Universidade Estadual de Campinas
Instituto de Matemática Estatística e Computação Científica
Departamento de Matemática

Funções Ordens Fracas e a Distância Mínima dos Códigos Geométricos de Goppa

Ercílio Carvalho da Silva
Doutorado em Matemática - Campinas - SP

Orientador: Prof. Dr. Fernando Eduardo Torres Orihuela

Funções Ordens Fracas e a Distância Mínima dos Códigos Geométricos de Goppa

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Ercílio Carvalho da Silva** e aprovada pela comissão julgadora.

Campinas, 30 de julho de 2004.

.....

Prof. Dr. Fernando Eduardo Torres Orihuela

(Orientador)

Banca Examinadora:

1. Prof. Dr. Fernando Eduardo Torres Orihuela
2. Prof. Dr. Cícero Fernandes de Carvalho
3. Prof. Dr. Daniel Levcovitz
4. Prof. Dr. Reginaldo Palazzo
5. Prof. Dr. José Plínio de Oliveira Santos
6. Prof. Dr. Paulo Roberto Brumatti

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

A Deus

"Senhor, se hoje percorro este caminho é porque vós o trilhares para mim;
Me formastes desde o ventre de minha mãe e,
me designastes ser um instrumento em tuas mãos;
Me destes sabedoria para aprender e discernir;
coragem para lutar e, perseverança para vencer...
Obrigado Senhor, por ser o que sou e, por hoje chegar onde estou!"

Aos meus Pais

Erci Brandão da Silva e Maria Mercedes Carvalho

"De vocês recebi o dom mais precioso do universo: A vida.
Já por isso seria infinitamente grato, mas vocês não se contentaram em presentear-me
apenas com ela: revestiram minha existência de amor, carinho e dedicação, cultivaram na criação todos os valores.
Abriram as portas do meu futuro, iluminando o meu caminho com a luz mais brilhante que puderam encontrar: o estudo.
Trabalharam dobrado, sacrificando seus sonhos em favor dos meus e não foram apenas pais,
mas amigos e companheiros, mesmo nas horas em que meus ideais pareciam distantes e inatingíveis.
Divido, pois, com vocês, os méritos desta conquista, porque ela lhes pertence, ela é tão de vocês quanto minha.
Obrigado, meus pais, por tudo que fizeram e fazem por mim sem que ao menos eu saiba.
Obrigado pelo sonho que realizo.
E, sobretudo, obrigado pela lição de amor que me ensinaram durante toda a vida.
Tomara Deus que eu possa transmití-la no exercício de minha profissão."

À minha Esposa

Ilma Aparecida Marques Silva

"Aquela que deu um novo sentido à minha vida!
Nada melhor do que um sonho para criar um futuro!
Obrigado, eternamente, por tudo!"

"Uma grande descoberta resolve um grande problema,
mas há sempre uma pitada de descoberta na resolução de qualquer problema.
O problema pode ser modesto,
mas se ele desafiar a curiosidade e puser em jogo as faculdades inventivas,
quem o resolver por seus próprios meios,
experimentará a tensão e gozará o triunfo da descoberta.
Experiências tais, numa idade susceptível,
poderão gerar o gosto pelo trabalho mental e deixar,
por toda vida,
a sua marca na mente e no caráter."

Agradecimentos

Agradeço:

Em especial, ao meu orientador Prof. Dr. Fernando Torres, pela excelente orientação, paciência, atenção, e valiosos ensinamentos proporcionados durante a realização deste trabalho.

Ao professor Cícero Carvalho, pelo constante apoio e incentivo para seguir sempre em frente na conquista de cada etapa e também pelas valiosas discussões, sugestões, e ainda por sua amizade, paciência e atenção.

Aos professores da banca examinadora: Prof. Dr. Cícero Fernandes de Carvalho, Prof. Dr. Daniel Levcovitz, Prof. Dr. Reginaldo Palazzo, Prof. Dr. José Plínio de Oliveira Santos, Prof. Dr. Paulo Roberto Brumatti.

Ao meu grande e eterno mestre, prof. Luiz Alberto Duran Salomão.

Aos meus tios Astramiro e Cecília, que me acolheram no início dos meus estudos.

Aos meus queridos irmãos Emerson, Eliezer, Evandro, Tânia, Vânia e Ercília.

Aos funcionários da Unicamp, em especial Cidinha, Ednaldo e Tânia, pela contribuição e disponibilidade.

Aos colegas Amauri, Mércio, Paulo César, Cristiane, Daniela e Marcela, pela amizade.

À Capes, pelo apoio financeiro.

À Universidade Federal de Uberlândia e a Faculdade de Matemática, pelo respaldo financeiro e apoio irrestrito durante todo o período do doutorado.

Resumo

Como uma generalização do conceito de Função Ordem, introduzido por T. Høholdt, J. H. van Lint e R. Pellikaan, nesta tese apresentamos a noção de **Função Ordem Fraca** com o objetivo de obter construções alternativas dos códigos geométricos de Goppa.

Os códigos obtidos por Høholdt, van Lint e Pellikaan estão tipicamente associados aos códigos pontuais de Goppa; já os nossos, correspondem aos códigos bi-pontuais. Em vários destes casos, a cota inferior para a distância mínima do código é melhor que qualquer cota correspondente conhecida na literatura.

Abstract

Hoholdt, van Lint and Pellikaan introduced the order functions and apply them to the construction of good codes. For the case of curves, their theory fits very well for the so-called one-point Goppa codes. In this work we define the notion of "weak order function"and show that we can construct good two-point Goppa codes.

Sumário

Notações

CGG: Código de Goppa Geométrico;

$\mathcal{X}$: curva projetiva, não singular e absolutamente irredutível;

K: corpo;

$K(\mathcal{X})$: corpo de funções da curva $\mathcal{X}$;

$C_\Omega(D, G)$: código geométrico de Goppa associado aos divisores D e G;

$\mathbf{F}_q$: corpo finito com q elementos;

$\mathcal{X}(\mathbf{F}_q)$: quantidade de pontos $\mathbf{F}_q$-racionais da curva $\mathcal{X}$;

$\Omega(G - D)$: espaço das diferenciais w sobre $\mathcal{X}$ tal que $\mathrm{div}(w) + (G - D) \succeq 0$;

$\mathrm{res}_P(w)$: resíduo da diferencial w sobre $\mathcal{X}$ no ponto P;

$\mathrm{div}(f)$: divisor da função $f \in K(\mathcal{X})$;

$\mathrm{div}_\infty(f)$: divisor dos pólos da função $f \in K(\mathcal{X})$;

$d(l)$: cota ordem;

d_G: cota de Goppa;

$\mathbf{N}$: conjunto dos inteiros positivos;

$\mathbf{N}_0$: conjunto dos inteiros não negativos;

$\mathbf{R}$: K-álgebra (anel comutativo com unidade contendo K);

$H(Q_1, \cdots, Q_m)$: semigrupo de Weierstrass associado aos pontos $Q_1, \cdots, Q_m$;

$G(Q_1, \cdots, Q_m)$: conjunto das lacunas de Weierstrass nos pontos $Q_1, \cdots, Q_m$;

$G_0(Q_1, \cdots, Q_m)$: conjunto das lacunas puras de Weierstrass nos pontos $Q_1, \cdots, Q_m$;

$\mathcal{L}(G)$: espaço das funções $f \in K(\mathcal{X})$ tal que $\mathrm{div}(f) + G \succeq 0$, unido com o 0;

$\Gamma(P, Q)$: relação entre as lacunas de P e lacunas de Q;

$\deg(G)$: grau do divisor G;

$R(P)$: anel das funções que têm pólos, possivelmente, em P;

$R(P, Q)$: anel das funções que têm pólos, possivelmente, em P e|ou Q;

$R(Q_1, \cdots, Q_m)$: anel das funções que têm pólos, possivelmente, nos pontos $Q_1, \cdots, Q_m$;

v_P: valorização no ponto P;

$\omega(y)$: peso da palavra y;

$d(l, m)$: cota ordem fraca.

Introdução

A Teoria dos Códigos Corretores de Erros foi fundada pelo matemático C. E. Shannon, do Laboratório Bell, num trabalho publicado em 1948. Inicialmente, os maiores interessados em Teoria dos Códigos foram os matemáticos que a desenvolveram consideravelmente nas décadas de 50 e 60. A partir da década de 70, com as pesquisas espaciais e a popularização dos computadores, essa teoria começou a interessar também aos engenheiros. Hoje em dia, os códigos corretores de erros são utilizados sempre que se deseja transmitir ou armazenar dados. São exemplos disso todas as comunicações via satélite, as comunicações internas de um computador, o armazenamento de dados em fitas ou disquetes magnéticos, ou o armazenamento ótico de dados.

A classe de códigos mais utilizada na prática é a classe dos **Códigos Lineares**. Um código linear C é um subespaço vetorial de $\mathbf{F}_q^n$ e $d(a,b) = \#\{i : a_i \neq b_i\}$ é a distância entre os elementos (palavras) a e b de C. Tal código é caracterizado pelos parâmetros $[n,k,d]$ onde n é o seu comprimento, k é a sua dimensão e $d = Min\{d(a,b) : a,b \in C \ \wedge \ a \neq b\}$ é a sua **distância mínima**. Este último parâmetro também é conhecido como o **peso do código** C, denotado por $\omega(C)$, onde $\omega(C) = Min\{\omega(c) : c \in C\backslash\{0\}\}$ e $\omega(c) = \#\{i : c \in C \ \wedge \ c_i \neq 0\}$, pois $d = \omega(C)$.

Os **Códigos Geométricos de Goppa** (ou simplesmente, CGG) formam uma subclasse especial na classe dos códigos lineares. Desde sua construção [7], [9], [8], resultados relevantes na Teoria dos Códigos Lineares foram provados; como por exemplo, o de Tsfasman-Vladut-Zink sobre a construção de uma sequência de códigos que excedem a cota de Gilbert-Varshamov [18], [17].

Um código geométrico de Goppa C está determinado pelos seguintes dados:

- Uma curva base $\mathcal{X}$ projetiva, absolutamente irredutível e não singular definida sobre $\mathbf{F}_q$ (ou simplesmente, uma curva sobre $\mathbf{F}_q$);
- Dois divisores $\mathbf{F}_q$-racionais sobre $\mathcal{X}$, $D = P_1 + \cdots + P_n$ e G tais que seus suportes não se interceptam, $P_i \neq P_j$ para $i \neq j$ e $P_i \in \mathcal{X}(\mathbf{F}_q)$ para todo i.

Logo,

$$C = C_\Omega(D, G) := \{(\mathrm{res}_{P_1}(w), \cdots, \mathrm{res}_{P_n}(w)) \in \mathbf{F}_q^n : w \in \Omega(G - D)\},$$

onde $\Omega(G - D)$ é o espaço das diferenciais sobre $\mathcal{X}$ tal que $w = 0$ ou $\mathrm{div}(w) \succeq G - D$. Na Teoria dos Códigos Lineares, a distância mínima tem papel relevante, pois é dela que se obtém a capacidade de detecção e correção de erros. Em geral, não se conhece este valor exato. Assim, a busca por cotas inferiores para este valor passou a ser fonte de pesquisa. No caso dos CGG, um dos principais aspectos é que sua distância mínima é limitada inferiormente pela chamada **cota de Goppa** d_G; isto é,

$$d \geq d_G := \deg(G) - (2g - 2), \tag{1}$$

onde $\deg(G)$ denota o grau do divisor G.

Neste trabalho, estamos interessados na possibilidade de melhorar a cota de Goppa, equação (1). Se C é pontual, isto é, $G = lQ$, Goppa observou que uma seleção adequada de l com respeito ao semigrupo de Weierstrass em Q pode implicar $d \geq d_G + 1$ [8, p. 139-141]; este fato foi generalizado por Garcia e Lax [6]. No caso em que C é "bi-pontual", isto é, $G = a_1Q_1 + a_2Q_2$, Homma-Kim [12] e Matthews [15] provaram que $d \geq d_G + 2$ e $d \geq d_G + 3$, respectivamente, sempre que (a_1, a_2) seja selecionado adequadamente com respeito ao semigrupo de Weierstrass em (Q_1, Q_2). As curvas básicas utilizadas neste caso foram as Hiperelípticas, as Hermitianas (e alguns de seus quocientes) e as de Suzuki. De forma natural, C. Carvalho e F. Torres [4] generalizaram o resultado de Homma-Kim para m pontos, de modo que $d \geq d_G + m$.

Em [10], Høholdt, van Lint e Pellikaan propuseram um método alternativo ao de Goppa, sobre construção de códigos lineares, utilizando rudimentos de Álgebra Linear em vez de conhecimentos de Curvas Algébricas. Nesta situação, a curva $\mathcal{X}$ foi substituída por uma $\mathbf{F}_q$-álgebra $\mathbf{R}$ e o espaço $\Omega(G - D)$ foi substituído pela noção de **Função Ordem**. Em outras palavras, estes autores propuseram uma generalização dos códigos geométricos de Goppa pontuais, chamando-os de **Códigos Avaliados**. A construção de tais códigos é feita via um morfismo $\varphi : \mathbf{R} \to \mathbf{F}_q^n$ de $\mathbf{F}_q$-álgebras, onde n é o comprimento do código. Mais precisamente, um código avaliado é o dual da imagem de um certo subespaço de $\mathbf{R}$ por φ. Tal subespaço é gerado pelos elementos de uma $\mathbf{F}_q$-base de $\mathbf{R}$ e esta, por sua vez, é determinada por uma função ordem sobre $\mathbf{R}$. Assim como na construção feita por Goppa, existe uma cota inferior para a distância mínima destes códigos [10, p. 917], a qual é uma função numérica que depende da base usada. Em vários casos, a cota destes autores é melhor do que a cota de Goppa (Exemplo 1.26 e Exemplo 1.27)

Quando a função ordem é uma **Função Peso**, Matsumoto [16] mostrou que uma K-álgebra $\mathbf{R}$ (K corpo) munida de uma função peso ρ é nada mais do que o anel de

coordenadas de uma curva $\mathcal{X}$ com certo ponto distinguido P, onde $-\rho$ é igual a valorização em P; portanto, sob o ponto de vista de códigos, neste caso estamos lidando com os códigos geométricos de Goppa pontuais. A propriedade que distingue P é dada em termos de $\mathbf{R}$; isto é, $\mathbf{R} = R(P)$ é a interseção dos anéis de valorizações $\mathcal{O}_S$ do corpo de funções de $\mathcal{X}$ com $S \neq P$.

Generalizando o conceito de função ordem, no Capítulo 2 apresentamos a noção de **Função Ordem Fraca** e estudamos algumas de suas propriedades dentre as quais destacamos: (1) Caracterização de funções ordens em termos de funções ordens fracas (Lema 2.12); (2) Caracterização de uma K-álgebra em termos de uma função ordem fraca (Teorema 2.17); (3) Construção de funções ordens fracas sobre K-álgebras (Teorema 2.18); (4) Existência de bases sobre K-álgebras (Teorema 2.20). A justificativa para a palavra FRACA que aparece em nossa definição se deve ao enfraquecimento que fazemos nos Axiomas (4) e (5) da definição de função ordem (Definição 1.4). Na verdade, restringimos a validade destes axiomas a um subconjunto específico da K-álgebra, das **não-unidades**, que depende fundamentalmente da função em questão. No entanto, esta restrição torna nossa definição mais abrangente.

No Capítulo 3, discutimos cotas inferiores para códigos geométricos de Goppa bipontuais. Para isto, se $\mathcal{X}$ é uma curva, inicialmente consideramos uma situação análoga ao caso pontual; a saber, consideramos a $\mathbf{F}_q$-álgebra $\mathbf{R} = R(P, Q)$, interseção dos anéis de valorizações $\mathcal{O}_S$ do corpo de funções da curva $\mathcal{X}$ com $S \neq P$ e $S \neq Q$, e as funções ordens fracas

$$\rho(f) = \begin{cases} -\infty, & \text{se} \quad f = 0 \\ 0, & \text{se} \quad v_P(f) \geq 0 \text{ e } f \neq 0 \\ -v_P(f), & \text{se} \quad v_P(f) < 0 \end{cases}$$

e

$$\sigma(f) = \begin{cases} -\infty, & \text{se} \quad f = 0 \\ 0, & \text{se} \quad v_Q(f) \geq 0 \text{ e } f \neq 0 \\ -v_Q(f), & \text{se} \quad v_Q(f) < 0. \end{cases}$$

Em seguida, usando ρ e σ, geramos uma $\mathbf{F}_q$-base especial de $R(P, Q)$. Munidos com esta base e um morfismo φ de $R(P, Q)$ em $\mathbf{F}_q^n$, construimos códigos avaliados e exibimos uma cota inferior para os mesmos, cujo cálculo depende fortemente das propriedades dos elementos da base. Em linhas gerais, se $\{f_0, f_1, \cdots\} \cup \{g_1, g_2, \cdots\}$ é a tal base, fixando os elementos $g_1, \cdots, g_a$, um código avaliado é o dual da imagem do subespaço vetorial $\langle f_0, \cdots, f_l \rangle \oplus \langle g_1, \cdots, g_a \rangle$ pela aplicação φ. Finalmente, provamos um resultado (Teorema 3.9) que nos fornece uma cota maior ou igual à cota estabelecida por Goppa e exibimos alguns exemplos onde a mesma supera a de Goppa.

Pergunta: Existe uma caracterização de K-álgebras munidas com funções pesos fracos? (cf. [16])

Capítulo 1

Preliminares

O objetivo deste capítulo é familiarizar o leitor sobre alguns resultados com respeito aos semigrupos de Weierstrass e sua ligação com CGG, assim como fatos básicos do trabalho de Høholdt, van Lint e Pellikaan em [10]. Neste capítulo, K denotará um corpo.

1.1 Semigrupos de Weierstrass e Códigos Geométricos de Goppa

Seja $\mathcal{X}$ uma curva sobre K de gênero g, K finito, e sejam $Q_1, \cdots, Q_m$ pontos K-racionais de $\mathcal{X}$, distintos dois a dois. O conjunto

$$\begin{aligned} H &= H(Q_1, \cdots, Q_m) \\ &:= \{\vec{a} := (a_1, \cdots, a_m) \in \mathbf{N}_0^m : \exists f \in K(\mathcal{X}) \text{ com } \mathrm{div}_\infty(f) = a_1Q_1 + \cdots + a_mQ_m\}, \end{aligned}$$

é um subsemigrupo de $(\mathbf{N}_0^m, +)$ e é chamado de **semigrupo de Weierstrass** de $\mathcal{X}$ em $Q_1, \cdots, Q_m$. Os elementos do complemento $G = G(Q_1, \cdots, Q_m)$ de H em $\mathbf{N}_0^m$ são chamados de **lacunas de Weierstrass** de $\mathcal{X}$ em $Q_1, \cdots, Q_m$. Tais conjuntos tem as seguintes caracterizações (veja [4]):

- $\vec{a} \in H \Leftrightarrow \ell(\vec{a}) = \ell(\vec{a} - \vec{e}_i) + 1$ para todo $i = 1, \ldots, m$;
- $\vec{a} \in G \Leftrightarrow$ existe $i \in \{1, \ldots, m\}$ tal que $\ell(\vec{a}) = \ell(\vec{a} - \vec{e}_i)$;

onde $\#K \geq m$, $\vec{e}_i$ denota o vetor em $\mathbf{N}_0^m$ com 1 na i-ésima posição e 0 nas demais, $\ell(\vec{a}) = \dim_K \mathcal{L}(\vec{a})$ e $\mathcal{L}(\vec{a}) = \mathcal{L}(a_1Q_1 + \cdots + a_mQ_m) = \{f \in K(\mathcal{X})^* : (a_1Q_1 + \cdots + a_mQ_m) + \mathrm{div}(f) \succeq 0\} \cup \{0\}$. Para aplição em CGG, há interesse especial nas assim chamadas **lacunas de Weierstrass puras**, que são aquelas lacunas $\vec{a}$ tais que $\ell(\vec{a}) = \ell(\vec{a} - \vec{e}_i)$, para todo $i = 1, \cdots, m$. Tal conjunto é denotado por $G_0(Q_1, \cdots, Q_m)$.

O caso $m = 1$ é o semigrupo clássico e a noção para $m \geq 2$ foi introduzida por Arbarello, Cornalba, Griffiths a Harris [2, p. 365]. Deste semigrupo, espera-se obter informações relevantes de $\mathcal{X}$. O caso $m = 2$ foi extensivamente estudado por Homma e Kim [11], [12], [13]. Eles mostraram a existência de um conjunto mínimo $\Gamma(P, Q)$ gerador de $H(P, Q)$. Para descrever $\Gamma(P, Q)$, sejam $G(P) = \{\ell_1 < \cdots < \ell_g\}$ e $G(Q) = \{\ell'_1 < \cdots < \ell'_g\}$. Para cada lacuna ℓ_i em P, o inteiro $Min\{a \in \mathbf{N}_0 : (\ell_i, a) \in H(P, Q)\}$ é uma lacuna em Q, digamos $\ell'_{\tau(i)}$, e esta correspondência dá uma bijeção entre $G(P)$ e $G(Q)$ [13, Lema 2.6]. Assim, τ é uma permutação no conjunto $\{1, \ldots, g\}$ e consequentemente,

$$\Gamma(P, Q) = \{(\ell_1, \ell'_{\tau(1)}), \ldots, (\ell_g, \ell'_{\tau(g)})\}.$$

No caso em que $m > 2$, há um resultado análogo [4, Cor. 2.11]. Nesta situação, a descrição de $\Gamma(Q_1, \ldots, Q_m)$ é mais complicada. Um critério que determina o subconjunto mínimo de $H(Q_1, \ldots, Q_m)$ que o gera, foi obtido por Matthews [14]. Outros resultados foram obtidos por Ballico e Kim [3], Delgado [5], Carvalho e Torres [4].

Agora, considere C um CGG com $G = a_1Q_1 + \cdots + a_mQ_m$. O problema em consideração é obter um limitante inferior para $d(C)$ maior do que d_G. Um caminho que nos permite dar uma resposta a esta questão, está ligado ao conceito de lacunas de Weierstrass. Para ilustrar, brevemente, tal ligação, considere as duas situações particulares a seguir. Primeiro, considere $G = 3Q_1$ e $C = C_\Omega(D, 3Q_1)$. Assim, já sabemos que $d(C) > d_G = 3 + (2g - 2)$. Suponha que $\mathcal{L}(3Q_1) = \mathcal{L}(4Q_1)$; isto é, $4 \in G(Q_1)$. Assim, $\Omega(3Q_1 - D) = \Omega(4Q_1 - D)$ e, portanto, $C = C_\Omega(D, 3Q_1) = C_\Omega(D, 4Q_1)$. Logo, $d(C) > 4 + (2g - 2) = d_G + 1$. Agora, considere $G = 3Q_1 + 5Q_2$ e $C = C_\Omega(D, G)$. Assim, $d(C) > d_G = 8 + (2g - 2)$. Suponha que $\mathcal{L}(G) = \mathcal{L}(4Q_1 + 6Q_2)$. Pelo mesmo raciocínio da situação anterior, $C = C_\Omega(D, G) = C_\Omega(D, 4Q_1 + 6Q_2)$. Logo, $d(C) > 10 + (2g - 2) = d_G + 2$.

Agora, citamos alguns resultados que melhoram a cota de Goppa. Para isto, sejam $\mathcal{X}$ uma curva sobre $\mathbf{F}_q$ de gênero g, $D = P_1 + \cdots + P_n$ com $P_1, \ldots, P_n$ pontos $\mathbf{F}_q$-racionais, distintos dois a dois, G um divisor sobre $\mathcal{X}$ cujo suporte $\{Q_1, \ldots, Q_m\}$ é disjunto do suporte de D e $C = C_\Omega(D, G)$. Suponha também que $Q_1, \ldots, Q_m$ são pontos $\mathbf{F}_q$-racionais.

Teorema 1.1 *([15, Teorema 2.1]) Assuma que $(a_1, a_2) \in G(Q_1, Q_2)$ com $a_1 \geq 1$ e $\ell(a_1Q_1 + a_2Q_2) = \ell((a_1 - 1)Q_1 + a_2Q_2)$. Suponha que $(n_1, n_2 - t - 1) \in G(Q_1, Q_2)$ para todo $t = 0, \ldots, Min\{n_2 - 1, 2g - 1 - (a_1 + a_2)\}$. Seja $G = (a_1 + n_1 - 1)Q_1 + (a_2 + n_2 - 1)Q_2$. Se a dimensão de C é positiva, então*

$$d(C) > \deg(G) - 2g + 3 = d_G + 1.$$

Teorema 1.2 *([12, Teorema 3.3]) Sejam* $(a_1, a_2), (n_1, n_2) \in \mathbf{N}^2$ *e coloque* $t_i := n_i - a_i$ *para* $i = 1, 2$. *Assuma que* $t_i \geq 0$ *para* $i = 1, 2$, *e*

$$\{(p_1, p_2) : a_1 \leq p_1 \leq n_1,\ a_2 \leq p_2 \leq n_2\} \subseteq G_0(Q_1, Q_2).$$

Se $G = (a_1 + n_1 - 1)Q_1 + (a_2 + n_2 - 1)Q_2$ *e* $C \neq 0$, *então*

$$d(C) > \deg(G) - (2g - 2) + t_1 + t_2 + 2 = d_G + t_1 + t_2 + 2.$$

O próximo resultado generaliza o Teorema 1.2.

Teorema 1.3 *([4, Teorema 3.4]) Suponha que* $a_i \leq n_i$ *para todo* $i = 1, \ldots, m$, *e que cada* m*-upla* $(p_1, \ldots, p_m) \in G_0(Q_1, \ldots, Q_m)$, *com* $a_i \leq p_i \leq n_i$ *para todo* $i = 1, \ldots, m$. *Seja* $G = \sum_{i=1}^{m}(a_i + n_i - 1)Q_i$. *Se* $C \neq 0$, *então*

$$d(C) > \deg(G) - (2g - 2) + m + \sum_{i=1}^{m}(n_i - a_i) = d_G + m + \sum_{i=1}^{m}(n_i - a_i).$$

Nestes resultados (Teoremas 1.1 1.2, 1.3) foi utilizado o conceito de lacunas de Weierstrass na determinação de cotas melhores do que a cota de Goppa. No que segue, o caminho escolhido para obtenção de cotas melhores do que a cota de Goppa é outro, o caminho das **funções ordens**.

1.2 Códigos Geométricos de Goppa Segundo Høholdt, van Lint e Pellikaan

Nesta seção revisaremos o material contido em [10]. Como já foi mencionado na introdução, é possível construir códigos sem ter que fazer uso da Teoria de Curvas Algébricas. Para esse fim, será introduzido o conceito de função ordem (peso).

No que segue, $\mathbf{R}$ denotará uma K-álgebra, isto é, $\mathbf{R}$ é um anel comutativo com unidade contendo K.

1.2.1 Funções ordens

Definição 1.4 *Uma função* $\rho : \mathbf{R} \to \mathbf{N}_0 \cup \{-\infty\}$ *é chamada uma* **função ordem** *sobre* $\mathbf{R}$ *se as seguintes propriedades são satisfeitas. Sejam* $f, g, h \in \mathbf{R}$.

(1) $\rho(f) = -\infty$ *se, e somente se,* $f = 0$;

(2) *Para* $\lambda \in K^*$, $\rho(\lambda f) = \rho(f)$;

(3) $\rho(f+g) \leq \max\{\rho(f), \rho(g)\}$, *e a igualdade vale sempre que* $\rho(f) \neq \rho(g)$;

(4) *Se* $\rho(f) < \rho(g)$ *e* $h \neq 0$, *então* $\rho(fh) < \rho(gh)$;

(5) *Se* $\rho(f) = \rho(g) \neq 0$, *então existe* $\lambda \in K^*$ *tal que* $\rho(f - \lambda g) < \rho(g)$.

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

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

Aqui, $-\infty + n = -\infty$ para todo $n \in \mathbf{N}_0 \cup \{-\infty\}$.

Exemplo 1.5 *Um exemplo de uma* K*-álgebra* $\mathbf{R}$ *com uma função peso* ρ *é obtida tomando* $\mathbf{R} = K[X]$ *e fazendo* $\rho(f) = grau(f)$ *para* $f \in \mathbf{R}$.

Exemplo 1.6 *Seja* $K(\mathcal{X})$ *o corpo de funções de uma curva* $\mathcal{X}$ *sobre* K. *Seja* P *um ponto* K*-racional. Seja* $\mathbf{R} := R(P)$ *a* K*-álgebra dada pela interseção dos anéis locais* $\mathcal{O}_S$ *de* $K(\mathcal{X})$, *nos pontos* S, *com* $S \neq P$. *Seja* v_P *a valorização em* P. *Portanto,* $v_P(f) \leq 0$ *para todo* f *não nulo em* $\mathbf{R}$. *Defina* $\rho(f) := -v_P(f)$ *para* $f \in \mathbf{R}$. *É consequência imediata das propriedades de valorização discreta que* ρ *é uma função peso.*

Observação 1.7 *No Exemplo 1.6 acima temos que* $\rho(\mathbf{R}^*) = H(P)$ *onde* $\mathbf{R}^* = \mathbf{R} - \{0\}$ *e* $H(P)$ *é o semigrupo de Weierstrass no ponto* P.

O resultado abaixo estabelece propriedades de uma função ordem qualquer.

Lema 1.8 *Seja* ρ *uma função ordem sobre* $\mathbf{R}$. *Então,*
(1) Se $\rho(f) = \rho(g)$ *então* $\rho(fh) = \rho(gh)$ *para todo* $h \in \mathbf{R}$.
(2) Se $f \in \mathbf{R}$ *e* $f \neq 0$ *então* $\rho(1) \leq \rho(f)$.
(3) $K = \{f \in \mathbf{R} : \rho(f) \leq \rho(1)\}$.
(4) Se $\rho(f) = \rho(g)$ *então existe um único* $\lambda \in K^*$ *tal que* $\rho(f - \lambda g) < \rho(g)$.

Proposição 1.9 *Se existe uma função ordem* ρ *sobre* $\mathbf{R}$, *então* $\mathbf{R}$ *é um domínio de integridade.*

Agora daremos um contra-exemplo para a recíproca da Proposição 1.9.

Exemplo 1.10 *A K-álgebra $\mathbf{R} = K[X,Y]/(XY-1)$ é um domínio de integridade. Vamos mostrar que não existe função ordem sobre $\mathbf{R}$. Denote x para a classe $X+(XY-1)$ e y para a classe $Y+(XY-1)$. Logo, $\mathbf{R} = K[x]+K[y]$. É claro que, $x \neq 0$ e $y \neq 0$. Se ρ é uma função ordem sobre $\mathbf{R}$ então $\rho(1) \leq \rho(x)$ e assim $\rho(y) \leq \rho(xy) = \rho(1)$. Logo, $\rho(y) = \rho(1)$ e da mesma forma obtemos que $\rho(x) = \rho(1)$. Portanto, $\rho(f) \leq \rho(1)$ para todo $f \in \mathbf{R}$. Isto nos mostra que $\mathbf{R} = K$, por (3) do Lema 1.8. Isto é uma contradição, pois $x \notin K$.*

Agora veremos que a existência de funções ordens sobre $\mathbf{R}$ está ligada à existência de certas K-bases de $\mathbf{R}$. O próximo teorema nos mostra que se existe uma função ordem sobre uma K-álgebra $\mathbf{R}$ então existe uma K-base de $\mathbf{R}$, $\mathbf{R}$ visto como K-espaço vetorial, com certas propriedades. Tal base nos permite construir os chamados Códigos Avaliados e suas respectivas propriedades serão de fundamental importância para a determinação de uma cota inferior para a distância mínima dos mesmos.

Teorema 1.11 *Seja $\mathbf{R}$ uma K-álgebra com função ordem ρ. Assuma que $\mathbf{R} \neq K$.*
(1) Então existe uma base $\{f_i : i \in \mathbf{N}\}$ de $\mathbf{R}$ sobre K tal que $\rho(f_i) < \rho(f_{i+1})$ para todo i.
(2) Se $f \in \mathbf{R}$ e $f = \lambda_1 f_1 + \cdots + \lambda_i f_i$ onde $\lambda_1, \cdots \lambda_i \in K$ e $\lambda_i \neq 0$ então $\rho(f) = \rho(f_i)$.
(3) Seja $l(i,j) := l$ tal que $\rho(f_i f_j) = \rho(f_l)$. Assim, $l(i,j) < l(i+1,j)$ para todo i e j.
(4) Seja $\rho_i := \rho(f_i)$. Se ρ é função peso então $\rho_{l(i,j)} = \rho_i + \rho_j$.

O próximo resultado nos fornece um caminho a ser seguido quando buscamos exemplos de funções ordens sobre uma K-álgebra dada qualquer. O Exemplo 1.10 nos mostra que nem sempre isso é possível.

Teorema 1.12 *Seja $\mathbf{R}$ uma K-álgebra. Seja $\{f_i : i \in \mathbf{N}\}$ uma K-base de $\mathbf{R}$ como espaço vetorial com $f_1 = 1$. Seja L_i o espaço vetorial gerado por $f_1, \cdots, f_i$. Seja $l(i,j)$ o menor inteiro l tal que $f_i f_j \in L_l$. Suponha que $l(i,j) < l(i+1,j)$ para todo $i,j \in \mathbf{N}$. Seja $(\rho_i : i \in \mathbf{N})$ uma sequência estritamente crescente de inteiros não negativos. Defina $\rho(0) = -\infty$ e $\rho(f) = \rho_i$ se i é o menor inteiro tal que $f \in L_i$. Então ρ é uma função ordem sobre $\mathbf{R}$.*

O exemplo a seguir ilustra o Teorema 1.12.

Exemplo 1.13 *Considere a ordem lexicográfica graduada $\prec$ no conjunto dos monômios $\{X^a Y^b : a,b \in \mathbf{N}_0\}$, isto é, $X^a Y^b \prec X^c Y^d$ se, e somente se, $a+b < c+d$ ou $a+b = c+d$ e $(a,b) \prec_L (c,d)$ onde $\prec_L$ é a ordem lexicográfica. Sejam $f_1, f_2, \cdots$ a enumeração do conjunto dos monômios tal que $f_i \prec f_{i+1}$, para todo $i \in \mathbf{N}$. Abaixo apresentamos*

duas matrizes. Uma corresponde ao conjunto dos monômios e a outra corresponde aos respectivos índices, segundo a enumeração acima.

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
Y^6	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\ldots$	22	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\ldots$
Y^5	XY^5	$\cdot$	$\cdot$	$\cdot$	$\ldots$	16	23	$\cdot$	$\cdot$	$\cdot$	$\ldots$
Y^4	XY^4	X^2Y^4	$\cdot$	$\cdot$	$\ldots$	11	17	24	$\cdot$	$\cdot$	$\ldots$
Y^3	XY^3	X^2Y^3	X^3Y^3	$\cdot$	$\ldots$	7	12	18	25	$\cdot$	$\ldots$
Y^2	XY^2	X^2Y^2	X^3Y^2	$\cdot$	$\ldots$	4	8	13	19	$\cdot$	$\ldots$
Y	XY	X^2Y	X^3Y	X^4Y	$\ldots$	2	5	9	14	20	$\ldots$
1	X	X^2	X^3	X^4	X^5	1	3	6	10	15	21

Seja $\mathbf{R} := K[X,Y]$ *e* $f = \lambda_1 f_1 + \cdots + \lambda_n f_n$ *em* $\mathbf{R}$. *Defina* $\rho(0) = -\infty$ *e* $\rho(f) = n-1$ *se* $\lambda_n \neq 0$. *É fácil de ver que* ρ *é função ordem sobre* $\mathbf{R}$. *Neste caso,* $f_8 = XY^2$, $f_9 = X^2Y$ *e* $f_8 f_9 = X^3Y^3 = f_{25}$. *Logo,* $l(8,9) = 25$.

Para generalizar $\prec$ *basta introduzir um "peso"nas variáveis* X *e* Y. *Por exemplo, se o "peso"de* X *é* 4 *e o "peso"de* Y *é* 5 *então* $X^aY^b \prec X^cY^d$ *se, e somente se,* $4a+5b < 4c+5d$ *ou* $4a+5b = 4c+5d$ *e* $(a,b) \prec_L (c,d)$. *No primeiro caso os "pesos"de* X *e* Y *são iguais a* 1.

O próximo resultado trata da existência de funções pesos para uma classe específica de K-álgebras.

Proposição 1.14 *Seja* I *o ideal em* $K[X,Y]$ *gerado por um polinômio da forma* $X^aY^c + uY^{b+c} + G$ *com* $u \in K^*$, $G \in K[X,Y]$, $\deg_X(G) = d < a$, $\deg(G) < b+c$ *e* $mdc(a,b) = 1$. *Seja* $S = K[X,Y]/I$, $x = X + I$ *e* $y = Y + I$. *Seja* $\mathbf{R}$ *o espaço vetorial gerado por* $\{x^\alpha y^\beta : \alpha, \beta \in \mathbf{N}_0 \ \wedge \ \alpha < a \ \wedge \ c\alpha \leq (a-d)\beta\}$. *Então* $\mathbf{R}$ *é uma* K*-álgebra com função peso* ρ *tal que* $\rho(x) = b$ *e* $\rho(y) = a$.

Vejamos alguns exemplos que ilustram a Proposição 1.14

Exemplo 1.15 *Seja* $q = r^2$, *onde* r *é potência de um número primo. Considere a curva Hermitiana sobre* $\mathbf{F}_q$ *com equação afim*

$$X^{r+1} - Y^r - Y = 0.$$

Então esta equação é da forma $X^aY^c + uY^{b+c} + G = 0$, *como na Proposição 1.14, com* $a = r+1$, $b = r$, $c = d = 0$, $u = -1$ *e* $G = -Y$. *Considere o caso* $r = 4$. *Seja* $\mathbf{R}$ *a* $\mathbf{F}_{16}$*-álgebra dada por* $\mathbf{R} = \mathbf{F}_{16}[X,Y]/(X^5 - Y^4 - Y)$. $\mathbf{R}$ *tem*

$$\{x^\alpha y^\beta : \alpha < 5\}$$

como base. Então $\rho(x^\alpha y^\beta) = 4\alpha + 5\beta$ *dá uma função peso sobre* $\mathbf{R}$. *A sequência* $(f_l : l \in \mathbf{N})$ *é uma enumeração crescente da base, com relação aos seus pesos. Os primeiros termos e seus respectivos pesos são:*

1	x	y	x^2	xy	y^2	x^3	x^2y	xy^2	y^3	x^4	x^3y	x^2y^2	xy^3	y^4	x^4y	$\cdots$
0	4	5	8	9	10	12	13	14	15	16	17	18	19	20	21	$\cdots$.

Neste caso, $l(4,7) = 15$ pois $f_4 = x^2$, $f_7 = x^3$ e $f_4 f_7 = x^5 = y^4 + y = f_{15} + f_3$. Note também que $\rho_l = \rho(f_l) = l + 5$, para todo $l \geq 7$.

Exemplo 1.16 *A quártica de Klein sobre* $\mathbf{F}_8$ *com equação afim*

$$X^3Y + Y^3 + X = 0,$$

é da forma $X^aY^c + uY^{b+c} + G = 0$, *como na Proposição 1.14, com* $a = 3$, $b = 2$, $c = d = 1$, $u = 1$ *e* $G = X$. *Seja* $\mathbf{R}$ *a* F_8*-subálgebra de* $\mathbf{F}_8[X,Y]/(X^3Y + Y^3 + X)$ *gerada pelos elementos* $x^\alpha y^\beta$ *tais que* $\alpha < 3$ *e* $\alpha \leq 2\beta$. *Então* $\mathbf{R}$ *tem*

$$\{1\} \cup \{x^\alpha y^\beta : \alpha \leq 2 \ \wedge \ 1 \leq \beta\}$$

como base, com $\rho(1) = 0$ *e* $\rho(x^\alpha y^\beta) = 2\alpha + 3\beta$ *gerando uma função peso sobre* $\mathbf{R}$. *A sequência* $(f_l : l \in \mathbf{N})$ *é uma enumeração crescente da base, com relação aos seus pesos. Os primeiros termos e seus respectivos pesos são:*

1	y	xy	y^2	x^2y	xy^2	y^3	x^2y^2	xy^3	y^4	x^2y^3	$\cdots$
0	3	5	6	7	8	9	10	11	12	13	$\cdots$.

Neste caso, $l(3,5) = 10$ *pois* $f_3 = xy$, $f_5 = x^2y$ *e* $f_3 f_5 = x^3y^2 = -y^4 - xy = -f_{10} - f_3$. *Note também que* $\rho_l = \rho(f_l) = l + 2$, *para todo* $l \geq 3$.

1.2.2 Códigos avaliados e distância mínima dual

Seja ρ uma função ordem sobre $\mathbf{R}$ e $K = \mathbf{F}_q$. Apresentamos nesta subseção os Códigos Avaliados sobre $\mathbf{R}$ e exibimos uma cota para a distância mínima dos respectivos códigos duais.

O Teorema 1.11 nos mostra que existe $\{f_i : i \in \mathbf{N}\}$ base de $\mathbf{R}$ sobre $\mathbf{F}_q$ tal que $\rho(f_i) < \rho(f_{i+1})$ para todo $i \in \mathbf{N}$, e para todo $0 \neq f \in \mathbf{R}$ existe um $j \in \mathbf{N}$ com $\rho(f) = \rho(f_j)$. Seja L_l o espaço gerado por $f_1, \cdots, f_l$. Então, para todo $0 \neq f \in \mathbf{R}$ temos que $\rho(f) = \rho(f_l)$ se, e somente se, l é o menor inteiro tal que $f \in L_l$. Assim, $l(i,j)$ é o menor inteiro l tal que $f_i f_j \in L_l$ pois $l(i,j) := l$ tal que $\rho(f_i f_j) = \rho(f_l)$.

Com o objetivo de tornar $\mathbf{F}_q^n$ uma $\mathbf{F}_q$-álgebra introduzimos a seguinte multiplicação $*$ em $\mathbf{F}_q^n$. Sejam $a, b \in \mathbf{F}_q^n$. Por definição, $a * b := (a_1 b_1, \cdots, a_n b_n)$ onde $a = (a_1, \cdots, a_n)$ e $b = (b_1, \cdots, b_n)$. O espaço vetorial $\mathbf{F}_q^n$ com a multiplicação $*$ torna-se um anel comutativo com unidade $(1, \cdots, 1)$. Identificando $\{(\lambda, \cdots, \lambda) : \lambda \in \mathbf{F}_q\}$ com $\mathbf{F}_q$, temos que $\mathbf{F}_q^n$ é uma $\mathbf{F}_q$-álgebra.

Definição 1.17 *A aplicação*

$$\varphi : \mathbf{R} \longrightarrow \mathbf{F}_q^n,$$

é chamada um **morfismo** *de $\mathbf{F}_q$-álgebras se φ é $\mathbf{F}_q$-linear e*

$$\varphi(fg) = \varphi(f) * \varphi(g).$$

O Código Avaliado *E_l e seu dual C_l são dados por*

$$E_l = \varphi(L_l) =< \varphi(f_1), \cdots, \varphi(f_l) >,$$

$$C_l = \left\{ c \in \mathbf{F}_q^n : c \cdot \varphi(f_i) = 0 \text{ para todo } i \leq l \right\}.$$

A sequência de códigos $(E_l : l \in \mathbf{N})$ é crescente com respeito a inclusão e todos eles são subespaços de $\mathbf{F}_q^n$. Logo, existe um N natural tal que $E_l = E_N$ para todo $l \geq N$. Naturalmente, $E_N = \varphi(\mathbf{R})$. Seja $\mathbf{h_i} := \varphi(f_i)$ para todo $i \leq N$.

Exemplo 1.18 *Considere o conjunto $\mathcal{P}$ consistindo dos n pontos distintos $P_1, \cdots, P_n$ em $\mathbf{F}_q^m$. Seja $\mathbf{R} = \mathbf{F}_q[X_1, \cdots, X_m]$. Considere a aplicação avaliação*

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

dada por $av_{\mathcal{P}}(f) = (f(P_1), \cdots, f(P_n))$. Isto é um morfismo de $\mathbf{F}_q$-álgebras, pois $FG(P) = F(P) * G(P)$ para quaisquer polinômios F e G e qualquer ponto P em $\mathbf{F}_q^m$.

Com isto, podemos exibir um morfismo de uma curva em $\mathbf{F}_q^n$. De fato, suponha que I é um ideal no anel $\mathbf{F}_q[X_1, \cdots, X_2]$ e $P_1, \cdots, P_n$ são zeros de I. Então, a aplicação avaliação induz uma aplicação linear (bem definida)

$$\begin{array}{rccc} av_{\mathcal{P}} & : & \mathbf{F}_q[X_1, \cdots, X_m]/I & \longrightarrow & \mathbf{F}_q^n \\ & & f + I & \longmapsto & (f(P_1), \cdots, f(P_n)) \end{array}$$

a qual é também um morfismo de $\mathbf{F}_q$-álgebras.

Agora vamos mostrar a importante conexão entre Códigos Avaliados construídos sobre $R(P) = \bigcap_{S \neq P} \mathcal{O}_P$ com a função ordem $\rho = -v_P$ e CGG (pontuais) no ponto P.

Exemplo 1.19 *Sejam* $\mathbf{R}$*,* P *e* ρ *como no Exemplo 1.6. Agora, tome* $P_1, \cdots, P_n$ *pontos, distintos dois a dois,* $\mathbf{F}_q$*-racionais de* $\mathcal{X}$ *diferentes de* P *e considere o divisor* $D := P_1 + \cdots + P_n$*. Sejam* $(f_i : i \in \mathbf{N})$ *base de* $\mathbf{R}$ *tal que* $\rho_i := \rho(f_i) < \rho(f_{i+1}) =: \rho_{i+1}$*. Da Observação 1.7 segue que* $H(P) = \{\rho_i : i \in \mathbf{N}\}$ *é o semigrupo de Weierstrass de* P *(ou o conjunto das não-lacunas de* P*). Como* $\mathcal{L}(\rho_l P) = \{f \in \mathbf{R} : \rho(f) \leq \rho_l\}$*, então os elementos da base de* $\mathbf{R}$ *que estão em* $\mathcal{L}(\rho_l P)$ *formam uma* $\mathbf{F}_q$*-base de* $\mathcal{L}(\rho_l P)$*. Portanto,* $\mathcal{L}(\rho_l P) =< f_1, \cdots, f_l >= L_l$*. Logo, podemos concluir que*

$$E_l = av_{\mathcal{P}}(L_l) = av_{\mathcal{P}}(\mathcal{L}(\rho_l P)) = C(D, \rho_l P)$$

onde $C(D, \rho_l P)$ *denota o Código Geométrico de Goppa associado aos divisores* D *e* $\rho_l P$*. Assim,*

$$C_l = E_l^{\perp} = C(D, \rho_l P)^{\perp} = C_{\Omega}(D, \rho_l P),$$

onde a última igualdade é um resultado conhecido sobre CGG.

Nosso próximo passo é construir uma cota inferior $d(l)$ para a distância mínima d_l de C_l. No caso particular do Exemplo 1.19, esta cota será uma cota inferior para a distância mínima d_l de $C_{\Omega}(D, \rho_l P)$. Recordando, Goppa mostrou que neste caso

$$d_l \geq \rho_l - (2g - 2),$$

onde g denota o gênero de $\mathcal{X}$. Veremos, por meio dos exemplos, que para alguns valores de $l \leq N$ a cota $d(l)$ é melhor do que a cota de Goppa. Mais precisamente,

$$d_l \geq d(l) > \rho_l - (2g - 2).$$

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

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

onde $s_{ij}(y) := y \cdot (h_i * h_j)$. Assim, $\mathbf{S}(y)$ é uma submatriz de $\widetilde{\mathbf{S}}(y)$ e, portanto, $posto\,(\mathbf{S}(y)) \leq posto\left(\widetilde{\mathbf{S}}(y)\right)$. O próximo resultado nos mostra uma relação entre o peso de um elemento y de $\mathbf{F}_q^n$, denotado por $\omega(y)$, com o posto das matrizes acima contruídas.

Lema 1.20 *Seja $y \in \mathbf{F}_q^n$ e $\mathbf{D}(y)$ a matriz diagonal com y na diagonal. Então*

$$\widetilde{\mathbf{S}}(y) = \widetilde{\mathbf{H}}\mathbf{D}(y)\widetilde{\mathbf{H}}^{\mathbf{T}} \quad e \quad \omega(y) = posto\left(\widetilde{\mathbf{S}}(y)\right) \geq posto\left(\mathbf{S}(y)\right).$$

Observação 1.21 *Em [10], os autores trabalham a todo momento com a hipótese de que φ seja* **sobrejetora**. *Neste caso, $\widetilde{\mathbf{H}} = \mathbf{H}$ e $\widetilde{\mathbf{S}}(y) = \mathbf{S}(y)$. Na verdade, eles provaram o Lema 1.20 nesta situação específica. Mas afirmamos que isso não nos trará nenhum problema pois a demonstração é exatamente a mesma para $\widetilde{\mathbf{S}}(y)$ e $\widetilde{\mathbf{H}}$. O que mais importa é que $\omega(y) \geq posto\left(\mathbf{S}(y)\right)$ sendo φ sobrejetora ou não.*

Com base nos dois resultados que vem a seguir, poderemos expressar uma cota para a distância mínima de C_l para todo $l \leq N$. O lema abaixo vale apenas para os elementos de $\mathbf{S}(y)$.

Lema 1.22 *(1) Se $y \in C_l$ e $l(i,j) \leq l$ então $s_{ij}(y) = 0$.*
(2) Se $y \in C_l \backslash C_{l+1}$ e $l(i,j) = l+1$ então $s_{ij}(y) \neq 0$.

Para $l \in \mathbf{N}_0$ considere as seguintes definições:

$$\begin{aligned} N_l &:= \{(i,j) \in \mathbf{N}^2 : l(i,j) = l+1\}; \\ \nu_l &:= \#N_l. \end{aligned}$$

Se ρ é uma função peso então

$$N_l = \left\{(i,j) \in \mathbf{N}^2 : \rho(f_i) + \rho(f_j) = \rho(f_{l+1})\right\}.$$

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

Proposição 1.23 *Se $y \in C_l \backslash C_{l+1}$ então $\omega(y) \geq \nu_l$.*

Finalmente, enunciamos o principal resultado desta seção. Este, é consequência imediata da proposição 1.23. Para isto, considere o seguinte número:

$$d(l) := Min\{\nu_m : m \geq l\}.$$

Teorema 1.24 *O número $d(l)$ é cota inferior para a distância mínima de C_l, ou seja,*

$$d(C_l) \geq d(l).$$

Vejamos alguns exemplos.

Exemplo 1.25 *Sejam* $\mathbf{R} = \mathbf{F}_q[X]$ *e* $\rho(f) = grau(f)$ *a função ordem do Exemplo 1.5. Seja* $f_i = X^{i+1}$. *Para um elemento primitivo* α *de* $\mathbf{F}_q$ *e* $n = q-1$ *seja* $\varphi : \mathbf{R} \to \mathbf{F}_q^n$ *definida por* $\varphi(f) = (f(\alpha^0), \cdots, f(\alpha^{n-1}))$. *Então* $C_l = \{c \in \mathbf{F}_q^n : c \cdot \varphi(f_i) = 0,\ 1 \leq i \leq l\}$ *é um código cíclico com*

$$\begin{aligned} \nu_l &= \#\{(i,j) : f_i f_j = f_{l+1}\} = \#\{(i,j) : X^{i-1}X^{j-1} = X^l\} \\ &= \#\{(i,j) : i + j = l + 2\} \\ &= l + 1. \end{aligned}$$

e portanto $d(l) = l + 1$.

Nos dois exemplos seguintes temos que ρ é uma função peso. Assim

$$N_l = \{(i,j) : \rho_i + \rho_j = \rho_{l+1}\},$$

onde $\rho_i = \rho(f_i)$. Também, sejam P e D como no Exemplo 1.19. Logo, $C_l = C_\Omega(D, \rho_l P)$ e $H(P) = \{\rho_i : i \in \mathbf{N}\}$. Em cada caso, P será descrito. Veremos nos exemplos abaixo que $d(l) > d_G(l)$, para alguns valores de l.

Exemplo 1.26 *Este é uma continuação do Exemplo 1.16 com a quártica de Klein de gênero* $g = 3$. *Neste caso, o semigrupo de Weierstrass de* $P = (0:1:0)$ *é* $\{0, 3, 5, 6, 7, \ldots\}$ *e* $\mathbf{R} = R(P)$ *[1, Lema 3.4]. A tabela abaixo nos fornece uma lista dos valores* ρ_l, ν_l, $d(l)$ *e* $d_G(l)$ *com* $1 \leq l \leq 9$.

l	1	2	3	4	5	6	7	8	9
ρ_l	0	3	5	6	7	8	9	10	11
ν_l	2	2	3	2	4	4	5	6	7
$d(l)$	2	2	2	2	4	4	5	6	7
$d_G(l)$	-4	-1	1	2	3	4	5	6	7

É fácil de ver que $d(l) = \nu_l = l - 2 = d_G(l)$ *para todo* $l \geq 6$.

Exemplo 1.27 *Este é uma continuação do Exemplo 1.15 com a curva Hermitiana sobre* $\mathbf{F}_{16}$ *de gênero* $g = 6$. *Neste caso, para qualquer ponto* $\mathbf{F}_{16}$*-racional é sabido que seu semigrupo de Weierstrass é* $\{0, 4, 5, 8, 9, 10, 12, 13, \ldots\}$. *Para* $P = (0:1:0)$ *temos que* $\mathbf{R} = R(P)$. *A tabela abaixo nos fornece uma lista dos valores de* ρ_l, ν_l, $d(l)$ *e* $d_G(l)$ *onde* $1 \leq l \leq 16$.

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

Temos também que $d(l) = \nu_l = l - 5 = d_G(l)$, *para todo* $l > 16$.

Capítulo 2

Funções Ordens Fracas

Este capítulo é parte fundamental desta tese. Nele, estendemos os conceitos de função ordem e função peso, e apresentamos alguns resultados. Para modificarmos tais conceitos, vamos introduzir a seguintes notações. Seja

$$\rho : \mathbf{R} \longrightarrow \mathbf{N}_0 \cup \{-\infty\}$$

uma função. As **não-unidades** e **unidades** de $\mathbf{R}$ com respeito a ρ são, respectivamente, os conjuntos:

$$\mathcal{M} = \mathcal{M}_\rho := \{f \in \mathbf{R} : \rho(f) > \rho(1)\} \text{ e}$$

$$\mathcal{U} = \mathcal{U}_\rho := \{f \in \mathbf{R} : f \neq 0 \text{ e } \rho(f) \leq \rho(1)\}.$$

Ao longo deste capítulo, $\mathbf{R}$ denotará uma K-álgebra **diferente** de K.

Definição 2.1 *A função ρ é chamada uma* **função ordem fraca** *sobre $\mathbf{R}$ se as seguintes propriedades são satisfeitas. Sejam $f, g, h \in \mathbf{R}$.*

(I) *$\rho(f) = -\infty$ se, e somente se, $f = 0$;*

(II) *Para $\lambda \in K^*$, $\rho(\lambda f) = \rho(f)$;*

(III) *$\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$, e a igualdade vale sempre que $\rho(f) \neq \rho(g)$;*

(IV) *Se $\rho(f) < \rho(g)$ e $h \in \mathcal{M}$, então $\rho(fh) < \rho(gh)$;*

(V) *Se $\rho(f) = \rho(g)$ e $f, g \in \mathcal{M}$, então existe $\lambda \in K^*$ tal que $\rho(f - \lambda g) < \rho(g)$.*

A função ρ é chamada de **função peso fraco** *sobre $\mathbf{R}$, se além de $(I) - (V)$ também satisfaz:*

(VI) $\rho(fg) = \rho(f) + \rho(g)$ *sempre que* $f, g \in \mathcal{M}$.

Vejamos alguns exemplos.

Exemplo 2.2 *Naturalmente, uma função ordem é uma função ordem fraca com* $\mathcal{U} = K^*$ *(Lema 1.8(3)).*

Exemplo 2.3 (Função Constante) *Seja* $c \in \mathbf{N}_0$. *Para* $f \in \mathbf{R}$ *definimos* $\rho(f) = -\infty$ *se* $f = 0$ *e* $\rho(f) = c$ *se* $f \neq 0$. *Assim,* $\mathcal{U} = \mathbf{R}^*$ *e* $\mathcal{M} = \emptyset$. *Note que, por vacuidade, os Axiomas (IV) e (V) são satisfeitos. É imediato que* ρ *é função ordem fraca sobre* $\mathbf{R}$ *mas* **NÃO** *é função ordem sobre* $\mathbf{R}$. *De fato, lembre que* $\mathbf{R} \neq K$. *Seja* $f \in \mathbf{R} \backslash K$. *Assim,* $\rho(f) = \rho(1)$. *Se* ρ *é função ordem, segue do Axioma (5) que existe* $\lambda \in K^*$ *tal que* $\rho(f - \lambda 1) < \rho(1) = c$. *Ou seja,* $\rho(f - \lambda 1) = -\infty$ *e, portanto,* $f - \lambda 1 = 0$. *Logo,* $f = \lambda \in K$, *o que é uma contradição.*

A aplicação em códigos será feita sobre as K-álgebras do próximo exemplo.

Exemplo 2.4 (Generaliza o Exemplo 1.6) *Seja* $K(\mathcal{X})$ *o corpo de funções de uma curva* $\mathcal{X}$ *sobre* K. *Sejam* P *e* Q *pontos distintos e* K*-racionais de* $\mathcal{X}$. *Seja* $\mathbf{R} := R(P, Q)$ *a* K*-álgebra dada pela interseção dos anéis locais* $\mathcal{O}_S$ *de* $K(\mathcal{X})$, *nos pontos* S, *com* $S \neq P$ *e* $S \neq Q$. *Seja* $v := v_P$ *a valorização em* P *e* ρ *a função definida por*

$$\rho(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ 0, & \text{se } v(f) \geq 0 \text{ and } f \neq 0 \\ -v(f), & \text{se } v(f) < 0 \end{cases}$$

para $f \in \mathbf{R}$. *Vamos mostrar que* ρ *é uma* **função ordem fraca** *sobre* $\mathbf{R}$. *Os Axiomas (I) e (II) seguem, respectivamente, da definição de* ρ *e da propriedade* $v(f) = v(\lambda f)$.

Axioma (III): sejam $f, g \in \mathbf{R}$ *tal que* $\rho(f) \leq \rho(g)$ $(*)$*; primeiro vamos mostrar que* $\rho(f + g) \leq \rho(g)$. *Por absurdo, suponha que* $\rho(f + g) > \rho(g)$. *Então,* $v(g) < 0$ *ou* $v(f+g) < 0$. *No primeiro caso,* $v(f+g) < 0$ *e assim* $v(f+g) < v(g)$. *De* $(*)$, $v(g) < v(f)$. *Pela propriedade de valorização temos que* $v(g) = v(f + g) < v(g)$, *uma contradição. No outro caso,* $v(g) \geq 0$. *Logo,* $(*)$ *nos mostra que* $v(f) \geq 0$ *e portanto* $0 \leq v(f+g) < 0$, *uma contradição. Agora vamos mostrar que* $\rho(f + g) = \rho(g)$ *se* $\rho(f) < \rho(g)$ $(*_1)$. *Se* $v(g) \geq 0$, *de* $(*_1)$ *temos que* $\rho(f) < 0$, *assim* $f = 0$ *e o resultado segue trivialmente. Seja* $v(g) < 0$. *A desigualdade* $(*_1)$ *nos permite concluir que* $v(g) < v(f)$ *e portanto* $v(f + g) = v(g)$, *ou seja,* $\rho(f + g) = \rho(g)$.

Axioma (IV): sejam $f, g, h \in \mathbf{R}$ *tal que* $\rho(f) < \rho(g)$ *e* $\rho(1) = 0 < \rho(h) = -v(h)$. *Vamos mostrar que* $\rho(fh) < \rho(gh)$. *Temos que* $v(f) < 0$ *ou* $v(g) < 0$. *No primeiro caso,* $v(g) < 0$ *e portanto* $-v(f) < -v(g)$. *Assim,* $\rho(fh) = -v(fh) < -v(gh) = \rho(gh)$. *No outro caso,* $v(f) \geq 0$. *Desde que* $\rho(gh) = -v(gh) > 0$ $(*_2)$, *podemos assumir que* $v(fh) < 0$. *Devemos mostrar que* $-v(fh) < -v(g)$, *ou equivalentemente,* $-v(f) < -v(g)$. *Isto segue de* $(*_2)$.

Axioma (V): Sejam $f, g \in \mathbf{R}$ *tais que* $0 = \rho(1) < \rho(f) = \rho(g)$. *Então* $v(f) = v(g)$ *e assim existe* $\lambda \in K^*$ *tal que* $v(f - \lambda g) > v(g)$. *Se* $v(f - \lambda g) \geq 0$, $\rho(f - \lambda g) \leq 0 < \rho(g)$. *Por outro lado, se* $v(f - \lambda g) < 0$, $\rho(f - \lambda g) = -v(f - \lambda g) < -v(g) = \rho(g)$.

Na verdade, ρ *é função peso fraco sobre* $\mathbf{R}$, *pois* $v(fg) = v(f) + v(g)$ *para todo* $f, g \in \mathbf{R}$. *Neste caso,* $\mathcal{U} = R(Q)^*$. *Isto nos mostra que* ρ *não é função ordem sobre* $\mathbf{R}$. *Além disso,* ρ *não satisfaz os Axiomas (4), (5) e (6) da definição de função ordem. Está função peso fraco sobre* $\mathbf{R} = R(P, Q)$ *pode ser definida sobre uma* K*-álgebra mais geral. A saber, sejam* $P, Q_1, \cdots, Q_m$ *pontos* K*-racionais da curva* $\mathcal{X}$, *diferentes entre si. Seja* $\mathbf{R} := R(P, Q_1, \cdots, Q_m)$ *a* K*-álgebra dada pela interseção dos anéis locais* $\mathcal{O}_S$ *de* $K(\mathcal{X})$, *nos pontos* S, *com* $S \neq P$ *e* $S \neq Q_i$ *para todo* i *tal que* $1 \leq i \leq m$. *Nesta situação,* $\mathcal{U} = R(Q_1, \cdots, Q_m)^*$.

Observe (Exemplos 2.3 e 2.4) que já temos funções ordens fracas diferentes de funções ordens. Os próximos exemplos também gozam desta propriedade. Neste momento, não justificaremos, utilizando a definição de função ordem fraca (Definição 2.1), que as funções apresentadas abaixo são funções ordens fracas. Queremos apenas evitar cálculos enfadonhos e repetitivos. Na verdade, a construção destes exemplos se enquadram numa situação mais geral; isto é, existe um método que nos permite construir funções ordens fracas sobre K-álgebras. Mais a frente exibiremos este método, e aí sim justificaremos que tais exemplos são de fato funções ordens fracas.

Exemplo 2.5 (Generaliza o Exemplo 1.13) *Consideremos a ordem lexicográfica graduada* $\prec$ *no conjunto dos monômios* $\mathbf{R}_1 = \{X^a Y^b : a, b \in \mathbf{N}_0 \ \wedge \ a + b \geq 2\}$, *isto é,* $X^a Y^b \prec X^c Y^d$ *se, e somente se,* $a + b < c + d$ *ou* $a + b = c + d$ *e* $(a, b) \prec_L (c, d)$ *onde* $\prec_L$ *é a ordem lexicográfica. Sejam* $f_1, f_2, \cdots$ *a enumeração do conjunto dos monômios acima tal que* $f_i \prec f_{i+1}$ *para todo* $i \in \mathbf{N}$. *Abaixo, apresentamos duas matrizes. Uma corresponde ao conjunto dos monômios e a outra corresponde aos respectivos índices,*

segundo a enumeração acima.

$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
Y^6	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\ldots$	19	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\ldots$
Y^5	XY^5	$\cdot$	$\cdot$	$\cdot$	$\ldots$	13	20	$\cdot$	$\cdot$	$\cdot$	$\ldots$
Y^4	XY^4	X^2Y^4	$\cdot$	$\cdot$	$\ldots$	8	14	21	$\cdot$	$\cdot$	$\ldots$
Y^3	XY^3	X^2Y^3	X^3Y^3	$\cdot$	$\ldots$	4	9	15	22	$\cdot$	$\ldots$
Y^2	XY^2	X^2Y^2	X^3Y^2	$\cdot$	$\ldots$	1	5	10	16	$\cdot$	$\ldots$
	XY	X^2Y	X^3Y	X^4Y	$\ldots$		2	6	11	17	$\ldots$
		X^2	X^3	X^4	X^5			3	7	12	18

Seja $\mathbf{R} := K[X, Y]$ *e* $\mathbf{R}_0 := \{1, X, Y\}$. *Assim,* $\mathbf{R} = \langle \mathbf{R}_0 \rangle \oplus \langle \mathbf{R}_1 \rangle$. *Se* $f \in \mathbf{R}$ *então existem únicos* $f_0 \in \langle \mathbf{R}_0 \rangle$ *e* $\lambda_1, \cdots, \lambda_t \in K$ *tais que*

$$f = f_0 + (\lambda_1 f_1 + \cdots + \lambda_t f_t).$$

A função ρ *definida por*

$$\rho(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ t, & \text{se } f \neq 0 \end{cases}$$

é uma função ordem fraca sobre $\mathbf{R}$ *com* $\mathcal{U} = \langle \mathbf{R}_0 \rangle^*$. *A mesma construção pode ser feita, considerando* $\mathbf{R}_0 = \{X^a Y^b : a, b \in \mathbf{N}_0 \ \wedge \ a + b \leq n\}$ *e* $\mathbf{R}_1 = \{X^a Y^b : a, b \in \mathbf{N}_0 \ \wedge \ a + b \geq n + 1\}$. *Assim,*

$$\mathbf{R} = \langle \mathbf{R}_0 \rangle \oplus \langle \mathbf{R}_1 \rangle$$

e $\mathcal{U} = \langle \mathbf{R}_0 \rangle^*$. *Note que* $\mathcal{U} \cup \{0\}$ *NÃO é um anel.*

Exemplo 2.6 (Generaliza o Exemplo 1.5) *Seja* $\mathbf{R} := K[X]$. *Logo,* $\mathbf{R} = \langle 1, \cdots, X^n \rangle \oplus \langle X^{n+1}, X^{n+2}, \cdots \rangle$ *para qualquer* $n \in \mathbf{N}_0$ *fixo. Assim, para* $f \in K[X]$ *existem únicos* $f_0 \in \langle 1, \cdots, X^n \rangle$ *e* $\lambda_1, \cdots, \lambda_t \in K$ *tais que*

$$f = f_0 + (\lambda_1 X^{n+1} + \cdots + \lambda_t X^{n+t}).$$

A função ρ *definida por*

$$\rho(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ 0, & \text{se } grau(f) \leq n, \\ t, & \text{se } grau(f) = n + t > n \end{cases}$$

é uma função ordem fraca sobre $\mathbf{R}$ *com* $\mathcal{U} = \langle 1, \cdots, X^n \rangle^*$. *Aqui,* $\mathcal{U} \cup \{0\}$ *tampouco é um anel.*

Agora, vamos provar alguns resultdos análogos aos apresentados na Subseção 1.2.1. O primeiro, refere-se ao Lema 1.8(1).

Lema 2.7 *Seja ρ uma função ordem fraca. Se $f, g, h \in \mathcal{M}$ e $\rho(f) = \rho(g)$ então $\rho(fh) = \rho(gh)$.*

Prova. Pelo Axioma (V), existe $\lambda \in K^*$ tal que $\rho(f - \lambda g) < \rho(g)$. Disto, aplicando os Axiomas (IV) e (II), respectivamente, temos que $\rho(fh - \lambda gh) < \rho(gh) = \rho(\lambda gh)$. Portanto, aplicando o Axioma (III) para as funções $(fh - \lambda gh)$ e λgh, concluímos que

$$\rho(fh) = \rho((fh - \lambda gh) + \lambda gh) = \rho(\lambda gh) = \rho(gh).$$

□

O próximo resultado nos mostra uma generalização da Proposição 1.9. Seja

$$\widetilde{\mathcal{U}} := \mathcal{U} \cup \{0\}.$$

Proposição 2.8 *A K-álgebra $\mathbf{R}$ é um domínio de integridade se, e somente se, existe uma função ordem fraca ρ sobre $\mathbf{R}$ tal que $\widetilde{\mathcal{U}} := \mathcal{U} \cup \{0\}$ é um subanel de $\mathbf{R}$ que é um domínio.*

Prova. Suponha que $\mathbf{R}$ é um domínio de integridade. Tome ρ a função ordem fraca constante (veja Exemplo 2.3). Assim, $\widetilde{\mathcal{U}} = R$.

Agora, seja ρ função ordem fraca sobre $\mathbf{R}$ tal que $\widetilde{\mathcal{U}}$ é domínio de integridade. Tome $f, g \in \mathbf{R}^*$. Devemos mostrar que $fg \neq 0$. Se $f, g \in \widetilde{\mathcal{U}}$, por hipótese, não há nada a fazer. Assim, suponha que $f \in \mathcal{M}$ ou $g \in \mathcal{M}$. Sem perda de generalidade, admita que $f \in \mathcal{M}$, isto é, $\rho(1) < \rho(f)$. Como $g \neq 0$, então $\rho(0) < \rho(g)$. Logo, aplicando o Axioma (IV), temos que $\rho(0) < \rho(fg)$. Portanto, $fg \neq 0$. □

Observação 2.9 *O Exemplo 1.10 exibe uma K-álgebra, mais precisamente um domínio, que não possui função ordem. No nosso caso, isto não é possível como prova a proposição anterior (ρ = constante), sempre que $\mathbf{R} \neq K$. No próximo exemplo exibimos uma função ordem fraca, diferente da constante, neste mesmo domnío.*

Exemplo 2.10 *Seja $\mathbf{R} = K[X, Y]/(XY - 1) = K[x] + K[y]$ a K-álgebra do Exemplo 1.10, onde $x = \overline{X}$, $y = \overline{Y}$ e $xy = 1$. Vamos exibir uma função ordem fraca ρ,diferente da constante, que não é função ordem. Como nos exemplos acima, não provaremos neste momento que ρ é função ordem fraca. A mesma é construída utilizando o método que em*

breve apresentaremos. Assim, $\mathbf{R} = K[x] \oplus \langle y, y^2, y^3, \cdots \rangle$ *e portanto, para todo* $f \in \mathbf{R}$*, existem únicos* $f(x)$ *e* $f(y)$ *com* $\deg(f(y)) \neq 0$ *tais que*

$$f = f(x) + f(y).$$

Seja ρ *tal que*

$$\rho(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ 0, & \text{se } f(y) = 0 \\ \deg(f(y)), & \text{se } f(y) \neq 0. \end{cases}$$

Temos que ρ *é uma função ordem fraca com* $\mathcal{U} = K[x]^*$.

Podemos questionar se existe K-álgebra que não possui função ordem fraca diferente da constante. O exemplo abaixo dá resposta a isto.

Exemplo 2.11 *Seja* $\mathbf{R}$ *uma* K*-álgebra diferente de* K *e* $g \in \mathbf{R} \backslash K$*. A função* $\rho := \rho_g$ *definida por*

$$\rho_g(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ 0, & \text{se } f \in \langle g \rangle \setminus \{0\} \\ 1, & \text{se } f \notin \langle g \rangle \end{cases}$$

é uma função ordem fraca com $\mathcal{U}_\rho = \mathbf{R}^*$*. Vamos provar isso. Da definição, é imediato que os Axiomas (I) e (II) são satisfeitos. Por vacuidade, os Axiomas (IV) e (V) são satisfeitos. Resta-nos testar o Axioma (III). Primeiro vamos mostrar que* $\rho_g(f + h) \leq Max\{\rho_g(f), \rho_g(h)\}$*. Sejam* $f, h \in \mathbf{R}$*. Se* $f + h = 0$*, segue o que queremos. Se* $0 \neq f + h = \lambda g$ *então* $f \neq 0$ *ou* $h \neq 0$ *e, portanto,* $\rho_g(f + h) = 0 \leq \rho_g(f)$ *ou* $\rho_g(f + h) \leq \rho_g(h)$*. Se* $0 \neq f + h \notin \langle g \rangle$ *então* $f \notin \langle g \rangle$ *ou* $h \notin \langle g \rangle$ *e, portanto,* $\rho_g(f + h) = 1 = \rho_g(f)$ *ou* $\rho_g(f + h) = 1 = \rho_g(h)$*. Agora vamos mostrar que vale a igualdade se* $\rho_g(f) < \rho_g(h)$*. Se* $f = 0$*, é imediato o que queremos. Se* $0 \neq f \in \langle g \rangle$ *então* $h \notin \langle g \rangle$*,* $f + h \notin \langle g \rangle$ *e portanto* $\rho_g(f + h) = \rho_g(h)$.

O resultado abaixo caracteriza a função ordem em termos da função ordem fraca.

Lema 2.12 *Seja* $\rho : \mathbf{R} \longrightarrow \mathbf{N}_0 \cup \{-\infty\}$ *uma função. Então* ρ *é uma função ordem se, e somente se,* ρ *é uma função ordem fraca tal que* $\mathcal{U} = K^*$.

Prova. Admita que ρ é uma função ordem. Da definição segue que ρ é função ordem fraca. Do Lema 1.8(3) segue que $K^* = \mathcal{U}$.

Suponha que ρ é função ordem fraca com $\mathcal{U} = K^*$. Temos que provar que ρ satisfaz os axiomas da definição de ordem fraca (veja 1.4). Da definição de função ordem fraca é

imediato que ρ satisfaz os Axiomas (1), (2) e (3). Sejam $f, g, h \in \mathbf{R}$ tal que $h \neq 0$. Note que $\mathbf{R} = \mathcal{M} \cup \mathcal{U} = \mathcal{M} \cup K^*$. Primeiro, vamos provar que ρ satisfaz o Axioma (4). De fato, admita que $\rho(f) < \rho(g)$. Se $h \in \mathcal{M}$ então pelo Axioma (IV) temos que $\rho(fh) < \rho(gh)$. Se $h \in \mathcal{U} = K^*$ então pelo Axioma (II) temos que $\rho(fh) = \rho(f) < \rho(g) = \rho(gh)$. Portanto, ρ satisfaz o Axioma (4). Para finalizar, provaremos que ρ satisfaz o Axioma (5). Suponha que $-\infty < \rho(f) = \rho(g)$. Se $f, g \in \mathcal{M}$ então pelo Axioma (V) existe $\lambda \in K^*$ tal que $\rho(f - \lambda g) < \rho(f)$. Se $f, g \in \mathcal{U} = K^*$ tome $\lambda := \frac{f}{g}$. Assim, $\rho(f - \lambda g) < \rho(f)$. Logo, ρ satisfaz o Axioma (5). □

Agora trataremos da unicidade de $\lambda \in K^*$ satisfazendo o Axioma (V). No caso de ρ ser função ordem esta questão foi tratada no Lema 1.8(4).

Lema 2.13 *Se $\rho(1) < \rho(f) = \rho(g)$ então existe único $\lambda \in K^*$ tal que $\rho(f - \lambda g) < \rho(f)$.*

Prova. A existência é garantida pelo Axioma (V). Vamos mostrar a unicidade. É imediato que $g \neq 0$. Admita que existem $\lambda, \mu \in K^*$ tais que $\rho(f - \lambda g) < \rho(f)$ e $\rho(f - \mu g) < \rho(f)$. Assim, dos Axiomas (II) e (III) segue que

$$\rho((\mu - \lambda)g) = \rho((f - \lambda g) - (f - \mu g)) \leq Max\{\rho(f - \lambda g), \rho(f - \mu g)\}.$$

Logo,

$$\rho((\mu - \lambda)g) < \rho(g).$$

Isto acontece apenas se $\mu - \lambda = 0$, pois $g \neq 0$. Disto temos que $\mu = \lambda$. □

Nosso objetivo agora é provar um resultado análogo ao Teorema 1.11. Para isto, precisamos dos lemas auxiliares abaixo.

Lema 2.14 *Seja ρ função ordem fraca tal que $\mathcal{U} \neq \mathbf{R}^*$. Então $\mathcal{M} \neq \emptyset$ e o conjunto $\rho(\mathcal{M})$ possui infinitos elementos.*

Prova. É imediato que $\mathcal{M} \neq \emptyset$, pois do contrário $\mathcal{U} = \mathbf{R}^*$. Seja $f \in \mathcal{M}$. Aplicando o Axioma (IV) sucessivas vezes temos que

$$\rho(1) < \rho(f) < \rho(f^2) < \rho(f^3) < \cdots \quad .$$

Isto nos mostra que $\rho(\mathcal{M})$ possui infinitos elementos. □

Observação 2.15 *Para ρ como no lema anterior, admita que*

$$\rho(\mathcal{M}) = \{\rho_1 < \rho_2 < \rho_3 < \cdots \quad \}.$$

Seja $F := \{f_i \in \mathcal{M} : i \in \mathbf{N}\}$ tal que $\rho(f_i) = \rho_i$, para todo $i \in \mathbf{N}$. Assim, $\rho(F) = \rho(\mathcal{M})$.

Lema 2.16 *Seja ρ função ordem fraca com $\mathcal{U} \neq \mathbf{R}^*$ e F nas condições da observação acima. Se $f \in \mathcal{M}$ e $\rho(f) = \rho(f_n)$ então existem únicos $\lambda_1, \cdots, \lambda_n \in K$, $\lambda_n \neq 0$ tais que*

$$f - (\lambda_1 f_1 + \cdots + \lambda_n f_n) \in \widetilde{\mathcal{U}} \, .$$

Prova. Vamos provar a existência. Usaremos indução sobre n. Suponha que $\rho(f) = \rho(f_1)$. Pelo Axioma (V), existe $\lambda_1 \in K^*$ tal que

$$\rho(f - \lambda_1 f_1) < \rho(f_1).$$

Isto nos mostra que $(f - \lambda_1 f_1) \in \widetilde{\mathcal{U}}$, pois $\rho(h) \geq \rho(f_1)$ para todo $h \in \mathcal{M}$ por construção. Suponha que vale a propriedade para $m < n$. Se $\rho(f) = \rho(f_n)$, pelo Axioma (V) existe $\lambda_n \in K^*$ tal que

$$\rho(f - \lambda_n f_n) < \rho(f_n).$$

Caso $f - \lambda_n f_n = 0$, tome $\lambda_1 = \cdots = \lambda_{n-1} = 0$. Assim,

$$f - (\lambda_1 f_1 + \cdots + \lambda_n f_n) \in \widetilde{\mathcal{U}} \, .$$

Caso contrário, existe $a < n$ tal que $\rho(f - \lambda_n f_n) = \rho(f_a)$. Pela hipótese de indução, existem $\lambda_1, \cdots, \lambda_a \in K$, $\lambda_a \neq 0$, tal que

$$(f - \lambda_n) - (\lambda_1 f_1 + \cdots + \lambda_a f_a) \in \widetilde{\mathcal{U}} \, .$$

Fazendo $\lambda_{a+1} = \cdots = \lambda_{n-1} = 0$, se necessário for, temos que

$$f - (\lambda_1 f_1 + \cdots + \lambda_n f_n) \in \widetilde{\mathcal{U}} \, .$$

Vamos mostrar a unicidade. Suponha que existam $\lambda_1, \cdots, \lambda_n \in K$ e $\mu_1, \cdots, \mu_n \in K$ tais que $\lambda_n \neq 0$, $\mu \neq 0$ e

$$h_1 := f - (\lambda_1 f_1 + \cdots + \lambda_n f_n) \in \widetilde{\mathcal{U}} \quad \text{e}$$

$$h_2 := f - (\mu_1 f_1 + \cdots + \mu_n f_n) \in \widetilde{\mathcal{U}} \, .$$

Assim,

$$\rho(f - \lambda_n f_n) = \rho(h_1 + \lambda_1 f_1 + \cdots + \lambda_{n-1} f_{n-1}) < \rho(f_n) \quad \text{e}$$

$$\rho(f - \mu_n f_n) = \rho(h_2 + \mu_1 f_1 + \cdots + \mu_n f_n) < \rho(f_n).$$

Do Lema 2.13 segue que $\lambda_n = \mu_n$. Argumento análogo nos mostra que $\lambda_i = \mu_i$ para todo i tal que $1 \leq i \leq n - 1$. □

Teorema 2.17 (Análogo ao Teorema 1.11) *Seja ρ uma função ordem fraca sobre $\mathbf{R}$ tal que $\mathcal{U} \neq \mathbf{R}^*$.*
(1) Existe um conjunto linearmente independente $F = \{f_i : i \in \mathbf{N}\} \subseteq \mathcal{M}$ tal que $\rho(f_i) < \rho(f_{i+1})$ e $\rho(F) = \rho(\mathcal{M})$.
(2) Seja $f \in \mathbf{R}$. Então f pode ser escrito, de maneira única, da forma

$$f = f_0 + \lambda_1 f_1 + \cdots + \lambda_n f_n$$

onde $f_0 \in \widetilde{\mathcal{U}}$ e $\lambda_1, \ldots, \lambda_n \in K$. Em outras palavras,

$$\mathbf{R} = \widetilde{\mathcal{U}} \oplus \langle F \rangle .$$

Se $f \neq 0$ e n é o menor inteiro tal que f pode ser escrito da forma acima, então $\rho(f) = \rho(f_n)$.
(3) Seja $l(i,j)$ o menor inteiro l tal que $\rho(f_i f_j) = \rho(f_l)$. Então $l(i,j) < l(i+1,j)$ para todo $i \in \mathbf{N}_0$ e $j \in \mathbf{N}$. Se ρ é função peso fraco e $i, j \in \mathbf{N}$, então

$$\rho_{l(i,j)} = \rho_i + \rho_j$$

onde $\rho(f_i) = \rho_i$.

Prova. (1) Da Observação 2.15 segue que existe $F = \{f_i : i \in \mathbf{N}\} \subseteq \mathcal{M}$ tal que $\rho(f_i) < \rho(f_{i+1})$ e $\rho(F) = \rho(\mathcal{M})$. Vamos mostrar que F é linearmente independente. Suponha que

$$\lambda_1 f_1 + \cdots + \lambda_n f_n = 0.$$

Sem perda de generalidade, admita que $\lambda_n \neq 0$. Assim,

$$0 < \rho(f_n) = \rho(\lambda_1 f_1 + \cdots + \lambda_n f_n) = \rho(0) = -\infty.$$

contradição. Logo, $\lambda_1 = \cdots = \lambda_n = 0$.

(2) Se $f = 0$ o resultado é imediato. Suponha $f \in \mathbf{R}^*$. Se $f \in \mathcal{U}$, não há nada a provar. Assim, $f \in \mathcal{M}$ e existe $n \in \mathbf{N}$ tal que $\rho(f) = \rho(f_n)$. Do Lema 2.16, existem únicos $\lambda_1, \cdots, \lambda_n \in K$, $\lambda_n \neq 0$, tal que

$$f_0 := f - (\lambda_1 f_1 + \cdots + \lambda_n f_n) \in \widetilde{\mathcal{U}} .$$

Isto nos mostra que f_0 é único. Portanto, f pode ser escrito de maneira única. Agora, admita que n é o menor inteiro tal que

$$0 \neq f = f_0 + \lambda_1 f_1 + \cdots + \lambda_n f_n.$$

Se $f \in \widetilde{\mathcal{U}}$ então $f = f_0$ e $\rho(f) = \rho(f_0)$. Se $f \in \mathcal{M}$ então $\lambda_n \neq 0$. Dos Axiomas (II) e (III) segue que $\rho(f) = \rho(\lambda_n f_n) = \lambda(f_n)$.

(3) Já sabemos que $\rho(f_i) < \rho(f_{i+1})$ para todo $i \in \mathbf{N}_0$. Aqui, f_0 representa qualquer elemento de $\widetilde{\mathcal{U}}$. Seja $j \in \mathbf{N}$. Assim, $f_j \in \mathcal{M}$ e pelo Axioma (IV) temos que $\rho(f_i f_j) < \rho(f_{i+1} f_j)$, como queríamos demonstrar. Da definição de função peso fraco segue que $\rho_{l(i,j)} = \rho_i + \rho_j$, sempre que $i, j \in \mathbf{N}$. □

Finalmente, vamos exibir o método que nos permite construir funções ordens fracas sobre uma K-álgebra.

Teorema 2.18 *Seja $\{f_i : i \in \mathbf{N}\} \subseteq \mathbf{R} \backslash K$ um conjunto linearmente independente e $\mathbf{R}_0$ o seu completamento que determina uma K-base de $\mathbf{R}$. Assim,*

$$\mathbf{R} = \langle \mathbf{R}_0 \rangle \oplus \langle f_1, f_2, \cdots \rangle .$$

Sejam $L_0 = \langle \mathbf{R}_0 \rangle$, $L_l = \mathbf{R}_0 \oplus \langle f_1, \cdots, f_l \rangle$ para todo $l \in \mathbf{N}$ e $l(i,j) = Min\{l : f_i f_j \in L_l\}$. Para todo $i \in \mathbf{N}_0$, suponha que

$$l(i,j) < l(i+1,j)$$

para todo $j \in \mathbf{N}$ e que

$$l(i,0) \leq l(i+1,0).$$

Seja $(\rho_i : i \in \mathbf{N}_0)$ uma sequência estritamente crescente de inteiros não negativos. Defina $\rho(0) = -\infty$ e $\rho(f) = \rho_l$ se l é o menor inteiro tal que $f \in L_l$. Então ρ é uma função ordem fraca sobre $\mathbf{R}$. Se além disso, $\rho_{l(i,j)} = \rho_i + \rho_j$ para todo $i, j \in \mathbf{N}$, então ρ é uma função peso.

Prova. Os Axiomas (I), (II), (III) e (V) são consequências imediatas das definições. Vamos provar que o Axioma (IV) é satisfeito. Sejam $f, g, h \in \mathbf{R}$ tais que

$$f = f_0 + \lambda_1 f_1 + \cdots + \lambda_r f_r ,$$

$$g = g_0 + \beta_1 f_1 + \cdots + \beta_s f_s ,$$

$$h = h_0 + \gamma_1 f_1 + \cdots + \gamma_t f_t ,$$

$r < s$ e $1 \leq t$. Assim, $\rho(f) = \rho_r < \rho_s = \rho(g)$. Se $f = 0$ o Axioma (IV) é satisfeito. Suponha que $f \neq 0$. Logo, $s \geq 1$. Para $1 \leq i \leq s$ temos que $f_i h \in L_{l(t,i)}$ e $g_0 h \in L_{l(t,0)}$, pois $L_{l(0,i)} \subseteq L_{l(1,i)} \subseteq L_{l(t,i)}$. Portanto, $gh \in L_{l(t,s)}$. Pelo mesmo raciocínio, temos que

$fh \in L_{l(t,r)}$. Por hipótese, $l(i,j) < l(i+1,j)$ para todo $j \in \mathbf{N}$. Assim, como $t \geq 1$ segue que $t \in \mathbf{N}$ e, portanto,

$$l(t,r) < l(t,r+1) < l(t,r+2) < \cdots .$$

Consequentemente,

$$l(t,r) < \cdots < l(t,s-1) < l(t,s)$$

pois $r \leq s-1 < s$. Isto nos mostra que,

$$\rho(fh) \leq \rho_{l(t,r)} < \rho_{l(t,s)} = \rho(gh)$$

onde a última igualdade vale pois $gh \in L_{l(t,s)} \backslash L_{(t,s-1)}$. Do contrário, $f_s f_t \in L_{l(t,s-1)}$ o que é um absurdo. Logo, podemos concluir que ρ é função ordem fraca. Agora veremos que ρ é função peso sobre $\mathbf{R}$. Já sabemos que $1 \leq s,t$. Se $\rho_{l(i,j)} = \rho_i + \rho_j$ para todo $i,j \in \mathbf{N}$ então

$$\rho(gh) = \rho_{l(t,s)} = \rho_t + \rho_s = \rho(h) + \rho(g) = \rho(g) + \rho(h).$$

Isto mostra que ρ é função peso. □

Com isto podemos justificar que nossos exemplos anteriores são funções ordens fracas. Em cada um dos exemplos, devemos mostrar a condição imposta sobre $l(i,j)$.

(1) Justificando Exemplo 2.5:
Sejam $f_i = X^a Y^b \prec f_{i+1} = X^c Y^d$ e $f_j = X^r Y^s$ com $2 \leq r+s$. Assim, é fácil ver que

$$f_i f_j \prec f_{i+1} f_j$$

para todo $i,j \in \mathbf{N}_0$, pois $(a+r)+(b+s) < (c+r)+(d+s)$ ou $(a+r,b+s) \preceq_L (c+r,d+s)$ se $(a+r)+(b+s) = (c+r)+(d+s)$. Logo, $l(i,j) < l(i+1,j)$. □

(2) Justificando Exemplo 2.10:
Lembremos que $f_i = y^i$ para todo $i \geq 1$, $f_0 \in K[x]$ e $xy = 1$. Também, $\rho(f_i) = \deg_y(f_i)$. Assim, se $1 \leq j$ então

$$\begin{aligned} \rho(f_i f_j) &= \deg_y(f_i f_j) \\ &\leq \deg_y(f_i) + \deg_y(f_j) \\ &< \deg_y(f_{i+1}) + \deg(f_j) \\ &= \deg_y(f_{i+1} f_j) \\ &= \rho(f_{i+1} f_j). \end{aligned}$$

Logo, $l(i,j) < l(i+1,j)$. Se $j = 0$, é imediato que

$$\rho(f_i f_j) = \deg_y(f_i f_0) \leq \deg_y(f_{i+1} f_0) = \rho(f_{i+1} f_0).$$

Portanto, $l(i,0) \leq l(i+1,0)$. □

Agora, vamos fazer algumas considerações com o objetivo de se determinar uma K-base para $\mathbf{R}$ por meio de funções ordens fracas. Recordemos que, se ρ é uma função ordem fraca sobre $\mathbf{R}$ então existe um subconjunto $F = \{f_i : i \in \mathbf{N}\} \subseteq \mathcal{M}$, linearmente independente sobre K, tal que

$$\mathbf{R} = \widetilde{\mathcal{U}_\rho} \oplus \langle F \rangle .$$

Portanto, ρ gerou um conjunto linearmente independente sobre K, que por sua vez pode ser completado gerando uma K-base de $\mathbf{R}$. Agora, imagine que σ é uma outra função ordem fraca sobre $\mathbf{R}$ tal que $\mathcal{U}_\rho \nsubseteq \mathcal{U}_\sigma$, isto é, $\mathcal{U}_\rho \cap \mathcal{M}_\sigma \neq \emptyset$. Em alguns exemplos, vimos que $\widetilde{\mathcal{U}_\rho}$ não é um anel. Particularizando, admita que $\widetilde{\mathcal{U}_\rho}$ é um anel. Logo, $\sigma_1 := \sigma\big|_{\widetilde{\mathcal{U}_\rho}}$ é função ordem fraca sobre $\widetilde{\mathcal{U}_\rho}$ com $\mathcal{U}_{\sigma_1} = \mathcal{U}_\rho \cap \mathcal{U}_\sigma$. Assim, existe $G = \{g_i : i \in \mathbf{N}\} \subseteq \mathcal{M}_{\sigma_1} = \mathcal{M}_\sigma \cap \widetilde{\mathcal{U}_\rho}$, linearmente independente sobre K, tal que $\widetilde{\mathcal{U}_\rho} = \widetilde{\mathcal{U}_{\sigma_1}} \oplus \langle G \rangle$. Portanto,

$$\mathbf{R} = \widetilde{\mathcal{U}_{\sigma_1}} \oplus \langle G \rangle \oplus \langle F \rangle = \widetilde{\mathcal{U}_\rho \cap \mathcal{U}_\sigma} \oplus \langle G \rangle \oplus \langle F \rangle .$$

Se $\mathcal{U}_\rho \cap \mathcal{U}_\sigma = K^*$ então

$$\mathbf{R} = K \oplus \langle G \rangle \oplus \langle F \rangle ,$$

e portanto ρ e σ "geram"uma K-base de $\mathbf{R}$. Esta análise motiva a próxima definição e também nos faz entender as condições suficientes que aparecem no teorema abaixo.

Definição 2.19 *Dizemos que uma função ordem fraca ρ sobre $\mathbf{R}$, tem a* **propriedade de anel** *quando $\widetilde{\mathcal{U}_\rho}$ é um subanel de $\mathbf{R}$.*

Agora vamos construir uma K-base de $\mathbf{R}$. O próximo resultado generaliza o ítem (1) do Teorema 1.11.

Teorema 2.20 *Sejam $\rho_1, \cdots, \rho_n$ funções ordens fracas sobre $\mathbf{R}$ com a propriedade de anel, $\mathcal{U}_i = \mathcal{U}_{\rho_i}$ e $\mathcal{M}_i = \mathcal{M}_{\rho_i}$ para $1 \leq i \leq n$. Suponha que*

$$\mathbf{R}^* \supsetneq \mathcal{U}_1 \supsetneq \mathcal{U}_1 \cap \mathcal{U}_2 \supsetneq \cdots \supsetneq \mathcal{U}_1 \cap \cdots \cap \mathcal{U}_n = K^*.$$

Então, existem $F_1 := \{f_{1j} : j \in \mathbf{N}\} \subseteq \mathcal{M}_1$ e $F_i := \{f_{ij} : j \in \mathbf{N}\} \subseteq (\mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{i-1}) \cap \mathcal{M}_i$ para $2 \leq i \leq n$ tais que:

(1) $\rho_i(f_{ij}) < \rho_i(f_{i(j+1)})$ *para* $1 \leq i \leq n$ *e* $j \in \mathbf{N}$*;*

(2) $\rho_1(F_1) = \rho_1(\mathcal{M}_1)$ *e* $\rho_i(F_i) = \rho_i(\mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i)$*;*

(3) O conjunto $F_1 \cup \cdots \cup F_n \cup \{1\}$ *forma uma* K*-base de* $\mathbf{R}$*. Ou seja,*

$$\mathbf{R} = \langle F_1 \rangle \oplus \cdots \langle F_n \rangle \oplus \langle 1 \rangle .$$

Prova. Provaremos usando indução sobre n. Se $n = 1$, então $\mathcal{U}_1 = K^*$ e portanto ρ_1 é uma função ordem sobre $\mathbf{R}$ (Lema 2.12). Pelo Teorema 1.11(1) segue o resultado. Admita, por hipótese de indução que o resultado é verdadeiro para $m < n$. Aplicando o Teorema 2.17 para ρ_1, temos que existe $F_1 = \{f_{1j} : j \in \mathbf{N}\} \subseteq \mathcal{M}_1$, linearmente independente sobre K, tal que

$$\rho_1(f_{1j}) < \rho_1(f_{1(j+1)}) \quad \text{e}$$
$$\mathbf{R} = \langle F_1 \rangle \oplus \widetilde{\mathcal{U}_1} \, . \tag{2.1}$$

Agora, para $2 \leq i \leq n$ considere $\rho_i' := \rho_i\big|_{\widetilde{\mathcal{U}_1}}$. Assim, $\rho_2', \cdots, \rho_n'$ são funções ordens fracas sobre $\widetilde{\mathcal{U}_1}$, com a propriedade de anel, tais que

$$\mathcal{U}_i' := \mathcal{U}_{\rho_i'} = \mathcal{U}_1 \cap \mathcal{U}_i \quad \text{e} \quad \mathcal{M}_i' := \mathcal{M}_{\rho_i'} = \mathcal{U}_1 \cap \mathcal{M}_i.$$

Logo,

$$\mathcal{U}_2' \cap \cdots \cap \mathcal{U}_i' = \mathcal{U}_1 \cap \mathcal{U}_2 \cap \cdots \mathcal{U}_i$$

e portanto

$$\widetilde{\mathcal{U}_1}^* \supsetneq \mathcal{U}_2' \supsetneq \cdots \supsetneq \mathcal{U}_2' \cap \cdots \cap \mathcal{U}_n' = K^*$$

pois

$$\widetilde{\mathcal{U}_1}^* = \mathcal{U}_1 \supsetneq \mathcal{U}_1 \cap \mathcal{U}_2 \supsetneq \cdots \supsetneq \mathcal{U}_1 \cap \cdots \cap \mathcal{U}_n = K^*.$$

Pela hipótese de indução, existem

$$F_2 = \{f_{2j} : j \in \mathbf{N}\} \subseteq \mathcal{M}_2' = \mathcal{U}_1 \cap \mathcal{M}_2 \quad \text{e}$$

$$F_i = \{f_{ij} : j \in \mathbf{N}\} \subseteq \mathcal{U}_2' \cap \cdots \cap \mathcal{U}_{i-1}' \cap \mathcal{M}_i' = \mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i$$

para $3 \leq i \leq n$ tais que

$$\rho_i(f_{ij}) = \rho_i'(f_{ij}) < \rho_i'(f_{i(j+1)}) = \rho_i(f_{i(j+1)}) \quad \text{e}$$

$$\rho_i(F_i) = \rho_i'(F_i) = \rho_i'(\mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i) = \rho_i(\mathcal{U}_1 \cap \cdots \cap \mathcal{U}_{i-1} \cap \mathcal{M}_i)$$

para todo $2 \leq i \leq n$. Mais ainda,

$$F_2 \cup \cdots \cup F_n \cup \{1\}$$

é uma K-base de $\widetilde{\mathcal{U}_1}$. Portanto, da equação 2.1 segue que

$$F_1 \cup F_2 \cup \cdots \cup F_n \cup \{1\}$$

gera $\mathbf{R}$. Para terminar, vamos mostrar que o conjunto acima é linearmente independente. Sejam $f = \sum_{j=1}^{r_1} \alpha_{1j} f_{1j} \in \langle F_1 \rangle$ e $g = \sum_{i=2}^{n} \sum_{j=1}^{r_i} \alpha_{ij} f_{ij} \in \langle F_2 \cup \cdots \cup F_n \{1\} \rangle = \widetilde{\mathcal{U}_1}$ tais que

$$\sum_{j=1}^{r_1} \alpha_{1j} f_{1j} + \sum_{i=2}^{n} \sum_{j=1}^{r_i} \alpha_{ij} f_{ij} = 0.$$

Sem perda de generalidade, suponha que $\alpha_{1r_1} \neq 0$. Então, pelos Axioma (II) e (III), temos que

$$0 \leq \rho_1(1) < \rho_1(f_{1r_1}) = \rho_1(\alpha_{1r_1} f_{1r_1}) = \rho_1(f) = \rho_1(f+g) = \rho_1(0) = -\infty.$$

Contradição. Assim, $\alpha_{1r_1} = 0$. Pelo mesmo raciocínio, segue que $\alpha_{11} = \cdots = \alpha_{1(r_1-1)} = 0$. Como $F_2 \cup \cdots \cup F_n \cup \{1\}$ é um conjunto linearmente independente sobre K, segue que $\alpha_{ij} = 0$ para todo $2 \leq i \leq n$ e $1 \leq j \leq r_i$. Portanto, $F_1 \cup F_2 \cup \cdots \cup F_n \cup \{1\}$ é uma K-base de $\mathbf{R}$. □

Capítulo 3

Sobre a Distância Mínima de Códigos bi-Pontuais

Neste capítulo, utilizaremos as funções ordens fracas para construirmos códigos em m pontos, da mesma forma que Høholdt, van Lint e Pellikaan fizeram utilizando funções ordens. Aqui, também apresentaremos uma cota para a distância mínima dos códigos duais que construiremos e veremos exemplos onde esta cota é melhor do que a cota de Goppa.

Primeiro vamos estudar o caso $m = 2$ para em seguida fazermos a generalização. Para isso, vamos fixar alguns elementos. Seja $\mathbf{R}$ a K-álgebra vista no Exemplo 2.4. Recordando, seja $K(\mathcal{X})$ o corpo de funções de uma curva $\mathcal{X}$ sobre K de gênero g. Sejam P e Q pontos K-racionais. Seja $\mathbf{R} := R(P, Q)$ a K-álgebra dada pela interseção dos anéis locais $\mathcal{O}_S$ de $K(\mathcal{X})$, nos pontos S, com $S \neq P$ e $S \neq Q$. Seja $v := v_P$ a valorização em P e ρ a função ordem fraca definida por

$$\rho(f) := \begin{cases} -\infty, & \text{se } f = 0 \\ 0, & \text{se } v(f) \geq 0 \text{ e } f \neq 0 \\ -v(f), & \text{se } v(f) < 0 \end{cases}$$

para $f \in \mathbf{R}$. Na verdade, ρ é função peso fraco sobre $\mathbf{R}$. Da mesma forma, assossiada ao ponto Q, definimos σ. Assim, $\mathcal{U}_\rho = R(Q)^*$, $\mathcal{U}_\sigma = R(P)^*$ e

$$\mathcal{U}_\rho \cap \mathcal{U}_\sigma = K^*.$$

Logo,

$$\mathbf{R}^* \supsetneq \mathcal{U}_\rho \supsetneq \mathcal{U}_\rho \cap \mathcal{U}_\sigma = K^*.$$

Aplicando o Teorema 2.20, existe $F \cup G_1 \cup \{1\} \subseteq \mathbf{R}$ uma K-base de $\mathbf{R}$ tal que:

$$\begin{cases} \begin{cases} F = \{f_i : i \in \mathbf{N}\} \subseteq \mathcal{M}_\rho \\ \rho(f_i) < \rho(f_{i+1}) \\ \rho(F) = \rho(\mathcal{M}_\rho) \end{cases} \\ \begin{cases} G_1 = \{g_i : i \in \mathbf{N}\} \subseteq \mathcal{U}_\rho \cap \mathcal{M}_\sigma = R(Q)^* \cap \mathcal{M}_\sigma = R(Q)\backslash K \\ \sigma(g_i) < \sigma(g_{i+1}) \\ \sigma(G_1) = \sigma(\mathcal{U}_\rho \cap \mathcal{M}_\sigma) = \sigma(R(Q)\backslash K) \end{cases} \\ \begin{cases} \mathbf{R} = \langle F \rangle \oplus \langle G_1 \rangle \oplus \langle 1 \rangle \\ \quad = \langle f_0, f_1, f_2, \cdots \rangle \oplus \langle g_1, g_2, g_3, \cdots \rangle \quad \text{onde} \quad f_0 = 1. \end{cases} \end{cases} \tag{3.1}$$

O próximo lema relaciona os elementos da base com elementos do semigrupo de Weierstrass em P, Q e (P, Q).

Lema 3.1
(1) $\rho(\mathcal{M}_\rho) = \mathbf{N}$*;*
(2) $\sigma(\mathcal{U}_\rho \cap \mathcal{M}_\sigma) = \sigma(R(Q)\backslash K) = H(Q)^*$.

Prova. (1) Da definição, é imediato que $\rho(\mathcal{M}_\rho) \subseteq \mathbf{N}$. Agora, seja $n \in \mathbf{N}$. Se $n \in H(P)$, então existe $f \in K(\mathcal{X})$ tal que $\text{div}_\infty(f) = nP$. Assim, $f \in R(P) \subseteq R(P, Q) = \mathbf{R}$ e $\rho(f) = n$. Caso $n \in G(P)$, então existe $m \in G(Q)$ tal que $(n, m) \in H(P, Q)$ e $m = Min\{s \in \mathbf{N} : (n, s) \in H(P, Q)\}$ (seção 1.1). Em outras palavras, existe $f \in K(\mathcal{X})$ tal que $\text{div}_\infty(f) = nP + mQ$. Logo, $f \in \mathbf{R}$ e $\rho(f) = n$. Portanto, $\rho(\mathcal{M}_\rho) = \mathbf{N}$.

(2) Imediato. □

Ainda estabelecendo as condições sobre os elementos de F e G_1, suponha que $H(Q) = \{0 < m_1 < m_2 < \cdots\}$. De acordo com a demonstração do lema anterior, para todo $i \in \mathbf{N}$

temos:

$$\begin{cases} \rho(f_i) = i \\ \\ \sigma(f_i) = \begin{cases} 0 & \text{se } i \in H(P) \\ Min\{a : (i,a) \in H(P,Q)\} \in G(Q) & \text{se } i \in G(P) \end{cases} \\ \\ \sigma(g_i) = m_i \ . \end{cases} \tag{3.2}$$

De agora em diante, consideramos as funções $f_i, g_i \in \mathbf{R} = R(P,Q)$ satisfazendo as condições dadas em (3.1) e (3.2). Também, considere que

$$G(Q) = \{l'_1 < \cdots < l'_g\}.$$

Seja G um divisor sobre a curva $\mathcal{X}$.

A prova da proposição a seguir nos permitirá fazer a conexão entre códigos avaliados e códigos geométricos de Goppa (equação 3.5). Como consequência, exibiremos uma cota para a distância mínima dos mesmos (Teorema 3.9). Também, a proposição seguinte juntamente com o Teorema 3.9 nos fornecerá um caminho na busca por códigos MDS (Corolário 3.11). No entanto, o resultado da proposição a seguir é interessante por si só.

Proposição 3.2 *Se $G = lP + mQ$ e $l'_g \leq m$ então*

$$\ell(G) = deg(G) + 1 - g.$$

Prova. Sabemos que $\mathcal{L}(G) \subseteq \mathbf{R}$ e que $F \cup G_1 \cup \{1\}$ $(*)$ é uma K-base de $\mathbf{R}$. Vamos mostrar que $A := \{f_0, \cdots, f_l\} \cup \{g_j : m_j \leq m\}$ é uma K-base de $\mathcal{L}(G)$. Já sabemos que o conjunto é linearmente independente. Da construção de f_i e g_j, é imediato que $A \subseteq \mathcal{L}(G)$. Resta-nos mostrar que o conjunto A gera $\mathcal{L}(G)$. Seja $f \in \mathcal{L}(G)$. Logo, $f \in \mathbf{R}$. De $(*)$, existem $i \in \mathbf{N}_0$, $j \in \mathbf{N}$, $\lambda_1, \cdots, \lambda_i \in K$ e $\gamma_1, \cdots, \gamma_j \in K$ tais que

$$f = \lambda_0 f_0 + \cdots + \lambda_i f_i + \gamma_1 g_1 + \cdots + \gamma_j g_j.$$

Sem perda de generalidade, suponha que $\lambda_i \neq 0$. Assim,

$$i = \rho(f_i) = \rho(f) = \begin{cases} 0, & \text{se} \quad i = 0 \\ -v_P(f), & \text{se} \quad i \geq 1. \end{cases}$$

Como $-v_P(f) \leq l$, pois $f \in \mathcal{L}(G)$, segue que

$$i \leq l. \qquad (*_1)$$

Também, sem perda de generalidade, suponha que $\gamma_j \neq 0$. Assim,

$$m_j = \sigma(g_j) = \sigma(\gamma_1 g_1 + \cdots + \gamma_j g_j) = \sigma(f - (\lambda_0 f_0 + \cdots + \lambda_i f_i)).$$

Agora,

$$\sigma(f) = \begin{cases} 0, & \text{se} \quad v_Q(f) \geq 0 \\ -v_Q(f), & \text{se} \quad v_Q(f) < 0. \end{cases}$$

Disto e do fato de f estar em $\mathcal{L}(G)$, segue que $\sigma(f) \leq m$. Lembre que, por construção, $\sigma(f_i) \leq l'_g$ para todo $i \in \mathbf{N}_0$. Consequentemente, $\sigma(\lambda_0 f_0 + \cdots + \lambda_i f_i) \leq l'_g$. Portanto,

$$\begin{aligned} m_j &= \sigma(f - (\lambda_0 f_0 + \cdots + \lambda_i f_i)) \\ &\leq Max\{\sigma(f), \sigma(\lambda_0 f_0 + \cdots + \lambda_i f_i)\} \\ &\leq Max\{m, l'_g\} = m. \qquad (*_2) \end{aligned}$$

Logo, $(*_1)$ e $(*_2)$ nos mostram que A gera $\mathcal{L}(G)$. Assim sendo,

$$\begin{aligned} \ell(G) &= \#A \\ &= (l+1) + \#\{g_j : m_j \leq m\} \end{aligned}$$

Agora, $l'_g \leq m$ nos diz que existem exatamente $(m-g)$ elementos no conjunto $\{g_j : m_j \leq m\}$. De fato, existem exatamente $(m-g)$ elementos m_j, maiores que 1 e menores ou iguais a m (tiramos as g lacunas). Portanto,

$$\ell(G) = (l+1) + (m-g) = deg(G) + 1 - g.$$

□

Corolário 3.3 *Se $G = lP + mQ$ e $l'_g \leq m$ então*

$$\ell(W - G) = 0,$$

onde W é um divisor canônico.

Prova. Segue da Proposição 3.2 e do Teorema de Riemann-Roch. □

Observação 3.4 *O resultado do corolário anterior já era conhecido sempre que $2g-1 \leq l+m$. O corolário anterior nos diz que podemos ter $l+m < 2g-1$, mas ainda $\ell(W-G) = 0$ se $l'_g \leq m$.*

Agora vamos fazer uma **aplicação aos Códigos Geométricos de Goppa**, assim como fizeram Høholdt, van Lint e Pellikaan na Subseção 1.2.2. Só que no nosso caso os códigos serão bi-pontuais.

De agora em diante, vamos trabalhar com $K = \mathbf{F}_q$.

Sejam $P_1, \cdots, P_n$ pontos $\mathbf{F}_q$-racionais de $\mathcal{X}$, diferentes dois a dois, e diferentes de P e Q.

Consideremos $m \in \mathbf{N}$. Seja $a \in \mathbf{N}$ tal que $m_a \leq m < m_{a+1}$.

Considere, como na Subseção 1.2.2, o morfismo de $\mathbf{F}_q$-álgebras

$$\begin{array}{rccc} \varphi: & \langle f_0, f_1, \cdots \rangle \oplus \langle g_1, g_2, \cdots \rangle & \longrightarrow & \mathbf{F}_q^n \\ & f & \longmapsto & (f(P_1), \cdots, f(P_n)) \,. \end{array}$$

Para $l \in \mathbf{N}_0$, sejam

$$L_l := \langle f_0, \cdots, f_l \rangle \oplus \langle g_1, \cdots, g_a \rangle \,,$$

$$E_l := \varphi(L_l),$$

$$C_l := E_l^{\perp}.$$

Logo, existe $N \in \mathbf{N}$ tal que $E_N = E_l$ e $C_N = C_l$ para todo $N \leq l$. Assim,

$$E_0 \subseteq E_1 \subseteq \cdots \subseteq E_N \subseteq \mathbf{F}_q^n$$

$$C_0 \supseteq C_1 \supseteq \cdots \supseteq C_N \supseteq \{0\}.$$

Para $l, s \in \mathbf{N}$, sejam

$$c(s) := Max\{\sigma(f_0), \cdots, \sigma(f_s)\},$$

$$N(l,m) := \{(i,j) \in \mathbf{N}_0^2 : i + j = l + 1 \quad \wedge \quad \sigma(f_i) + c(j) < m + 1\},$$

$$\nu(l,m) := \#N(l,m).$$

Mais adiante exploraremos as propriedades das funções numéricas $c(s)$ e $\nu(l,m)$.

Admita que

$$N(l,m) = \{(i_1, j_1), \cdots, (i_t, j_t)\}$$

com $i_1 < \cdots < i_t$. Logo, $j_1 > \cdots > j_t$.

Por outro lado, para $y \in \mathbf{F}_q^n$ recordemos que

$$\omega(y) \geq posto\left(S(y)\right),$$

onde $S(y) = \left(s_{ij}(y) = y \cdot (h_i * h_j) : 1 \leq i, j \leq N\right)$ e $h_i = \varphi(f_i)$ (Lema 1.20).

Fixemos $l \in \mathbf{N}$ tal que

$$l + 1 < N.$$

Agora estamos prontos para provar um resultado de fundamental importância na determinação de uma cota para a distância mínima do código C_l.

Proposição 3.5 *Se* $y \in C_l \backslash C_{l+1}$ *então*

$$\omega(y) \geq \nu(l, m).$$

Prova. Seja $(i_u, j_u) \in N(l, m)$.

Primeiro, vamos mostrar que $s_{i_u j_v} = 0$ se $t \geq v > u \geq 1$. De fato, como $(i_u, j_u) \in N(l, m)$ então

$$i_u + j_u = l + 1 \quad \text{e} \quad \sigma(f_{i_u}) + \sigma(f_{j_v}) \leq m$$

se $v > u$. Em outras palavras,

$$i_u + j_v \leq l \quad \text{e} \quad \sigma(f_{i_u} f_{j_v}) \leq \sigma(f_{i_u}) + \sigma(f_{j_v}) \leq m$$

se $v > u$. Logo, $f_{i_u} f_{j_v} \in L_l$ se $v > u$. Isto nos mostra que $\varphi(f_{i_u} f_{j_v}) \in E_l$ se $v > u$ e, portanto,

$$s_{i_u j_v}(y) = y \cdot \varphi(f_{i_u} f_{j_v}) = 0,$$

pois $y \in C_l$.

Agora, vamos mostrar que $s_{i_u j_u}(y) \neq 0$. Neste caso, recordemos que

$$i_u + j_u = l + 1 \quad \text{e} \quad \sigma(f_{i_u} f_{j_u}) \leq \sigma(f_{i_u}) + \sigma(f_{j_u}) \leq m.$$

Isto nos mostra que $f_{i_u} f_{j_u} \in L_{l+1} \backslash L_l$. Assim, existem $\lambda_{l+1} \in \mathbf{F}_q^*$ e $f \in L_l$ tais que

$$f_{i_u} f_{j_u} = \lambda_{l+1} f_{l+1} + f.$$

Logo,

$$\begin{aligned} s_{i_u j_u}(y) &= y \cdot \varphi(f_{i_u} f_{j_u}) \\ &= \lambda_{l+1} y \cdot \varphi(f_{l+1}) + y \cdot \varphi(f) \\ &= \lambda_{l+1} y \cdot \varphi(f_{l+1}) \neq 0 \end{aligned}$$

pois $y \notin C_{l+1}$ e $\lambda_{l+1} \neq 0$.

Para finalizar, vamos mostrar que

$$posto\,(S(y)) \geq t.$$

Aplicando operações elementares sobre a matriz $S(y)$, primeiro coloque as linhas $i_1, \cdots, i_t$ como as t primeiras linhas e em seguida coloque as colunas $j_t, \cdots, j_1$ como as t primeiras colunas. Assim, temos que

$$S(y) = (s_{ij}(y)) \sim \begin{pmatrix} s_{i_1 j_t}(y) & s_{i_1 j_{t-1}}(y) & \cdots & s_{i_1 j_2}(y) & s_{i_1 j_1}(y) & \cdots \\ s_{i_2 j_t}(y) & s_{i_2 j_{t-1}}(y) & \cdots & s_{i_2 j_2}(y) & & \\ \vdots & \vdots & \cdot & & & \\ s_{i_{t-1} j_t}(y) & s_{i_{t-1} j_{t-1}} & & & & \\ s_{i_t j_t}(y) & & & & & \\ \vdots & & & & & \end{pmatrix}.$$

Se $y \in C_l \backslash C_{l+1}$, dos dois parágrafos anteriores segue que

$$S(y) \sim \begin{pmatrix} 0 & 0 & \cdots & 0 & \underbrace{s_{i_1 j_1}(y)}_{\neq 0} & \cdots \\ 0 & 0 & \cdots & \underbrace{s_{i_2 j_2}(y)}_{\neq 0} & & \\ \vdots & \vdots & \cdot & & & \\ 0 & \underbrace{s_{i_{t-1} j_{t-1}}}_{\neq 0} & & & & \\ \underbrace{s_{i_t j_t}(y)}_{\neq 0} & & & & & \\ \vdots & & & & & \end{pmatrix}.$$

Portanto,

$$\omega(y) \geq posto\,(S(y)) \geq t = \nu(l, m).$$

□

Note que o morfismo $\varphi : R(P, Q) \longrightarrow \mathbf{F}_q^n$ é sobrejetor pois $\varphi\big|_{R(P)}$ é sobrejetor. Assim, $E_N = \mathbf{F}_q^n$ e $C_N = \{0\}$. Logo, podemos fazer a seguinte definição.

Definição 3.6 *Sejam $l, m \in \mathbf{N}$ tal que $l+1 < N$. O número $d(l,m)$ é chamado de* **cota ordem fraca** *onde*

$$d(l,m) := Min\{\nu(r,m) : r \geq l\}.$$

Teorema 3.7 *O número $d(l,m)$ é uma cota inferior para a distância mínima de C_l, isto é,*

$$d(C_l) \geq d(l,m).$$

Prova. O teorema é consequência direta da Definição 3.6 e da Proposição 3.5. □

Observação 3.8 *Note que o número $d(l,m)$ depende, exclusivamente, da K-base $F \cup G_1 \cup \{1\}$ de $R(P,Q)$, pois $N(l,m)$, e consequentemente $\nu(l,m)$, depende de $F \cup G_1 \cup \{1\}$. No caso de Høholdt, van Lint e Pellikaan isto não acontecia. A justificativa para isto, é que no caso deles, a imagem da K-base $\{f_i : i \in \mathbf{N}_0\}$ de $\mathbf{R}$ pela função ordem ρ é invariante. Já no nosso caso, a imagem dos elementos $f_i \in F$ pela aplicação ρ é invariante, PORÉM, a imagem dos mesmos pela aplicação σ não é invariante (veja Observação 2.15).*

Com o objetivo de comparar o número $d(l,m)$ com a cota de Goppa d_G (Teorema 3.9), vamos, neste momento, dar uma expressão para o mesmo. Para isto, vamos examinar o conjunto $N(l,m)$. Primeiro, vamos fixar o conjunto das lacunas de P por

$$G(P) = \{l_1 < \cdots < l_g\}.$$

Recorde que já definimos o conjunto das lacunas de Q por

$$G(Q) = \{l'_1 < \cdots < l'_g\}.$$

Observe que

$$\nu(l,m) \leq l+2.$$

De agora em diante, **considere**

$$l'_g \leq m.$$

Assim, $(i,j) \in N(l,m)$ sempre que $i+j = l+1$ e $i \in H(P)$. De fato, neste caso

$$\sigma(f_i) + c(j) = 0 + c(j) \leq l'_g \leq m.$$

Portanto, para determinar $N(l,m)$ basta verificar se o par $(l_i, l+1-l_i) \in N(l,m)$ para todo $l_i \leq l$. Disto, concluímos que

$$\nu(l,m) = l+2 - \#\{l_i \leq l : (l_i, l+1-l_i) \notin \mathbf{N}(l,m)\}. \tag{3.3}$$

Para podermos formalizar o que dissemos acima, lembre que Kim [13] mostrou a existência de uma permutação τ de $\{1, \cdots, g\}$ tal que $\left(l_i, l'_{\tau(i)}\right) \in H(P,Q)$ e $l'_{\tau(i)} = Min\{s : (l_i, s) \in H(P,Q)\}$. Então

$$\Gamma(P,Q) := \left\{(l_1, l'_{\tau(1)}), \cdots, (l_g, l'_{\tau(g)})\right\}.$$

O estudo de $N(l,m)$ passa, primeiro, pelo estudo de $c(s)$. Lembre que

$$c(s) = Max\{\sigma(f_0), \cdots, \sigma(f_s)\}.$$

Esta função tem as seguintes propriedades:

(1) $c(s) = Max\{l'_{\tau(i)} : l_i \leq s\}$;

(2) $c(s) = l'_g$ se $s \geq l_g$;

(3) $c(1) = l'_{\tau(1)}$;

(4) $c(s)$ é não-decrescente: $c(s) \leq c(s')$ se $s \leq s'$.

Agora, para $l \in N$ e $m \in N_0$ definimos:

$$B(l,m) := \left\{ l_i \in G(P) : l_i \leq l \quad \wedge \quad l'_{\tau(i)} + c(l+1-l_i) \geq m+1 \right\};$$

$$b(l,m) := \#B(l,m).$$

A função $b(l,m)$ tem as seguintes propriedades:

(i) $0 \leq b(l,m) \leq g$;

(ii) $b(l,0) = g$ se $l \geq l_g$;

(iii) $b(1,m) = \begin{cases} 0 & \text{se} \quad 2l'_{\tau(1)} < m+1 \\ 1 & \text{se} \quad 2l'_{\tau(1)} \geq m+1; \end{cases}$

(iv) $b(l,m+1) \leq b(l,m) \leq b(l+1,m)$.

É imediato da definição de $b(l,m)$ e da equação 3.3 que

$$\nu(l,m) = l + 2 - b(l,m).$$

Portanto,

$$\begin{aligned} d(l,m) &= Min\{\nu(j,m) : j \geq l\} \\ &= Min\{j + 2 - b(j,m) : j \geq l\}. \end{aligned}$$

Como $b(j,m) \leq g$ para todo $j \geq 1$, temos que

$$j + 2 - b(j,m) \geq j + 2 - g \geq l + 2 - b(l,m),$$

sempre que $j \geq l + g - b(l,m)$. Isto nos mostra que

$$d(l,m) = Min\{j + 2 - b(j,m) : l \leq j \leq l + g - b(l,m)\}. \tag{3.4}$$

Com o objetivo de ver o código C_l como um código de Goppa, note que a prova da Proposição 3.2 nos mostra que

$$L_l = \mathcal{L}(lP + mQ),$$

e portanto

$$C_l = C_\Omega(D, lP + mQ). \tag{3.5}$$

Desta forma, assim como fizeram Høholdt, van Lint e Pellikaan, podemos comparar $d(l,m)$ com $d_G(l,m) = l + m - (2g-2)$. Veremos que em algumas situações, $d(l,m) > d_G(l,m)$.

Agora, vamos enunciar o Teorema Principal deste capítulo.

Teorema 3.9 *Seja $G = lP+mQ$ tal que $l'_g \leq m$ e $l+m < n$. Então $C := C_\Omega(D,G) \neq \{0\}$ e*

$$d(C) \geq d(l,m).$$

Além disso, se $d(l,m) = j + 2 - b(j,m)$, para algum j onde $l \leq j \leq l + g - b(l,m)$ e $m \leq 2g + (j-l) - b(j,m)$ então

$$d(C) \geq d(l,m) \geq d_G(l,m).$$

Prova. A condição $l + m < n$ nos mostra que o morfismo $\varphi\big|_{L_l}$ não é sobrejetor. Assim, $E_l \subsetneq \mathbf{F}_q^n$ e, portanto, $C_l \neq \{0\}$. A condição $l'_g \leq m$ implica que $C = C_l$ (equação (3.5)) e que $d(C) \geq d(l,m)$ (Teorema 3.7).

Agora, das condições $d(l,m) = j + 2 - b(j,m)$ e $m \leq 2g + (j-l) - b(j,m)$ é imediato que $d(l,m) \geq d_G(l,m)$. □

Corolário 3.10 *Considere o código C do Teorema 3.9. Se $k = \dim C$, então*

$$k = n - \ell(G).$$

Prova. Como C é o dual de $C_{\mathcal{L}}(D, G)$, então

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

Por outro lado, Goppa mostrou que

$$\dim C_{\mathcal{L}}(D, G) = \ell(G) - \ell(G - D) = \ell(G),$$

pois $\deg G = l + m < n = \deg D$. Logo,

$$k = n - \ell(G).$$

□

Corolário 3.11 *Considere o código C do Teorema 3.9. Se d denota a distância mínima de C, então*

$$d(l, m) \leq d \leq n - k + 1 = l + 2 + (m - g).$$

Em particular, quando $d(l, m) = l + 2$ temos

$$l + 2 \leq d \leq l + 2 + (m - g).$$

Se além disso, $m = g$ então o código C é MDS.

Prova. A desigualdade $d(l, m) \leq d$ segue do Teorema 3.9. Agora, a desigualdade $d \leq n - k + 1$ é conhecida (Singleton). Já a igualdade $n - k + 1 = l + 2 + (m - g)$ segue do Corolário 3.10 e da Proposição 3.2. □

Observação 3.12 *O Corolário 3.11 nos fornece um caminho a ser seguido na busca por códigos MDS.*

Como nosso método primeiro fixa $m \geq l'_g$ e depois faz l variar, vamos determinar nesse momento uma **cota superior** (condição necessária) para m de acordo com o Teorema 3.9.

Observação 3.13 *Devemos testar os valores de m tais que $l'_g \leq m \leq 2g-1$.*

De fato, da definição (equação (3.4)) é imediato que $d(l,m) = j+2-b(j,m) \leq l+2-b(l,m)$ onde $l \leq j \leq l+g-b(l,m)$. Logo, $(j-l)-b(j,m) \leq -b(l,m)$. Assim, se $m \leq 2g+(j-l)-b(j,m)$ então

$$m \leq 2g+(j-l)-b(j,m) \leq 2g-b(l,m) \leq 2g,$$

e o Teorema 3.9 nos informa que

$$d(l,m) \geq d_G(l,m).$$

Se $m = 2g$, segue que $d(l,m) \leq l+2-b(l,m)$ e $d_G(l,m) = l+2$. Isto nos mostra que $d(l,m) \ngeq d_G(l,m)$. Portanto, devemos testar os valores m tais que $l'_g \leq m \leq 2g-1$.

Finalmente, vamos exibir alguns exemplos onde $d(l,m) > d_G(l,m)$. Recorde que, para se determinar $d(l,m)$ precisamos conhecer $\Gamma(P,Q)$. Em [13] Kim descreve $\Gamma(P,Q)$ em várias situações. Nossos exemplos estão baseados nestes casos. Aqui, n é o número de pontos racionais da curva $\mathcal{X}$ sobre $\mathbf{F}_q$ menos dois (P e Q), D é a soma destes n pontos e p é a característica de $\mathbf{F}_q$. Recorde também que, $G = lP+mQ$ e $C = C_\Omega(D,G)$.

Exemplo 3.14 *[13, Exemplo 2.2] Seja $\mathcal{X}$ uma quártica com $p > 5$; logo $g = 3$. Sejam P e Q pontos $\mathbf{F}_q$-racionais tais que*

$$\Gamma(P,Q) = \{(1,3),(2,1),(4,2)\}.$$

De acordo com a Observação 3.13, devemos testar os valores de m tais que $3 \leq m \leq 5$.
Caso $m = 3$:
Veja que $b(1,3) = 1$, $b(2,3) = b(3,3) = 2$ e que $b(l,3) = 3$ se $l \geq 4$. Logo,

$$d(l,3) = l+2-b(l,3).$$

Portanto, do Teorema 3.9 segue que

$$d(C) \geq d(l,3) > d_G(l,3) = l-1,$$

sempre que $1 \leq l \leq 3$.
Caso $m = 4$:
Neste caso, $b(1,4) = b(2,4) = b(3,4) = 1$ e $b(l,4) = 2$ se $l \geq 4$. Logo,

$$d(l,4) = l+2-b(l,4).$$

Portanto, do Teorema 3.9 segue que

$$d(C) \geq d(l,4) > d_G(l,4) = l,$$

sempre que $1 \leq l \leq 3$.
Caso $m = 5$:
Neste caso não melhoramos a cota de Goppa pois $d(l,5) = l+1 = d_G(l,5)$*, haja visto que* $b(l,5) = 1$ *se* $l \geq 1$.

Exemplo 3.15 *[13, Exemplo 2.3(2)] Seja* $\mathcal{X}$ *uma curva hiperelíptica de gênero* g, $p \neq 2$, P *e* Q *pontos* $\mathbf{F}_q$*-racionais tais que*

$$\Gamma(P,Q) = \{(1,g),(2,g-1),\ldots,(g-1,2),(g,1)\}.$$

De acordo com a Observação 3.13, devemos testar os valores de m *tais que* $g \leq m \leq 2g-1$. *Para* m *nessas condições e* $1 \leq l \leq g$, *temos que* $b(l,m) = l$. *Logo,*

$$d(l,m) = 2.$$

Portanto, do Teorema 3.9 segue que

$$d(C) \geq d(l,m) > d_G(l,m) = 2 + [(l+m) - 2g],$$

sempre que $l + m < 2g$.

No próximo exemplo, apresentamos um código onde a cota obtida para a distância mínima utilizando nosso método é melhor do que a cota encontrada por G. Mattews no Teorema 1.1. O código que apresentamos é um caso particular do Exemplo 3.15.

Exemplo 3.16 *No Exemplo 3.15, temos que*

$$G(P,Q) = \{(a,b) : a+b \leq g\} - \{(0,0)\}.$$

Agora vamos em busca de (a_1,a_2) *e* (n_1,n_2) *que satisfaçam as hipóteses do Teorema 1.1. Veja que* $(a_1,a_2) = (1,2) \in G(P,Q)$ *e* $\ell(P+2Q) = \ell(2Q) = 1$. *Também, para* $(n_1,n_2) = (1,g)$ *temos que* $(n_1, n_2 - t - 1) = (1, g-1-t) \in G(P,Q)$ *para todo* $t = 0,1,\cdots,g-1$. *Portanto, pelo Teorema 1.1 com* $G = (a_1+n_1-1)P + (a_2+n_2-1)Q = P + (g+1)Q$, *temos que a cota obtida por Gretchen é:*

$$d(C) \geq d_G(1,g+1) + 1 = -g + 5.$$

No nosso caso, pelo Exemplo 3.15, temos que

$$d(C) \geq d(1, g+1) = 2.$$

Portanto, para $g \geq 4$ *segue que*

$$d(C) \geq d(1, g+1) > d_G(1, g+1).$$

Exemplo 3.17 *[13, Exemplo 2.3(1)] Seja* $\mathcal{X}$ *uma curva hiperelíptica de gênero* g, $p \neq 2$, P *e* Q *pontos* $\mathbf{F}_q$*-racionais tais que*

$$\Gamma(P, Q) = \{(1,1), \ldots, (g,g)\}.$$

De acordo com a Observação 3.13, devemos testar os valores de m *tais que* $g \leq m \leq 2g-1$. *Neste caso, segue que:*
(1)

$$b(l, m) = 0$$

se $1 \leq l \leq g-1$.

(2)

$$b(l,m) = \begin{cases} g, & se \quad m = g \\ g-1, & se \quad m = g+1 \\ \vdots & \vdots \quad \vdots \\ 2g-l, & se \quad m = l \\ 0, & se \quad l+1 \leq m \leq 2g-1 \end{cases}$$

se $g \leq l \leq 2g-2$.

(3)

$$b(l,m) = \begin{cases} g, & se \quad m = g \\ g-1, & se \quad m = g+1 \\ \vdots & \vdots \quad \vdots \\ 2, & se \quad m = 2g-2 \\ 1, & se \quad m = 2g-1 \end{cases}$$

se $l \geq 2g-1$.

Assim sendo, para $1 \leq l \leq g-1$ *e* $m = g+u$ *onde* $1 \leq u \leq g-1$*, temos que*

$$\begin{aligned} d(l,m) &= Min \quad \{j+2-b(j,m) : l \leq j \leq l+g\} \\ &= Min \quad \big\{Min\{j+2-b(j,g+u) : l \leq j \leq g-1\} \; ; \\ &\qquad\quad Min\{j+2-b(j,g+u) : g \leq j \leq l+g\}\big\} \\ &= Min \quad \big\{Min\{j+2 : l \leq j \leq g-1\} \; ; \\ &\qquad\quad Min\{j+2-(g-u) : g \leq j \leq l+g\}\big\} \\ &= Min \quad \big\{l+2; u+2\big\}. \end{aligned}$$

Ou seja,

$$d(l,m) = \begin{cases} l+2, & se \quad l \leq u \\ u+2, & se \quad l > u \end{cases}$$

Isto nos mostra que

$$d(l,m) \neq l+2-b(l,m)$$

se $l > u$*.*
Do Teorema 3.9 segue que

$$d(C) \geq d(l,m) > d_G(l,m) = l+u+2-g,$$

sempre que $1 \leq l \leq g-1$ *e* $m = g+u$ *com* $1 \leq u \leq g-1$*.*

Para ilustrar o resultado, vamos considerar que $g = 10$ *e* $u = 5, 7$*, isto é,* $m = 15, 17$*. Assim, temos as seguintes tabelas:*

l	1	2	3	4	5	6	7	8	9
$d(l,15)$	3	4	5	6	7	7	7	7	7
$d_G(l,15)$	-2	-1	0	1	2	3	4	5	6

l	1	2	3	4	5	6	7	8	9
$d(l,17)$	3	4	5	6	7	8	9	9	9
$d_G(l,17)$	0	1	2	3	4	5	6	7	8

Agora, mencionaremos alguns problemas que, se resolvidos, deixariam esta tese mais completa.

Propostas para Futuros Trabalhos:

1) Construir códigos geométricos de Goppa m-pontuais e exibir uma cota inferior para a distância mínima dos mesmos via funções ordens fracas.

2) Fazer um estudo sobre a decodificação dos códigos avaliados.

3) Dar uma resposta à pergunta feita na introdução: existe uma caracterização de K-álgebras munidas com funções pesos fracos?

Referências Bibliográficas

[1] A. Aguglia, G. Korchmáros e F. Torres, *Plane maximal curves*, ACTA ARITH. XCVIII.2, 2001.

[2] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of algebraic curves*, Vol. I, Springer-Verlag, 1985.

[3] E. Ballico and S. J. Kim, *Weierstrass multiple loci of n-pointed algebraic curves*, J. Algebra **199**, 455-471, 1998.

[4] C. Carvalho and F. Torres, *On Goppa codes and Weierstrass gaps at several points*, a ser publicado.

[5] F. Delgado, *The symmetry of the Weierstrass generalized semigroups and affine embeddings*, Proc. of the Amer. Math. Soc. **108**(3), 627-631, 1990.

[6] A. Garcia and R. Lax, *Goppa Codes and Weierstrass gaps*, "Coding theory and algebraic geometry", Lectures Notes in Math. **1518**, 33-42, Springer-Verlag, Berlin-Heidelberg, 1992.

[7] G. van der Geer, *Error-correcting codes and curves of finite fields*, "Mathematics Unlimited - 2001 and Beyond", B. Engquist, W. Schmid Eds, 1115-1138, Springer-Verlag, 2001.

[8] V.D. Goppa, *Geometry and codes*, Mathematics and its applications, **24** Kluwer Academic Publisher, Dordrechet-Boston-London, 1988.

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

[10] T. Høholdt, J.H. van Lint and R. Pellikaan *Algebraic geometric codes*, in Handbook of Coding Theory, eds. V. Pless and W. C. Huffman, pp. 871-961, Elsevier, 1998.

[11] M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **67**, 337-348 (1996)

[12] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra **162**, 273-290, 2001

[13] S. J. Kim, *On the index of the Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **62**, 73-82 (1994).

[14] G. L. Matthews, *The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve*, preprint.

[15] G.L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Des. Codes Cryptog., **22**, 107-121, 2001.

[16] R. Matsumoto, *Miuras's Generalization of One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization*, IEICE Trans. Fundamentals, **E82-A**, $N^{\underline{o}}$ 10 October 1999.

[17] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

[18] M. A. Tsfasman e S. G. Vladut, *Algebraic-Geometry Codes*, Kluwer Academic Publisher, Dordrecht-Boston-London, 1991.