gerado pela seqüência telescópica $(a_1, \ldots, a_k)$. Suponha que $a_k = \max(A_k)$. Se

$$(j-1)a_k < \rho_{r+1} \leq ja_k \leq (d_{k-1} - 1)a_k\,,$$

então

$$\delta_{FR}(r) = j + 1\,.$$

Uma aplicação direta, destes resultados para o caso em consideração, obtém-se o seguinte resultado.

Proposição 2.25. Seja $GH^{\perp}_{\rho_s} = C_{\Omega}(D, \rho_s Q_{\infty})$. Então

$$\delta_{FR}(s) = \min\{\rho_t |\, \rho_t \geq s + 1 - g\} \,,$$

se $3g - 2 - (q^{r-2} - 1)(q^r + 1) < s \leq 3g - 2$ e $g \leq s$, onde $g = q^{r-1}(q^{r-1} - 1)/2$ e $r \geq 3$.

Demonstração: Ver na demonstração do Teorema 2.6 que $k = 3$, $d_{k-1} = d_2 = q^{r-2} > 1$ e $a_3 = q^r + 1$. □

Proposição 2.26. Com a notação como acima, se

$$(j-1)(q^r+1) < \rho_{s+1} \leq j(q^r+1) \leq (q^{r-2}-1)(q^r+1)\,,$$

então

$$\delta_{FR}(s) = j + 1\,.$$

Exemplo 2.27. [3, Exemplo 3.9] Para $q = 2$ e $r = 3$, temos que $g = 6$ e $n = 32$. Da Proposição 2.25 temos que $\delta_{FR}(s) = \min\{\rho_t : \rho_t \geq s - 5\}$, se $7 < s \leq 16$, $H(Q_{\infty}) = \langle 4, 6, 9\rangle$ e $d_s = s - 5$. Na tabela a seguir estão listadas a distância de Feng-Rao e a distância de Goppa para o código $GH^{\perp}_{\rho_s} = C_{\Omega}(D, \rho_s Q_{\infty})$.

$\mathbf{s}$	$\delta_{\mathbf{FR}}(\mathbf{s})$	$\mathbf{d_s}$
8	4	3
9	4	4
10	6	5
11	6	6
12	8	7
13	8	8
14	9	9
15	10	10
16	12	11

Exemplo 2.28. Consideremos também o caso $r = 3$ e $q = 3$. Então $g = 36$, $N = 244$ e portanto $n = 243 = \deg(D)$. Aplicando a Proposição 2.25 tem-se que $\delta_{FR}(s) = \min\{\rho_t |\, \rho_t \geq s - 35\}$, se $50 < s \leq 106$.

$$\begin{aligned} H(Q_{\infty}) \;=\; & \{0, 9, 12, 18, 21, 24, 27, 28, 30, 33, 36, 37, 39, 40, 42, 45, 46, 48, 49, 51, 52, \\ & 54, 55, 56, 57, 58, 60, 61, 63, 64, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, \ldots\} \end{aligned}$$

A dimensão do código $C(s) = GH^{\perp}_{\rho_s} = C_{\Omega}(D, \rho_s Q_{\infty})$ é $k = n + g - 1 - \rho_s$. Apresentamos na Tabela 2.2 alguns valores de s para os quais vemos que $\delta_{FR}(s) > d_s$, onde d_s é a distância mínima designada para o código de Goppa $C_{\Omega}(D, \rho_s Q_{\infty})$.

Tabela 2.2: Cotas Feng-Rao e Goppa para o Exemplo (2.28)

s	$\delta_{\mathbf{FR}}(\mathbf{s})$	$\mathbf{d_s}$	**s**	$\delta_{\mathbf{FR}}(\mathbf{s})$	$\mathbf{d_s}$	**s**	$\delta_{\mathbf{FR}}(\mathbf{s})$	$\mathbf{d_s}$
51	18	16	61	27	26	71	36	36
52	18	17	62	27	27	72	37	37
53	18	18	63	28	28	73	39	38
54	21	19	64	30	29	74	39	39
55	21	20	65	30	30	75	40	40
56	21	21	66	33	31	76	42	41
57	24	22	67	33	32	77	42	42
58	24	23	68	33	33	78	45	43
59	24	24	69	36	34	79	45	44
60	27	25	70	36	35	80	45	45

s	$\delta_{\mathbf{FR}}(\mathbf{s})$	$\mathbf{d_s}$	**s**	$\delta_{\mathbf{FR}}(\mathbf{s})$	$\mathbf{d_s}$
81	46	46	91	56	56
82	48	47	92	57	57
83	48	48	93	58	58
84	49	49	94	60	59
85	51	50	95	60	60
86	51	51	96	61	61
87	52	52	97	63	62
88	54	53	98	63	63
89	54	54	$99 - 105$	$64 - 70$	$64 - 70$
90	55	55	106	72	71

Exemplo 2.29. Para $q = 4$, temos que $g = 120$ e $n = 1024$. Então $H(Q_{\infty}) = \langle 16, 20, 65 \rangle$ e da Proposição 2.25 temos que $\delta_{FR}(s) = \min\{\rho_t : \rho_t \geq s - 119\}$ se $163 < s \leq 358$. Para

$s_1 = 164$ temos que $\delta_{FR}(164) = 48$ e $k_1 = 860$. Logo, sobre $\mathbb{F}_{64}$ temos o código $GH_{s_1}^{\perp}$ com parâmetros $[1024, 860, \geq 48]$.

Para terminar esta seção, aplicamos as Proposições 2.13, 2.19 e o cálculo da distância mínima de Feng-Rao para calcular as distâncias mínimas exatas dos códigos construídos no Exemplo 2.28. Apresentamos os cálculos na Tabela 2.3.

Tabela 2.3: Distâncias mínimas para os códigos $GH_s = C_{\mathcal{L}}(D, sQ_\infty)$ do Exemplo (2.28)

s	**d**	**s**	**d**	**s**	**d**	**s**	**d**	**s**	**d**	**s**	**d**	**s**	**d**	**s**	**d**
9	234	42	201	72	171	102	141	132	111	162	81	184	60	200	45
12	231	45	198	75	168	105	138	135	108	165	78	186	57	201	42
18	225	48	195	78	165	108	135	138	105	168	75	189	54	202	42
21	222	51	192	81	162	111	132	141	102	171	72	190	54	204	39
24	219	54	189	84	159	114	129	144	99	172	72	192	51	205	39
27	216	57	186	87	156	117	126	147	96	174	69	193	51	207	36
30	213	60	183	90	153	120	123	150	93	177	66	195	48	208	36
33	210	63	180	93	150	123	120	153	90	180	63	196	48	209	36
36	207	66	177	96	147	126	117	156	87	181	63	198	45	210	33
39	204	69	174	99	144	129	114	159	84	183	60	199	45	211	33

s	**d**	**s**	**d**
212	33	224	21
213	30	$225 - 230$	18
214	30	$231 - 233$	12
216	27	$234 - 245$	9
217	27	$246 - 257$	8
218	27	$258 - 261$	7
219	24	$262 - 273$	6
220	24	$274 - 285$	5
221	24	$286 - 289$	4
222	21	$290 - 301$	3
223	21	$302 - 313$	2

2.4 Automorfismos de Códigos Hermitianos Generalizados

Agora, estudamos *Automorfismos* de códigos Hermitianos generalizados. Seja $\epsilon \in \mathbb{F}_q \backslash \{0\}$, $\delta \in \mathbb{F}_{q^r}$ e $\mu^{q^{r-1}} + \cdots + \mu^q + \mu = \delta^{1+q} + \delta^{1+q^2} + \cdots + \delta^{q^{r-2}+q^{r-1}}$. Então para $\mu \in \mathbb{F}_{q^r}$, definimos um automorfismo $\sigma \in Aut(GH/\mathbb{F}_{q^r})$ da seguinte forma[1]:

$$\sigma(x) := \epsilon x + \delta \text{ e } \sigma(y) := \epsilon^2 y + (\delta^q + \delta^{q^2} + \cdots + \delta^{q^{r-1}})\epsilon x + \mu\,.$$

O conjunto de todos os automorfismos definidos como acima forma um grupo $\Sigma \subseteq Aut(GH/\mathbb{F}_{q^r})$ de ordem $q^{2r-1}(q-1)$. Isto vem do fato que $\epsilon \neq 0$ e δ são arbitrários, e para cada δ existem q^{r-1} possíveis valores de μ. Claramente $\sigma(Q_\infty) = Q_\infty$ para todo $\sigma \in \Sigma$, e σ permuta os lugares $P_{\alpha,\beta}$ de GH, pois são os únicos lugares em GH de grau 1 diferentes de Q_∞. Assim, mostramos a seguinte proposição.

Proposição 2.30. O grupo de Automorfismos $Aut(GH_s)$ contém o subgrupo Σ de ordem $q^{2r-1}(q-1)$.

Para $\delta, \mu \in \mathbb{F}_{q^r}$ tal que $\mu^{q^{r-1}} + \cdots + \mu^q + \mu = \delta^{1+q} + \delta^{1+q^2} + \cdots + \delta^{q^{r-2}+q^{r-1}}$ obtém-se um automorfismo τ definido por:

$$\tau(x) = x + \delta, \quad \tau(y) = y + (\delta^q + \cdots + \delta^{q^{r-1}})x + \mu\,,$$

Esses automorfismos constituem um subgrupo Γ de ordem q^{2r-1} no grupo $Aut(GH_s)$.

Proposição 2.31. Seja $s \geq 0$. Então

1. $$Aut(GH_s) \cong S_{q^{2r-1}}\ ,$$

   se $0 \leq s \leq q^{r-1} - 1$ ou $s > q^{2r-1} + q^{2r-2} - q^{r-1} - 2$, onde $S_{q^{2r-1}}$ é o grupo simétrico de comprimento q^{2r-1}.

2. $$Aut(GH_s) \cong GLA(2, q^r) \otimes S^{q^r}_{q^{r-1}}\ ,$$

[1] A exitência do automorfismo σ, vêm do fato que $(\sigma(x), \sigma(y))$ satisfaz a equação (2.1), o que é uma conseqüência da sua construção.

se $q^{r-1} \leq s < q^{r-2}+q^{r-1}$ ou $q^{2r-1}+q^{2r-2}-2q^{r-1}-q^{r-2}-2 \leq s \leq q^{2r-1}+q^{2r-2}-2q^{r-1}-2$, onde $GLA(2,q^r)$ é o grupo de transformações lineares afins sobre $\mathbb{F}_{q^r}$ e $S_{q^{r-1}}^{q^r}$ são q^r copias do grupo simétrico $S_{q^{r-1}}$.

Demonstração: *i*) Para $0 \leq s \leq q^{r-1}-1$ temos que GH_s é gerado por

$$(1,\ldots,1) \in (\mathbb{F}_{q^r})^{q^{2r-1}}.$$

Se $s \geq q^{2r-1}+q^{2r-2}-q^{r-1}-2$, então $GH_s = (\mathbb{F}_{q^r})^{q^{2r-1}}$, portanto a proposição segue do fato que

$$Aut(GH_{q^{2r-1}+q^{2r-2}-q^{r-1}-2-s}) = Aut(GH_s)\,.$$

ii) Se $s = q^{r-1}$ então GH_s é gerado pelos vetores

$$(1,\ldots,1) \text{ e } (x_1,\ldots,x_1,x_2,\ldots,x_2,\ldots,x_{q^r},\ldots,x_{q^r})\,,$$

portanto segue-se o resultado. □

2.5 Pesos Generalizados de Hamming sobre Códigos GH_s

A motivação principal para o estudo de pesos generalizados de Hamming e o peso hierárquico de um código é sua aplicação em criptografia, ver [31]. Nesta seção consideramos $r = 3$ e usando a mesma notação que na seção anterior temos que os códigos geométricos de Goppa construídos estão definidos sobre a curva

$$\mathcal{X}_{\mathbb{F}_{q^3}} : y^{q^2}+y^q+y = x^{1+q}+x^{1+q^2}+x^{q+q^2}\,.$$

Definição 2.32. Dizemos que um inteiro $s \leq n = q^5$ satisfaz a propriedade fraca estrela, se $s = i\cdot q^2 + j\cdot(q+q^2)$ com $i \geq 0$, $0 \leq j \leq q-1$, e $i \leq q^3-q-1$ ou $j = 0$.

Proposição 2.33. Se um inteiro s tem a propriedade fraca estrela, então existe um divisor D', $0 \preceq D' \preceq D$ tal que $D' \sim sQ_\infty$.

Demonstração: Para característica diferente de $p = 2$ a demonstração segue da Proposição 2.13. Para o caso particular $q = 2$ segue do Exemplo 2.20. □

O próximo corolário é uma conseqüência da Proposição 2.33.

Corolário 2.34. Se $s = iq^2 + j(q+q^2) \in H(Q_\infty)$, e $s \leq q^5 - q^3$ então s satisfaz a propriedade fraca estrela.

Seja $H(Q_\infty) = (\rho_i)_{i\in\mathbb{N}}$ o semigrupo de Weierstrass no ponto Q_∞. A seguir enunciamos alguns resultados importantes para obter informação sobre os pesos de Hamming generalizados nos códigos GH_s.

Proposição 2.35. Seja $GH_s = C_{\mathcal{L}}(D, sQ_\infty)$ o código de dimensão k e abundância $a \geq 0$. Para $1 \leq r \leq k$, se $s - \rho_{r+a}$ ou $n - s + \rho_{r+a}$ tem a propriedade fraca estrela, então

$$d_r(GH_s) \leq n - s + \rho_{r+a}\,.$$

Demonstração: Se $s - \rho_{r+a}$ é um número com a propriedade fraca estrela, então da Proposição 2.33 existe um divisor $0 \preceq D'' \preceq D$ tal que $(s - \rho_{r+a})Q_\infty \sim D''$, assim $\ell(sQ_\infty - D'') = \ell(\rho_{r+a}Q_\infty) = r + a$ e do Corolário 1.38 segue a desigualdade. Da mesma maneira, se $n-s+\rho_{r+a}$ satisfaz a propriedade fraca estrela, então existe um divisor $\bar{D} \sim (n-s+\rho_{r+a})Q_\infty$, $0 \preceq \bar{D} \preceq D$. Como $D \sim nQ_\infty$ obtém-se que $D'' = D - \bar{D} \sim (s - \rho_{r+a})Q_\infty$ com $0 \preceq D'' \preceq D$, e de forma semelhante obtemos o resultado. □

Proposição 2.36. Seja $GH_s = C_{\mathcal{L}}(D, sQ_\infty)$ um código de abundância $a > 0$. Então para todo r tal que $1 \leq r \leq g - a$ e $\rho_{r+1} = iq^2 + j(q + q^2)$ temos que

$$d_r(GH_s) \leq \rho_{r+1}\,.$$

Demonstração: Como $r \leq g - a$ tem-se que $\rho_{r+1} < q^4 - q^2 < q^5 - q^3$. Assim, segue-se que ρ_{r+1} satisfaz a propriedade fraca estrela, e da Proposição 2.33 existe um divisor efetivo $D' \preceq D$ tal que $D' \sim \rho_{r+1}Q_\infty$. Logo, $\ell(D') = r + 1$ e da Proposição 1.39 obtém-se que $d_r(GH_s) \leq \deg(D') = \rho_{r+1}$. □

A seguir enunciamos, para alguns valores de s, um resultado sobre o segundo peso generalizados de Hamming para os códigos GH_s.

Proposição 2.37. Seja $s = iq^2 + j(q + q^2)$ tal que $i \geq 1$, $0 \leq j < q$ e $q^2 \leq s < q^5$. Então

$$d_2(GH_s) = q^5 + q^2 - s\,.$$

Demonstração: Da Proposição 2.3 tem-se que a gonalidade da curva $\gamma = \gamma_2 = q^2$. Aplicando-se a Proposição 1.40 obtemos que $d_2(GH_s) \geq q^5 + q^2 - s$. Primeiro suponha que $q^2 \leq s \leq q^5 - q^3 + q^2$. Como $i \geq 1$ e $s - q^2 = (i-1)q^2 + j(q + q^2) \leq q^5 - q^3$,

dizemos que $s - q^2$ satisfaz a propriedade fraca estrela, logo da Proposição 2.35 segue que $d_2(GH_s) \leq q^5 + q^2 - s$. Agora, suponha que $q^5 - q^3 + q^2 \leq s < q^5$. Analogamente, $n + q^2 - s = q^5 + q^2 - iq^2 - j(q + q^2) = (q^3 - q - i)q^2 + (q - j)(q + q^2) \leq q^3$, e como $i \geq 1$ então segue que $q^5 + q^2 - s$ satisfaz a propriedade fraca estrela, logo da Proposição 2.35 segue que $d_2(GH_s) \leq q^5 + q^2 - s$. □

Proposição 2.38. Seja $s = j(q + q^2) \in H(Q_\infty)$ com $1 \leq j \leq q - 1$. Então,

$$q^5 - (j-1)(q+q^2) - q \leq d_2(GH_s) \leq q^5 - (j-1)(q+q^2)\,.$$

Demonstração: A primeira desigualdade segue da Proposição 1.40. A outra desigualdade segue da Proposição 1.41. □

A seguinte proposição segue das Proposições 1.41 e 2.13.

Proposição 2.39. Seja $GH_s = C_{\mathcal{L}}(D, sQ_\infty)$ o código de dimensão k e abundância $a \geq 0$. Então para todo r, $1 \leq r \leq \min\{g - a, k\}$ temos que

$$d_r(GH_s) \leq \begin{cases} n - s + \rho_{r+a} + bq & \text{Se } s - \rho_{r+a} = q^5 - q^4 - q^3 + aq^2 + bq \text{ com} \\ & q^2 + b \leq a \leq q^2 - q - 2, 1 \leq b \leq q - 2\,; \\ n - (\widetilde{s - \rho_{r+a}}) & \text{caso contrário}\,, \end{cases}$$

onde $\widetilde{s - \rho_{r+a}}$ é o maior elemento no semigrupo $H(Q_\infty)$ que é menor ou igual a $s - \rho_{r+a}$.

Proposição 2.40. Para $1 \leq s \leq n + 2g - 2 = q^5 + q^4 - q^2 - 2$ e $1 \leq r \leq \dim_{\mathbb{F}_{q^3}}(GH_s) - 1$, temos que

$$d_r(GH_s) \leq d_r(GH_{s-1}) \leq d_{r+1}(GH_s)\,.$$

Demonstração: A primeira desigualdade segue do fato que $GH_{s-1} \subseteq GH_s$, e a outra desigualdade vem do Corolário 1.38. □

Observação 2.41. Dado GH_s um código de dimensão k, temos que o único subespaço vetorial de GH_s de dimensão k é ele mesmo, e como a palavra $(1, 1 \ldots, 1) \in GH_s$, então segue que

$$d_k(GH_s) = n\,.$$

Exemplo 2.42. Se $s = n = q^5$ então o código $GH_{q^5} = C_{\mathcal{L}}(D, q^5 Q_\infty)$ tem abundância $a = 1$, logo para todo r, $1 \leq r \leq g - 1$ tal que $q^5 - \rho_{r+1}$ satisfaz a propriedade fraca estrela, então tem-se que

$$\gamma_{r+1} \leq d_r(GH_{q^5}) \leq \rho_{r+1}\,.$$

Exemplo 2.43. Continuamos com os mesmos dados do Exemplo 2.20. Aplicando a Proposição 1.34 obtém-se que $\gamma_1 = 0, \gamma_2 = 4, \gamma_3 = ?, \gamma_4 = 8, \gamma_5 = 9, \gamma_6 = 10$. Para $r > g = 6$, segue da Proposição 1.40 que $d_r(GH_s) = 32 - k + r$, onde k é a dimensão do código GH_s. Aplicando os resultados desta seção, e as propriedades de monotonicidade e dualidade dos pesos generalizados de Hamming, obtemos na tabela a seguir uma lista de valores dos pesos generalizados para os códigos $GH_s = C_{\mathcal{L}}(D, sQ_\infty)$.

s	4	6	8	9	10	12	13	14	15
$\mathbf{d_1}$	28	26	24	23	22	20	19	18	17
$\mathbf{d_2}$	32	31	28	$27-28$	26	24	23	22	$21-22$
$\mathbf{d_3}$	–	32	31	30	$27-28$	26	$24-26$	$23-24$	$22-23$
$\mathbf{d_4}$	–	–	32	31	30	28	27	26	25
$\mathbf{d_5}$	–	–	–	32	31	30	28	27	26
$\mathbf{d_6}$	–	–	–	–	32	31	30	28	28

s	16	17	18	19	20	21
$\mathbf{d_1}$	16	15	14	13	12	12
$\mathbf{d_2}$	20	19	18	17	16	$15-16$
$\mathbf{d_3}$	$21-22$	$22-20$	$19-20$	$18-19$	$17-18$	$16-18$
$\mathbf{d_4}$	24	23	22	21	20	19
$\mathbf{d_5}$	25	24	23	22	21	20
$\mathbf{d_6}$	26	26	24	23	22	22

Observação 2.44. No Exemplo 2.43 é suficiente calcular os pesos generalizados de Hamming para todo s entre $4 \leq s \leq 21$, pois, para os valores de s $22 \leq s \leq 42$ podem ser deduzidos facilmente pela propriedade de dualidade, Proposição 1.31, dos pesos calculados.

Agora, estudamos os pesos generalizados para $s \geq n$.

Lema 2.45. Para $2 \leq r \leq q$ temos que:

1. $d_r(GH_s) \leq q + q^2$ para $s = n + (r-2)q^2$;

2. $d_r(GH_s) \leq q^2$ para $s = n + (r-2)q^2 + (r-1)q$.

Demonstração: Se $s = n+(r-2)q^2$. Seja $a = \ell((r-2)q^2Q_\infty)$ a abundância do código GH_s, logo $\rho_a = (r-2)q^2$. Disso segue que $\rho_{r+a} = (r-1)q^2 + q$ e o número $n - s + \rho_{r+a} = q^2 + q$ satisfaz a propriedade fraca estrela. Portanto, da Proposição 2.35 obtém-se o resultado. Da mesma forma, para $s = n + (r-2)q^2 + (r-1)q$ temos que a abundância do código GH_s é $a = \ell((r-2)q^2 + (r-2)q)$, logo $\rho_a = (r-2)q^2 + (r-2)q$ e assim obtém-se que $\rho_{r+a} = (r-1)q^2 + (r-1)q$. Como $n - s + \rho_{r+a} = q^2$ satisfaz a propriedade fraca estrela segue-se o resultado. □

Proposição 2.46. Para $s = n+(a-2)q^2+(a-1)q$ com $2 \leq a \leq q$ e para todo r, $1 \leq r \leq a$ temos que:

$$d_r(GH_s) = q^2 - a + r\,.$$

Demonstração: Do Lema 2.45 segue que $d_a(GH_s) \leq q^2$ para todo a, $2 \leq a \leq q$. Como $s^\perp = (q^2-a)q^2 + (q-a)q + (q-2)$ e $q^2 - a = (q-1)q + (q-a)$, então da Proposição (2.19) obtém-se que $d_1(GH_s) = q^2 + 1 - a$. Logo, pela propriedade de monotonicidade segue-se que

$$q^2 = d_1(GH_s) + a - 1 \leq d_a(GH_s) \leq q^2\,,$$

desta forma temos igualdade. □

A seguir expomos o desempenho dos códigos no canal Wire-Tap do tipo II, isto é, uma aplicação do peso hierárquico de um código sobre o canal de comunicação wire-tap (de fio grampeado) do tipo II. Em [25], Ozarow e Wyner estudaram o canal wire-tap do tipo II; este sistema de comunicação permite que a um usuário não autorizado intercepte através do canal parte da mensagem transmitida, e o objetivo neste processo de transmissão de informação é maximar a incerteza do usuário não autorizado com respeito a mensagem enviada pelo canal sem o uso de uma chave privada para ocultar a mensagem.

O diagrama do sistema de comunicação esta dado na seguinte figura.

A seguir descrevemos a situação e os passos do algoritmo para estabelecer uma comunicação via o canal wire-tap do tipo II.

1. O usuário **A** deseja transmitir uma palavra $\mathbf{s}$ com k letras do alfabeto $\mathbb{F}_q$, $\mathbf{s} = (s_1, \ldots, s_k) \in \mathbb{F}_q^k$ para o usuário **B** usando o canal wire-tap do tipo II;

2. Se fixa C um $[n, n-k]$ código linear com matriz teste de paridade $H_{k\times n}$ (este código e esta matriz são conhecidas por qualquer usuário);

3. O usuário **A** calcula $\mathbf{x} \in \mathbb{F}_q^n$ uma solução do sistema $H\mathbf{x}^t = \mathbf{s}^t$;

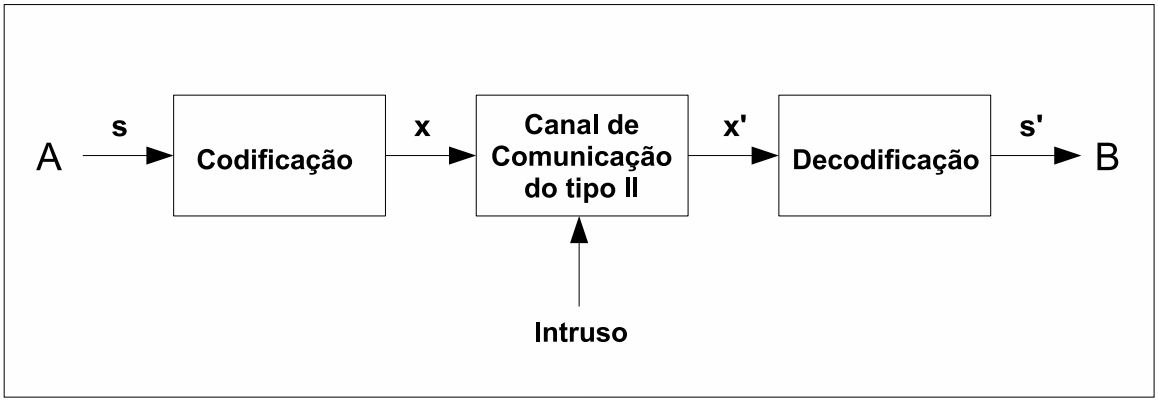


Figura 2.1: Canal Wire-Tap do tipo II

4. O conjunto de soluções é a classe lateral de $\mathbf{x}$ segundo C,

$$\mathbf{x} + C = \{\mathbf{x} + c : c \in C\} \subseteq \mathbb{F}_q^n ;$$

5. O usuário **A** envia aleatoriamente um elemento do conjunto $\mathbf{x} + C$ para o usuário **B**;

6. O Usuário não autorizado (ou intruso) escuta μ letras da mensagem enviada pelo usuário **A**;

7. O canal de comunicação é assumido sem barulho, assim que a correta decodificação da mensagem enviada não é o problema aqui. O foco do problema está em prevenir que o usuário não autorizado não obtenha informação suficiente com a qual possa conhecer a mensagem original que foi enviada;

8. A incerteza do usuário não autorizado é medida pelo peso hierárquico do código $C^{\perp}$.

Exemplo 2.47. Seja o código $C = GH_{30}$ com parâmetros $[32, 25]$ sobre $\mathbb{F}_8$ e matriz teste paridade $H_{7\times 32}$. O usuário **A** deseja transmitir uma palavra $\mathbf{s} \in \mathbb{F}_8^7$, então o usuário **A** escolhe um elemento aleatóriamente da classe lateral $\mathbf{x} + C$ onde $H_{7\times 32} \cdot \mathbf{x}_{32\times 1}^t = \mathbf{s}^t$. O peso hierárquico de GH_{12} é $\{20, 24, 26, 28, 30, 31, 32\}$. O seguinte gráfico mostra a incerteza do usuário não autorizado ao escutar μ letras da mensagem enviada. Note que a equivocação ou incerteza do usuário não autorizado vai diminuindo em exatamente os pesos generalizados de Hammnig do código $GH_{30}^{\perp} = GH_{12}$. Isto foi mostrado por Wei [31, Corolário A].

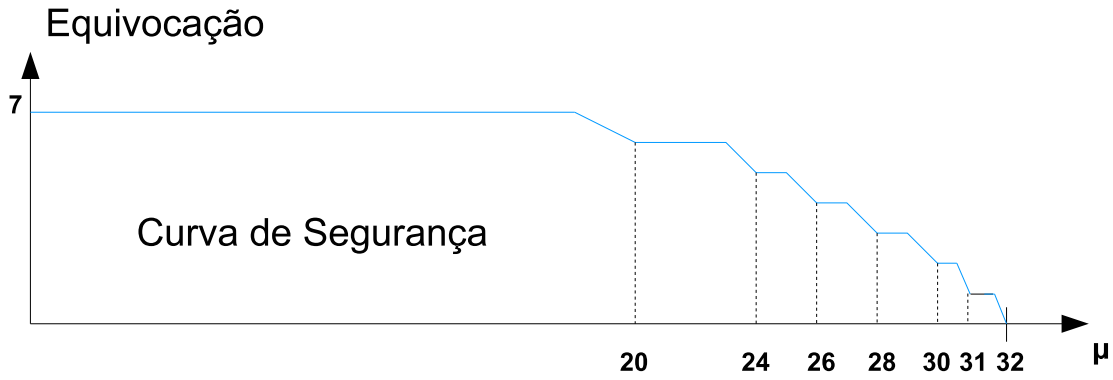


Figura 2.2: Curva de segurança do código GH_{30}

2.6 Subextensões Galoisianas dos corpos GH

Nesta seção, construímos explícitamente subextensões Galoisianas dos corpos GH com uma separação definida, isto é, extensões do corpo de funções racionais $\mathbb{F}_{q^r}(x)$, onde todos os lugares racionais são completamente separáveis e o lugar no infinito Q_∞ é totalmente separável. Para maior informação de extensões Galoisianas em corpos de funções algébricas, ver [28, Seções III.7 e III.8].

Em [5], Deolalikar com o propósito de mostrar que o quociente N/g era maior numa subextensão do corpo de funções GH (no caso particular $r = 3$) construiu o seguinte exemplo:

Dado $F = \mathbb{F}_{q^3}(x)$, $b \in \mathbb{F}_{q^3}$ tal que $\mathrm{Tr}_{\mathbb{F}_{q^3}|\mathbb{F}_q}(b) = 0$. Considerou o corpo de funções $E^1 = F(y_1)$, onde y_1 satisfaz

$$y_1^q + (1 + b^{q^2-q})y_1 = x^{1+q} + x^{1+q^2} + x^{q+q^2} .$$

Esta é uma subcobertura do corpo de funções $E = F(y)$ onde y satisfaz

$$y^{q^2} + y^q + y = x^{1+q} + x^{1+q^2} + x^{q+q^2} .$$

Para $q = 2$, Deolalikar observou que $\dfrac{N(E^1)}{g(E^1)} = \dfrac{17}{2} = 8.5$, e $\dfrac{N(E)}{g(E)} = \dfrac{33}{6} = 5.5$. Portanto, é interessante o estudo das subextensões dos corpos GH. Este exemplo foi restrito ao caso $r = 3$ da curva (2.1), e nós generalizamos este tipo de construção para qualquer valor de r.

A seguir, lembramos algumas definições e uma relação entre o diferente e os grupos de ramificação em extensões de corpos de funções e enunciamos um resultado de [5] para calcular o número de lugares racionais e o gênero da construção de subcorpos que definiremos.

Definição 2.48. Seja F'/F uma extensão finita e separável de corpos de funções. Então, o diferente de F'/F, denotado por $Dif(F'/F)$, é um divisor em F' dado por

$$Dif(F'/F) = \prod_{P' \in F'} d(P'|P) \cdot P' \,,$$

onde $d(P'|P)$ é o expoente diferente do lugar P' sobre $P \in \mathbb{P}_F$. O grau de $Dif(F'/F)$, denotado por $\deg(Dif(F'/F))$, é o grau deste divisor.

Proposição 2.49 (Formula do gênero de Hurwitz)**.** Seja F'/F uma extensão finita separável de corpo de funções. Então,

$$2g(F') - 2 = [F' : F](2g(F) - 2) + \deg(Dif(F'|F)) \,.$$

Definição 2.50 (Grupos de Ramificação)**.** Seja F'/F uma extensão Galoisiana de corpo de funções. Seja $P \subseteq P'$, onde P e P' são lugares em F e F', respectivamente. Para qualquer $i \geq 1$ definimos o *i-ésimo grupo de ramificação* de $G = Gal(F'/F)$ relativo a P' é

$$G_i := G_i(P'|P) = \{\sigma \in G : \upsilon_{P'}(\sigma(z) - z) \geq i + 1 \ \text{ para todo } \ z \in \mathcal{O}_{P'}\} \,.$$

Então, G_{-1} é o *grupo de decomposição*, G_0 o *grupo de inercia* de P' sobre P e G_{-1}/G_0 é $Gal(F'_{P'}/F_P)$, onde F_P e $F'_{P'}$ são o corpo residuo de P e P' respectivamente. Além disso, G_i é um subgrupo normal de G_{-1} como também de G_{i-1}, para $i \geq 0$. G_1 é um p-grupo e G_0/G_1 é um grupo cíclico de ordem coprimo com p.

A proposição a seguir nos dará uma forma de calcular o diferente $d(P'|P)$, usando os grupos de ramificação.

Proposição 2.51 (Fórmula do diferente de Hilbert)**.** Seja F'/F uma extensão de Galois de corpo de funções. Seja $P \subseteq P'$, onde P e P' são lugares em F e F', respectivamente. Então temos que

$$d(P'|P) = \sum_{i=0}^{\infty} (|G_i| - 1) \,.$$

Seja $f(x) \in \mathbb{F}_{q^r}[x]$, onde $q = p^t$. Na definição a seguir, um "termo" em $f(x)$ significa um monômio com coeficiente não nulo.

Definição 2.52. Um termo em $f(x)$ é chamado de um *termo coprimo* se o seu grau é coprimo com p.

Definição 2.53. Um termo coprimo em $f(x)$ de grau d é chamado *totalmente coprimo* se $f(x)$ não tem termos de grau dp^i para $i > 0$.

Definição 2.54. O grau coprimo de $f(x)$ é definido como o grau maior dos termos totalmente coprimos em $f(x)$, se $f(x)$ tem termos totalmente coprimos, e zero se $f(x)$ não tem termos totalmente coprimos. O grau coprimo de $f(x)$ é denotado por $cop(f)$.

Lema 2.55. [5, Lema 5.4] Seja $f(x) \in \mathbb{F}_{q^r}[x]$ um (r, q)-polinômio quase simétrico[2]. Se o grau coprimo de $f(x)$ é positivo, então este é no máximo $q^{r-1} + 1$.

Teorema 2.56. [5, Teorema 5.6] Seja K um subcorpo de $\bar{\mathbb{F}}_p$, não necessáriamente proprio, e seja $f(x) \in K[x]$. Suponha que V é um subgrupo finito do grupo aditivo de K e seja $a_V(T) := \prod_{v \in V}(T - v)$. Seja E uma extensão de $K(x)$ obtida por adjuntar uma raíz y do polinômio irredutível $a_V(T) - f(x)$. Então se cumpre que

i) $E/K(x)$ é Galois com grupo de Galois $G = \{y \to y + v\}_{v \in V}$.

ii) O único lugar ramificado de $K(x)$ é o lugar no infinito P_∞, e este é totalmente ramificado em E.

iii) Se Q_∞ é o único lugar de E que está acima de P_∞, então os grupos de ramificação de Q_∞ contém a seqüência inicial

$$G = G_0 = G_1 = \cdots = G_{cop(f)}\,.$$

Agora, definimos as subextensões dos corpos GH.

Seja $F = \mathbb{F}_{q^r}(x)$, $b \in \mathbb{F}_{q^r} \setminus \{0\}$ tal que $\mathrm{Tr}_{\mathbb{F}_{q^r}|\mathbb{F}_q}(b) = 0$. Considere o corpo de funções $E^j = F(y_j)$, onde y_j satisfaz

$$y_j^{q^j} - \left(\frac{1}{b^{q^j-q^{j-1}}} + \frac{1}{b^{q^j-q^{j-2}}} + \cdots + \frac{1}{b^{q^j-1}}\right) y_j^{q^{j-1}} - \cdots - \left(\frac{1}{b^{q^2-q}} + \frac{1}{b^{q^2-1}}\right) y_j^q - \frac{1}{b^{q-1}} y_j = S_r(x)\,,$$

tal que $S_r(x) := x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-2}+q^{r-1}}$. O corpo de funções sobre esta curva é coberto pelo corpo de funções definido pela curva (2.1), através da seguinte relação

$$\begin{aligned} y_j \;=\; & y^{q^{r-j-1}} + (b^{q^{r-1}-1} + \cdots + b^{q^{r-j}-1} + 1) y^{q^{r-j-2}} + \cdots + (b^{q^{r-1}-1} + \cdots + b^{q^3-1} + 1) y^q \\ & + (b^{q^{r-1}-1} + \cdots + b^{q^2-1} + 1) y. \end{aligned}$$

[2]Um polinômio $f(x)$ é chamado *quase simétrico* se é fixado pelo ciclo $\epsilon = (1\,2 \ldots r) \in \Gamma_r$, onde Γ_r é o grupo de permutações de r elementos.

Como conseqüência do Teorema 2.56 e do Lema 2.55 na construção feita anteriormente, obtemos a seguinte proposição.

Proposição 2.57. Para $j = 1, \ldots, r-2$ se cumpre que:

1. Para $Q_\infty^j \in E^j$ e $G = Gal(E^j/F)$ o grupo de Galois de E^j/F, tem-se que

$$G = G_0 = G_1 = \cdots = G_{cop(S_r(x))} = G_{q^{r-1}+1}\,,$$

e $G_{q^{r-1}+2} = G_{q^{r-1}+2}(Q_\infty|P_\infty) = \{id\}$, onde id representa o automorfismo identidade.

2. O gênero do subcorpo E^j é

$$g = \frac{(q^j-1)q^{r-1}}{2}\,.$$

3. O número de lugares racionais do subcorpo E^j é

$$N = q^{r+j} + 1\,.$$

Agora, com o intuito de construir códigos sobre estes subcorpos, calculamos o semigrupo de Weierstrass no ponto $Q_\infty^j \in E^j$.

Lema 2.58. Para $j = 1, \ldots, r-2$ e $Q_\infty^j \in E^j$ temos que

$$H(Q_\infty^j) = \left\langle q^j, q^{r-1}+1 \right\rangle\,.$$

Demonstração: Da equação da curva base sobre a qual está definida o subcorpo E^j tem-se que $(x)_\infty = q^j Q_\infty^j$. Por outro lado, define-se a função

$$z := x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^{r-2}} - y_j^{q^{j-1}}\,.$$

Observe que $z^q = x^{q+q^2} + x^{q+q^3} + \cdots + x^{q^{r-2}+q^{r-1}} - y^{q^j}$, e pela equação da curva sobre a qual está construído o subcorpo E^j obtém-se que $(z)_\infty = (q^{r-1}+1)Q_\infty^j$. Logo, $\langle q^j, q^{r-1}+1\rangle \subseteq H(Q_\infty^j)$. Assim, pelo gênero do subcorpo E^j segue o lema. □

Do Lema acima obtemos o seguinte resultado, importante para determinar os parâmetros dos códigos a construir-se sobre os subcorpos E^j.

Proposição 2.59. Seja $s \geq 0$ e $Q_\infty^j \in E^j$. Então

$$\mathcal{L}(sQ_\infty^j) = \left\langle x^i z^k : i \cdot q^j + k \cdot (q^{r-1}+1) \leq s\ ;\ i \geq 0, 0 \leq k < q^j \right\rangle\,,$$

onde $z := x^{1+q} + x^{1+q^2} + \cdots + x^{q^{r-3}+q^{r-2}} - y_j^{q^{j-1}}$.

Demonstração: É de forma análoga à demonstração da Proposição 2.9. □

O objetivo agora é construir códigos sobre os subcorpos E^j e comparar-los entre si, e também com os códigos construídos sobre os corpos GH.

Definição 2.60. Para $s \in \mathbb{N}_0$, seja

$$E_s^j := C_{\mathcal{L}}(D, sQ_\infty^j)\,,$$

onde

$$D := \sum_{\beta_j^{q^j} - \left(\frac{1}{b^{q^j-q^{j-1}}}+\cdots+\frac{1}{b^{q^j-1}}\right)\beta_j^{q^{j-1}} - \cdots - \left(\frac{1}{b^{q^2-q}}+\frac{1}{b^{q^2-1}}\right)\beta_j^q - \frac{1}{b^{q-1}}\beta_j = S_r(\alpha)} P_{\alpha,\beta}\,,$$

é a soma de todos os lugares racionais, exceto Q_∞^j, do corpo de funções $E^j/\mathbb{F}_{q^r}$.

Os códigos E_s^j são códigos de comprimento $n = q^{r+j}$ sobre $\mathbb{F}_{q^r}$. Da mesma forma como os códigos GH_s, tem-se que os códigos E_s^j são interessantes para

$$0 < s \leq q^{r+j} + q^{r+j-1} - q^{r-1} - 2\,.$$

Note que a curva base do subcorpo E^j

$$y_j^{q^j} - \left(\frac{1}{b^{q^j-q^{j-1}}} + \frac{1}{b^{q^j-q^{j-2}}} + \cdots + \frac{1}{b^{q^j-1}}\right) y_j^{q^{j-1}} - \cdots - \left(\frac{1}{b^{q^2-q}} + \frac{1}{b^{q^2-1}}\right) y_j^q - \frac{1}{b^{q-1}} y_j = S_r(x)$$

pode ser escrita como

$$y_j^{q^j} + (b^{q^{r-1}-q^j} + \cdots + b^{q^{j+1}-q^j} + 1) y_j^{q^{j-1}} + \cdots + (b^{q^{r-1}-q} + \cdots + b^{q^2-q} + 1) y_j = S_r(x)$$

e portanto esta curva tem a forma

$$(f(y_j))^q + y_j = g(x)\,,$$

onde $f(y_j) =$

$$c\left[y_j^{q^{j-1}} + \left(b^{q^{r-2}-q^{j-1}} + \cdots + b^{q^j-q^{j-1}} + 1\right) y_j^{q^{j-2}} + \cdots + \left(b^{q^{r-2}-q} + \cdots + b^{q^2-q} + 1\right) y_j\right]$$

tal que $c = \frac{1}{b^{q^{r-2}-1}+\cdots+b^{q-1}+1}$ e $g(x) = \frac{1}{b^{q^{r-1}-q}+\cdots+b^{q^2-q}+1} S_r(x)$.

Desta observação e da construção da curva tem-se que os corpos de funções E^j satisfazem as condições do Teorema 4.2 em [3] e portanto para o dual dos códigos E_s^j obtém-se a seguinte proposição.

Proposição 2.61. O código dual de E_s^j é

$$(E_s^j)^{\perp} = E^j_{n+2g(E^j)-2-s}\,.$$

Análogamente ao feito para o caso dos corpos GH, tem-se que a distância mínima dos códigos $\mathcal{X}_s$ para s um múltiplo de q^j é

$$d(\mathcal{X}_s) = n - s\,,$$

e para $q^{r+j} - q^j \leq s \leq q^{r+j}$ tem-se que

$$d(\mathcal{X}_s) = q^j\,.$$

Exemplo 2.62. Em particular, quando $r = 3$ e $q = 2$ a subextensão do corpo GH é uma curva Hiperelíptica sobre $\mathbb{F}_8$, com gênero $g = 2$ e o número de lugares de grau 1 do corpo de funções racionais sobre esta curva é $N = 17$. Aplicando os resultados desta seção, calculamos os parâmetros dos códigos $\mathcal{X}_s$, para alguns valores de $s \in H(Q^1_\infty)$.

Parâmetros dos códigos $\mathcal{X}_s$

s	$[\mathbf{n}, \mathbf{k}, \mathbf{d}]$
2	$[16, 2, 14]$
4	$[16, 3, 12]$
6	$[16, 5, 10]$
8	$[16, 7, 8]$
10	$[16, 9, 6]$
12	$[16, 11, 4]$
13	$[16, 12, 4]$
14	$[16, 13, 2]$
15	$[16, 14, 2]$
16	$[16, 14, 2]$

A distância mínima dos códigos $\mathcal{X}_s$ que atinge as melhores cotas conhecidas usamos negrito.

Na tabela a seguir, apresentamos os parâmetros dos códigos GH_s e $\mathcal{X}_s$ no caso $q = 2$, para alguns valores de s.

Parâmetros dos códigos GH_s e $\mathcal{X}_s$

s	$[\mathbf{n}, \mathbf{k}, \mathbf{d}]$
4	$[32, 2, 28]$
8	$[32, 4, 24]$
12	$[32, 7, 20]$
16	$[32, 11, 16]$
20	$[32, 15, 12]$
24	$[32, 19, 8]$
25	$[32, 20, 8]$
28	$[32, 23, 4]$
29	$[32, 24, 4]$
32	$[32, 26, 4]$

s	$[\mathbf{n}, \mathbf{k}, \mathbf{d}]$
2	$[16, 2, 14]$
4	$[16, 3, 12]$
6	$[16, 5, 10]$
8	$[16, 7, 8]$
10	$[16, 9, 6]$
12	$[16, 11, 4]$
13	$[16, 12, 4]$
14	$[16, 13, 2]$
15	$[16, 14, 2]$
16	$[16, 14, 2]$

Nas tabelas anteriores, podemos ver uma relação entre o código construído sobre a subextensão do corpo $GH/\mathbb{F}_8$, no caso $r = 3$. Note que o grau da subextensão de corpos neste caso é 2, então os códigos construídos sobre esta subextensão tem a metade do comprimento, e observamos também que no caso em que o valor de s na subextensão é a metade do valor de s no código sobre o corpo GH, a distância mínima se reduz a metade. Então, em primeira instância se esperaria que a dimensão do código também fosse reduzida a metade, mas isto não é o que acontece, pois como já se tinha observado, o quociente N/g é maior na subextensão do corpo GH.

Ainda existem vários tópicos a ser estudados sobre as subestensões dos corpos GH.

CAPÍTULO 3

Conclusões e Propostas Futuras de Trabalho

A seguir apresentamos algumas conclusões dos resultados obtidos durante o trabalho de tese.

- Na seção 2.2, com a construção da função racinal $z = x^{q+1} - y^q + x^{q-1}y$ do corpo de funções GH, conseguimos generalizar todos os resultados obtidos por Bulygin em [3].

- Na seção 2.3, calculamos distâncias mínimas exatas para os códigos GH_s com $0 \leq s \leq n + 2g - 2$, e desta forma melhoramos as distâncias mínimas obtidas por Bulygin. Na proposição 2.13, podemos observar que existe um intervalo de s onde falta calcular as distâncias mínimas exatas dos códigos GH_s, e em especial para os valores de $s = iq^{r-1} + j(q^{r-2} + q^{r-1}) + k(q^r + 1)$ com $k > 0$. Para o caso $q = 3$ e $r = 3$ calculamos os parâmetros dos códigos GH_s sobre $\mathbb{F}_{27}$, e pela propriedade da curva neste caso especial obtemos códigos com bons parâmetros. Assim, podemos pensar que estes parâmetros seríam melhores em alguns casos, se na literatura existissem códigos construídos sobre o mesmo corpo e com o mesmo comprimento.

- Na seção 2.4, calculamos um subgrupo do grupo de automorfismos dos códigos GH_s. Pela construção deste subgrupo, se pode pensar que este subgrupo seja o grupo de todos automorfismos dos códigos GH_s, mas ainda não faltaria mostrar.

- Na seção 2.5, foram calculadas para alguns valores de s, cotas para os pesos generalizados de Hamming e o valor exato do segundo peso generalizado de Hamming dos códigos GH_s. Devido ao fato de não conhecermos a seqüência de gonalidade do corpo de funções GH (que é um problema em aberto para corpos de funções algébricas com pelo menos um lugar singular), fica difícil encontrar todos os pesos generalizados de Hamming.

- Na seção 2.6, calculamos as fórmulas explícitas das subextensões dos corpos GH e construímos códigos sobre estas subextensões obtendo, em alguns casos, códigos com bons parâmetros comparados com os códigos conhecidos até o momento. Podemos observar aquí também uma estreita relação com respeito aos parâmetros entre os códigos construídos nos corpos GH com os códigos construídos nas subextensões destes corpos.

Por último, enunciamos algumas propostas futuras de pesquisa a continuar.

- Calcular pesos hierárquicos dos códigos GH_s e refinar as cotas encontradas usando a generalização da distância Feng-Rao [22], [1], e complexidade de treliças [23].

- Implementar algoritmos de codificação e decodificação para os códigos GH_s, em forma análoga ao feito para códigos Hermitianos [24], [27]. Durante o trabalho de tese conseguimos calcular um semigrupo do grupo de automorfismos dos códigos propostos GH_s, o qual pode-nos ajudar na implementação de algoritmos de decodificação.

- Continuar estudando os códigos sobre as subextensões dos corpos GH, com o propósito de obter informação sobre os códigos construídos nos corpos GH e, recíprocamente.

  Recentes pesquisas tem mostrado que o conceito de gênero passou a ser de grande importância para o estudo de sistemas de comunicação digital [4]. Esta relação motiva o estudo dos códigos geométricos de Goppa com bons parâmetros e de gênero pequeno. Desta relação, estudar os códigos sobre as subextensões dos corpos GH é também de interesse para possíveis aplicações nos sistemas de comunicação digital.

BIBLIOGRAFIA

[1] A.I. Barbero e C. Munuera, *The Weight Hierarchy of Hermitian Codes*, Siam J. Discrete Math. **13 (1)**, 79–104 (2000).

[2] E. Biglieri e M. Elia, *Cyclic-Group Codes for the Gaussian Channel*, IEEE Trans. Inform. Theory **22**, 624–629 (1976).

[3] S.V. Bulygin, *Generalized Hermitian Codes Over* $GF(2^r)$, IEEE Trans. Inform. Theory **52 (10)**, 4664–4669 (2006).

[4] R.G. Cavalcante, H. Lazari, J. de Deus Lima e R. Paalazzo, *A New Approach to the Design of Digital Communications Systems*, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **68**, 145–177 (2005).

[5] V. Deolalikar, *Explicitly constructed extensions of the rational function field with prescribed splitting*, Finite Fields Appl. **9**, 222–236 (2003).

[6] T. Ericson e V. Zinoviev, *Codes on Euclidean Spheres*, Elsevier Science Pub Co, 2001.

[7] G.L. Feng, K.K. Tzeng e V.K. Wei, *On the generalized Hamming weights for several classes of cyclic codes*, IEEE Trans. Inform. Theory **38**, 1125–1130 (1992).

[8] A. Garcia e H. Stichtenoth, *Elementary Abelian p-extensions of algebraic function fields*, Manuscripta Math. **72**, 67–79 (1991).

[9] A. Garcia e H. Stichtenoth, *A class of polynomials over finite fields*, Finite Fields Appl. **55**, 424–435 (1999).

[10] G. van der Geer e M. van der Vlugt, *Tables of Curves with Many Points*, Abril 22 (1998). Disponível em http://www.science.uva.nl/∼geer

[11] V.D. Goppa, *Algebraic-Geometric codes*, Math. USRR-Izv. **21 (1)**, 75–93 (1983).

[12] M. Grassl, *Bounds on the minimum distance of linear codes*, disponível no site http://www.codetables.de. (Último acesso foi em 02/01/2008)

[13] V. Guruswami, *List Decoding From Erasures: Bounds and Code Constructions*, IEEE Trans. Inform. Theory **49 (11)**, 2826–2832 (2003).

[14] T. Høholdt, J.H. van Lint, e R. Pellikaan, *Algebraic geometry codes*, in Handbook of Coding Theory, V.S.Pless, W.C. Huffman, and R.A. Brualdi, Eds. Amsterdam, The Netherlands: Elsevier **1**, 871–961 (1998).

[15] I. Ingemarsson, *Commutative Group Codes for the Gaussian Channel*, IEEE Trans. Inform. Theory **19**, 215–219 (1973).

[16] C. Kirfel e R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41 (6)**, 1720–1732 (1995).

[17] P.V Kumar e K. Yang, *On the true minimum distance of Hermitian codes*, (H. Stichtenoth and M.F. Tsfasman, eds.) Lecture Notes in Math. **1518**, Coding Theory and Algebraic Geometry, Springer-Verlag, 99–107 (1992).

[18] P.V. Kumar, H. Stichtenoth e K. Yang, *On the weight hierarchy of Geometric Goppa Codes*, IEEE Trans. Inform. Theory **40 (3)**, 913–920 (1994).

[19] R. Lidl e H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications 20, Cambridge Univ. Press, Cambidge, xiv+755 pp, (1997).

[20] J.H. van Lint, Introduction to coding theory, Graduate Text in Mathematics, Springer Verlag, Berlin (1999).

[21] C. Munuera, *On the Generalized Hamming Weights of Geometric Goppa Codes*, IEEE Trans. Inform. Theory **40 (6)**, 2092–2099 (1994).

[22] C. Munuera e D. Ramirez, *The Second and Third Generalized Hamming Weights of Hermitian Codes*, IEEE Trans. Inform. Theory **45 (2)**, 709–712 (1999).

[23] C. Munuera e F. Torres, *Bounding the trellis state complexity of algebraic geometric codes*, Appl. Algebra Engrg. Comm. Comput. **15**, 81–100 (2004).

[24] M.E. O'Sullivan, *Decoding of Hermitian Codes: The Key Equation and Efficient Error Evaluation*, IEEE Trans. Inform. Theory **46 (2)**, 512–523 (2000).

[25] L.H. Ozarow e A.D. Wyner, *Wire-Tap-channel II*, AT&T Bell Labs. Tech. J. **63 (10)**, 2135–2157 (1984).

[26] R. Siqueira e S.I.R. Costa, *Minimum Distance Upper Bounds for Commutative Group Codes*, Proc. IEEE Inform. Theory Workshop, Uruguay Março 13–17 (2006).

[27] B.-Z. Shen, *On encoding and decoding of the codes from Hermitian curves*, in Cryptography and Coding III, IMA Conf. Proc., Serie 45. Oxford, U.K.: Oxford Univ. Press, 337–356 (1993).

[28] H. Stichtenoth, Algebraic function fields and codes, Universitext, Springer Verlag, Berlin (1993).

[29] M.A. Tsfasman, S.G. Vladut, e T. Zink: *Modular curves, Shimura curves and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109**, 21–28 (1982).

[30] M.A. Tsfasman e S.G. Vladut, *Algebraic-Geometric Codes*, Kluwer Academic Publisher, Dordrecht-Boston-London, (1991).

[31] V.K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37**, 1412–1418 (1991).

[32] V.K. Wei e K. Yang, *On the generalized Hamming weight of product codes*, IEEE Trans. Inform. Theory **39**, 1709–1713 (1993).

[33] S. Wesemeyer, *On the Automorphism Group of Various Goppa Codes*, IEEE Trans. Inform. Theory **44 (2)**, 630–643 (1998).