Moisés Ceni de Almeida

Códigos Hermitianos

Rio de Janeiro
2014

Moisés Ceni de Almeida

Códigos Hermitianos

Dissertação apresentada ao Instituto de Matemática da Universidade Federal do Rio de Janeiro, para a obtenção de Título de Mestre em Matemática, na Área de Matemática.

Orientador: Luciane Quoos Conte

Rio de Janeiro
2014

Códigos Hermitianos

Moisés Ceni de Almeida

Orientadora: Luciane Quoos Conte

Dissertação de Matemática submetida ao Programa de Pós-graduação do Instituto de Matemática da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada por:

_____

Dra. Luciane Quoos Conte.
Universidade Federal do Rio de Janeiro - UFRJ.

_____

Dra. Ariane M. Masuda.
The City University of New York - CUNY.

_____

Dra. Cecília Salgado Guimarães da Silva.
Universidade Federal do Rio de Janeiro - UFRJ.

_____

Dra. Miriam Del Milagro Abdon.
Universidade Federal Fluminense - UFF.

Rio de Janeiro, 13 de Agosto de 2014.

Dedicatória...

Epígrafe

Conta o número das estrelas,
e chama-as pelos seus nomes.

Salmos 147.4.

Agradecimentos

Agradeço a Deus, por tudo.

Agradeço a toda minha família, em especial a minha mãe Dinazard, e aos meus irmãos Geziel e Rafael pelo grande apoio acadêmico. Meus demais irmãos e meu pai, vocês todos são minha vida.

Agradeço a CAPES, que financiou meus estudos durante minha formação de mestre.

No meio acadêmico, agradeço primeiramente a minha excelente orientadora, Luciane Quoos Conte, por toda paciência. Agradeço aos meus excelentes professores do Instituto de Matemática que tive o prazer de conhecer. Agradeço a Felipe Bottega Diniz, que contribuiu com meu trabalho me ajudando no aplicativo em linguagem C para os códigos Hermitianos.

Agradeço meus amigos mais próximos que tinham a mesma missão que eu, em especial, Kaísa Pereira, Taynara, Diego, Vinícius, Deise, Felipe, Daniel e Zanardi. A todos vocês dedico este trabalho.

Resumo

O corpo de funções Hermitiano é o corpo de funções algébricas em uma variável $\mathcal{H} = \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$, onde $y^q + y = x^{q+1}$ e $\mathbb{F}_{q^2}$ é o corpo finito com cardinalidade q^2. Este corpo de funções algébricas atinge a Cota de Hasse-Weil para o número de pontos racionais sobre $\mathbb{F}_{q^2}$ e tem sido objeto de intenso estudo desde a década de oitenta tanto em relação a teoria de códigos, bem como a teoria de curvas maximais. Neste trabalho determinamos todos os parâmetros (comprimento, dimensão e distância mínima) dos códigos Hermitianos, que são os Códigos Algébricos Geométricos com suporte em um ponto construídos a partir do corpo de funções Hermitiano.

Palavras-chave: códigos, dimensões, distância mínima.

Abstract

The Hermitian function field is the algebraic functions field $\mathcal{H} = \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ where $y^q + y = x^{q+1}$ and $\mathbb{F}_{q^2}$ is the finite field with cardinality q^2. This algebraic function field attains the Hasse-Weil bound for the number of rational points on $\mathbb{F}_{q^2}$ and has been object of intense study since the eighties, both in relation to coding theory and the theory of maximal curves. In this work we determine all parameters (length, dimension and minimum distance) of Hermitian codes, which are the Algebraic Geometry Codes supported in one point constructed from of the Hermitian function field.

Keywords: codes, dimensions, minimum distances.

Sumário

Capítulo 1

Introdução

1.1 Corpos de Funções

O primeiro capítulo deste trabalho é dedicado a apresentar os principais conceitos e ferramentas dos Corpos de Funções algébricas. Neste sentido, o principal objetivo é apresentar os conceitos de Espaços de Riemann Roch e suas conexões com os parâmetros de um código algébrico geométrico, que são códigos contruídos a partir de um corpo de funções. Para a caracterização dos Códigos Hermitianos, que são um caso particular dos códigos algébricos geométricos, precisaremos dos Teoremas de Kummer e Artin Schreier.

Neste capítulo usamos principalmente a teoria do livro de Stichtenoth [(16)].

Durante esta seção K denotará um corpo arbitrário.

Definição 1. *Um corpo de funções algébricas F/K em uma variável sobre K ou simplesmente um corpo de funções é uma extensão de corpos $F \supset K$ tal que F é uma extensão algébrica finita de $K(x)$, onde $x \in F \setminus K$ é transcendente sobre K.*

Seja $z \in F$ um elemento diferente de x que também é transcendente sobre K.

Claramente, z e x não podem ser algebricamente independentes, pois F/K tem grau de transcendência 1. Segue que existe um polinômio não nulo $p(T_1, T_2) \in K[T_1, T_2]$ tal que $p(x,z) = 0$. Logo, x é algébrico sobre $K(z)$ e

$$[F : K(z)] = [F : K(x,z)][K(x,z) : K(z)] \leq [F : K(x)][K(x,z) : K(z)] < \infty$$

Isto, em particular, quer dizer que ambas as extensões $F/K(z)$ e $F/K(x)$ têm grau finito e F/K continua a ser um corpo de funções independentemente do elemento transcendente escolhido. Mas, em geral, não temos que $[F : K(x)] = [F : K(z)]$.

Definição 2. *O corpo $\widetilde{K} = \{z \in F \mid z$ é algébrico sobre $K\}$ é chamado o corpo de constantes de F/K. Dizemos que K é algebricamente fechado em F se $\widetilde{K} = K$.*

Definição 3. *Um anel $\mathcal{O} \subset F$ é dito um anel de valorização de F/K se:*

i. $K \subsetneq \mathcal{O} \subsetneq F$,

ii. Para cada $z \in F$, temos $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Exemplo 1. *Seja $F = K(x)$ o corpo de funções racionais. O conjunto*

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x], deg(f(x)) \leq deg(g(x)) \right\}$$

é um anel de valorização de $K(x)/K$, como é de fácil verificação.

Proposição 1 ((16), Proposição 1.1.5)**.** *Seja $\mathcal{O}$ um anel de valorização do corpo de funções F/K. Então:*

i. $\mathcal{O}$ *possui um único ideal maximal* $P = \mathcal{O} \setminus \mathcal{O}^*$, *onde*

$$\mathcal{O}^* := \{z \in \mathcal{O} \mid \exists\ w \in \mathcal{O}\ com\ zw = 1\}$$

é o grupo das unidades de $\mathcal{O}$,

ii. Temos $\widetilde{K} \subseteq \mathcal{O}$ *e* $\widetilde{K} \cap P = \{0\}$.

Teorema 1 ((16), Teorema 1.1.6)**.** *Sejam* $\mathcal{O}$ *um anel de valorização do corpo de funções* F/K *e* P *seu único ideal maximal. Então:*

i. P *é um ideal principal,*

ii. Se $P = t\mathcal{O}$, *então cada* $0 \neq z \in F$ *tem uma única representação na forma* $z = t^n u$ *onde* $n \in \mathbb{Z}$ *e* $u \in \mathcal{O}^*$. *Neste caso, dizemos que* t *é um elemento primo para* P,

iii. $\mathcal{O}$ *é um domínio de ideais principais. Mais precisamente, se* $P = t\mathcal{O}$ *e* $\{0\} \neq I \subset \mathcal{O}$ *é um ideal, então* $I = t^n\mathcal{O}$ *para algum* $n \in \mathbb{Z}$.

Sejam t_1 e t_2 dois elementos primos de P, então $P = t_1\mathcal{O} = t_2\mathcal{O}$. Logo, como $t_1 \in t_1\mathcal{O} = t_2\mathcal{O}$, temos que existe $w_2 \in \mathcal{O}$, tal que $t_1 = t_2 w_2$. De modo análogo concluímos que existe $w_1 \in \mathcal{O}$ tal que $t_2 = t_1 w_1$. Assim $t_1 = t_1 w_1 w_2$ e concluímos que w_1 e w_2 são unidades em $\mathcal{O}$.

Definição 4. *Um lugar* P *de um corpo de funções* F/K *é o ideal maximal de algum anel de valorização* $\mathcal{O}$ *de* F/K *e* $\mathbb{P}_{F/K}$ *é o conjunto de todos os lugares de* F/K.

Evidentemente, se $\mathcal{O}$ é um anel de valorização e P é seu ideal maximal, $\mathcal{O}$ está unicamente determinado por P da seguinte maneira $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Desse modo vamos escrever $\mathcal{O}_P$ no lugar de $\mathcal{O}$.

Definição 5. *Uma valorização de F/K é uma função $v : F \to \mathbb{Z} \cup \infty$ tal que:*

i. $\exists\ z \in F, v(z) = 1$,

ii. $v(a) = 0, \forall\, a \in K \setminus \{0\}$,

iii. $v(x) = \infty \Leftrightarrow x = 0$,

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

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

É importante ressaltar que, dados $x,y \in F$ tais que $v(x) \neq v(y)$ então

$$v(x + y) = min\{v(x),v(y)\}.$$

Esta é a desigualdade triangular estrita, [(16), Lema 1.1.11].

Definição 6. *Para um lugar $P \in \mathbb{P}_{F/K}$ definimos $v_P : F \to \mathbb{Z} \cup \{\infty\}$ da seguinte maneira: se t é um elemento primo para P e $z = t^n u$ com $u \in \mathcal{O}^*$ e $n \in \mathbb{Z}$, então $v_P(z) = n$ e $v_P(0) = \infty$.*

Vamos mostrar que v_P está bem definida, de fato, se t_1 e t_2 são elementos primos para P e $z \in F^*$, podemos escrever $z = t_1^n u = t_2^n(w^n u)$, onde $w^n u \in \mathcal{O}^*$ é tal que $t_1 = t_2 w$. Deste modo $v_P(z)$ não depende do elemento primo escolhido para P.

Definição 7. *Para um lugar $P \in \mathbb{P}_{F/K}$ definimos o corpo das classes residuais no lugar P, $F_P := \mathcal{O}/P$. O homomorfismo canônico de $\mathcal{O}_P$ em $F_P (x \mapsto x(P))$, é dito o mapa da classe residual com relação a P. Finalmente, $deg(P) := [F_P : K]$ é o grau de P.*

Repare que faz sentido falar de grau de P, pois F_P é corpo, já que P é um ideal maximal.

Definição 8. *Para $z \in F$, $m \in \mathbb{N}$ e $P \in \mathbb{P}_F$ dizemos que P é um pólo de ordem m de z se $v_P(z) = -m < 0$, e que P é um zero de ordem m de z se $v_P(z) = m > 0$.*

Proposição 2 ((16), Corolário 1.1.20)**.** *Se $z \in F$ é transcendente sobre K, então z tem pelo menos um pólo e um zero.*

Em particular, $\mathbb{P}_{F/K} \neq \emptyset$.

Definição 9. *Um divisor D do corpo de funções F/K é uma soma formal*

$$D = \sum n_P P,$$

onde $n_P \in \mathbb{Z}, P \in \mathbb{P}_{F/K}$ e $n_P = 0$ para quase todo P.
O conjunto de divisores de F/K, denotado por $Div(F)$, é um grupo abeliano (aditivo) livremente gerado.
O Suporte de um divisor D é definido como $supp(D) := \{P \in \mathbb{P}_{F/K} \mid n_P \neq 0\}$.
Um divisor da forma $D = P$, onde P é um lugar, é chamado de divisor primo.
Para Q um lugar de F/K e $D = \sum n_P P$ um divisor, definimos $v_Q(D) = n_Q$.
Podemos definir ainda uma ordem parcial em $Div(F)$:

$$D_1 \leq D_2 \Leftrightarrow v_Q(D_1) \leq v_Q(D_2), \forall Q \in \mathbb{P}_{F/K}.$$

Um divisor satisfazendo $D \geq 0$ é chamado de divisor efetivo.
Dado um divisor D, definimos o seu grau por $deg(D) = \sum_{P \in \mathbb{P}_{F/K}} v_P(D) \cdot deg(P)$.

Definição 10. *Para um elemento não nulo $z \in F$, sejam Z o conjunto de zeros de z e N o conjunto de pólos de z. Definimos:*

$$(z)_0 := \sum_{P \in Z} v_P P,$$

o divisor de zeros de z,

$$(z)_\infty := \sum_{P \in N} v_P P,$$

o divisor de pólos de z e

$$(z) := (z)_0 - (z)_\infty = \sum_{P \in \mathbb{P}_{F/K}} v_P P,$$

o divisor de z.
Um divisor é dito divisor principal se ele é o divisor de alguma função $z \in F$.

Dois divisores $D, D' \in Div(F)$ são ditos equivalentes e denotamos por $D \sim D'$ ou $D \equiv D'$ se $D = D' + (x)$ para algum $x \in F \setminus \{0\}$.

Definição 11. *Para $A \in Div(F)$ definimos*

$$\mathcal{L}(A) := \{x \in F; (x) \geq -A\} \cup \{0\},$$

que é um espaço vetorial sobre K, chamado de Espaço de Riemann-Roch associado ao divisor A.

Note que $x \in \mathcal{L}(A)$ se, e somente se $v_P(x) \geq -v_P(A), \forall\, P \in \mathbb{P}_{F/K}$.
A Proposição a seguir será crucial no estudo dos códigos de Goppa, pois veremos que a dimensão destes códigos nada mais é que a dimensão do espaço de Riemann-

Roch de um certo divisor.

Proposição 3 ((16), Observação 1.4.5, Lema 1.4.6, Lema 1.4.7)**.** *Para $A \in Div(F)$ valem:*

i. $\mathcal{L}(A) \neq \{0\} \Leftrightarrow \exists\ A' \in Div(F)$ *equivalente a* A *tal que* $A' \geq 0$,

ii. *se* A' *é equivalente a* A *então* $\mathcal{L}(A)$ *é isomorfo como espaço vetorial a* $\mathcal{L}(A')$,

iii. $\mathcal{L}(0) = K$ *e*,

iv. *se* $A < 0$, *então* $\mathcal{L}(A) = \{0\}$.

Adotamos a seguinte notação $dim(\mathcal{L}(A)) = l(A)$.

As seguintes definições serão ferramentas importantes para os cálculos das dimensões dos códigos.

Definição 12. *Um Adele de F/K é um mapa:*

$$\alpha : \begin{cases} \mathbb{P}_{F/K} & \longrightarrow F, \\ P & \longmapsto \alpha_P \end{cases}$$

tal que $\alpha_P \in \mathcal{O}_P$ para quase todo lugar de F/K.

Definimos ainda $\mathcal{A}_F := \{\alpha \,|\, \alpha \text{ é um adele de } F/K\}$ e

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \,|\, v_P(\alpha) \geq v_P(A), \forall\, P \in \mathbb{P}_{F/K}\},$$

onde $v_P(\alpha) = v_P(\alpha_P)$ e α_P é o P-ésimo componente de α.

Definição 13. *Uma Diferencial de Weil de F/K é um mapa $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(A) + F$ para algum $A \in Div(F)$. Analogamente aos adeles,*

definimos $\Omega_F := \{\omega \,|\, \omega \text{ é uma diferencial de Weil de } F/K\}$ *e*

$$\Omega_F(A) := \{\omega \in \Omega_F \,|\quad \omega \text{ se anula em } \quad \mathcal{A}_F(A) + F\}.$$

Definição 14. *Um divisor* (ω) *de uma diferencial de Weil é o único divisor de* F/K *satisfazendo: (1)* ω *se anula em* $\mathcal{A}_F((\omega)) + F$ *e (2) se* ω *se anula em* $\mathcal{A}_F(A) + F$ *então* $A \leq (\omega)$.

Definição 15. *Um divisor* W *tal que existe uma diferencial* ω *em* Ω_F *com* $W = (\omega)$ *é chamado de divisor canônico.*

A garantia da existência e unicidade de (ω) na definição 14 é dada por [(16), Lema 1.5.10].

Proposição 4. *Existe uma constante* $\gamma \in \mathbb{Z}$ *tal que para todos os divisores* $A \in Div(F)$ *vale:*

$$deg(A) - l(A) \leq \gamma.$$

É importante ressaltar que a constante γ acima não depende do divisor $A \in Div(F)$, dependendo somente do corpo de funções F/K.

Definição 16. *O gênero* g *do corpo de funções* F/K *é definido como*

$$g := max\{deg(A) - l(A) + 1 \,|\, A \in Div(F)\}.$$

Naturalmente, o gênero está bem definido pela Proposição 4.

O seguinte Teorema é um dos mais importantes da teoria dos corpos de funções, pois fornece um meio efetivo de calcular a dimensão de um espaço de Riemann-Roch.

Teorema 2. (Teorema de Riemann-Roch) *[(16), Teorema 1.5.15]: Para cada divisor $A \in Div(F)$ vale*

$$l(A) = deg(A) + 1 - g + l(W - A)$$

onde W é um divisor canônico de F/K.

Teorema 3. *Se $A \in Div(F)$ e $deg(A) \geq 2g - 1$, então:*

$$l(A) = deg(A) + 1 - g.$$

Segue então que se $deg(A) = 2g - 1$, a dimensão do espaço de Riemann-Roch associado a A é $l(A) = 2g - 1 + 1 - g = g$.

1.2 Códigos e Corpos de Funções

Definição 17. *Um código linear C sobre o alfabeto $\mathbb{F}_q$ é um subespaço vetorial de $\mathbb{F}_q^n$, $n \geq 1$. Os elementos de C são chamados palavras, enquanto n é dito o comprimento de C e $dim(C)$ é a dimensão de C como espaço vetorial sobre $\mathbb{F}_q$. Um $[n,k]$ código é um código de comprimento n e dimensão k.*

Os $[n,k]$ códigos sobre $\mathbb{F}_2$ foram utilizados nas sondas que viajaram até Marte, na transmissão das fotografias para a Terra. No caso de CDs de música, utiliza-se o corpo $\mathbb{F}_{2^8}$ [(12)].

Definição 18. (Distância de Hamming)

Sejam $a = (a_1, a_2, \ldots, a_n)$ e $b = (b_1, b_2, \ldots, b_n)$ em $\mathbb{F}_q^n$ definimos a distância entre

a e b:

$$d(a,b) := |\{i, a_i \neq b_i\}|.$$

É fácil ver que d é uma métrica em $\mathbb{F}_q^n$.

O peso de um elemento $a \in \mathbb{F}_q^n$ *é definido como* $wt(a) := d(a,0)$.

A distância mínima $d(C)$ *de um código* C *é definida como*

$$d(C) := min\{d(a,b); a,b \in C, a \neq b\} = min\{wt(c), 0 \neq c \in C\}.$$

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

Definição 19. *Seja* $t \in \mathbb{N}$. *Dizemos que em um código* C *há* t *erros no envio da palavra* $a \in C$ *se a palavra recebida é* $a + w$ *onde* w *tem peso* t.
Um código C *é* t*-detector de erros se é capaz de detectar quaisquer* t *erros em qualquer palavra e é dito* t*-corretor de erros se* C *corrige quaisquer* t *erros.*

Repare que $d(a,b)$ indica a quantidade de erros se a é a palavra enviada e b a recebida.

Exemplo 2. *Seja* C_1 *um código que permite dar comandos a televisão, através de um comando a distância:*
Avançar de canal: 00.
Retroceder de canal: 01.
Aumentar volume: 10.
Diminuir volume: 11.
Isto é, $C_1 = \{00, 01, 10, 11\}$.
Se carregamos o comando para diminuir o volume, que corresponde a palavra 11

do código, o comando transmite esta palavra para a televisão. Suponhamos porém, que tenha havido um erro e a palavra transmitida seja 10, que corresponde ao comando de aumentar o volume. O receptor não terá nenhum modo de corrigir tal erro, pois $10 \in C_1$ *e* C_1 *é um código definido sobre o alfabeto* $\mathbb{F}_2$*, que possui palavras de comprimentos 2 e, por isto, é um código muito pobre.*
Considere agora o código C_3 *que repete as palavras de* C_1 *três vezes:*
Avançar de canal: 00000. Retroceder de canal: 010101. Aumentar volume: 101010. Diminuir volume: 111111.
Naturalmente C_3 *corrige erros singulares (erros simples), pois digamos novamente que queremos diminuir o volume e, portanto damos o comando 111111 e haja um erro singular, de modo que a mensagem transmitida seja 101111. Naturalmente, 101111 não é uma palavra de* C_3 *e como houve apenas um erro singular, o receptor corrige automaticamente 101111 para a palavra "mais próxima"do código, que é 111111. É claro também que* C_3 *não corrige erros duplos (ou triplos).*

No exemplo dado acima, $d(C_1) = 1$ e $d(C_3) = 3$. Quanto maior é a distância mínima de um código, melhor é o código no sentido de ser mais eficiente para corrigir erros.
Um dos objetivos então, na construção de códigos é que os mesmos tenham as palavras mais afastadas, mas isto limita a quantidade de palavras no código e, portanto sua capacidade de armazenar informações.
Ou seja, existem relações intrincadas entre k, d e n. A seguir damos a mais simples delas dada pelo Teorema da cota de Singleton.

Proposição 5. *[(16), Proposição 2.1.8]* **(Cota de Singleton)** *Num* $[n,k,d]$ *código vale*

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

Um código cujos parâmetros satisfazem $k+d=n+1$, é dito um código MDS (*maximum distance separable*).

Se $a \in C$ e $t \in \mathbb{N}$, a bola de centro em a e raio t é o conjunto:

$$D(a,t) = \{u \in \mathbb{F}_q^n; d(u,a) \leq t\}.$$

Lema 1. *Sejam* C *um código com distância mínima* d *e* $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$*, onde* $\lfloor x \rfloor$ *indica a parte inteira de um número real* x*. Se* c *e* c' *são duas palavras distintas de* C *então:*

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

Demonstração. Suponha, por absurdo, que exista x em $D(c,\kappa) \cap D(c',\kappa)$. Segue que $d(c,x) \leq \kappa$ e $d(c',x) \leq \kappa$. Portanto, pela desigualdade triângular temos:

$$d(c,c') \leq d(c,x) + d(x,c') \leq 2\kappa \leq d-1.$$

Mas isto é absurdo, pois c e c' estão em C, de modo que $d(c,c') \geq d$. □

O exemplo acima motiva ainda o seguinte Teorema:

Teorema 4. *Seja* C *um código com distância mínima* d*. Então,* C *pode corrigir até* $\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$ *erros e detectar até* $d-1$ *erros.*

Demonstração. Suponha que tenhamos transmitido a palavra c e tenha havido $t \leq \kappa$ erros, ou seja, caso a palavra recebida seja r, então $d(c,r) = t \leq \kappa$. Segue

do Lema 1, que qualquer outra palavra de C está a uma distância de r maior que κ. Isso determina c univocamente a partir de r e κ e o código portanto corrigirá o erro.
Dada uma palavra c qualquer do código, $D(c,d-1) \cap C = \emptyset$ pela definição de distância mínima. Logo, é claro que C detectará o erro. □

Usando o exemplo dado, C_1 é 0-detector de erros e 0-corretor de erros, enquanto que C_3 é um 2-detector de erros e um 1-corretor de erros.
Pelo Teorema 4, a quantidade de erros que um código pode corrigir (ou até mesmo detectar) está limitado superiormente pela distância mínima. Logo, se quisermos um código mais eficiente, devemos ter uma distância mínima o maior possível.

Definição 20. *Dados, $a = (a_1, \ldots, a_n)$ e $b = (b_1, \ldots, b_n)$ em $\mathbb{F}_q^n$ definimos o produto interno (canônico) de a e b como*

$$\langle a,b \rangle := \sum_{i=1}^{n} a_i b_i.$$

Definição 21. *Se $C \subset \mathbb{F}_q^n$ é um código, então*

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

é chamado o código dual de C. O código C é dito auto dual (resp., auto-ortogonal) se $C = C^{\perp}$ (resp., $C \subseteq C^{\perp}$).

Segue da teoria da álgebra linear em dimensão finita que o Código dual de um $[n,k]$ código é um $[n,n-k]$ código e $(C^{\perp})^{\perp} = C$ e, se C é auto dual, C tem comprimento par e sua dimensão será $n/2$.

Definição 22. *Uma matriz $k \times n$ é dita geradora do $[n,k]$-código C sobre $\mathbb{F}_q$ se suas colunas formam uma base de C. A matriz H, geradora do código dual $C^{\perp}$, é chamada de matriz de paridade para C.*

Lema 2. *Seja $C \subset \mathbb{F}_q^n$ um código com matriz geradora G. Então:*

$$\mathbf{x} \in C^{\perp} \Leftrightarrow G\mathbf{x}^t = 0.$$

Portanto, se H é uma matriz geradora de $C^{\perp}$ temos:

$$v \in C \Leftrightarrow Hv^t = 0.$$

Demonstração. Por definição, $\mathbf{x} \in C^{\perp}$ se, e somente se, $\mathbf{x}$ é ortogonal a todos os elementos de C, o que é equivalente a dizer que $\mathbf{x}$ é ortogonal a todos os elementos de uma base de C, isto é, $G\mathbf{x}^t = 0$, pois as colunas de G são uma base de C. Agora, como $(C^{\perp})^{\perp} = C$ temos $v \in C$ se, e somente se, $v \in (C^{\perp})^{\perp}$. Logo, pela primeira parte deste Lema, $Hv^t = 0$. □

Teorema 5. *Seja $C \subset \mathbb{F}_q^n$ um código com matriz de paridade H e distância mínima $d(C)$. Então, $d(C)$ é maior ou igual a s se, e somente se, quaisquer $s-1$ colunas de H são lineamente independentes.*

Demonstração. Suponha que cada conjunto de $s-1$ colunas de H é linearmente independente e sejam $c = (c_1, \ldots, c_n)$, uma palavra não nula de C, e $h^1, \ldots, h^n$ as colunas de H. Pelo Lema 2, temos $Hc^t = 0$, ou seja:

$$0 = Hc^t = \sum c_i h^i \tag{1.1}$$

Visto que $wt(c)$ é a quantidade de componentes não nulas de c, segue que se $wt(c) \leq s-1$, teríamos por 1.1 uma combinação nula de um número t, com $1 \leq t \leq s-1$, de colunas de H, absurdo. Logo, $wt(c) \geq s$ e, portanto, $d(C) \geq s$. Reciprocamente, suponha que $d(C) \geq s$. Suponha ainda, por absurdo, que H tenha $s-1$ colunas lineamente dependentes, digamos $h_{i_1}, \ldots, h_{i_{s-1}}$. Assim, existiriam $c_{i_1}, \ldots, c_{i_{s-1}}$ em $\mathbb{F}_q$, nem todos nulos, tais que

$$c_{i_1}h_{i_1}, \ldots, c_{i_{s-1}}h_{i_{s-1}} = 0.$$

Pelo Lema 2 segue que $c = (0, \ldots, c_{i_1}, 0, \ldots, c_{i_2}, 0, \ldots, c_{i_{s-1}}, 0, \ldots, 0) \in C$ e, consequentemente, $w(c) \leq s-1 < s$, absurdo, pois $d(C) \geq s$. □

Vamos agora introduzir os **Códigos Algébricos Geométricos**, para isso vamos fixar a seguinte notação:

i. $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g,

ii. $P_1, P_2, \ldots, P_n$ lugares de grau um de $F/\mathbb{F}_q$, dois a dois distintos,

iii. D o divisor $D = P_1 + P_2 + \ldots + P_n$,

iv. G um divisor de $F/\mathbb{F}_q$ cujo suporte não tem interseção com o suporte de D.

Considere o mapa

$$ev_D := \begin{cases} \mathcal{L}(G) & \longrightarrow \mathbb{F}_q^n, \\ x & \longmapsto (x(P_1), x(P_2), \ldots, x(P_n)) \end{cases}$$

Repare que ev_D está bem definido já que o suporte de G é disjunto do suporte de D e todos os lugares têm grau um.

Definição 23. *O código algébrico geométrico $C_{\mathcal{L}}(D,G)$ associado aos divisores D e G é definido como:*

$$C_{\mathcal{L}}(D,G) := Im(ev_D) = \{(x(P_1), x(P_2), \ldots, x(P_n)) \,|\, x \in \mathcal{L}(G)\}.$$

Teorema 6. *O código $C_{\mathcal{L}}(D,G)$ é um $[n,k,d]$ código com parâmetros satisfazendo:*

$$k = l(G) - l(G-D) \quad e \quad d \geq n - deg(G). \tag{1.2}$$

Demonstração. O núcleo do mapa ev_D é dado por:

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

Segue do Teorema do Núcleo e da Imagem da álgebra linear em dimensão finita que $k = dim C_{\mathcal{L}}(D,G) = l(G) - l(G-D)$.
Seja $x \in \mathcal{L}(G)$ de peso d, ou seja, tal que $wt(ev_D(x)) = d$. Segue que exatamente $n-d$ lugares $P_{i_1}, \ldots, P_{i_{n-d}}$ no suporte de D são zeros de x, o que significa que $0 \neq x \in \mathcal{L}(G - (P_{i_1} + \ldots + P_{i_{n-d}}))$. Logo,

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

E o resultado segue. □

Proposição 6. *Com a mesma notação do Teorema 6, seja $C_{\mathcal{L}}(D,G)$ um $[n,k,d]$ código e suponha que o grau de G seja estritamente menor que n. Então o mapa ev_D é injetivo e:*

i. $d \geq n - deg(G)$ *e* $k = l(G) \geq deg(G) + 1 - g$.

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

iii. Se $\{x_1, x_2, \ldots, x_k\}$ *é uma base de* $\mathcal{L}(G)$ *então a matriz*

$$\begin{pmatrix} x_1(P_1) & x_1(P_2) & \ldots & x_1(P_n) \\ x_2(P_1) & x_2(P_2) & \ldots & x_2(P_n) \\ \vdots & \vdots & \ddots & \vdots \\ x_k(P_1) & x_k(P_2) & \ldots & x_k(P_n) \end{pmatrix}$$

é a matriz geradora de $C_{\mathcal{L}}(D,G)$.

Demonstração. Como, por hipótese, G tem grau estritamente menor que D, então $l(G-D) = 0$ e $l(G) \geq deg(G) + 1 - g$ pelo Teorema de Riemann-Roch. Já (ii) segue do Teorema 3 e (iii) é imediato. □

Repare que, nas condições da Proposição acima, decorre do ítem (i) que $k + d \geq n + 1 - g$. Comparando com a cota de Singleton, já tínhamos que $k + d \leq n + 1$. Deste modo temos que, num código algébrico geométrico, $n + 1 - g \leq k + d \leq n + 1$.

Os códigos duais terão papel fundamental tanto na determinação das dimensões de códigos bem como na determinação das distâncias mínimas. No caso de códigos algébricos geométricos, seus duais são ainda algébricos geométricos. Os seguintes Teoremas explicitam os códigos duais dos códigos algébricos geométricos e nos dão informações a respeito dos seus parâmetros.

Definição 24. *Seja* $C_{\Omega}(D,G)$ *definido por*

$$C_{\Omega}(D,G) := \{(\omega_{P_1}(1), \omega_{P_2}(1), \ldots, \omega_{P_n}(1)) \,|\, \omega \in \Omega(G-D)\},$$

onde $\Omega(G-D)$ *é o espaço vetorial (sobre* K*) das diferenciais de Weil que se anulam no divisor* $\mathcal{A}(G-D)+F$*.*

Teorema 7. *[(16), Teorema 2.2.7]:* $C_\Omega(D,G)$ *é um* $[n,k',d']$ *código com parâmetros satisfazendo:*

$$k' = i(G-D) - i(G) \quad e \quad d' \geq deg(G) - (2g-2),$$

onde, para $A \in Div(F)$*,* $i(A) := l(A) - deg(A) + g - 1$*.*
Vale ainda,

$$v_P(w) \geq r \Leftrightarrow w_P(x) = 0, \forall x, v_P(x) \geq -r, \tag{1.3}$$

onde w *é uma diferencial de Weil com* $v_P(w) \geq -1$*.*

Teorema 8. *[(16), Teorema 2.2.8]: Os códigos* $C_\mathcal{L}(D,G)$ *e* $C_\Omega(D,G)$ *são duais um do outro, i.e.,*

$$C_\mathcal{L}(D,G) = C_\Omega(D,G)^\perp.$$

Demonstração. Primeiro provamos o seguinte: considere $P \in \mathbb{P}_{F/K}$ um lugar racional, uma diferencial de Weil w com $v_P(w) \geq -1$ e um elemento $x \in F$ com $v_P(x) \geq 0$. Afirmamos que $w_P(x) = x(P)w_P(1)$. De fato, escreva $x = a + y$, com $a = x(P) \in \mathbb{F}_q$ e $v_P(y) > 0$. Segue que, $w_P(x) = w_P(a) + w_P(y) = aw_P(1) + 0 = x(P)w_P(1)$, pois $a \in K$ e $w_P(y) = 0$ segue da Equação 1.3.
Seja $P \in \mathbb{P}_{F/K} \setminus \{P_1, \ldots, P_n\}$. Como $x \in \mathcal{L}(G)$ e $w \in \Omega(G-D)$, segue que $v_P(x) \geq -v_P(w)$. Segue da Equação 1.3 que $w_P(x) = 0$.
Para mostrar que $C_\mathcal{L}(D,G)^\perp \supseteq C_\Omega(D,G)$, basta observarmos que, para $w \in$

$\Omega(G-D)$, temos

$$\begin{aligned} 0 = w(x) = & \sum_{P\in\mathbb{P}_{F/K}} w_P(x) \\ & = \sum_{i=1}^{n} w_{P_i}(x) \\ & = \sum_{i=1}^{n} x(P_i) w_{P_i}(1) \\ & = \langle (x(P_1),\ldots,x(P_n)), (w_{P_1}(1),\ldots,w_{P_n}(1)) \rangle. \end{aligned}$$

Agora que provamos uma inclusão, basta demonstrarmos que ambos os códigos têm a mesma dimensão:

$$\begin{aligned} dimC_{\Omega}(D,G) &= i(G-D) - i(G) \\ &= l(G-D) - deg(G-D) + g - 1 - (l(G) - deg(G) + g - 1) \\ &= deg(D) + l(G-D) - l(G) \\ &= n - (l(G) - l(G-D)) \\ &= n - dimC_{\mathcal{L}}(D,G) = dimC_{\mathcal{L}}(D,G)^{\perp}. \end{aligned}$$

□

Definição 25. *Sejam F/K um corpo de funções e M um espaço vetorial sobre F. Um mapa $\delta : F \to M$ é dito ser uma derivação de F/K se δ é K-linear e vale a relação $\delta(u \cdot v) = u\delta(v) + v\delta(u)$ para todo $u,v \in F$.*

Sobre derivações, é provado em (16), Proposição 4.1.4 que se $x \in F$ é um elemento separável (isto é, tal que $F/K(x)$ é uma extensão algébrica separável) de F/K e $N \supseteq F$ é um corpo, então existe uma única derivação $\delta_x = \delta : F \to N$ de F/K com $\delta(x) = 1$.

No conjunto $z := \{(u,x) \in F \times F \,|\, x \text{ é um elemento separável}\}$ nós definimos a relação de equivalência $(u,x) \sim (v,y) :\Leftrightarrow v = u \cdot \delta_y(x)$, que está bem definida por

(16), Lema 4.1.6. A classe de equivalência $(1,x)$ é simplesmente denotada por dx. O principal fato sobre as derivações é que elas e as diferenciais de Weil estão fortemente relacionadas e se $z \in F$ então $z \cdot dx$ é uma diferencial de Weil como se observa em (16), Observação 4.3.7.

Proposição 7. *[(16), Proposição 8.1.2] Seja $t \in F$ com $v_{P_i}(t) = 1, i = 1, \ldots, n$. Então:*

i. A diferencial $\eta = dt/t$ satisfaz $v_{P_i}(t) = 1$,

ii. $C_\Omega(D,G) = C_\mathcal{L}(D, D - G + (dt) - (t))$.

A Proposição 7 acima nos garante que os códigos $C_\Omega(D,G)$ também são códigos algébricos geométricos, no sentido da definição 23.

1.3 Os Teoremas de Kummer e Artin Schreier

Apresentaremos nesta seção o Teorema das Extensões de Artin Schreier e o Teorema de Kummer, centrais no estudo do corpo de funções Hermitiano.
Além destes, apresentaremos uma série de ferramentas a serem utilizadas no Capítulo 2.

1.3.1 A Diferente e as Bases Inteiras

Definição 26. *Dizemos que o corpo de funções F'/K' é uma extensão algébrica do corpo de funções F/K se $F' \supseteq F$ é uma extensão algébrica e $K' \supseteq K$.*

Definição 27. *Seja F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'/K'}$. Dizemos que P' é uma extensão de $P \in \mathbb{P}_{F/K}$ se $P \subseteq P'$.*
Denotamos esta relação por $P'|P$.

O inteiro $e(P'|P) := e > 0$ tal que $v_{P'}(x) = e \cdot v_P(x), \forall x \in F$ é chamado de índice de ramificação de P' sobre P. A existência e unicidade de $e(P'|P)$ está garantida em [(16), Proposição 3.1.4].
Chamamos de grau relativo de P' sobre P ao inteiro $[F'_{P'} : F_P]$.

Definição 28. *Seja F'/K' uma extensão algébrica de F/K de grau $[F' : F] = n$. Dizemos que P se decompõe completamente em F'/F se existem exatamente n lugares distintos $P' \in \mathbb{P}_{F'/K'}$ com $P'|P$ e que P é totalmente ramificado se existe um único lugar $P' \in \mathbb{P}_{F'/K'}$ com $P'|P$ e $e(P'|P) = n$.*

As bases inteiras são uma ferramenta importante para a caracterização das bases dos Espaços de Riemann Roch associados aos códigos Hermitianos.

Definição 29. *Dizemos que o elemento $z \in F$ é inteiro sobre $\mathcal{O}_P$ se $f(z) = 0$ para algum polinômio mônico $f(X) \in \mathcal{O}_P[X]$.*
Para o lugar $P \in \mathbb{P}_{F/K}$ defina o conjunto

$$\mathcal{O}'_P = \{z \in F \,|\, z \quad \text{é inteiro sobre} \quad \mathcal{O}_P\}.$$

Este conjunto é de fato um anel e é chamado de fecho inteiro de $\mathcal{O}_P$ em F.

Proposição 8 ((16), Corolário 3.3.5)**.** *Se F'/F é uma extensão finita e separável do corpo de funções F/K e $P \in \mathbb{P}_{F/K}$, então existe uma base $\{u_1, u_2, \ldots, u_n\}$ de F'/F tal que $\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot u_i$. Cada base $\{u_1, u_2, \ldots, u_n\}$ é chamada de base inteira de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$.*

Definição 30. *Para $P \in \mathbb{P}_{F/K}$ e $\mathcal{O}'_P$ o fecho inteiro de $\mathcal{O}_P$ sobre F' definimos o conjunto $\mathcal{C}_P = \{z \in F' \,|\, Tr_{F'/F}(z \cdot \mathcal{O}'_P) \subset \mathcal{O}_P\}$, o qual é chamado de módulo*

complementar sobre $\mathcal{O}_P$. *Para* $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ *definimos a diferente de* P' *sobre* P *como*

$$d(P'|P) := -v_{P'}(t).$$

É bem conhecido que a diferente é zero para quase todo lugar $P \in \mathbb{P}_{F/K}$, *logo podemos definir o divisor diferente como:*

$$Dif(F'|F) = \sum_{P \in \mathbb{P}_{F/K}} \sum_{P'|P} d(P'|P) \cdot P'$$

A existência e unicidade de t na definição acima é garantida por [(16), Proposição 3.4.2(c)].

O seguinte Teorema nos fornece um critério para encontrarmos uma base inteira para F'/F.

Teorema 9. *[(16), Teorema 3.5.10] Suponha que* $F' = F(y)$ *é uma extensão finita e separável de um corpo de funções* F/K *e que grau* $[F' : F] = n$. *Seja* $P \in \mathbb{P}_{F/K}$ *tal que o polinômio mínimo* $\phi(T)$ *de* y *sobre* F *tenha seus coeficientes em* $\mathcal{O}_P$ *e sejam* $P_1, P_2, \ldots, P_r$ *todos os lugares de* F' *que são extensões de* P. *Então, valem:*

i. $d(P_i|P) \leq v_{P_i}(\phi'(y)), 0 \leq i \leq r$.

ii. $\{1, y, y^2, \ldots, y^{n-1}\}$ *é uma base inteira de* F'/F *se e somente se* $d(P_i|P) = v_{P_i}(\phi'(y))$ *para* $0 \leq i \leq r$.

A próxima Proposição 9 adiante é importante na determinação dos códigos duais dos códigos Hermitianos. Por sua vez, os códigos duais serão fundamentais na determinação das dimensões dos códigos Hermitianos.

Proposição 9. *[(16), Observação 4.3.7, (c)] Sejam F/K um corpo de funções e $x \in F \setminus \tilde{K}$. Então, vale a relação $(dx) = -2(x)_\infty + Dif(F/K(x))$.*

1.3.2 Semigrupo de Weierstrass

Apresentaremos agora o conceito de Semigrupo de Weierstrass. Tais semigrupos estão intimamente relacionados às dimensões dos códigos algébricos geométricos.

Definição 31. *Um inteiro $n \geq 0$ é dito uma não-lacuna em $Q \in \mathbb{P}_{F/K}$ se existe $x \in F$ com $(x)_\infty = nQ$. Caso contrário dizemos que n é uma lacuna em Q.*

Vale ressaltar que n é uma não-lacuna em Q se, e somente se $l(nQ) > l((n-1)Q)$ (já que o elemento $x \in F$ satisfazendo a definição estará em $\mathcal{L}(nQ) \setminus \mathcal{L}((n-1)Q)$, de modo que x terá uma única não-lacuna em Q de ordem n).
Se g é o gênero do corpo de funções F/K e $n \geq 2g$ então n é uma não-lacuna em Q, para todo $Q \in \mathbb{P}_{F/K}$, pois, pelo Teorema 3,

$$l((n-1)Q) = (n-1)deg(Q) + 1 - g$$

e

$$l(nQ) = (n)deg(Q) + 1 - g$$

e, portanto, $\mathcal{L}((n-1)Q) \subsetneq \mathcal{L}(nQ)$.
Deste modo, existe um elemento $x \in \mathcal{L}(nQ) \setminus \mathcal{L}((n-1)Q)$, o qual tem divisor de pólos nQ.
Dado $Q \in \mathbb{P}_{F/K}$, o conjunto de não-lacunas em Q formam um semigrupo aditivo. De fato, se n_1 e n_2 são duas não-lacunas de um lugar Q, então $n_1 + n_2$ também é uma não-lacuna em Q. De fato, $(x_1)_\infty = n_1Q$ e $(x_2)_\infty = n_2Q$ então $(x_1x_2)_\infty =$

$(n_1 + n_2)Q$.

Teorema 10. (Teorema das lacunas de Weierstrass) *Seja F/K um corpo de funções de gênero $g > 0$ e um lugar $Q \in \mathbb{P}_{F/K}$ de grau um. Então existem g lacunas $i_1 < \ldots < i_g$ em Q. Temos ainda que $i_1 = 1$ e $i_g \leq 2g - 1$.*

Demonstração. Seja $Q \in \mathbb{P}_{F/K}$ um lugar racional e considere a sequência de espaços de Riemann Roch

$$\mathcal{L}(0) \subseteq \mathcal{L}(Q) \subseteq \mathcal{L}(2Q) \subseteq \ldots \subseteq \mathcal{L}((2g-1)Q),$$

Como já demonstramos acima, se n é lacuna em Q, $n \leq 2g - 1$, logo $i_g \leq 2g - 1$. Naturalmente, $l(0) = 1$ e $l((2g-1)Q) = g$, pelo Teorema 3. Como $dim(\mathcal{L}(iQ)) \leq dim(\mathcal{L}((i-1)Q)) + 1$, devemos ter exatamente $g - 1$ números $1 \leq i \leq 2g - 1$ com $\mathcal{L}((i-1)Q) \subsetneq \mathcal{L}(iQ)$. Pela caracterização anterior, estes $g - 1$ números são não-lacunas em Q, e os outros g restantes são lacunas em Q.

Para demonstrarmos que 1 é uma lacuna em Q, suponha por absurdo, que 1 seja uma não-lacuna em Q. Deste modo, como as não-lacunas em Q formam um semigrupo aditivo, todo $n \in \mathbb{N}$ também será uma não-lacuna em Q, contradição, já que $g > 0$. □

Definição 32. *Seja Q um lugar racional do corpo de funções F/K. Denote por $H(Q) \subset \mathbb{N}$ ao conjunto de não-lacunas em Q. Como $H(Q)$ é um semigrupo de $\mathbb{N}$ com relação a adição, chamamos $H(Q)$ de* ***Semigrupo de Weierstrass*** *de Q.*

1.3.3 Extensões de Artin Schreier

Os seguintes Teoremas serão utilizados na caracterização do corpo de funções Hermitiano. No caso específico do Teorema de Kummer a seguir, poderemos obter a caracterização dos lugares racionais do corpo de funções Hermitiano.

Teorema 11. *[(16), Corolário 3.3.8] (**Teorema de Kummer**): Seja* $\phi(T) = T^n + f_{n-1}(x)T^{n-1} + \ldots + f_0(x) \in K(x)[T]$ *um polinômio irredutível sobre o corpo de funções racionais* $K(x)$.

Considere $K(x,y)/K$ *onde* y *é tal que* $\phi(y) = 0$ *e* $\alpha \in K$ *com* $f_j(\alpha) \neq \infty, 0 \leq j \leq n-1$. *Seja ainda* $P_\alpha \in \mathbb{P}_{K(x)/K}$ *o zero de* $x - \alpha$. *Suponha que o polinômio*

$$\phi_\alpha(T) = T^n + f_{n-1}(\alpha)T^{n-1} + \ldots + f_0(\alpha)$$

tenha a seguinte decomposição em $K[T]$:

$$\phi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T)$$

com os $\psi_i \in K[T]$ *mônicos, irredutíveis, dois a dois dintintos. Então:*

i. Para cada $i = 1, \ldots, r$ *existe um único lugar* $P_i \in \mathbb{P}_{K(x,y)/K}$ *tal que* $x - \alpha \in P_i$ *e* $\psi_i(y) \in P_i$. *Temos que* $x - \alpha$ *é um elemento primo para* P_i *e o corpo de classes residuais de* P_i *é* K*-isomorfo a* $K[T]/(\psi_i(T))$.

ii. Se $deg(\psi_i(T)) = 1$ *para pelo menos um* $i \in \{1, 2, \ldots, r\}$ *então* K *é o corpo completo de constantes de* $K(x,y)$.

iii. Se $\phi_\alpha(T)$ *tem* n *raízes distintas* $\beta \in K$, *então, para cada* β *tal que* $\phi_\alpha(\beta) = 0$ *existe um único lugar* $P_{\alpha,\beta} \in \mathbb{P}_{K(x,y)/K}$ *tal que*

$x - \alpha \in P_{\alpha,\beta}$ *e* $x - \beta \in P_{\alpha,\beta}$ *e* $P_{\alpha,\beta}$ *é um lugar de grau um.*

iv. Se $deg(\psi_i(T)) = 1$, *para todo* $i = 1, \ldots, n$, *isto é, se* $\phi(T)$ *se decompõe completamente, então o conjunto* $\{1, \ldots, y^{n-1}\}$ *é uma base inteira para cada* $P_{\alpha,\beta}$.

Definição 33. *Sejam* K *um corpo e* $a(T) \in K[T]$. *Dizemos que* $a(T)$ *é um polinômio aditivo se:*

$$a(u + v) = a(u) + a(v), \forall u, v \in K.$$

É possível provar que, se $char(K) = p$, então $a(T)$ tem a seguinte forma:

$$a(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \ldots + a_1 T^p + a_0 T.$$

Lema 3. *[(16), Lema 3.7.7]: Sejam* F/K *um corpo de funções com* $char(K) = p > 0$. *Dado um elemento* $u \in F$ *e um lugar* $P \in \mathbb{P}_{F/K}$ *vale apenas uma das seguintes afirmações:*

i. Ou existe um elemento $z \in F$ *tal que* $v_P(u - (z^p - z)) \geq 0$,

ii. Ou, para algum $z \in F$, $v_P(u - (z^p - z)) = -m < 0$, *onde* $m \not\equiv 0 \ mod \ p$.

Portanto, m *é um inteiro unicamente determinado por* u *e* P.

É importante ressaltar que, se $a(T) \in K[T]$ é um polinômio aditivo separável sobre K, cujas raízes estão todas sobre K, então essas raízes formam um subgrupo do grupo aditivo de K de ordem p^n.

Teorema 12. *[(16), Proposição 3.7.10] (**Extensões de Artin Schreier**): Considere um corpo de funções F/K com corpo de constantes K com característica $p > 0$ e um polinômio separável aditivo $a(T)$ de grau p^n, de modo que todas as raízes de $a(T)$ estão em K. Seja $u \in F$ e suponha que, para cada $P \in \mathbb{P}_{F/K}$ exista $z \in F$ (dependendo de P) tal que:*

$$v_P(u - a(z)) \geq 0 \tag{1.4}$$

ou

$$v_P(u - a(z)) = -m, m > 0, m \not\equiv 0 \ (mod\ p) \tag{1.5}$$

Defina $m_P = -1$ caso $v_P(u - a(z)) \geq 0$ e $m_P = m$ no segundo caso. Então m_P é bem definido, por hipótese. Considere a extensão $F' = F(y)$ onde y satisfaz

$$a(y) = u.$$

Se existe pelo menos um lugar Q tal que $m_Q > 0$ então valem:

i. F'/F é Galois, $[F' : F] = p^n$ e o grupo de Galois de F'/F é isomorfo ao grupo aditivo $\{\alpha \in K, a(\alpha) = 0\}$ e, portanto é isomorfo a $(\mathbb{Z}/p\mathbb{Z})^n$.

ii. K é algebricamente fechado em F'.

iii. Cada $P \in \mathbb{P}_{F/K}$ com $m_P = -1$ não se ramifica na extensão F'/F.

iv. Cada $P \in \mathbb{P}_{F/K}$ com $m_P > 0$ é totalmente ramificado em F'/F e $d(P'|P) = (p^n - 1)(m_P + 1)$.

v. Seja g' (resp., g) o gênero de F' (resp., F). Então:

$$g' = p^n \cdot g + \frac{p^n - 1}{2}(-2 + \sum_{P \in \mathbb{P}_{F/K}} (m_P + 1) \cdot deg(P))$$

Repare que o Teorema 12 acima só é válido para polinômios aditivos separáveis para os quais

$$m_P := \begin{cases} -1 & v_P(u - a(z)) \geq 0 \\ m & v_P(u - a(z)) = -m < 0 \end{cases},$$

é um inteiro bem definido.

Lema 4. *Seja K um corpo de característica $p > 0$. Considere o corpo $F = K(x)$ tal que F/K é um corpo de funções, $F' = K(x,y)$ e a extensão algébrica F'/F de F/K onde*

$$y^q + \mu y = f(x),$$

onde, $f(X) \in K[X]$, $q = p^s > 1$ é uma potência de p e $0 \neq \mu \in K$.
Sejam $a(T) = T^q + \mu T$, $u = y^q + \mu y = f(x) \in K(x)$ e $u' = y^p + \mu y$.
Assuma que $deg(f) = m$ é primo com p, e que todas as raízes de $T^q + \mu T = 0$ estão em K.
Considere o lugar $P \in \mathbb{P}_{F/K}$ e uma extensão $P \in \mathbb{P}_{F'/K}$ de P. Então m_P é um inteiro bem definido.

Demonstração. Primeiramente repare que $a(T)$ é separável aditivo, pois $a'(T) = \mu \neq 0$.
Afirmamos que existe $z \in F$ tal que $v_P(f(x) - a(z)) \geq 0$ ou $v_P(f(x) - a(z)) < 0$. De fato, seja $z \in F$ uma raíz de $a(z)$. Assim se, P é pólo de x, $v_P(f(x) - a(z)) = -m = -deg(f(x))$. Se, por outro lado, P é um zero de x,$v_P(f(x) - a(z)) \geq m =$

$deg(f(x))$.

Suponha por absurso que existam z_1 e z_2 em F tais que

$$\text{i. } v_P(y^q + \mu y - (z_1^q + \mu z_1)) = v_P((y - z_1)^q + \mu(y - z_1)) \geq 0,$$

$$\text{ii. } v_P(y^q + \mu y - (z_2^q + \mu z_2)) = v_P((y - z_2)^q + \mu(y - z_2)) < 0.$$

Vamos mostrar que isto implica em uma contradição com o Lema 3, para $u' = y^p + \mu y$, z_1 e z_2.

De (ii), segue que

$$min\{qv_{P'}(y - z_2)), v_{P'}(y - z_2)\} \leq v_{P'}((y - z_2)^q + \mu(y - z_2)) < 0,$$

pois $e(P'|P) > 0$, o que implica que $v_{P'}(y - z_2) < 0$.

Assim,

$$v_{P'}(y^p + \mu y - (z_2^p + \mu z_2)) = v_{P'}((y - z_2)^p + \mu(y - z_2)) = min\{pv_{P'}(y - z_2), v_{P'}(y - z_2)\} < 0.$$

Por outro lado,

$$v_{P'}((y - z_1)^q + \mu(y - z_1)) \geq min\{qv_{P'}(y - z_1), v_{P'}(y - z_1)\}.$$

E, por (i), $v_P((y - z_1)^q + \mu(y - z_1)) \geq 0$, segue $v_{P'}(y - z_1) \geq 0$.

Assim,

$$v_{P'}(y^p + \mu y - (z_1^p + \mu z_1)) = v_{P'}((y - z_1)^p + \mu(y - z_1)) = min\{pv_{P'}(y - z_1), v_{P'}(y - z_1)\} \geq 0.$$

Deste modo, temos uma contradição com o Lema 3. □

Capítulo 2

Códigos Hermitianos

2.1 O Corpo de Funções Hermitiano

Primeiramente apresentamos os códigos Hermitianos utilizando principalmente a teoria desenvolvida no livro *Algebraic Function Fields and Codes*, (16) e no artigo *A Note on Hermitian Codes Over GF(q^2)*, (15). Finalizamos o capítulo com o estudo do artigo *On the True Minimum Distances of Hermitian Codes*, (9), onde é calculada a distância mínima para os códigos Hermitianos.

O nosso interesse nos códigos Hermitianos se dá pelo fato deles serem códigos longos, de maior comprimento possível para um código algébrico geométrico definido por um corpo de funções.

Como motivação para o caso Hermitiano, considere o seguinte Teorema:

Teorema 13. *Seja K um corpo de característica $p > 0$. Considere o corpo $F = K(x)$ tal que F/K é um corpo de funções, $F' = K(x,y)$ e a extensão*

algébrica F'/F de F/K onde

$$y^q + \mu y = f(x),$$

onde, $f(X) \in K[X]$, $q = p^s > 1$ é uma potência de p e $0 \neq \mu \in K$. Assuma que $deg(f) = m$ é primo com p, e que todas as raízes de $T^q + \mu T = 0$ estão em K. Então:

i. $[F' : F] = q$,

ii. *O pólo $P_\infty \in \mathbb{P}_{F/K}$ de x em F tem um única extensão $Q_\infty \in \mathbb{P}_{F'/K}$. Logo Q_∞ é um lugar de F'/K de grau um,*

iii. *P_∞ é o único lugar de $F = K(x)$ que se ramifica em F'/F,*

iv. *O gênero de F'/K é $g = (q-1)(m-1)/2$,*

v. *O divisor de pólos de x (resp., y) é qQ_∞ (resp., mQ_∞),*

vi. *O divisor da diferencial dx é*

$$(dx) = (2g-2)Q_\infty = ((q-1)(m-1)-2)Q_\infty,$$

vii. *Seja $r \geq 0$, os elementos $x^i y^j$ com $0 \leq i, 0 \leq j \leq q-1, qi+mj \leq r$ formam uma base do espaço $\mathcal{L}(rQ_\infty)$ sobre K.*

Demonstração. Mostraremos inicialmente que estamos nas condições do Teorema das Extensões de Artin Schreier.

Seguindo a notação do Teorema 12, usaremos aqui $a(T) = T^q + \mu T$, o qual é um polinômio separável aditivo em $K[T]$, pois, por hipótese, todas as raízes de $a(T)$ estão em K(em particular, estão em F'), $a'(T) = \mu \neq 0$ e q é uma potência da

característica da K.

Sejam então $P_\infty \in \mathbb{P}_{F/K}$ o pólo de x e $z \in F'$ uma raiz de $a(T)$. Segue que $v_{P_\infty}(f(x) - a(z)) = v_{P_\infty}(f(x)) = -m$ onde $m = deg(f(x))$, ou seja, $m_{P_\infty} = m$, o qual está bem definido pelo Lema 4.

Precisamos ainda que o corpo K seja o corpo de constantes de F'/K, mas isto nada mais é que o item (ii) do Teorema 11, de Kummer, já que o polinômio se $a(T)$ se decompõe completamente em $K[T]$.

Finalmente, escreva $a(y) = f(x)$. Assim suprimos todas as condições necessárias. Do item (i) do Teorema de Artin Schreier, segue que $[F' : F] = q$.

Para o item (ii), como $v_{P_\infty}(f(x)-a(z)) = -m$, então $m_P = m > 0$, pela definição de m_P. Logo, pelo Teorema 12, item (iv), P_∞ é totalmente ramificado, de modo que P_∞ é o único pólo de x e é racional.

Faremos agora o item (iii). Para qualquer $P \in \mathbb{P}_{F/K} \setminus \{P_\infty\}$, temos que $v_P(f(x)-a(z)) \geq 0$, já que P_∞ é o único pólo de x. Neste caso, $m_P = -1$, e o item (iii) do Teorema 12 das Extensões garante que P não se ramifica.

(iv) Para o gênero, é um fato bem conhecido que um corpo de funções racionais têm gênero zero. Se $P \in \mathbb{P}_{F/K} \setminus \{P_\infty\}$, teremos $m_p + 1 = 0$, enquanto que, $(-2 + (m_{P_\infty} + 1)degP_\infty) = (m - 1)$ e o resultado segue diretamente do item (v) do Teorema 12.

Com relação ao item (v) temos $v_{Q_\infty}(x) = e(Q_\infty|P_\infty)v_{P_\infty}(x) = qv_{P_\infty}(x)$. Segue então do item (ii) que $(x)_\infty = qQ_\infty$.

Afirmamos que os elementos x e y têm os mesmos pólos, logo Q_∞ é o único pólo de y também.

De fato, escrevendo $f(x) = a_0 + \ldots + a_m x^m, a_i \in K$, seja $P \in \mathbb{P}_{F/K}$ tal que

$v_P(x) = -1$, segue que

$$v_P(f(x)) = min\{v_P(a_0), v_P(x), \ldots, iv_P(x), \ldots, mv_P(x)\} = mv_P(x) = -m < 0,$$

Considere agora a extensão $P'|P$, pólo de x em F'. Pela igualdade $f(x) = y^q + \mu y$ temos $v_{P'}(y^q + \mu y) < 0$.

Logo, $v_{P'}(y^q + \mu y) = min\{qv_{P'}(y), v_{P'}(y)\} = qv_{P'}(y) < 0$, já que $\mu \in K$.

Assim, concluímos que $v_{P'}(y) < 0$.

Seja agora $P' \in \mathbb{P}_{F'/K}$ um pólo de y.

Concluímos então que $v_{P'}(y^q + \mu y) = qv_{P'}(y)$. Novamente, pela relação $f(x) = y^q + \mu y$, vemos que $v_{P'}(f(x)) < 0$.

Agora, como $v_{P'}(a_i x^i) \neq v_{P'}(a_j x^j)$ para $i \neq j$ e $v_{P'}(a_i) = 0$ com $i = 0, \ldots, m$, segue que $v_{P'}(x) < 0$.

Logo, como Q_∞ é o único pólo de x em F', então Q_∞ é o único pólo de y também e, deste modo, $qv_{Q_\infty}(y) = v_{Q_\infty}(y^q + \mu y) = v_{Q_\infty}(f(x)) = -mq$, de onde concluímos que $(y)_\infty = mQ_\infty$.

Para (vi), a diferente de F'/F é $Dif(F'/F) = (q-1)(m+1)Q_\infty$ seguindo diretamente de aplicar o Teorema 12, de Artin Schreier, item (iv). Logo, pela Proposição 9, vale

$$(dx) = -2(x)_\infty + Dif(F'/F) = ((q-1)(m+1) - 2q)Q_\infty = (2g-2)Q_\infty.$$

Finalmente para (vii), os elementos $1, y, \ldots, y^{q-1}$ formam uma base inteira para F'/F em todos os lugares $P \in \mathbb{P}_{F/K}$ diferentes de P_∞, pelo Teorema 11, item iv. Segue do Teorema 9 que o polinômio mínimo $\Phi(T) = T^q + \mu T - f(x)$ de y sobre

$K(x)$ está em $\mathcal{O}_P[T]$ e para todo $Q|P$,

$$v_Q(\Phi'(y)) = v_Q(\mu) = 0 = d(Q|P).$$

Seja $z \in \mathcal{L}(rQ_\infty)$. Como Q_∞ é o único pólo de z, z é inteiro sobre $\mathcal{O}_P$ para todo $P \in \mathbb{P}_{K(x)/K}$, $P \neq P_\infty$. Escrevendo z na base $\{1, \ldots, y^{q-1}\}$ temos $z = \sum_{j=0}^{q-1} z_j y^j$, com $z_j \in K[x]$, pois $z_j \in K(x)$ e z_j não tem pólos diferentes de P_∞. Logo,

$$z = \sum_{j=0}^{q-1} \sum_{i \geq 0} a_{ij} x^i y^j, a_{ij} \in K. \tag{2.1}$$

Os elementos $x^i y^j$ com $0 \leq j \leq q-1$, $0 \leq i$ e $qi + mj \leq r$ têm ordens de pólo duas a duas distintas, pois $v_{Q_\infty}(x) = -q$, $v_{Q_\infty}(y) = -m$ e m e q são relativamente primos. Logo a desigualdade triangular estrita nos dá

$$v_{Q_\infty}(x) = min\{-iq - jm | a_{ij} \neq 0\}.$$

Disso podemos concluir que os elementos $x^i y^j$ com $0 \leq j \leq q-1$, $0 \leq i$ e $qi + mj \leq r$ são linearmente independentes. De fato, suponha que serão linearmente dependentes, ou seja, existe alguma combinação do tipo:

$$\sum_{j=0}^{q-1} \sum_{i \geq 0} b_{ij} x^i y^j = 0,$$

onde algum $b_{ij} \in K$ é não nulo.

Teremos que

$$v_{Q_\infty}(\sum_{j=0}^{q-1} \sum_{i \geq 0} b_{ij} x^i y^j) = v_{Q_\infty}(0)$$

Por um lado, teremos $v_{Q_\infty}(\sum_{j=0}^{q-1}\sum_{i\geq 0} b_{ij}x^i y^j) = min\{-iq - jm | b_{ij} \neq 0\}$. Por outro, $v_{Q_\infty}(0) = \infty$, absurdo.

Isto termina a prova do Teorema. □

Proposição 10. *Considere as condições do Teorema 13 e seja $\alpha \in K$ tal que a equação $T^q + \mu T = f(\alpha)$, $f(X) \in K[X]$, tenha q raízes distintas em K. Então, para cada β tal que $\beta^q + \mu\beta = f(\alpha)$, existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_{F'/K}$ com $P_{\alpha,\beta}|P_\alpha$ e $y(P_{\alpha,\beta}) = \beta$. Portanto, P_α tem q extensões distintas em $F'/K(x)$, cada uma de grau um, onde $P_\alpha \in \mathbb{P}_{K(x)/K}$ é o zero de $x - \alpha$.*

Demonstração. Uma vez que $\beta^q + \mu\beta = f(\alpha)$ então $(\beta+\gamma)^q + \mu(\beta+\gamma) = f(\alpha)$ para todo γ tal que $\gamma^q + \mu\gamma = 0$. Logo,

$$T^q + \mu T - f(\alpha) = \prod_{j=1}^{q} (T - \beta_j)$$

com elementos $\beta_j \in K$ dois a dois distintos. Pelo Teorema 11 existe, para cada $j = 1, \ldots, q$, um único lugar $P_j \in \mathbb{P}_{F'/K}$ com $P_j|P_\alpha$ e $y - \beta_j \in P_j$ e P_j de grau um. □

Proposição 11. *Seja $F = \mathbb{F}_{q^2}(x, y)$ com $y^q + y = x^m$ e $m|(q+1)$. Então $F/\mathbb{F}_{q^2}$ tem $N = 1 + q(1 + (q-1)m)$ lugares de grau um.*

Demonstração. O pólo Q_∞ de x é um deles. Pela Proposição 10, precisamos contar, para cada elemento $\alpha \in \mathbb{F}_{q^2}$ o número de raízes $\beta \in \mathbb{F}_{q^2}$ do polinômio:

$$g(T) = T^q + T - \alpha^m \tag{2.2}$$

Sabemos que a função traço $\beta \mapsto \beta^q + \beta$, de $\mathbb{F}_{q^2}$ em $\mathbb{F}_q$, é sobrejetiva. Logo, a Equação 2.2 tem uma raiz β em $\mathbb{F}_{q^2}$ se e somente se $\alpha^m \in \mathbb{F}_q$. Seja $U \subseteq \mathbb{F}_{q^2}^*$ o

subgrupo cíclico de ordem $(q-1)m$ (aqui usamos o fato de que $m|(q+1)$). Logo, para $\alpha \in \mathbb{F}_{q^2}$ temos $\alpha^m \in \mathbb{F}_q$ se e somente se $\alpha \in U \cup \{0\}$.
De onde concluímos que $N = 1 + q((q-1)m+1)$. □

Definição 34. *Um corpo de funções $\mathcal{H}$ é dito Hermitiano se*

$$\mathcal{H} = \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2} \quad com \quad y^q + y = x^{q+1}.$$

O corpo de funções Hermitiano é um caso especial do Teorema 13.
Repare que do Teorema 13 e da Proposição 11 podemos concluir que:

Lema 5. *Para o corpo de funções Hermitiano $\mathcal{H}$ valem as seguintes propriedades:*

i. O gênero de $\mathcal{H}$ é $g = q(q-1)/2$,

ii. $\mathcal{H}$ tem q^3+1 lugares de grau um, nomeadamente:

A. O único pólo de x, que também é o único pólo de y: Q_∞,

B. Para cada $\alpha \in \mathbb{F}_{q^2}$ existem q elementos $\beta \in \mathbb{F}_{q^2}$ com $\beta^q + \beta = \alpha^{q+1}$ e para cada par (α, β) existe um único lugar $P_{\alpha,\beta} \in \mathbb{P}_\mathcal{H}$ de grau um com $x(P_{\alpha,\beta}) = \alpha$ e $y(P_{\alpha,\beta}) = \beta$,

iii. O divisor da diferencial $(dx) = (q(q-1)-2)Q_\infty$,

iv. Para $r \geq 0$, os elementos $x^i y^j$ com $0 \leq i, 0 \leq j \leq q-1$ e $iq + j(q+1) \leq r$ formam um base para $\mathcal{L}(rQ_\infty)$.

Um dos grandes feitos do século vinte foi a prova da Hipótese de Riemann sobre corpos finitos feita pelo matemático francês André Weil (1906-1998), finalizando o projeto começado pelo Teorema de Hasse para curvas elípticas sobre corpos finitos. Dado um corpo de funções $F/\mathbb{F}_q$ de gênero g, o número de lugares

racionais N é limitado superiormente pela atualmente conhecida como Cota de Hasse-Weil:

$$N \leq 1 + q + 2gq^{1/2}.$$

Dizemos que um corpo de funções é *maximal* quando temos uma igualdade na equação acima. Um dos principais resultados sobre o corpo de funções Hermitiano sobre $\mathbb{F}_{q^2}$ é a sua caracterização como sendo o único corpo de funções, a menos de isomorfismos, que é maximal com gênero $q(q-1)/2$. Note que, como o corpo de funções Hermitiano possui q^3+1 lugares racionais, obtemos a maximalidade desejada. Esta caraterização foi provada em 1994 pelos Matemáticos Rück, H. e Stichtenoth, H.. Deste modo o corpo de funções Hermitiano foi utilizado para a construção de códigos longos, conhecidos como Códigos Hermitianos, que possuem parâmetros bem determinaremos. Esta particularidade é um contraponto ao caso geral, pois, em geral é complicado determinar todos os parâmetros de código dado, o que tem sido objeto de intensa pesquisa nos últimos anos.

2.2 Códigos Hermitianos

Nesta seção estudaremos os códigos Hermitianos, que são os códigos algébricos geométricos contruídos a partir do corpo de funções Hermitiano estudado na seção anterior.

Definição 35. *Seja $\mathcal{H} = \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$, onde $y^q + y = x^{q+1}$, o corpo de funções Hermitiano e $Q_\infty \in \mathbb{P}_\mathcal{H}$ o único pólo de x. Para $r \in \mathbb{Z}$ nós definimos o código:*

$$C_r := C_\mathcal{L}(D, rQ_\infty), \tag{2.3}$$

onde

$$D := \sum_{\beta^q+\beta=\alpha^{q+1}} P_{\alpha,\beta} \tag{2.4}$$

é a soma de todos os lugares de grau um (exceto Q_∞) do corpo de funções Hermitiano $\mathcal{H}$. Os códigos C_r são chamados de códigos Hermitianos.

Segue do Lema 5 que o comprimento dos códigos Hermitianos é $n = q^3$.

Exemplo 3. *Os códigos Hermitianos para $q = 2$ são os códigos C_r sobre a curva $y^2 + y = x^3$ no alfabeto $\mathbb{F}_4$. Estes códigos têm dimensão 8, isto é, $C_r \subseteq \mathbb{F}_4^{2^3}$.*

2.2.1 Dimensão dos Códigos Hermitianos

Estudaremos agora a dimensão dos códigos Hermitianos, separando-os em três casos: $r < 0$, $0 \leq r \leq q^3 + q^2 - q - 2$ e $q^3 + q^2 - q - 2 < r$.

Para o estudo das dimensões nossa principal estratégia será comparar a dimensão do espaço de Riemann Roch de um certo divisor com o semigrupo de Weierstrass do mesmo divisor.

Antes, fazemos uma observação básica de que se $r \leq s$ então $C_r \subseteq C_s$, pois

$$x \in \mathcal{L}(rQ_\infty) \Rightarrow (x) \geq -rQ_\infty \geq -sQ_\infty,$$

ou seja, $x \in \mathcal{L}(sQ_\infty)$. Segue que, se $r \leq s$, então $d(C_s) \leq d(C_r)$.

Vamos aos casos: Primeiramente observe que se $r < 0$, então $\mathcal{L}(rQ_\infty) = \{0\}$ e, portanto, $C_r = \{0\}$ e sua dimensão é zero.

Por outro lado, se $r > q^3 + q^2 - q - 2 = n + (2g - 2)$, estamos nas condições do

Teorema 6 e do Teorema de Riemann-Roch, logo

$$dim(C_r) = l(rQ_\infty) - l(rQ_\infty - D) = (r + 1 - g) - (r - q^3 + 1 - g) = q^3 = n.$$

Logo, $C_r = \mathbb{F}_{q^2}^n = \mathbb{F}_{q^2}^{q^3}$.

Portanto temos um único caso de interesse: o intervalo $0 \leq r \leq q^3 + q^2 - q - 2$.

Acompanharemos este caso a partir de agora:

Proposição 12. *O código dual de C_r é*

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

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

Demonstração. Considere o elemento

$$t = \prod_{\alpha \in \mathbb{F}_{q^2}} (x - \alpha) = x^{q^2} - x.$$

Vamos calcular o divisor de t: primeiramente, seja $P' \in \mathbb{P}_\mathcal{H}$ um pólo de t. Logo:

$$0 > v_{P'}(x^{q^2} - x) = v_{P'}(\prod_{\alpha_i \in \mathbb{F}_{q^2}} (x - \alpha_i)) = \sum_{i=1}^{q^2} v_{P'}(x - \alpha_i) = \sum_{i=1}^{q^2} e(P' \mid P) v_P(x - \alpha_i).$$

Se $P = P_{\alpha_i}$, o lugar com parâmetro local $x - \alpha_i$, então $v_{P_{\alpha_i}}(x - \alpha_i) = 1$ e $v_{P_{\alpha_i}}(x - \alpha_j) = 0$, para $j \neq i$.

Por outro lado, se $P = P_\infty$, então $v_{P_\infty}(x - \alpha_i) = -1$, para cada i, pois $v_{P_\infty}(x) = -1$ e $v_{P_\infty}(\alpha_i) = 0$ e $\sum v_{P_\infty}(x - \alpha_i) = -q^2$. Deste modo, $P = P_\infty$ e pelo Teorema

13, $P' = Q_\infty$ e $e(Q_\infty \mid P_\infty) = q$. Concluímos então que:

$$v_{Q_\infty}(x^{q^2} - x) = -q^3.$$

Analogamente, se $P' \in \mathbb{P}_\mathcal{H}$ é um zero de t, então:

$$0 < v_{P'}(x^{q^2} - x) = v_{P'}(\prod_{\alpha_i \in \mathbb{F}_{q^2}} (x - \alpha_i)) = \sum_{i=1}^{q^2} v_{P'}(x - \alpha_i) = \sum_{i=1}^{q^2} e(P' \mid P) v_P(x - \alpha_i).$$

Assim, se $P = P_\infty$ teríamos $\sum e(P' \mid P) v_P(x - \alpha_i) < 0$, o que é absurdo e, se $P = P_{\alpha_i}$, entao $v_{P_{\alpha_i}}(x - \alpha_i) = 1$ e $v_{P_{\alpha_i}}(x - \alpha_j) = 0$, para $j \neq i$ e, como $e(P_{\alpha,\beta} \mid P_\alpha) = 1$ temos $P' = P_{\alpha,\beta}$ e:

$$v_{P_{\alpha,\beta}}(x^{q^2} - x) = 1.$$

Logo:

$$(t) = \sum_{\beta^q + \beta = \alpha^{q+1}} P_{\alpha,\beta} - q^3 Q_\infty.$$

Assim, t é um elemento primo para cada $P_{\alpha,\beta} \leq D$, pois, pelo Teorema de Kummer, cada lugar $P_\alpha \in \mathbb{P}_{K(x)/K}$ possui q extensões no $supp(D)$.
Como $dt = d(x^{q^2} - x) = -dx$, pois q é uma potência da característica do corpo, segue que $(dt) = (dx) = (q^2 - q - 2)Q_\infty$, pelo Lema 5. Segue do Teorema 8 e da Proposição 7 que $C_r^\perp = C_\Omega(D, rQ_\infty) = C_\mathcal{L}(D, D - rQ_\infty + (dt) - (t)) = C_\mathcal{L}(D, (q^3 + q^2 - q - 2 - r)Q_\infty) = C_{q^3+q^2-q-2-r}$. □

Observação 1. *Defina* $r_\perp := q^3 + q^2 - q - 2 - r$.

Evidentemente temos $C_{r_\perp} = C_r^\perp$.

Vamos agora determinar a dimensão de C_r, quando $0 \leq r \leq q^3 + q^2 - q - 2$.

Considere o semigrupo de Weierstrass $H(Q_\infty)$ de Q_∞, i.e.:

$$H(Q_\infty) = \{n \geq 0 \,|\, \exists\ z \in \mathcal{H}\, e\, (z)_\infty = nQ_\infty\}.$$

Ou, em outras palavras, $H(Q_\infty)$ é o conjunto dos $n \geq 0$ que não são lacunas em Q_∞.

Definição 36. *Para $s \geq 0$, seja*

$$H(Q_\infty)_s := \{n \in H(Q_\infty) \,|\, n \leq s\}. \tag{2.5}$$

Lema 6. *Para $s \geq 0$, $|H(Q_\infty)_s| = l(sQ_\infty)$.*

Demonstração. De fato, a igualdade é óbvia para $s = 0$. Suponha que o resultado seja válido para $s_0 = k$ e seja $s_1 = k + 1$. Se s_1 é lacuna, $l(s_1Q_\infty) = l(s_0Q_\infty)$ e $H(Q_\infty)_{s_0} = H(Q_\infty)_{s_1}$. Por outro lado, se s_1 é não-lacuna, segue do Teorema das lacunas de Weierstrass que $l(s_1Q_\infty) = l(s_0Q_\infty)+1$ e $|H(Q_\infty)_{s_1}| = |H(Q_\infty)_{s_0}|+1$. Em ambos os casos, $|H(Q_\infty)_{s_1}| = l(s_1Q_\infty)$. □

Podemos obter uma outra caracterização para $H(Q_\infty)_s$ utilizando os Lemas 5 e 6 da seguinte maneira:

$$H(Q_\infty)_s = \{n \leq s \,|\, n = iq + j(q+1)\, e\, i \geq 0, 0 \leq j \leq q-1\}.$$

Estamos finalmente em condições de determinar a dimensão dos códigos Hermitianos no nosso intervalo de interesse:

Proposição 13. *Suponha que* $0 \leq r \leq q^3 + q^2 - q - 2$. *Então:*

$$dim\ C_r = \begin{cases} |H(Q_\infty)_r|, & se \quad 0 \leq r \leq q^2 - q - 2; \\ r + 1 - (q^2 - q)/2, & se \quad q^2 - q - 2 < r < q^3; \\ q^3 - |H(Q_\infty)_{r_\perp}|, & se \quad q^3 \leq r \leq q^3 + q^2 - q - 2. \end{cases}$$

onde $r_\perp := q^3 + q^2 - q - 2 - r$.

Demonstração. Caso 1: Para $0 \leq r < q^3 = n$, segue da Proposição 6 que:

$$dim\ C_r = dim\ \mathcal{L}(rQ_\infty) = l(rQ_\infty) = |H(Q_\infty)_r|$$

Caso 2: Considere $2g - 2 = q^2 - q - 2 < r < q^3$. Segue da Proposição 6 que

$$dim\ C_r = l(rQ_\infty) = r + 1 - g = r + 1 - (q^2 - q)/2.$$

Caso 3: Já para $q^3 \leq r \leq q^3 + q^2 - q - 2$, $0 \leq r_\perp \leq q^2 - q - 2 < q^3$. Aplicando o primeiro caso para $r_\perp$, obtemos:

$$dim\ C_r = q^3 - dim\ C_{r_\perp} = q^3 - |H(Q_\infty)_{r_\perp}|.$$

□

Já sabemos a dimensão de C_r, quando $r < 0$ e $r > q^3 + q^2 - q - 2$. Pela Proposição 6, sabemos que se $2g - 2 = q^2 - q - 2 < r < q^3 = n$ então a dimensão de C_r será $r - g + 1$ e g é facilmente determinável.
Podemos determinar a dimensão de C_r quando $r \leq q^2 - q - 2$ e quando $q^3 \leq r \leq q^3 + q^2 - q - 2$ explicitamente. Vejamos:

Definição 37. *Seja $r \geq 0$. Defina $\tilde{r} = max\{c \,|\, c \in H(Q_\infty)_r\}$, a maior não lacuna em Q_∞ que é menor ou igual a r.*

É claro que, $H(Q_\infty)_r = H(Q_\infty)_{\tilde{r}}$, já que qualquer inteiro positivo maior que $\tilde{r}$ e menor que r não acrescenta nada a $H(Q_\infty)_r$ e, para $0 \leq r \leq q^3+q^2-q-2$, temos $C_r = C_{\tilde{r}}$ (pois, $C_{\tilde{r}} \subset C_r$ e a dimensão é a mesma, já que $H(Q_\infty)_r = H(Q_\infty)_{\tilde{r}}$).

Lema 7. *Assuma que $r \leq q^2 - q - 2$ e $\tilde{r} = aq + b$ com $0 \leq b \leq q-1$. Então:*

$$|H(Q_\infty)_r| = 1 + a(a+1)/2 + min\{a, b\}.$$

Demonstração. Todo $c \in H(Q_\infty)_r = H(Q_\infty)_{\tilde{r}}$ tem uma representação única da forma $c = iq + (q+1)j = (i+j)q + j$, com $0 \leq i, 0 \leq j \leq q-1$. Logo, $iq+(q+1)j \leq aq+b$ se, e somente se, $i+j \leq a-1$ ou $i+j = a$ e $j \leq b$. Teremos agora que contar quantos elementos satisfazem essas condições:
Primeiramente, se $i+j \leq a-1$, teremos as seguintes possibilidades para as duplas (i, j):

$$\begin{array}{rl} (0,0), (0,1), \ldots, (0,a-2), (0,a-1) & a \textit{ casos} \\ (1,0), (1,1), \ldots, (1,a-2) & a-1 \textit{ casos} \\ \vdots & \vdots \\ (a-2,0), (a-2,1) & 2 \textit{ casos} \\ (a-1,0) & 1 \textit{ caso.} \end{array}$$

Somando teremos $a(a+1)/2$ possibilidades.
Agora, com relação ao caso $i + j = a$ e $j \leq b$, suponha inicialmente que $a \leq b$.

Então temos as possibilidades:

$$(0,a),(1,a-1),\ldots,(a,0) \quad a+1 \; casos.$$

Por outro lado, se $b \leq a$, teremos:

$$(a,0),(a-1,1),\ldots,(a-b,b) \quad b+1 \; casos.$$

Deste modo, para o segundo caso, teremos $min\{a,b\}+1$ possibilidades e alcançamos o resultado desejado. □

Estamos em condições determinar as dimensões dos códigos em qualquer caso. Pelo Lema 16 e pela Proposição 13, a dimensão de C_r quando $r \leq q^2-q-2$ é $a(a+1)+1+min\{a,b\}$. Por outro lado, se $q^3 \leq r \leq q^3+q^2-q-r$, então $r_\perp = q^3+q^2-q-2-r \leq q^2-q-2$, pois $r \geq q^3$. Logo, novamente pelo Lema 16 e pela Proposição 13, a dimensão de $C_r^\perp$ é $a(a+1)/2+1+min\{a,b\}$, onde $\tilde{r}_\perp = aq+b, b \geq q-1$. Segue que a dimensão de C_r é $q^3-(a(a+1)/2+1+min\{a,b\})$.

Observação 2. *Uma vez que*

$$H(Q_\infty)_s = \{n \leq s | n = (i+j)q+j; i \geq 0, 0 \leq j \leq q-1\},$$

é claro que δ é uma lacuna em Q_∞ se, e somente se, $\delta = aq+b$ e $0 \leq a \leq b \leq q-1$. Esta caracterização será fundamental na próxima seção.

Por esta caracterização e pelo fato de $\tilde{r} = aq+b, b \leq q-1$ ser uma não lacuna (isto é, $\tilde{r} \in H(Q_\infty)$), é claro que $min\{a,b\} = b$.

Resumindo as informações demontradas nesta seção:

$$dim\, C_r = \begin{cases} 0 & se \quad r < 0, \\ 1 + a(a+1)/2 + b & se \quad 0 \leq r \leq q^2 - q - 2 \, e \, \tilde{r} = aq + b, \\ r + 1 - (q^2 - q)/2 & se \quad q^2 - q - 2 < r < q^3, \\ q^3 - (1 + a(a+1)/2 + b) & se \quad q^3 \leq r \leq q^3 + q^2 - q - 2 \, e \, \tilde{r} = aq + b, \\ q^3 & se \quad q^3 + q^2 - q - 2 < r. \end{cases}$$

2.2.2 Distâncias mínimas

Vamos estudar agora as distâncias mínimas dos códigos Hermitianos. Para tal, usaremos duas estratégias: um caminho natural a ser tomado é o da álgebra linear em dimensão finita. Outro caminho é utilizar as propriedades da curva algébrica $y^q + y = x^{q+1}$.

Seja $d(C_r)$ a distância mínima do código C_r.

Note que, para $r < 0$, $\mathcal{L}(rQ_\infty) = \{0\}$ e $d(C_r)$ não existe (lembre que precisamos de dois elementos distintos para falarmos de distância mínima) e para, $r > q^3 + q^2 - q - 2 = q^3 + 2g - 2$ já foi demonstrado na seção anterior que $C_r = \mathbb{F}_{q^2}^{q^3}$ e, deste modo, a distância mínima é 1 para todo r.

É importante ressaltar neste momento que $f \in \mathcal{L}(rQ_\infty)$ se, e somente se, o único pólo de f é Q_∞ e sua ordem é menor ou igual a r.

Vamos ao nosso caso de interesse: $0 \leq r \leq q^3 + q^2 - q - 2$.

Sabemos que $d(C_r) \geq n - deg(rQ_\infty) = q^3 - r$ pelo Teorema 6.

Teorema 14. *Assuma que* $r = iq + j(q+1) \leq q^3 - 1$ *com* $0 \leq i, 0 \leq j \leq q - 1$ *e também que uma das afirmações a seguir é verdadeira:*

i. $j = 0$ *ou*

ii. $r \leq q^3 - q^2$.

Então $d(C_r) = q^3 - r$.

Demonstração. Caso 1: Se $r = iq \leq q^3 - 1$, então existe um elemento $0 \neq t \in \mathcal{L}(rQ_\infty)$ com exatamente r zeros distintos (todos de grau um).

De fato, escolha um subconjunto $I \subseteq K = \mathbb{F}_{q^2}$ com $|I| = i$ e seja t o elemento $t = \prod_{\alpha \in I}(x - \alpha)$, o qual tem $iq = r$ zeros distintos, pois, $x - \alpha$ corresponde a um lugar de grau um em $K(x)$, o qual tem q extensões no $supp(D)$.

Repare que $t \in \mathcal{L}(rQ_\infty)$, pois pelo Teorema 12, se $P_\alpha \in \mathbb{P}_{K(x)/K}$ é o lugar correspondente a $x - \alpha \in K(x)$ então:

$$(t) = \sum_{\alpha \in I, \beta^q + \beta = \alpha^{q+1}} P_{\alpha,\beta} - rQ_\infty,$$

onde, $\beta \in \mathbb{F}_{q^2}$, com $\beta^q + \beta = \alpha^{q+1}$.

Portanto, a palavra correspondente $(t(P_1), \ldots, t(P_{q^3}))$ tem peso $q^3 - r$.

Caso 2: Assuma que $r = iq + j(q+1) \leq q^3 - q^2$ com $0 \leq i, 0 \leq j \leq q-1$. Então existe um elemento $0 \neq t \in \mathcal{L}(rQ_\infty)$ com exatamente r zeros distintos (todos de grau um).

De fato, se $r = q^3 - q^2$, então o resultado segue do caso 1. Podemos assumir então que $r < q(q^2 - q)$. Logo nós temos $i \leq q^2 - q - 1$ (como j é no máximo $q - 1$ temos $iq + (q-1)(q+1) < q(q^2 - q)$. Segue que $iq + q^2 \leq q(q^2 - q)$ e, portanto, $i \leq q^2 - q - 1$, já que q é inteiro maior que 1). Escolha $\gamma \in \mathbb{F}_q \setminus \{0\}$ e considere o conjunto $A := \{\alpha \in \mathbb{F}_{q^2} | \alpha^{q+1} \neq \gamma\}$. Então, $|A| = q^2 - (q+1) \geq 1$ e

podemos escolher $\alpha_1, \ldots, \alpha_i \in A$. Então, o elemento

$$t_1 := \prod_{v=1}^{i} (x - \alpha_v) \in \mathcal{L}(iqQ_\infty).$$

tem iq zeros distintos $P_{\alpha,\beta} \leq D$, já que cada par (α,β) corresponde a um lugar $P_{\alpha,\beta}$ e a função traço é sobrejetiva, e se P_{α_v} correspondente a $x - \alpha_v \in K(x)$, P_{α_v} tem q extensões $P_{\alpha,\beta}$ no $supp(D)$ e, portanto:

$$(t_1) = \sum_{v=1}^{i} P_{\alpha_v,\beta} - iqQ_\infty.$$

Agora, escolha j elementos distintos $\beta_1, \ldots, \beta_j \in \mathbb{F}_{q^2}$ tais que $\beta_\mu^q + \beta_\mu = \gamma$ e defina

$$t_2 := \prod_{\mu=1}^{j} (y - \beta_\mu) \in \mathcal{L}(j(q+1)Q_\infty).$$

Então, t_2 tem $j(q+1)$ zeros distintos $P_{\alpha,\beta}$, já que cada par (α,β) corresponde a um lugar $P_{\alpha,\beta}$ e cada um deles é distinto dos zeros de t_1, pois $\beta_\mu^q + \beta_\mu = \gamma \neq \alpha_v^{q+1}$ para $\mu = 1, \ldots, j$ e $v = 1, \ldots, i$ e

$$(t_2) = \sum_{\mu=1}^{j} P_{\alpha,\beta_\mu} - j(q+1)Q_\infty.$$

Logo $t := t_1 t_2 \in \mathcal{L}((iq + j(q+1))Q_\infty) = \mathcal{L}(rQ_\infty)$ tem r zeros distintos $P_{\alpha,\beta} \leq D$. Portanto, a palavra correspondente tem peso $q^3 - r$. □

Observação 3. *Repare que podemos concluir da demonstração do Teorema 14, que, para $r \leq q^3$ e $r = iq$ ou $r \leq q^3 - q^2$, r é nao-lacuna se, e somente se, existe uma função $f \in \mathcal{L}(rQ_\infty)$ com exatamente r zeros distintos no $supp(D)$.*

Lema 8. *Assuma que* $0 \leq r \leq n = q^3$ *e seja* $\delta = q^3 - r$. *Então existe uma função* $f \in \mathcal{L}(rQ_\infty)$ *tendo exatamente* r *zeros distintos no* $supp(D)$ *se, e somente, se existe* $h \in \mathcal{L}(\delta Q_\infty)$ *tendo exatamente* δ *zeros distintos no* $supp(D)$.

Demonstração. Seja $u = x^{q^2} - x$. Como $(u) = D - q^3 Q_\infty$, basta considerar a função u/f (e u/h) para uma dada f (resp., h) satisfazendo as condições do Lema. □

Estamos interessados agora em determinar as distâncias mínimas em códigos Hermitianos C_r quando $q^3 - q^2 \leq r < q^3$. Sabemos que se $n \geq 2g$ então n é certamente uma não-lacuna em Q_∞. No corpo de funções Hermitiano, $2g = q^2 - q$, pelo Lema 5. Lembrando que $\tilde{r} = max\{c \,|\, c \in H(Q_\infty)_r\}$, a maior não-lacuna em Q_∞ que é menor ou igual a r, temos, neste intervalo, $r = \tilde{r}$, pois $r \geq q^3 - q^2 \geq q^2 - q = 2g$.

Note que, para r no intervalo dado, podemos escrevê-lo como $r = q^3 - q^2 + aq + b$, com $0 \leq a, b \leq q-1$. No caso em que $r = q^3 - q^2 + aq$ $(b = 0)$, temos $d(C_r) = q^3 - r$, pelo Teorema 14.

Teorema 15. *Assuma que* $r = q^3 - q^2 + aq + b$ *onde* $0 \leq a, b \leq q - 1$. *Se* $a < b$ *então*

$$d(C_r) = q^3 - r = q^2 - aq - b \tag{2.6}$$

Demonstração. É suficiente mostrar que existe uma função $f \in \mathcal{L}(rQ_\infty)$ tal que f tem exatamente r zeros distintos no $supp(D)$. Pelo Lema 8 é suficiente mostrar que existe uma função em $\mathcal{L}(\delta Q_\infty)$ com δ zeros distintos, onde $\delta = q^3 - r$. Repare

que

$$\delta = q^3 - r = q^2 - aq - b = (q - (a+1))q + (q - b).$$

Como $(q-(a+1)) \geq q-b$, δ não é uma lacuna em Q_∞, pela Observação 2, então, pela Observação 3, existe uma função $h \in \mathcal{L}(\delta Q_\infty)$ tendo exatamente δ distintos zeros no $supp(D)$, pois $\delta \leq q^3 - q^2$. □

Proposição 14. *Assuma que* $r = q^3 - q^2 + aq + a$ *onde* $0 \leq a \leq q-1$. *Seja* $f \in \mathcal{L}(rQ_\infty)$ *uma função não nula. Então* f *tem no máximo* $r-a$ *zeros distintos no* $supp(D)$.

Demonstração. Seja $\delta_m = q^3 - r + m$, onde $0 \leq m \leq a-1$ então nós temos

$$\delta_m = q^2 - aq - a + m = (q - a - 1)q + (q - a + m).$$

Como $0 \leq q - a - 1 < q - a + m \leq q - 1$, temos que δ_m é uma lacuna de Q_∞ para qualquer m com $0 \leq m \leq a-1$, pela Observação 2.

Segue então da Observação 3 e do Lema 8, que não existe uma função $f \in \mathcal{L}((r-m)Q_\infty), r-a+1 \leq r-m \leq r$, com exatamente $r-m$ zeros distintos no $supp(D)$.

Já provamos que não existe $h \in \mathcal{L}((r-m)Q_\infty)$ com $r-m$ zeros distintos no $supp(D)$. Provaremos agora não existe $f \in \mathcal{L}(rQ_\infty)$ com $r-m$ zeros distintos, para todo $m = 0, \ldots, a-1$ no $supp(D)$ e com isso concluímos a demonstração. De fato, pois sendo $r - m \geq r - (a-1) > r - a$, então f teria no máximo $r-a$ zeros distintos no $supp(D)$.

Suponha então que exista $f \in \mathcal{L}(rQ_\infty)$ com $r-m$ zeros distintos no $supp(D)$, onde $r - a + 1 \leq r - m \leq r$. Logo, como $f \in \mathcal{L}(rQ_\infty) \setminus \mathcal{L}((r-m)Q_\infty)$, então

deve existir um r' com $r - m \leq r' \leq r$,

$$(f) = E + S - r'Q_\infty,$$

onde E é um divisor efetivo com $E \leq D$, $deg(E) = r - m$ e S é um divisor efetivo tal que $supp(S) \cap supp(D) \subset supp(E), Q_\infty \notin supp(S)$ e $s := deg(S) = r' - (r - m)$. Agora, como $r - m \leq r' \leq r$ e $0 \leq m \leq a - 1 \leq q - 2$, nós temos $0 \leq s \leq m \leq q - 2$. Logo,

$$\left(\frac{x^{q^2} - x}{f}\right) = D - E - S - (q^3 - r')Q_\infty.$$

Considere a extensão por constantes F' composta por F e por $\tilde{K}$, o fecho algébrico de $K = \mathbb{F}_{q^2}$. Em [(16), Teorema 3.6.3] é provado que F' tem o mesmo gênero de F. Desejamos mostrar que, mesmo em F', a função $(\frac{x^{q^2}-x}{f})$, com o divisor dado acima, não pode existir. Em F' todos os lugares tem grau um. Dado um ponto $P_{\alpha,\beta} \subset supp(S)$, considere a reta $y - \beta$ passando por $P_{\alpha,\beta}$.

Afirmamos que $(y - \beta) = P_{\alpha,\beta} + J - (q + 1)Q_\infty$ onde $\beta^q + \beta = \alpha^{q+1}$, $J \geq 0$ e $Q_\infty \notin supp(J)$. De fato, fixado β, existem $q+1$ elementos α tais que $\beta^q + \beta = \alpha^{q+1}$, já que a função norma é sobrejetiva. Assim, cada um destes $q + 1$ pares (α, β) corresponderá a um lugar $P_{\alpha,\beta}$ no $supp(D)$. Deste modo, o pólo Q_∞ de $y - \beta$ tem ordem $q + 1$.

Logo, temos que o divisor $P_{\alpha,\beta}$ é equivalente ao divisor $-J + (q + 1)Q_\infty$, ou seja, $P_{\alpha,\beta} \sim -J + (q + 1)Q_\infty$. Somando cada lugar racional no suporte de S e escrevendo da forma acima encontramos

$$S \sim -R + s(q + 1)Q_\infty,$$

onde $R \geq 0$ e $Q_\infty \notin supp(R)$. Logo, como $\left(\frac{x^{q^2}-x}{f}\right) = D - E - S - (q^3 - r')Q_\infty$, concluímos que

$$\left(\frac{x^{q^2}-x}{f}\right) \sim D - E + R - (q^3 - r' + s(q+1))Q_\infty, \tag{2.7}$$

onde $D - E + R \geq 0$ (pois $E \leq D$ e $0 \leq R$) e $Q_\infty \notin supp(D-E) \cup supp(R)$. Assim, a Relação 2.7 nos diz que $(q^3 - r' + s(q+1))$ é não-lacuna em Q_∞.
Por outro lado, seja $r' = r - j$ com $0 \leq j \leq m$. Como $r - m \leq r' \leq r$, segue que $s = r' - (r-m) = r - j - (r-m) = m - j$. Então:

$$\begin{aligned} q^3 - r' + s(q+1) &= q^3 - r + j + s(q+1) \\ &= q^2 - aq - a + j + s(q+1) \\ &= (q - a + s - 1)q + (q - a + s + j). \end{aligned}$$

Como $0 \leq (q-a+s-1) \leq (q-a+s+j) = q-a+m \leq q-1$, $q^3 - r' + s(q+1)$ é uma lacuna em Q_∞ para qualquer r com $r - m \leq r' \leq r$, de onde obtemos uma contradição. □

Teorema 16. *Se $r = q^3 - q^2 + aq + a$, onde $0 \leq a \leq q-1$. Então:*

$$d(C_r) = q^3 - r + a = q^2 - aq. \tag{2.8}$$

Demonstração. Repare que $d(C_r) \leq d(C_{q^3-q^2+aq})$ (pois $r \geq q^3 - q^2 + aq$ e, portanto $C_{q^3-q^2+aq} \subset C_r$) e $d(C_{q^3-q^2+aq}) = q^3 - (q^3 - q^2 + aq) = q^2 - aq$ pelo Teorema 14, isto é, $d(C_r) \leq q^2 - aq$. Por outro lado, pela Proposição 14, não existe uma função $f \in \mathcal{L}(rQ_\infty)$ tendo exatamente $r - m$ zeros distintos no $supp(D)$ para cada $m = 0, 1, \ldots, a-1$. Logo, $d(C_r) \geq q^3 - r + a = q^2 - aq$. □

Teorema 17. *Se* $r = q^3 - q^2 + aq + b$ *com* $0 \leq b < a \leq q-1$, *então:*

$$d(C_r) = q^2 - aq. \tag{2.9}$$

Demonstração. Como $r \geq q^3 - q^2 + aq$, $d(C_r) \leq d(C_{q^3-q^2+aq}) = q^2 - aq$. Por outro lado, $r < q^3 - q^2 + aq + a$, logo $d(C_r) \geq d(C_{q^3-q^2+aq+a}) = q^2 - aq$, pelo Teorema 16. □

Estamos interessados agora em estudar o comportamento das distâncias mínimas no intervalo $q^3 \leq r \leq q^3+q^2-q-2$. Note que, como $q^3 \leq r \leq q^3+q^2-q-2$ temos $0 \leq r_\perp \leq q^2-q-2 = 2g-2$, já que $q^3 - r \leq 0$ e $r_\perp = q^3+q^2-q-2-r$. Utilizando a Observação 2 e o fato de que $0 \leq r_\perp \leq q^2-q-2$, repare que

$$\tilde{r}_\perp = aq + b,$$

onde $0 \leq b \leq a \leq q-2$ e $\tilde{r}_\perp$ é a maior não-lacuna em Q_∞ menor ou igual a $r_\perp$.

Teorema 18. *Seja* $q^3 \leq r \leq q^3+q^2-q-2$. *Se* $\tilde{r}_\perp = aq+b$, *onde* $0 \leq b \leq a \leq q-2$ *então:*

$$d(C_r) \leq \begin{cases} a+2 & se \quad b = a, \\ a+1 & se \quad b < a. \end{cases} \tag{2.10}$$

Demonstração. A demonstração vai ser dada como consequência do Teorema 5, ou seja, vamos determinar uma certa quantidade de colunas da matriz de paridade H do código C_r que são linearmente dependentes.

Seja $\alpha \in \mathbb{F}_{q^2}$ fixo e considere o conjunto de lugares racionais $P_{\alpha,beta}$ para o α fixo

tomado

$$\{R_i \,|\, R_i = P_{\alpha,\beta_i}, i = 1,2,\ldots,q\},$$

no $supp(D)$, onde $\beta_i^q + \beta_i = \alpha^{q+1}$ com $\beta_i \neq \beta_j$ quando $i \neq j$ e $a+2 \leq q$.

Caso 1: $b = a$. Uma base de $\mathcal{L}(\tilde{r}_\perp Q_\infty)$ é $\{1, x, y, \ldots, x^a, x^{a-1}y, x^{a-2}y^2, \ldots, y^a\}$, pelo Lema 5 (pois, $i + j \leq a$, $j \leq a$ e $0 \leq i$).

Já provamos anteriormente que, se $0 \leq r' \leq q^3 + q^2 - q - 2$, então $C_{r'} = C_{\tilde{r'}}$. Assim, como $0 \leq r_\perp \leq q^2 - q - 2$ para este Teorema, temos $C_{r_\perp} = C_{\tilde{r}_\perp}$.

Sejam $P_1, \ldots, P_{q^3}$, todos os lugares no $supp(D)$.

Considere a matriz geradora de $C_{r_\perp}$, ou seja, a matriz de paridade H de C_r:

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x(P_1) & x(P_2) & \ldots & x(P_{q^3}) \\ y(P_1) & y(P_2) & \ldots & y(P_{q^3}) \\ \vdots & \vdots & \ddots & \vdots \\ x^{a-1}y(P_1) & x^{a-1}y(P_2) & \ldots & x^{a-1}y(P_{q^3}) \\ \vdots & \vdots & \ddots & \vdots \\ y(P_1)^a & y(P_2)^a & \ldots & y(P_{q^3})^a \end{pmatrix}$$

Considere a submatriz H_1 de H com colunas correspondentes a $R_1, R_2, \ldots, R_{a+2}$, deste modo, $x(R_i) = \alpha$ e $y(R_i) = \beta_i$ para todo $i = 1, \ldots, a+2$ e reordene as

linhas da seguinte maneira:

$$H_1 = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \dots & \beta_{a+2} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_1^a & \beta_2^a & \dots & \beta_{a+2}^a \\ \alpha & \alpha & \dots & \alpha \\ \alpha^2 & \alpha^2 & \dots & \alpha^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^a & \alpha^a & \dots & \alpha^a \\ \alpha\beta_1 & \alpha\beta_2 & \dots & \alpha\beta_{a+2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha\beta_1^{a-1} & \alpha\beta_2^{a-1} & \dots & \alpha\beta_{a+2}^{a-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{a-1}\beta_1 & \alpha^{a-1}\beta_2 & \dots & \alpha^{a-1}\beta_{a+2} \end{pmatrix}$$

Como $\alpha \in \mathbb{F}_{q^2}$ está fixo, podemos usar o método de eliminação Gaussiana para transformar todas as linhas abaixo da linha L_{a+1} em linhas identicamente nulas. Por exemplo, a linha L_{a+2} pode ser eliminada com a operação $L_{a+2} - \alpha L_1$. A linha L_{2a+2} é eliminada com a operação $L_{2a+2} - \alpha L_2$. Prosseguindo com as eliminações

Gaussianas obtemos $\tilde{H}_1$ como se segue:

$$\tilde{H}_1 = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \beta_3 & \dots & \beta_{a+2} \\ \beta_1^2 & \beta_2^2 & \beta_3^2 & \dots & \beta_{a+2}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \beta_1^a & \beta_2^a & \beta_3^a & \dots & \beta_{a+2}^a \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Logo, H_1, tem posto $a+1$, já que $\tilde{H}_1$ possui uma submatriz que correponde a uma Matriz de Vandermonde, e tem $a+2$ colunas, de modo que as colunas são L.D. e, portanto, $d(C_r) \leq a+2$.

Caso 2: $b < a$. Como $\tilde{r}_\perp < aq + a$ e y^a tem pólo em Q_∞ de ordem $a(q+1)$, ele não pode estar contido em $\mathcal{L}(\tilde{r}_\perp Q_\infty)$, fazendo com que a linha correspondente a y^a seja transformada em uma linha identicamente nula da matriz $\tilde{H}_1$. Então, H_1 tem posto a e $a+1$ colunas e, portanto, $d(C_r) \leq a+1$. □

Nosso objetivo agora é provar a desigualdade contrária no Teorema 18. Neste sentido, pelo Teorema 5 devemos mostrar que para $\tilde{r}_\perp = aq + a$, quaisquer $a+1$ colunas da matriz de paridade H de C_r escolhidas arbitrariamente são linearmente independentes. A segunda desigualdade será consequência da primeira. Nossa estratégia será mostrar que qualquer submatriz $(a+1) \times (a+1)$, B de H, tem posto maior ou igual a $a+1$.

Considere $\tilde{r}_\perp = aq + a$, onde $0 \leq a \leq q-2$. Seja A uma submatriz de H com

$a+1$ colunas distintas arbitrárias de H. Cada coluna, corresponde a um lugar $P_{\alpha,\beta}$ de grau um e podemos reordenar as colunas de acordo com α, isto é, de acordo com:

$$\begin{matrix} P_{\alpha_1,\beta_{1,1}}, & P_{\alpha_1,\beta_{1,2}}, & \dots & P_{\alpha_1,\beta_{1,b_1}} \\ P_{\alpha_2,\beta_{2,1}}, & P_{\alpha_2,\beta_{2,2}}, & \dots & P_{\alpha_2,\beta_{2,b_2}} \\ \vdots & \vdots & \ddots & \vdots \\ P_{\alpha_r,\beta_{r,1}}, & P_{\alpha_r,\beta_{r,2}}, & \dots & P_{\alpha_r,\beta_{r,b_r}} \end{matrix} \tag{2.11}$$

onde os α_i são dois a dois distintos e $\sum_{i=1}^{r} b_i = a+1$ e $b_i \geq b_{i+1} \geq 1$.

Seja $B(r)$ a base inteira de $\mathcal{L}(rQ_\infty)$.

É fácil checar que $x^{i-1}y^{j_i} \in B(\tilde{r}_\perp), 0 \leq j_i \leq b_i - 1$.

Reescreva os elementos dessa base como:

$$\begin{matrix} 1, & y, & y^2, & \dots & y^{b_1-1} \\ x, & xy, & xy^2, & \dots & xy^{b_1-1} \\ x^2, & x^2y, & x^2y^2, & \dots & x^2y^{b_1-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x^{r-1}, & x^{r-1}y, & x^{r-1}y^2, & \dots & x^{r-1}y^{b_1-1} \end{matrix} \tag{2.12}$$

Podemos extrair uma submatriz B, $(a+1)\times(a+1)$ de A, da seguinte maneira:

i. Cada linha corresponde a uma função em 2.12 na ordem dada.

ii. Cada coluna corresponde a um lugar de grau um em 2.11.

iii. Cada entrada de B é obtida por evaluação.

Por evaluação, queremos dizer que $B = [B_{i,j}], i = 1, \dots, r$, onde $B_{i,j}$ é uma

matriz $(b_i \times b_j)$ tal que a (k,l)-ésima entrada é $\alpha_j^{i-1}\beta_{j,l}^{k-1}$, isto é,

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

com

$$D_{i,j} := \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \beta_{j,1} & \beta_{j,2} & \beta_{j,3} & \dots & \beta_{j,b_i} \\ \beta_{j,1}^2 & \beta_{j,2}^2 & \beta_{j,3}^2 & \dots & \beta_{j,b_i}^2 \\ \vdots & & \vdots & \ddots & \vdots \\ \beta_{j,1}^{b_i-1} & \beta_{j,2}^{b_i-1} & \beta_{j,3}^{b_i-1} & \dots & \beta_{j,b_i}^{b_i-1} \end{pmatrix}$$

Lema 9. *[(9), Lemma 2] Defina $\tau_j := \prod_{i=1}^{j-1}(\alpha_j - \alpha_i), j = 2,3,\dots,r$. Então,*

$$det(B) = (\prod_{i=1}^{r} det(D_{i,i}))(\prod_{j=2}^{r} \tau_j^{b_j})$$

Lema 10. *Assuma que $\tilde{r}_\perp = aq + a$ onde $0 \leq a \leq q-2$. Então $a+1$ colunas de H escolhidas arbitrariamente são linearmente independentes sobre $\mathbb{F}_{q^2}$.*

Demonstração. Escolha $a+1$ colunas de H e reordene-as de acordo com α de $P_{\alpha,\beta}$. Podemos construir submatrizes A e B como explicitado acima. Como os α_i são dois a dois distintos para $i = 1,2,\dots,r$, temos $\tau_j \neq 0$ para $j = 2,3,\dots,r$. Uma vez que os $\beta_{i,j}$ também são dois a dois distintos para $j = 1,2,\dots,b_i$ e um dado i teremos $det(D_{i,i}) \neq 0$. Logo, pelo Lema 9, $det(B) \neq 0$. Mas isto implica que $a+1 = posto(B) \leq posto(A) \leq a+1$, ou seja A tem posto $a+1$ e, portanto, as colunas de A são lineamente independentes em $\mathbb{F}_{q^2}$. □

Teorema 19. *Seja $q^3 \leq r \leq q^3 + q^2 - q - 2$. Assuma que $\tilde{r}_\perp = aq + b$ com*

$0 \leq b \leq a \leq q-2$. *Então:*

$$d(C_r) = \begin{cases} a+2 & se \quad b = a, \\ a+1 & se \quad b < a. \end{cases}$$

Demonstração. Se $b = a$, então quaisquer $a+1$ colunas de H são linearmente independentes sobre $\mathbb{F}_{q^2}$ pelo Lema 10, logo $d(C_r) \leq a+1$. Por outro lado, o Teorema 18 nos dá $d(C_r) \geq a+1$.

Se $b < a$, então seja $\tilde{r}'_\perp = (a-1)q + (a-1)$. Uma vez que $\tilde{r}'_\perp \leq \tilde{r}_\perp$, temos $C_r \subseteq C_{r'}$. Logo $d(C_r) \geq d(C_{r'}) = (a-1)+2 = a+1$ pela primeira parte deste Teorema. Novamente, pelo Teorema 18, concluímos que $d(C_r) = a+1$. □

Por último, temos a seguinte consequência do Teorema 19.

Proposição 15. *Se* $q^3 - q \leq r \leq q^3$, *então* $d(C_r) = q$.

Demonstração. Se $r = q^3$, então $r_\perp = q^3 + q^2 - q - 2 - r = q^2 - q - 2$ de modo que $\tilde{r}_\perp = (q-2)q + q - 2 = r_\perp$. Logo, $d(C_{q^3}) = q - 2 + 2$ pelo Teorema 19. Por outro lado, $d(C_{q^3-q}) = q$ pelo Teorema 14. Para $q^3 - q \leq r \leq q^3$, $C_{q^3-q} \subseteq C_r \subseteq C_{q^3}$ e, portanto, $q = d(C_{q^3}) \leq d(C_r) \leq d(C_{q^3-q}) = q$. □

O seguinte quadro resume as informações provadas até aqui.

Parâmetros dos Códigos Hermitianos		
r	Dimensão k	Distância Mínima d
$r < 0$	0	Não existe
$0 \leq r < q^2 - q, \tilde{r} = aq + b$	$a(a+1)/2 + b + 1$	$q^3 - r$
$q^2 - q \leq r < q^3 - q^2$	$r - (q^2 - q)/2 + 1$	$q^3 - r$
$q^3 - q^2 \leq r < q^3$, $r = q^3 - q^2 + aq + b$ $0 \leq a < b \leq q - 1$	$r - (q^2 - q)/2 + 1$	$q^3 - r$
$q^3 - q^2 \leq r < q^3$, $r = q^3 - q^2 + aq + b$ $0 \leq b \leq a \leq q - 1$	$r - (q^2 - q)/2 + 1$	$q^3 - r + b$
$q^3 \leq r \leq q^3 + q^2 - q - 2$, $r_\perp = q^3 - q^2 + aq + b - r$ $\tilde{r}_\perp = aq + b, 0 \leq b \leq a \leq q - 1$	$q^3 - (a(a+1)/2 + b + 1)$	$a + 2$ se $a = b$ $a + 1$ se $b < a$
$r > q^3 + q^2 - q - 2$	q^3	1

Façamos um último exemplo:

Exemplo 4. *Seja* $q = 2$. *Então* $\mathbb{F}_4(x,y)/\mathbb{F}_4$ *com* $y^2 + y = x^3$ *tem gênero* $g = 1$. *Temos* $K = \mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{0,1,\alpha,\alpha+1\}$ *onde* α *é um zero para* $x^2 + x + 1$.

Dado r *inteiro,* C_r *tem comprimento* 8.

Seja k *a dimensão de* C_r *e* d_r *sua distância mínima. Se* $r < 0$ *então* $k = 0$ *e não temos* d_r.

Se $0 \leq r < 2$, $\tilde{r} = aq + b$ *deve satisfazer* $0 \leq b \leq a \leq 1$. *Como* 0 *é certamente não-lacuna e* 1 *é uma lacuna,* $\tilde{r} = 0$. *Deste modo,* $k = 0 + 0 + 1 = 1$ *e* $d_0 = 8$ *e* $d_1 = 7$. *Para,* $2 \leq r < 4$, $k = r$ *e* $d_r = 8 - r$.

Para $4 \leq r < 8$ *teremos que analisar cada caso. Primeiramente, escreva* $r = 2a + b + 4$, *onde* $0 \leq a, b \leq 1$. *Para* $r = 4$, $a = b = 0$, $k = 4$ *e* $d_4 = 4$. *Para* $r = 5$, $a = 0$ *e* $b = 1$, *de modo que,* $k = 5$ *e* $d_5 = 3$. *Para* $r = 6$, $a = 1$ *e* $b = 0$ *e* $k = 6$ *e* $d_6 = 2$. *Finalmente para* $r = 7$, $a = b = 1$ *e* $k = 7$ *com* $d_7 = 2$.

Para o penúltimo caso, só temos a possibilidade de $r = 8$ *e, então,* $r_\perp = 0 = 0q + 0$. *Deste modo,* $k = 7$ *e* $d = 0 + 2 = 2$. *Por último, se* $r > 8$, $k = 8$ *e* $d = 1$.

O código é MDS para $r = 0$ *e* $r \geq 7$.

O código será auto dual se, e somente se, $r = 4$ *e auto ortogonal se e somente se* $r \leq 4$.

Para $r = 3$, *o conjunto* $\{1, x, y\}$ *é uma base para* $\mathcal{L}(3Q_\infty)$. *Para cada* $a \in \mathbb{F}_4$, *existem* 2 *elementos distintos em* $\mathbb{F}_4$ *tais que* $b^2 + b = a^3$ *e a cada par* (a,b) *corresponde um lugar racional* $P_{(a,b)}$ *com* $x(P_{(a,b)}) = a$ *e* $y(P_{(a,b)}) = b$. *Logo, os lugares racionais de* $F(x,y)/\mathbb{F}_4$ *exceto* Q_∞ *são* $P_{(0,0)}, P_{(0,1)}, P_{(1,\alpha)}, P_{(1,\alpha+1)}, P_{(\alpha,\alpha)}, P_{(\alpha,\alpha+1)}, P_{(\alpha+1,\alpha)}$ *e* $P_{(\alpha+1,\alpha+1)}$.

Concluímos então que $x(P_{(0,0)}) = 0, x(P_{(0,1)}) = 0, x(P_{(1,\alpha)}) = 1, x(P_{(1,\alpha+1)}) =$

$1, x(P_{(\alpha,\alpha)}) = \alpha, x(P_{(\alpha,\alpha+1)}) = \alpha, x(P_{(\alpha+1,\alpha)}) = \alpha+1, x(P_{(\alpha+1,\alpha+1)}) = \alpha+1$ *e* $y(P_{(0,0)}) = 0, y(P_{(0,1)}) = 1, y(P_{(1,\alpha)}) = \alpha, y(P_{(1,\alpha+1)}) = \alpha+1, y(P_{(\alpha,\alpha)}) = \alpha, y(P_{(\alpha,\alpha+1)}) = \alpha+1, y(P_{(\alpha+1,\alpha)}) = \alpha, y(P_{(\alpha+1,\alpha+1)}) = \alpha+1$.

Logo, já temos todas as informações necessárias para formar a matriz geradora de C_3*:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 0 & 1 & \alpha & \alpha+1 & \alpha & \alpha+1 & \alpha & \alpha+1 \end{pmatrix}$$

Fazendo a operação $L_3 \mapsto L_2 + L_3$*. Temos:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 0 & 1 & \alpha+1 & \alpha & 0 & 1 & 1 & 0 \end{pmatrix}$$

Como $d_3 = 5$ *e a linha* L_3 *tem* 5 *entradas não nulas, observamos que nenhuma palavra de* C_3 *tem peso menor que* L_3*. Para* $r = 5$*, o conjunto* $\{1, x, y, x^2, xy\}$ *é uma base para* $\mathcal{L}(5Q_\infty)$*. Logo, a matriz geradora de* C_5 *é:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 0 & 1 & \alpha & \alpha+1 & \alpha & \alpha+1 & \alpha & \alpha+1 \\ 0 & 0 & 1 & 1 & \alpha+1 & \alpha+1 & \alpha & \alpha \\ 0 & 0 & \alpha & \alpha+1 & \alpha+1 & 1 & 1 & \alpha \end{pmatrix}$$

Faça as operações, $L_3 \mapsto L_3 + L_5$, $L_4 \mapsto L_4 + L_2$ *e* $L_3 \mapsto L_3 + L_4$ *e teremos:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha+1 & \alpha+1 \\ 0 & 1 & 0 & 0 & 0 & \alpha+1 & \alpha & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & \alpha & \alpha+1 & \alpha+1 & 1 & 1 & \alpha \end{pmatrix}$$

Observe que a linha L_3 *da matriz acima, dada por* $L_3 = (0, 1, 0, 0, 0, \alpha+1, \alpha, 0)$ *tem peso 3. Como* $d_5 = 3$ *é impossível encontrar qualquer palavra com peso menor que* L_3.

No seguinte link pode ser feito o download de um aplicativo que calcula a distância mínima de um código Hermitiano, dados, pelo usuário, os valores de q e r (este aplicativo foi escrito em linguagem C):

`https://www.dropbox.com/s/0u7d9rthqucdt5e/MD%20for%20Hermitian%20Codes.exe`

Referências Bibliográficas

[1] Atiyah, M. e MacDonald, I., *Introduction to Commutative Algebra*, Add. Wesley, 1969.

[2] Buchweitz, R., *On Zariski's criterion for equisingularity and non smoothable monomial curves*, Thése, Paris VII, 1981.

[3] Bulygin, S., *Generalized Hermitian Codes over* $GF(2^r)$, IEEE Trans. Inform. Theory 52, pp. 4664-4669, 2006.

[4] Castellanos, A., *Sobre Códigos Hermitianos Generalizados*. Tése de Doutorado em Matemática/UNICAMP-SP. 2008.

[5] Garcia, A. e Stichtenoth, H., *A Class of Polynomials over Finite Fields*, Finite Fields Appl. 5, pp. 424-435, 1999.

[6] Garcia, A., Stichtenoth, H. e Xing, C., *On Subfields of the Hermitian Function Field*. Compositio Mathematica 120. Kluwer Academic Publishers, pp 137-170, 2000.

[7] Hefez, A. e Villela, M., *Códigos Corretores de Erros. Série de Computação e Matemática*. SBM. 2002.

[8] Herstein, I., *Topics in Algebra*. Second Edition. John Wiley & Sons. 1975.

[9] Kumar, P. e Yang, K., *On the True Minimum Distances of Hermitian Codes*. Coding Theory and Algebraic Geometry. Proceedings of the International Workshop Held in Luminy, France, pp 99-107,1991.

[10] Lidl, R. e Niederreiter, H., *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1986.

[11] Munuera, C., Sepúlveda, A. e Torres, F., *Generalized Hermitian Codes*. Designes, Codes and Criptography. Vol. 69, Issue 1, pp 123-130, 2013.

[12] Picado, J., *Corpos e Equações Algébricas. Universidade de Coimbra*. 2011. Disponível em
http://www.mat.uc.pt/ picado/corpos/apontamentos/CEA.pdf

[13] Rück, H. e Stichtenoth, H., *A characterization of Hermitian function fields over finite fields*. Journal für die reine und angewandt Mathematik. 1994.

[14] Salvador, C., *Topics in the Theory of Algebraic Function Fields*. Birkhäuser Boston. 2006.

[15] Stichtenoth, H., *A Note on Hermitian Codes Over* $GF(q^2)$. IEEE, Transactions on Information Theory, Vol. 34, no. 5, pp 1345-1348, 1988.

[16] Stichtenoth, H., *Algebraic Function Fields and Codes*. Graduates Texts in Mathematics. Springer. Second Edition.

[17] Xing, C. e Stichtenoth, H. *The Genus of Maximal Function Fields Over Finite Fields*. Manuscripta Mathematica. 1994.

Apêndice A

Algorítmo da Distância Mínima

Segue abaixo o algorítmo na linguagem C do aplicativo, no qual o usuário interage dando os valores de q e r e recebe como resultado a distância mínima d_r de C_r, o valor s para o qual o código é auto dual e se $q^3 \leq r \leq q^3 + q^2 - q - 2$ recebe também o valor de t que é o maior pólo tal que $t \leq q^3 + q^2 - q - 2 - r$.

```
#include<stdio.h>
#include<stdlib.h>

int main()
{
int q, r, d, a, b, rr, t, v = 0;
printf("Welcome to Program about Minimum Distance of Hermitian Codes. \n\n");
printf("Write a value for q (a power of p prime)
for Hermitian curve (not generalized): ");
scanf("%d", &q);
```

```
printf("Write a value for r(integer), parameter for the code C(r): ");
scanf("%d", &r);

if( (0 <= r) && (r < q*q*q - q*q) )
{ d = q*q*q - r;      printf("d = %d\n", d); }

else if( (q*q*q - q*q <= r) && (r < q*q*q) )
{
a = 0;
while( a < q )
{
b = 0;
while( b < q )
{
if( r == q*q*q - q*q + a*q + b ){ v = 1; break; }
b++;
}
if( v ) break;
a++;
}

if( a < b ) d = q*q*q - r;
else d = q*q*q - r + b;
printf("d = %d\n", d);
}
```

```
else if( (r >= q*q*q) && ( r <= q*q*q + q*q - q - 2) )
{
v = 0;

for(a = 0; a < q; a++)
{
b = 0;
while( b <= a )
{
t = a*q + b;
rr = q*q*q + q*q - q - 2 - t;
if( (rr > 0) && ( rr <= r) ){ v = 1; break; }
b++;
}
if( v ) break;
}

if( v ) printf("t = %d\n", t);
else printf("t nao pode ser definido.\n");

if( a == b ) d = a+2;
else d = a + 1;
printf("d = %d\n", d);
}
```

```
   else if ((r > q*q*q - q*q -q - 2))
{
         d=1;    printf("d = %d\n", d);
}

else{ d = 0; printf("d = %d\n", d); }

printf("s = (%d^3 + %d^2 - %d - 2)/2 = %f\n\n", q, q, q,
(float)((q*q*q + q*q - q - 2)/2));
    printf("s is the value for which the code is self-dual
and d is the minimum distance for C(r)!.\n\n");
    printf("t is the biggest polo number,
for t<= dual dimension. \n\n");
    printf("my email: moisesceni@oi.com.br \n\n");
    printf("THANK YOU FOR YOUR BUSINESS. \n\n");

system("PAUSE");
return 0;
}
```